01632
21

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

"ESTRATEGIAS, PROCEDIMIENTOS Y POLÍTICAS PARA IMPLEMENTAR LA SEGURIDAD INFORMÁTICA EN ORGANIZACIONES CON SISTEMAS LINUX RED HAT CASO: UNIDAD DE SERVICIOS DE CÓMPUTO ACADÉMICO DE LA FACULTAD DE INGENIERÍA"

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO EN COMPUTACIÓN

P R E S E N T A N:

MARGARITA CARRERA FOURNIER
ROBERTO CARLOS ZÚÑIGA RAMÍREZ
YESENIA CARRERA FOURNIER

DIRECTOR DE TESIS:

ING. NOÉ CRUZ MARÍN

Ciudad Universitaria

México, D.F. 2003

A

RECONOCIMIENTOS

A la Universidad Nacional Autónoma de México por brindarnos la oportunidad para estudiar una carrera.

Agradecemos a los sinodales: M.C. Ma. Jaquelina López Barrientos, Ing. Ma. Del Rosario Barragán Paz, Ing. Heriberto Olguín Romo e Ing. Jorge Ontiveros Junco, por el tiempo dedicado para revisar este trabajo y por enriquecerlo con nuevas ideas.

Al Ing. Noé Cruz Marín por creer en nosotros para este trabajo de tesis.

A la Unidad de Servicios de Cómputo Académico UNICA por todos las facilidades prestadas para terminar este trabajo de tesis.

A DIOS

Por todo lo que me ha dado, por darme una familia en la que reina la felicidad y el amor, pero sobre todo por dejar a mi lado a dos de los seres más importantes de mi vida, a mis padres .

A MIS PADRES

Florentino Carrera Murillo y Margarita Fournier Olivares

Por su apoyo, compresión y amor.
Por ser de mi lo que soy.
Por que siempre tuvieron una palabra de aliento cuando más lo necesite y que jamás me dejaron caer.
Mami gracias por enseñarme la responsabilidad y que siempre las cosas se pueden hacer mejor si uno quiere.
Papi gracias por ser tan paciente y consentidor conmigo, por ayudarme en muchas ocasiones cuando se me complicaba algo en la escuela.
"Por ser los padres más maravillosos del mundo, los amo".

A MI HERMANO Y HERMANAS

Kenia, Merlin, Yesenia, Vero, Elizabeth y José Israel.

Que siempre me han apoyado, me han hecho ver mis errores, por su cariño y por todo los buenos momentos que hemos compartido en familia. "Mejores hermanos no pude haber tenido,gracias".

A MIS COMPAÑEROS DE TESIS

Yesenia y Roberto

Por que sin ustedes no hubiera podido realizar este trabajo de tesis. Por su dedicación, pero sobre todo por su apoyo, comprensión y esperarme para que juntos nos tituláramos, "jamás lo olvidare".

A MI NOVIO

Víctor Hugo Sánchez Quijada.

Por llegar a mi vida y ser mi inspiración para superarme cada día. Por tu amor y apoyo para que lograra pasar mi examen de Inglés, y poder estar en este punto de mi vida agradeciéndole a todos mis seres queridos, porque lo creía imposible y gracias a ti no fue así. por todo lo bello que me has enseñado. Por demostrarme tu amor, comprensión, cariño, y por tu paciencia, para que nuestra relación sea la experiencia más bella y única de mi vida, "Te amo".

A LA MEMORIA DE MIS ABUELOS

Donaciano Carrera, Guadalupe Murillo y Basilia Olivares

Porque gracias a ellos tuve la bendición de tener los padres que tengo. Por el cariño que me demostraron .En especial a mi abue Basilia. "Dios sabe cuanto me hubiera gustado que estuvieran conmigo para que compartieran conmigo esta alegria".

A MI TÍA MARGARITA

Porque siempre me ha demostrado su cariño y amor en las buenas y en las malas. Por ser tan linda cuando tenemos la oportunidad de compartir momentos que jamás se olvidan y dejan algo hermoso en la vida de cualquier ser humano.

A MIS PRIMOS

Loyda, Roberto, Antonio, Dany, Esther y Heber

Porque que juntos hemos vivido aventuras y experiencias divertidas desde nuestra niñez. Ojalá y sigamos siempre unidos como hasta ahora. "Los quiero".

A MIS AMIGOS Y COMPAÑEROS DE TRABAJO

Alberto Axcana, Edgar Ricardo, Guillermo , José de Jesús y Victor Hugo.
Por su apoyo para llevar a cabo el trabajo en UNICA, sin ustedes no hubiera sido posible.
por todo lo que me han enseñado, al compartir sus conocimientos conmigo. Gracias muchachos

A MIS AMIGOS

No pondré nombres por que no quiero omitir ninguno, pero tampoco quiero dejar de agradecerles su apoyo y por que cada momento que compartí con ustedes ha dejado en mi algo bello de la vida.

A UNICA

Por darme la oportunidad de aprender gran parte de lo que se.

A TODOS aquellos que directa o indirectamente me ayudaron a realizar está tesis.

MAGO

GRACIAS

A Dios por los ojos para leer esto, por su infinito amor, ... en fin, por todo.

A mis Padres por el apoyo, cariño y confianza que me brindaron durante todo el camino y que me permitió llegar a esto.

A Calli por su apoyo y caminar un rato junto a mi.

A UNICA por todas la personas que ahí conocí.

A G por su valiosa colaboración.

A la Bola por ser mis amigos.

A todos los que de alguna manera contribuyeron a que esta tesis fuera posible (me siento como en un oscar).

ROBERTO

F

A DIOS

Por el regalo más preciado: la vida.
Por enseñarme a valorar lo que tengo.
Por darme más de lo que necesito.
Por que tengo tanto que agradecerle.
Por cuidarme en cada paso que doy.
Por tener la oportunidad de ser feliz.

A MIS PADRES

Florentino Carrera Murillo y Margarita Fournier Olivares

A ti papi por ser tolerante, por comprenderme, por tu amor, por tus consejos, por guiarme en la vida, por enseñarme el valor de las cosas, por ayudarme en mis estudios, gracias por estar horas conmigo ayudándome en proyectos de la escuela.

A ti mami, porque jamás vi una mujer con tanto ímpetu, por cada palabra tuya, por horas de preocupación, porque aprendí a que tú también lloras, porque eres una mujer difícil de vencer, por todo tu amor.

Agradezco a Dios el haber nacido en una familia donde el amor y el respeto siempre han estado presentes.

Por ayudarme a ver mis errores, por compartir mis triunfos y fracasos.

Gracias por luchar con todas sus fuerzas para seguir al lado de sus hijas.

Los amo y siempre estarán en mi corazón.

A MIS HERMANOS

A Kenia por sus juegos y adivinanzas que me hacen recordar mi niñez.

A Merlin porque escucha mis quejas y me ayuda a ver mis errores.

A Magus por ser la chiquita que me ha acompañado a lo largo de mi vida compartiendo alegrías y tristezas. Por su cariño, mil gracias.

A Vero por su ternura, por ser tan linda y enseñarme que hay personas que lo dan todo por los seres que ama.

A Eli que con sus ideas locas, me ha enseñado a que de vez en cuando es bueno divertirse.

A Israel porque es un ejemplo de que cuando se quiere se puede. Felicidades Lic.

Gracias a ustedes por llenar mi vida de alegría y deseo que siempre estemos unidos como hasta ahora. Los amo.

A MIS ABUELITOS

Que ya no se encuentran con nosotros, pero sé que nos cuidan desde donde están.

A mis abues Lupita y Chano que a pesar del poco tiempo que convivi con ellos, siempre me demostraron su amor. Gracias por hacer de mi papá un hombre ejemplar.

A mi abue Basilia a quien extraño mucho. Siempre tuvo para mi demostraciones de amor.

A MIS TÍOS

A mis tíos Rafael, María, Arturo y Jesús por formar parte de mi niñez y ayudarme cuando los he necesitado.

A mi tía Margarita por su alegría y apoyo incondicional. Gracias por tu amor.

A mi tío Juan que aunque ya no está con nosotros siempre fue cariñoso y divertido.

A MIS PRIMOS

A Daniel, Antonio, Esther, Loida, Roberto y Heber por hacer de mi niñez las más hermosa de todas. Gracias.

A Mari, Ivonne y Lore que me hacen reír con sus aventuras.

A RAFAEL

Por su comprensión, apoyo y amor desde que lo conocí. Por cuidar de mi a cada paso que doy. Por compartir sueños juntos. Por darme palabras de aliento cuando estoy triste. Por soportar mis histerias. Por hacerme descubrir lo maravilloso que es sentirse amado. Te amo mostrilio.

A MAGO Y ROBERTO

Por emprender este sueño juntos que ahora es una realidad. Gracias por su paciencia y dedicación. Gracias por ser mis amigos.

A ESTELIUX

Por comprenderme, por escucharme, por tolerarme, por ayudarme. Mil gracias mona. Te quiero mucho.

A UNICA

Ha sido una experiencia maravillosa pertenecer a la Unidad, la cual me ha permitido desarrollarme profesionalmente, proporcionándome todo lo necesario para lograrlo. El ambiente de trabajo en UNICA es ideal. Gracias a todos por hacer de UNICA lo que es hasta hoy.

Agradezco especialmente a Chary y Bety por su confianza y apoyo en lo que hago.

Al Ing. Enrique Barranco Vite por creer en mi trabajo.

A Adrián, Iliana, Julius, Javo, Héctor, Andrés, Manuel, Víctor Durán y Paulo porque si de alguien he aprendido es de ustedes, quizás no se los digo pero valen mucho. Mil gracias.

Al monsieur e Irene por su apoyo incondicional y cariño. Jamás los olvidaré.

A todos los becarios con los cuales he platicado y convivido aunque sea un poco quiero que sepan que los aprecio y siempre tendrán un lugar muy especial en mi corazón.

A TODOS

A compañeros de clase, profesores y a las personas que por alguna razón no me llevé bien.

YESENIA

ÍNDICE

7. HERRAMIENTAS DE SEGURIDAD

8. IMPLANTACIÓN DE MEDIDAS DE SEGURIDAD EN LA UNIDAD DE SERVICIOS DE CÓMPUTO ACADÉMICO

DEFINICIÓN DE LA PROBLEMÁTICA Y ALCANCE DE LA TESIS

Es evidente que hay muchos beneficios que la informática ha aportado a la sociedad, entre ellos la comunicación, acceso a información, a bases de datos, publicidad, etc.

Pero la informática también ha traído consigo conductas antisociales o delictivas. Los sistemas de computadoras han creado la posibilidad de cometer "delitos" de tipo tradicional en formas no tradicionales.

Por motivos diversos: desde la simple curiosidad, como es el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático. Los piratas informáticos o hackers acceden muy a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diferentes medios que se mencionan a continuación. El hacker puede aprovechar la falta de rigor en las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema, esto suele suceder con frecuencia en sistemas en los que los usuarios pueden emplear contraseñas comunes y sencillas.

La Universidad Nacional Autónoma de México, la Facultad de Ingeniería y la Unidad de Servicios de Cómputo Académico (UNICA) no son la excepción de tales conductas delictivas. La difusión de sistemas operativos accesibles (como LINUX) así como tener acceso a información donde se indica cómo vulnerar la seguridad de algunos sistemas ha hecho que en los últimos años se hallan desarrollado usuarios con conocimientos especializados (los que antes eran muy pocos). En los que se han dado algunas conductas delictivas como los siguientes:

- Usuarios "roban" claves de otros usuarios.
- Usuarios destruyen la información de otros; leen sus correos, cambian su ambiente, etc.
- Usuarios muy experimentados intentan obtener la clave del administrador del sistema, a veces sólo con la finalidad de ver, otras para modificar o destruir información.
- Usuarios sin derecho sobre el sistema de información ejecutan códigos, programas, comandos, con la finalidad de obtener, dañar, modificar o destruir información.
- Cambio de los contenidos de las páginas WEB.

Debido a que la Unidad de Servicios de Cómputo Académico (UNICA) tiene entre sus usuarios a: académicos, autoridades y alumnos, se hace imperativo la implementación de la seguridad del sistema.

Para llevar a cabo el punto anterior, consideraremos aspectos importantes de la seguridad, que en varias ocasiones no se toman en cuenta, estos son: realizar un análisis de riesgos, políticas de seguridad, procedimientos preventivos y correctivos, plan de contingencia, código de ética, herramientas de seguridad, creación de un área de seguridad y medidas de seguridad física.

PREFACIO

Unas cuantas líneas para explicar el alcance de este trabajo de tesis dedicado a la seguridad en un sistema informático. Las computadoras hoy en día juegan un papel cada vez más importante debido a que son la herramienta para almacenar, visualizar y procesar la información, la cual es esencial dentro de las organizaciones. De ahí la trascendencia del manejo y protección de la misma.

Cuando se habla de la seguridad en un sistema informático, normalmente se piensa en el término "privacidad de la información", en el que podemos incluir las contraseñas para tener acceso al sistema, los permisos de acceso a la información, mensajes cifrados y, en definitiva, todo lo relacionado con la protección y la confidencialidad de nuestros datos.

La razón de realizar este trabajo de tesis responde a las necesidades de seguridad que hoy en día es uno de los principales problemas que podemos encontrarnos en los sistemas informáticos, y va dirigido a todas aquellas personas involucradas y preocupadas por mantener la seguridad de su sistema.

El tema de tesis consta de ocho capítulos, los primeros siete conforman el marco teórico y dan las bases para la implementación de medidas de seguridad, descritas en el capítulo 8. A continuación se describen brevemente cada uno de los capítulos.

Capítulo 1. "Fundamentos".- Se presentan conceptos de seguridad, una breve historia del sistema operativo UNIX, así como otras definiciones importantes.

Capítulo 2. "Niveles de seguridad informática".- Los cuales son descritos por el Centro de Seguridad para Computación en los Estados Unidos de América, por ser la base para definirlos.

Capítulo 3. "Seguridad del sistema".- Se detalla la seguridad física, la seguridad lógica y la seguridad del sistema de archivos.

Capítulo 4. "Políticas de Seguridad".- Se explica la creación, responsabilidad, obligación y difusión de políticas de seguridad dentro de una organización.

Capítulo 5. "Procedimientos".- Se definen los pasos que se deben seguir antes y después de un incidente de seguridad.

Capítulo 6. "Ética en la informática".- Se hace referencia a la definición de ética informática, códigos deontológicos, así como la situación actual de la ética en la informática.

Capítulo 7. "Herramientas de seguridad".- Se listan las herramientas de seguridad que existen para disminuir el riesgo de ataque en un sistema de cómputo.

Capítulo 8. "Implantación de medidas de seguridad en la Unidad de Servicios de Cómputo Académico".- Se propone una solución integral con todos los elementos descritos en los capítulos anteriores. En el cual se elaboraron políticas, procedimientos preventivos y

correctivos, un código de ética, un plan de contingencia, medidas de seguridad física, bitácoras de las herramientas de seguridad, así como la creación de un área de seguridad para la Unidad de Servicios de Cómputo Académico.

Nuestra mayor recompensa será que se implanten las medidas de seguridad que proponemos en la Unidad de Servicios de Cómputo Académico y ser una referencia para cualquier otra institución relacionada con el cómputo que desee implantar seguridad en su sistema.

Margarita Carrera Fournier
Roberto C. Zúñiga Ramírez

OBJETIVO GENERAL DE LA TESIS

Establecer las estrategias, procedimientos y políticas de seguridad para implantar las medidas de seguridad en la Unidad de Servicios de Cómputo Académico con el fin de proteger la integridad, confidencialidad y disponibilidad de la información contra incidentes de seguridad.

OBJETIVOS PARTICULARES

- Definir los conceptos básicos de seguridad para tener las bases que permitan determinar la problemática en la Unidad de Servicios de Cómputo Académico.
- Proponer políticas de seguridad que permitan regular la manera de proteger los recursos de la Unidad de Servicios de Cómputo Académico para poder llevar a cabo los objetivos de seguridad.
- Proponer procedimientos preventivos que ayuden a minimizar los incidentes de seguridad y procedimientos correctivos que indiquen qué hacer ante un incidente de seguridad.
- Proponer un Plan de Contingencia que ayude a restablecer la operatividad de la Unidad de Servicios de Cómputo Académico en el menor tiempo posible ante un incidente de seguridad.
- Proponer algunas herramientas de seguridad que hagan menos vulnerable los sistemas de cómputo de la Unidad de Servicios de Cómputo Académico.
- Proponer un código de ética para establecer algunos puntos que regularán la conducta y el desempeño profesional de las personas que laboran en la Unidad de Servicios de Cómputo Académico.
- Proponer la creación de un área de seguridad para proteger la integridad, confidencialidad y disponibilidad de la información de los usuarios, en especial la que sea crítica para nuestras autoridades y académicos.
- Proponer medidas de seguridad física con la finalidad de mejorar la infraestructura de la Unidad de Servicios de Cómputo Académico.

Capítulo 1

Fundamentos

PAGINACIÓN DISCONTINUA

1.1 Concepto de seguridad

El concepto de seguridad puede tener un significado distinto de acuerdo al enfoque que le den las personas, por lo que es difícil proporcionar una definición exacta. Por esta razón, consideramos necesario definir antes el concepto de información.

Para explicar qué es **información**, antes hay que definir qué es un dato. Un dato es "la unidad mínima con la se compone cierta información".[1] Podemos entender de dos maneras el concepto de información. *Primero.* La información es el conjunto de datos que tiene un significado específico más allá de cada uno de éstos, y tendrá un sentido particular según cómo y quién la procese y la interprete. *Segundo.* La información es cualquier mensaje (conjunto de datos) que le interese al receptor, entienda o lo ignore antes de recibirlo.

A continuación, se mencionan diferentes definiciones de seguridad:

- Es el conjunto de medidas para mantener la información de un sistema libre de corrupción.[2]
- Cualidad de seguro. Se aplica a ciertos mecanismos que aseguran algún buen funcionamiento, precaviendo que éste falle, se frustre o se violente.[3]
- Es la calidad de algo seguro, y algo seguro es algo libre de todo daño y riesgo.[4]

De acuerdo con las definiciones anteriores, podemos decir que:

La seguridad se refiere a todo tipo de precauciones y protecciones que se llevan a cabo para evitar cualquier tipo de daño.

1.1.1 Seguridad de la Información

La Seguridad de la información tiene su nacimiento con la aparición de los ataques a la información por parte de intrusos interesados en el contenido de ésta. Por consiguiente, el término de **Seguridad de la Información** se refiere a la prevención y a la protección, a través de ciertos mecanismos, para evitar que ocurra de manera accidental o intencional, la transferencia, modificación, fusión o destrucción no autorizada de la información.

El objetivo de la Seguridad de la Información es:

- Mantener el secreto, evitando los accesos no autorizados.
- Mantener la autenticidad, evitando modificaciones no autorizadas.

---

[1] FERNÁNDEZ, Calvo Rafael. *Glosario básico inglés-español para usuarios de Internet* [en línea]: cuarta edición. España: Asociación de Técnicos de Informática y Novática, 5 de julio de 2001[Consulta: 3 abril 2002]. Disponible en: <http://www.ati.es/novatica/glosario/buscador/buscador_gloint.html>

[2] PIZARRO, Gil Julio. Diccionario General de Informática. Editorial ABETO. España.1999. p. 276.

[3] Diccionario de la Lengua Española. Real Academia Española. 1992. p. 1317.

[4] MOLINA, Diego. *Seguridad*[en línea]. Universidad del Salvador[Consulta: 3 abril 2002] Disponible en: <http://www.salvador.edu.ar/molina.htm#Seguridad>

1.1.2 Seguridad de la Red

Antes de empezar a definir lo que es la Seguridad de la Red, partiremos de lo que es una red de computadoras.

Una **red de computadoras** consiste de dos computadoras (desde un nivel básico) o más, conectadas por un canal de comunicación de manera tal que puedan compartir datos y recursos (espacio en discos duros, impresoras, programas, etc.). A cada una de las computadoras conectadas a la red se le denomina "nodo".

Los objetivos que se persiguen con el diseño e implantación de una red de computadoras son:

- Compartir los recursos a cualquier otro nodo sin importar su ubicación física.
- Proveer confianza teniendo alternativas de acceso a recursos; por ejemplo, un conjunto de datos puede estar almacenado en dos o más computadoras, y en el caso en que una de éstas sufra algún daño existe la posibilidad de tener acceso a la información almacenada en otra.
- Fomentar el ahorro económico que representa tener computadoras pequeñas en comparación con las computadoras principales de procesamiento conocidas como "*mainframes*" (computadoras del tamaño de un cuarto), las cuales tienen un factor de velocidad de procesamiento diez veces mayor a la de una computadora personal pero en costo es mucho mayor. En sustitución de una computadora principal de procesamiento (*mainframe*) se diseña un modelo con computadoras principales y pequeñas llamado **cliente-servidor**. El modelo **cliente-servidor** se basa en una computadora (llamada servidor), o un proceso ejecutándose en esta, que brinda servicios a las demás computadoras de la red. Un cliente es una computadora o un proceso que hace uso de los servicios que brindan otras computadoras en la red.
- Escalamiento de manera gradual del sistema basándose en el aumento de la carga de trabajo agregando más procesadores. Con el modelo cliente-servidor, nuevos clientes y nuevos servidores pueden ser agregados conforme a las necesidades.

El concepto de la **Seguridad de la Red** surge con la introducción de los sistemas distribuidos, aunado al uso de redes y las facilidades que el desarrollo de la tecnología proporciona a la comunicación, ya que con ésta se obtienen los elementos necesarios para transportar los datos entre una terminal de usuario y una computadora, o entre una computadora y otra. Dado el avance de la tecnología de red, la cual ha permitido que las computadoras de todo el mundo se encuentren interconectadas, las amenazas de seguridad son una gran preocupación para las organizaciones y los usuarios. La protección de los recursos de la red, la información y servicios contra las amenazas de seguridad recibe el nombre de **Seguridad de la Red**. Así, cualquier medida realizada tiene como objetivo proteger los datos durante su transmisión.

El principio de la Seguridad de la Red es proteger el entorno de cualquier tipo de amenazas de seguridad mediante servicios de seguridad, mecanismos y técnicas para hacer cumplir una política de seguridad.

1.1.3 Seguridad Informática

Al igual que el concepto de *seguridad,* el de Seguridad Informática presenta múltiples interpretaciones, como son las siguientes:

- La **Seguridad Informática** podría definirse como el conjunto de procedimientos y actuaciones destinados al funcionamiento del sistema de información.[5]

- Un concepto global de **Seguridad Informática** sería aquel definido como el conjunto de procedimientos y actuaciones encaminados a conseguir la garantía de funcionamiento del sistema de información, obteniendo eficacia (entendida como el cumplimiento de la finalidad para el que estaba establecido), manteniendo la integridad (entendida como la inalterabilidad del sistema por agente externo al mismo) y alertando la detección de actividad ajena (entendida como el control de la interacción de elementos externos al propio sistema).[6]

- **Seguridad Informática** es el conjunto de técnicas y procedimientos destinados a garantizar la protección, exactitud e integridad de las informaciones manejadas en un sistema informático.[7]

- La **Seguridad Informática** es el conjunto de metodologías, documentos, programas y dispositivos físicos, encaminados a lograr que los recursos de cómputo disponibles en un ambiente determinado donde tengan acceso única y exclusivamente quienes estén autorizados para hacerlo.

De acuerdo a lo anterior, la necesidad de herramientas automatizadas para proteger la información almacenada en la computadora se volvió más evidente, por lo que:

> *La* ***Seguridad Informática*** *es el nombre genérico dado a una colección de herramientas y procedimientos diseñados para proteger datos y detener a los intrusos; es decir, es la protección de los sistemas de cómputo para evitar amenazas de confidencialidad, integridad o disponibilidad.*

El objetivo de la Seguridad Informática es garantizar la privacidad de la información y la continuidad del servicio, tratando de minimizar la vulnerabilidad de los sistemas o de la información contenida en ellos, así como de proteger las redes privadas y sus recursos mientras que se mantienen los beneficios de la conexión a una red pública o a una red privada.

En la figura 1.1 se muestra el contexto de la seguridad informática, con lo cual se hace referencia a las condiciones que proponen las amenazas y que conforman el desarrollo y el uso de los escudos.[8]

---

[5] Guardia Civil. (2001). Seguridad informática. *En profundidad* [en línea], (Número 687).[Consulta: 24 Abril 2002] Disponible en : <http://www.guardiacivil.org/00revista/profundidad/index.asp?numrevista=687>

[6] Ibid.

[7] RINCÓN, Antonio. Diccionario conceptual de Informática y Comunicaciones. España, Editorial Paraninfo, 1998. p. 329.

[8] QUEZADA, Reyes Cinthia y GUTIÉRREZ, Rodríguez Sergio. Fundamentos de Seguridad de la Información. Tesis (Licenciatura en Ingeniería en Computación). México, D.F., Universidad Nacional Autónoma de México, Facultad de Ingeniería, 2001. pp. 29-30.

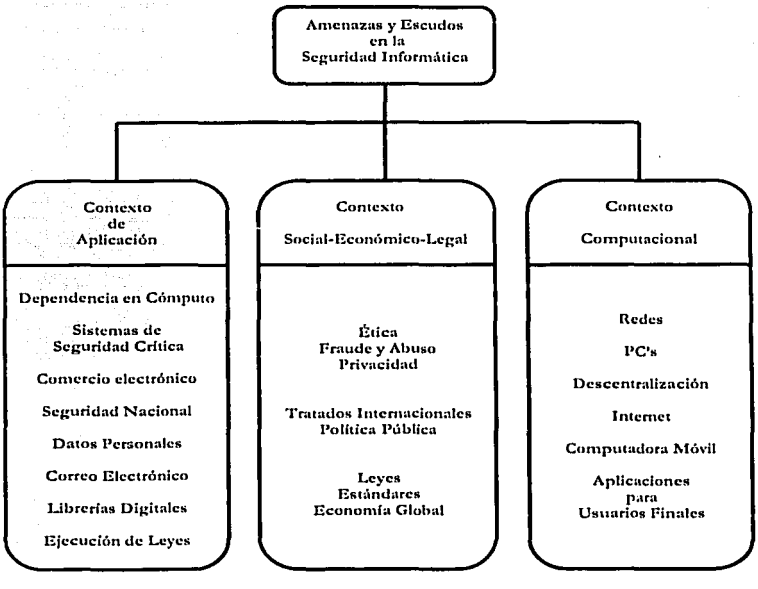


Figura 1.1. Contexto de la Seguridad Informática.

1.2 La seguridad en torno a los sistemas operativos

Para que una computadora funcione necesita una serie de programas que desempeñan tareas muy importantes. Tal vez el más importante es el sistema operativo, el cual es un conjunto de programas que administran los recursos de la computadora. Existen diferentes tipos y en ocasiones son dependientes de la computadora de la cual estemos hablando; en específico, en el área de las computadoras personales, los más importantes son de tipo Windows y Unix debido a la cantidad de usuarios que tienen.

En cualquier caso, se busca que un sistema operativo sea seguro, el cual pueda ofrecer entre otras las siguientes características: identificación y autenticación de todos los usuarios que ingresan al sistema, control del acceso a todos los recursos e informaciones, contabilidad de todas las acciones realizadas por los usuarios, auditoría de los acontecimientos que puedan representar amenazas a la seguridad, garantizar la integridad de los datos y mantenga la disponibilidad de los recursos e información.[9]

[9] MONTOYA, Edwin y ALONSO, Cañón Jorge (1997). Riesgos, Políticas y Herramientas de Seguridad en Redes. *Revista Universidad EAFIT* [en línea], (Número 107), 69-86. [Consulta: 12 Abril 2002]. Disponible en: <http://www.eafit.edu.co/revista/107/montoya.pdf>.

Aunque no se puede afirmar que un sistema tiene seguridad perfecta, existen los que ofrecen una mayor seguridad. De los sistemas operativos más conocidos y con una mayor difusión dentro del ambiente de las computadoras personales, se encuentran Windows (de la compañía Microsoft) y Unix. El primero tiene dividida sus versiones con base a la seguridad del sistema, por ejemplo la línea de Windows 95, Windows 98 y Windows Millenium tiene una seguridad en su sistema de archivos y autenticación al inicio muy pobre, mientras que las versiones de Windows NT, y la serie de Windows 2000 manejan una mayor seguridad.

El segundo, Unix, desde su creación fue pensado para que fuera multiusuarios y multiprocesos, por lo que el manejo de información se distribuyo de tal forma que los usuarios no se estorbaran entre sí. Aunque ha evolucionado mucho desde su creación, sus principios siguen siendo los mismos y se considera seguro. Uno de los creadores de Unix Dennis Ritchie dijo "*No se diseño para ser seguro, se diseño para que se pudiera usar la seguridad*".[10]

1.3 ¿Qué es Unix?

A mediados de los 60, en los laboratorios Bell de AT&T, en conjunto con el Instituto Tecnológico de Massachussets (MIT) y General Electric, se desarrolló un sistema operativo que se llamaba MULTICS (Multiplexed Information and Computing Service), un sistema modular que buscaba dar un servicio de cómputo las 24 horas del día, los 365 días del año, en una computadora que se pudiera hacer más rápida agregándole más partes.

Fue financiado por la agencia de proyectos de investigación avanzados (ARPA). Este proyecto también debía contemplar seguridad militar, por lo que resultó demasiado ambicioso y AT&T lo abandonó en 1969.

Un grupo de investigadores de AT&T que participaban en el proyecto, entre los que se encontraban Ken Thompson, Rudd Canaday, Doug Mellroy, Joe Hosanna y Dennis Ritchie, hicieron un sistema operativo cómodo, rápido y con características de MULTICS. Su sistema operativo se llamó UNIX y corrió por primera vez en una computadora PDP-7 de Digital Equipment Corporation (DEC), el cual se escribió en lenguaje ensamblador. Después para buscar una mayor portatibilidad, buscando que fuera más comprensible, se crea el Lenguaje C, en el cual se reescribe Unix.

Unix se caracteriza por ser:

- Sistema multiusuario y multitarea.
- Las especificaciones de diseño están disponibles públicamente, lo cual hace que se adapte a exigencias particulares.
- Está escrito en un lenguaje de alto nivel (Lenguaje C), que lo hace portátil.
- Enfoque de programación.
- Hace uso de direccionamiento de entrada, salida, filtros e interconexiones.
- Sistema de archivos consistente.
- La interfaz con los dispositivos se manejan igual que un archivo.
- Esconde la arquitectura del hardware que lo utiliza.

[10] O'REILLY. Seguridad Práctica en Unix e Internet. México, Editorial Mc Graw Hill, 1999. p. 13.

- Es fácil de utilizar.[11]

El primer sistema Unix en salir al mercado fue la versión 5. La versión 6 apareció en 1975. Su código era abierto, se enseñaba en las Universidades y existían folletos en los cuales venía descrito el sistema operativo línea por línea.

El que Unix fuera software libre y su enfoque orientado a la programación, hizo que tuviera una gran aceptación en universidades y dentro de los laboratorios Bell; y por su misma apertura, se podría adaptar a las necesidades específicas.

Esto dió lugar a que surgieran nuevas versiones de Unix, como la denominada BSD (Berkeley Software Distribution) que fue la más difundida. La versión oficial fue la 7, liberada en 1979. El enfoque que le daba AT&T cambio y dejó de ser libre y, de mostrar su código.

Como respuesta a esto, Andrew Tannebaum decide hacer un sistema operativo el cual pudiera seguir siendo usado con fines educativos, basándose en características de Unix versión 7, pero sin las restricciones que tenía ésta y crea Minix. Sin repetir el código que utilizaba la AT&T, Minix fue escrito en C, su nombre viene de Mini-Unix y se podía instalar en una computadora personal bajo una nueva licencia, la GNU.

La licencia GNU oficialmente viene de Licencia Pública General (General Public License), pero también se dice que su nombre es un acrónimo recursivo para "GNU No es Unix". Esta licencia busca garantizar la libertad de compartir y modificar software libre. Cuando se tiene un programa de software libre, se puede distribuir, copiar o modificar si se quiere y, es más, se puede cobrar por el servicio o no, pero no hay que pagar por derechos de autor, y tanto sus especificaciones como su código están en el alcance de todo el mundo.

Más adelante, algunas compañías empezaron a desarrollar versiones específicas; por ejemplo, en 1980, Microsoft desarrolló Xenix para microprocesadores de 16 bits. En el mismo año, DEC sacó al mercado la denominada Ultrix. Sun MicroSystem desarrolló su versión denominada SunOs basada en la versión 4.2 BSD, con facilidades para ambientes gráficos de ventanas e interfaz con ratón. A partir de entonces, surgieron muchísimas versiones tipo Unix, de los cuales unos eran licencia GNU; otros no, y algunos sólo para arquitecturas especiales.

1.3.1 Linux

Daremos una especial importancia al sistema operativo Linux Red Hat, debido a que este se maneja actualmente en UNICA.

Para 1990, Unix tenía un gran uso y se habían desarrollado muchas versiones, pero sólo en ciertos sectores de la industria. Un estudiante de 23 años de la Universidad de Helsinki llamado Linus Torvalds, comenzó a desarrollar una nueva versión de Unix como pasatiempo. Su proyecto estaba basado en el Minix. Quería llevar a cabo un sistema operativo que aprovechase la arquitectura de 32 bits para multitarea y eliminar las barreras del direccionamiento de memoria. Torvalds empezó escribiendo el núcleo del proyecto en ensamblador, y luego comenzó a añadir código en C.

[11] ALVAREZ, Ricardo y AMEZCUA Luis. UNIX. México, Editorial Facultad de Ingeniería, 1994. pp. 1-4.

La primera versión no la dio a conocer porque ni siquiera tenía drivers de disquete, además llevaba un sistema de almacenamiento de archivos muy defectuoso. Con el tiempo, esta versión tuvo mejoras, consiguiendo así que el sistema Linux empezara a crearse, y con el añadido de otras versiones como FreeBSD conseguiría llegar a un sistema operativo que actualmente es capaz de competir con los más innovadores de la época y bajo la Licencia GNU.

Se empezaron a realizar modificaciones y ampliaciones al código de Linux original, y se distribuían versiones de Linux con sus propios paquetes y modificaciones al kernel.

De aquí surgió el concepto de distribución. Hoy en día, se pueden obtener diferentes distribuciones como Red Hat, SuSE, Caldera, MandrakeSoft, etc. Cada una de ellas tiene características especiales, se diferencian en cosas como el tipo de computadora para el cual se va usar, paquetes o interfaz que utilizan, documentación y soporte. Actualmente, se calculan en 18 millones de usuarios de Linux en todo el mundo[12] y en México, la distribución más utilizada es Red Hat.

1.4 ¿De quién nos vamos a proteger?

A la persona que accede (o intenta acceder) sin autorización a un sistema ajeno, ya sea en forma intencional o no, se llama **intruso** o atacante.

Según Julio C. Ardita,[13] "los tipos de intrusos se podrían caracterizar de acuerdo con su nivel de conocimiento formando una pirámide, como lo muestra la figura 1.2:

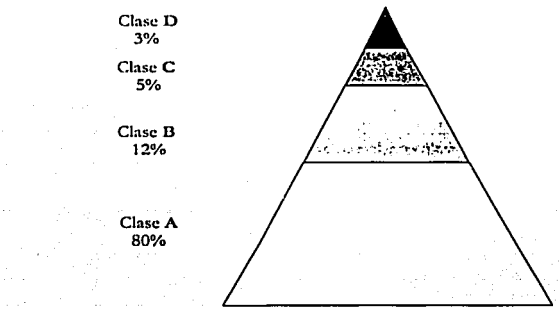


Figura 1.2. Pirámide del Nivel de Conocimiento.

[12] The Linux Counter. The Linux Webring [en línea]. [Consulta: 14 Mayo 2002]. Disponible en: <http://counter.li.org/>.

[13] ARDITA, Julio César. Director de Cybsec S.A. Security y exHacker. Entrevista realizada el día 15 de enero de 2001 por Cristian P. Borghelio en instalaciones de Cybsec S.A.

Clase A: 80% en la base son los nuevos intrusos que bajan programas de Internet y los prueban.

Clase B: 12%, son más peligrosos, saben compilar programas aunque no saben programar. Prueban programas, conocen como detectar que sistema operativo está usando la víctima y prueban las vulnerabilidades del mismo e ingresan por ellas.

Clase C: 5%, es gente que sabe, conoce y define sus objetivos. A partir de aquí, buscan todos los accesos remotos e intentan ingresar.

Clase D: 3% restante. Cuando entran a determinados sistemas buscan la información que necesitan.

Llegar desde la base hasta el último nivel tarda de 4 a 6 años, por el nivel de conocimiento que se requiere asimilar. Es práctica, conocer, programar, mucha tarea y mucho trabajo".

1.5 ¿Qué vamos a proteger?

En este punto, se tienen que identificar claramente los sistemas y/o servicios que se quieren proteger, basándose en un análisis de mayor importancia o de un posible mayor interés para los intrusos.

Los tres elementos a proteger en cualquier sistema de cómputo son el **software** (conjunto de programas que hacen funcional al hardware, tanto en sistemas operativos como en aplicaciones), el **hardware** (conjunto formado por todos los elementos físicos de un sistema informático como CPU's, terminales, cableado, medios de almacenamiento secundario como cintas, CD-ROM's, disquetes o tarjetas de red) y la **información**.

Aunque son varios los elementos que hay que proteger, la información, es el recurso más preciado sobre el cual se enfocan todos los esfuerzos para confiar en un nivel aceptable de seguridad.

Establecer el valor de la información es algo totalmente relativo, pues constituye un recurso que, en muchos casos, no se valora adecuadamente debido a su intangibilidad, lo cual no ocurre con los equipos, las aplicaciones y la documentación.

Existe información que **puede ser pública, accesible sin restricciones**: puede ser visualizada por cualquier persona; y aquella que **debe ser privada**: sólo puede ser visualizada por un grupo selecto de personas que trabaja con ella. En esta última, se deben maximizar los esfuerzos para preservarla, reconociendo las siguientes características en la información la cual es:

- Crítica: es indispensable para garantizar la continuidad operativa.
- Valiosa: es un activo con valor en sí mismo.
- Sensitiva: debe ser conocida por las personas que la procesan y sólo por ellas.

La **integridad** de la información es la característica que hace que su contenido permanezca sin alteraciones a menos que sea modificado por personal autorizado, y esta modificación sea registrada para posteriores controles o auditorías. La **disponibilidad u operatividad** de la información es su capacidad de estar siempre disponible para ser procesada por las

personas autorizadas. La **privacidad o confidencialidad** de la información es la necesidad de que la misma sólo sea conocida por personas autorizadas. El **control** sobre la información permite asegurar que sólo los usuarios autorizados pueden decidir cuándo y cómo permitir el acceso a la misma. Y la **autenticidad** permite definir que la información requerida es válida. Esta propiedad también permite asegurar el origen de la información, validando el emisor de la misma, para evitar suplantación de identidades.

1.6 Vulnerabilidades, amenazas y ataques

La seguridad es hoy en día, uno de los principales problemas que podemos encontrar en los grandes sistemas informáticos. Se define un sistema informático como un conjunto de elementos: hardware, software, datos/información y personal que hacen posible el almacenamiento, proceso y transmisión de la información con el objetivo de realizar determinada tarea. Todos estos elementos son susceptibles de ser atacados y sobre ellos tenemos una serie de amenazas.[14]

La **vulnerabilidad** es el debilitamiento o ausencia de la protección en un recurso. Los tipos de vulnerabilidad son las siguientes:

- **Físicas.** Está relacionado con poder acceder físicamente al sistema para robar, manipular o destruir el mismo.
- **Hardware y Software.** Existen ciertos dispositivos físicos que son más vulnerables que otros, como por ejemplo concentradores (hubs) frente a puentes (switchs), o algunas placas de red. Lo mismo ocurre con la parte del software. Existen sistemas operativos más seguros que otros y diversos programas con los que sucede lo mismo.
- **Emanación.** Si bien no son tan comunes o al menos difundidas, aquel que aplique un sistema de defensa con intensidad paranoica, deberá tenerlo en cuenta. Este punto trata sobre dispositivos electrónicos que emiten radiaciones que pueden ser descifradas o reconstruidas.
- **Comunicaciones.** La conexión de computadoras dentro de un entorno aumenta el grado de vulnerabilidad. El compartir recursos, la conexión a Internet, abren puertas de acceso que debemos tener muy en cuenta.

La **protección** son los controles físicos, mecanismos, políticas y procedimientos que protegen los recursos de las amenazas. Luego, el protector será el encargado de detectar cada una de las vulnerabilidades del sistema que pueden ser explotadas y empleadas, por la amenaza, para comprometerlo.

La **amenaza** es una persona, circunstancia, evento, fenómeno o una idea maliciosa que plantea algún daño a un recurso. Las amenazas pueden ser intencionales o accidentales y pueden provenir de diversas fuentes, entre ellas podemos mencionar las siguientes:

1. **De humanos:** surge por ignorancia en el manejo de la información, por descuido, por negligencia, por inconformidad (cuando un empleado es despedido).
2. **Errores de Hardware:** se da por fallas físicas que presenta cualquier elemento de los dispositivos que conforman a la computadora. Los problemas más identificados

[14] MONTOYA, Edwin y ALONSO, Cañón Jorge. p. 5.

para que el suministro de energía falle son el bajo voltaje, ruido electromagnético, distorsión, alto voltaje, variación de frecuencia.

3. **Errores de la Red:** se presenta cuando no se calcula bien el flujo de información que va a circular por el canal de comunicación; es decir, que un atacante podría saturar el canal de comunicación provocando la no disponibilidad de la red. Otro factor es la desconexión del canal.
4. **Problemas de tipo lógico:** se hace presente cuando un diseño bien elaborado de un mecanismo de seguridad, se implementa mal, es decir, no cumple con las especificaciones del diseño. La comunicación entre procesos puede resultar una amenaza cuando un intruso utilice una aplicación que permita enviar y recibir información, ésta podría consistir en enviar contraseñas y recibir el mensaje de contraseña válida, dándole al intruso elementos para un posible ataque.

Las amenazas pueden ser analizadas en tres momentos: antes del ataque, durante y después del mismo. Estos mecanismos conformarán políticas que garantizarán la seguridad de nuestro sistema informático.

a. **La prevención (antes):** mecanismos que aumentan la seguridad de un sistema durante su funcionamiento normal. Por ejemplo, el cifrado de información para su posterior transmisión.
b. **La detección (durante):** mecanismos orientados a revelar violaciones a la seguridad.
c. **La recuperación (después):** mecanismos que se aplican, cuando la violación del sistema ya se ha detectado, para retornar éste a su funcionamiento normal.

El **riesgo** es una medida del costo de la realización de una vulnerabilidad que incorpora la probabilidad de éxito de un ataque. El riesgo es alto si el valor del recurso vulnerable es alto y la probabilidad de éxito de un ataque es alto.

El **ataque** es la realización de una amenaza. Las amenazas intencionales son las más peligrosas ya que convierten a un ataque en **activo o pasivo.**

El **ataque pasivo** es aquel que no causa modificación o cambio en la información o recurso; es decir, únicamente la observa, escucha, obtiene o monitorea mientras está siendo transmitida. Son los más peligrosos, ya que los fines que se alcanzan son más letales y beneficiosos para el que los comete. Cualquier ataque pasivo tiene los siguientes objetivos principales:

- **Intercepción de datos:** consiste en el conocimiento de la información cuando existe una liberación de los contenidos del mensaje.
- **Análisis de tráfico:** consiste en la observación de todo el tráfico que pasa por la red.

Con los ataques pasivos se obtiene información que puede consistir en:

- **Obtención del origen y destinatario de la comunicación,** esto se logra cuando el atacante lee las cabeceras de los paquetes que continuamente está monitoreando. Con ello determina la localización y la identidad de los anfitriones (emisor, receptor).
- **Control de volumen de tráfico** intercambiado entre las entidades monitoreadas, de esta forma se obtienen todos los datos necesarios para percatarse de la

actividad o inactividad inusuales, se conoce la frecuencia y la longitud de los mensajes.

- **Control de las horas habituales** de intercambio de datos entre las entidades de la comunicación, con ello se extraen los datos acerca de los períodos de actividad. El atacante conoce la frecuencia con la que se transmiten los mensajes.

Desafortunadamente, los ataques pasivos son muy difíciles de detectar e interceptar, debido a que no provocan ninguna alteración de los datos. Aún cuando su detección es prácticamente imposible, es necesario tomar en cuenta que puede evitarse el éxito de este tipo de ataques si se considera el uso del cifrado de la información, así como la existencia y utilización de otros mecanismos.

El **ataque activo** es aquel que implica algún tipo de modificación del flujo de datos transmitido (modificación de la corriente de datos) o la creación de un falso flujo de datos (creación de una corriente falsa).

Los ataques activos pueden clasificarse de la siguiente manera:

a. **Enmascaramiento o Suplantación de identidad:** en este caso, el intruso se hace pasar por una entidad diferente. Normalmente, incluye alguna de las otras formas de ataque activo. Por ejemplo, las secuencias de autenticación pueden ser capturadas y repetidas, permitiendo a una entidad no autorizada acceder a una serie de recursos privilegiados suplantando a la entidad que posee esos privilegios, como el robar la contraseña de acceso a una cuenta.
b. **Réplica o Reactuación:** uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado debido a que se realiza una retransmisión subsecuente.
c. **Modificación de mensajes:** una porción del mensaje legítimo es alterada, o los mismos mensajes son retardados o reordenados, esto provoca que se produzca un efecto no autorizado.
d. **Degradación fraudulenta del servicio:** este tipo de acción impide o inhibe el uso normal o la gestión de recursos informáticos y de comunicaciones (medios de comunicación).

Considerando el tipo de flujo de información de un emisor y un receptor, se puede obtener la clasificación de los diferentes tipos de ataques a un sistema[15]:

- **Interrupción:** si se hace que un objeto del sistema se pierda, quede inutilizable o no disponible.
- **Intercepción:** si un elemento no autorizado consigue el acceso a un determinado objeto del sistema.
- **Modificación:** si además de conseguir el acceso consigue modificar el objeto.
- **Fabricación:** se consigue un objeto similar al original atacado de forma que es difícil distinguirlos entre sí.
- **Destrucción:** es una modificación que inutiliza el objeto.

[15] HOWARD, John D. An Analysis of security on the Internet 1989-1995.Tesis(Doctor en Filosofía)[en línea]. EE. UU., Carbegie Institute of Technology, Carnegie Mellon University, 1995. Capítulo 6, p. 59. [Consulta: 30 Abril 2002]. Disponible en: < http://www.cert.org/research/JHThesis/Word6/>

A continuación lo mostraremos de manera gráfica en la figura 1.3.

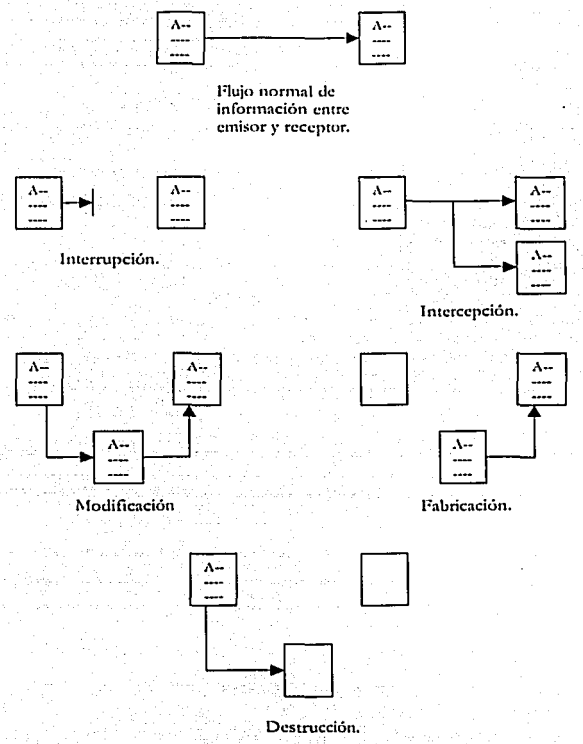
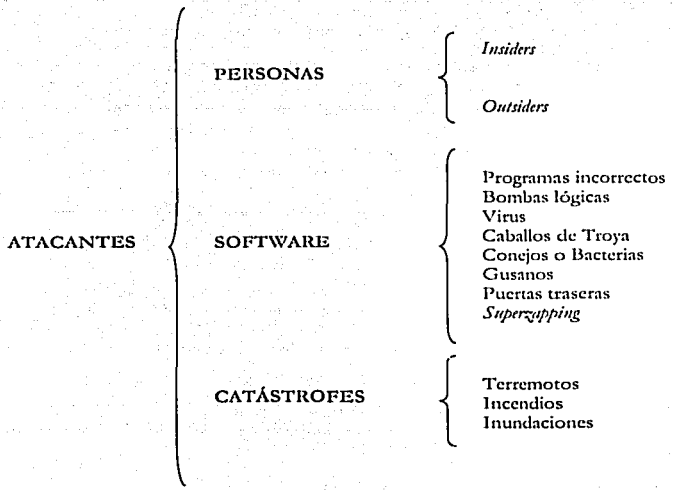


Figura 1.3. Tipos de ataques a un sistema de acuerdo al flujo de información.

Así como se tiene una clasificación del tipo de ataques, también se cuenta con otra para los diversos atacantes:



Cuadro 1.1. Tipos de atacantes a un sistema.

La mayor parte de los ataques a sistemas de cómputo, provienen de personas que intencionada o accidentalmente, pueden causar algún daño.

Los ***insiders*** pueden ser empleados disconformes o personas externas con acceso a sistemas dentro de la empresa u organización, los cuales utilizan sus permisos para alterar archivos o registros.

- **Personal.** Se trata de ataques o accidentes provocados por personal de la misma empresa. En el caso de accidentes, estos se deben a errores o desconocimiento de las normas básicas de seguridad; en el caso de ataques, son los más dañinos, puesto que nadie mejor que el personal de la empresa conoce el sistema y sus debilidades.
- **Ex empleados.** Generalmente, se trata de personas desconectadas con la empresa, que aprovechan las debilidades del sistema de seguridad para dañarlo.
- **Curiosos.** Suelen ser los atacantes más habituales del sistema. Son personas que tienen un alto interés en las nuevas tecnologías. En la mayoría de los casos son estudiantes intentando penetrar los servidores de su facultad o empleados consiguiendo privilegios para obtener información para él vedada. Generalmente, no se trata de ataques que causen algún daño, pero afectan la confiabilidad del sistema.

Los ***outsiders*** son personas que atacan desde fuera de la ubicación física de la organización, estas personas ingresan a la red simplemente averiguando una contraseña válida.

- ***Hackers.*** La palabra inglesa *hacker* proviene de los reparadores de cajas telefónicas (EE.UU. en la década de los 50's), cuya principal herramienta de reparación era un golpe seco al artefacto con fallas (un "hack"), de ahí que se les llamó "hackers". Un hacker es una persona que está en una continua búsqueda de información, vive para aprender y todo para él es un reto; no existen barreras, y lucha por la difusión libre de información (*Free Information*), distribución de software sin costo y la globalización de la comunicación. Para la sociedad no esta bien visto un hacker, porque parece siempre estar ligado a alguien que ha perpetrado un robo en un banco desde una computadora o alguien que hace daño a cualquier internauta o empresa. La poca o mala información sobre el tema, y la expansión de nuevos especímenes en la nueva "cibersociedad", infunda confusión.
- ***Cracker.*** Son hackers cuyas intenciones van más allá de la investigación. Es una persona que tiene fines maliciosos o de venganza; quiere demostrar sus habilidades pero de manera equivocada o simplemente personas que hacen daño sólo por diversión. La diferencia básica es que los hackers construyen cosas y los crackers las rompen.
- ***Lamer.*** Este grupo es quizás el que posee más número de miembros y, quizá, son los que mayor presencia tienen en la red. Normalmente son individuos con ganas de hacer *Hacking*, pero que carecen de cualquier conocimiento. Habitualmente son individuos que apenas saben lo que es una computadora, pero el uso de esta y las grandes oportunidades que brinda Internet, convierten al nuevo internauta en un obsesivo que rebusca y relee toda la información que le fascina y que se puede encontrar (normalmente, la posibilidad de girar un gráfico en la pantalla de otra computadora, le fascina enormemente).
- ***Copyhackers.*** Es un nuevo grupo sólo conocido en el terreno de crackeo de Hardware, mayoritariamente del sector de tarjetas inteligentes empleadas en sistemas de televisión de pago. Los copyhackers divagan entre la sombra del verdadero hacker y el lamer. Estos personajes poseen conocimientos de tecnología y son denominados por la obsesión de ser superiores, pero no terminan de aceptar su posición. Por ello "extraen" información del verdadero hacker para terminar su trabajo.
- ***Bucaneros.*** Son peores que los lamers, ya que no aprenden nada ni conocen la tecnología. Comparados con los piratas informáticos, los bucaneros sólo buscan el comercio negro de los productos entregados por los copyhackers. Los bucaneros sólo tienen cabida fuera de la red, ya que dentro de ella, los que ofrecen productos "Crackeados" pasan a denominarse "piratas informáticos". El bucanero es simplemente un comerciante, el cual no tiene escrúpulos a la hora de explotar un producto de *cracking* a nivel masivo.
- ***Phreaker.*** Este grupo es bien conocido en la red por sus conocimientos en telefonía. Un phreaker posee conocimientos profundos de los sistemas de telefonía, tanto terrestres como móviles. En la actualidad también poseen conocimientos de tarjetas prepago, ya que la telefonía celular las emplea habitualmente.
- ***Newbie.*** Es un novato, o más particularmente es aquel que navega por Internet, tropieza con una página de *hacking* y descubre que existe un área de descarga de buenos programas de hackeo. Después baja todo lo que puede y empieza a trabajar con los programas. Al contrario de los lamers, los newbies aprenden el *hacking*

siguiendo todos los cautos pasos para lograrlo y no se mofa de su logro, sino que aprende.

- ***Script Kiddie.*** Denominados Skid Kiddie o Script Kiddie, son el último eslabón de la red. Se trata de simples usuarios de Internet, sin conocimientos sobre Hack o el Crack. En realidad, son devotos de estos temas, pero no los comprenden. Simplemente, son internautas que se limitan a recopilar información de la red. En realidad, se dedican a buscar programas de *Hacking* en la red y después los ejecutan sin leer primero los archivos *Readme* de cada aplicación. Con esta acción, sueltan un virus, o se fastidian ellos mismos su propia computadora. Esta forma de actuar es de total desconocimiento del tema, lo que le lleva a probar consecutivamente aplicaciones de *Hacking*. Podrían llamarse los "pulsa botones" de la red. Los kiddies en realidad no son útiles en el progreso del *Hacking*.

El software es un conjunto de programas que de una forma u otra pueden dañar el sistema, pueden ser creados para este fin o por errores en su operación. Entre ellos, podemos mencionar:

- **Programas incorrectos.** Los ataques de este tipo provienen de errores (*bugs*) cometidos de forma involuntaria por los programadores de sistemas o de aplicaciones, que hacen que el programa opere incorrectamente.
- **Virus.** Es un fragmento de código que se inserta en un programa ejecutable, de modo que cuando el programa es ejecutado, se ejecuta también el virus. La función que un virus pretende realizar es propagarse a sí mismo por todo el sistema. Para ello, va infectando a otros programas en los que inserta el fragmento de código vírico.
- **Caballos de Troya.** Toman su nombre del famoso mito del caballo de Troya, son programas que imitan la ejecución de otros programas pero realizan otras funciones completamente distintas a las esperadas. Normalmente causan daños irreversibles.
- **Bombas.** Son muy parecidas a los caballos de Troya. Pueden ser tanto programas completos como fragmentos de código insertados en otros programas. La principal diferencia entre los caballos de Troya y las bombas es que estas últimas se activan cuando ocurre un determinado evento, caso de las bombas lógicas, o cuando se llega a una determinada fecha, caso de las bombas de tiempo.
- **Conejos o Bacterias.** Son programas que no hacen nada útil, sino que simplemente se dedican a reproducirse hasta que el número de copias acaba con los recursos del sistema. Normalmente, los recursos que tienden a obtener son el procesador, la memoria, el espacio en disco, etc.
- **Gusanos.** Son programas que se reproducen copiándose de una computadora a otra a través de la red. A diferencia de los virus, los gusanos son programas independientes y no necesitan otro programa en el cual alojarse. Normalmente, los gusanos no producen ningún tipo de daño en el sistema, excepto malgastar los recursos, llegando incluso a sobrecargar la red.
- **Puertas traseras.** Son mecanismos implementados en los programas por sus creadores, que les permiten a éstos realizar acciones determinadas sin tener que pasar por determinadas secciones del programa, como procesos de autenticación, mecanismos de seguridad, etc. Se suelen utilizar perfectamente en tareas de depuración en las que muchas veces es necesario ejecutar repetidamente partes de un programa, pero no se desea perder tiempo en realizar todos los pasos anteriores del programa que se desea depurar.

- ***Superzapping.*** Se denomina superzapping al uso no autorizado de un programa editor de archivos para alterar, borrar, copiar, insertar o utilizar en cualquier forma no permitida los datos almacenados en los soportes de una computadora. El nombre proviene de una utilidad llamada SUPERZAP diseñada para *Mainframes* y que permite acceder a cualquier parte de la computadora y modificarlo, su equivalente en una PC serían las Pctools o el Norton Disk Editor.

Las catástrofes o desastres surgen de las fuerzas naturales tales como las inundaciones, los terremotos, el fuego, el viento. Dichos desastres hacen surgir amenazas directas, pues repercute indiscutiblemente en el funcionamiento físico de las computadoras, redes, instalaciones, líneas de comunicación, etc.

1.7 Casos más renombrados de hackers y crackers

En este punto presentaremos algunos de los sucesos en los cuales han participado crackers y hackers, los cuales han influido por su infiltración en importantes sistemas informáticos.

El Phreaker ciego.

Tim Rosenbaum, un niño ciego con un excelente oído, tenía algo que fascinaba a los niños de Dollan, un pequeño pueblo costero al este de Maine, y esto eran sus silbidos. Era capaz de imitar a los pájaros de todas clases y sobre todo podía controlar el tono del silbido hasta alcanzar notas musicales.

A Tim le gustaban los teléfonos y sobre todo escuchar la voz del otro lado cuando alguien llamaba a casa. Cada vez que podía marcaba un número de teléfono cualquiera y se sentaba a escuchar la voz que decía: "Este número está fuera de servicio".

Hasta que un día Tim silbó al mismo tiempo que la voz decía la frase y calló de golpe. Esto sorprendió a Tim. Volvió a marcar otro número de teléfono, silbó y sucedió lo mismo. Años después descubría que era capaz de generar silbidos a una frecuencia perfecta de 2,600 ciclos, el tono que indica que el teléfono esta colgado.

El robo del banco.

Este ha sido uno de los casos más difundidos. Dos hackers tenían como objetivo ganar dinero fácil y de forma rápida. El objetivo era una sucursal de Citibank, en Nueva York.

Los dos hackers descubrieron, mientras monitorizaban la Red, que esta sucursal realizaba las transferencias a través de una compañía telefónica, y el sistema empleado era una red X.25. Decidieron que si podían monitorizar estas transacciones, podían redirigirlas a otra cuenta, pero había que retirar el dinero antes de que se dieran cuenta. Buscaron el prefijo del banco y probaron varios números en serie a partir de un par de prefijos que sabían de antemano, hasta que terminaron por conectarse con varias terminales VAX.

Después se quedaron con cinco terminales, donde una de ellas era la que controlaba las transacciones. Y una de ellas presentaba un *debug* o puerta abierta. Les fue fácil entrar en ella, empleando la clave de acceso del fabricante.

Cuando entraron al sistema, éste contenía menús que los guiaba a través de cuentas bancarias. Encontraron un paquete de herramientas que permitía crear directorios y programas. Los dos hackers crearon un programa, que interceptaba todas las entradas y salidas de la terminal. Después crearon un directorio y decidieron que éste sería el que capturaría las transacciones.

Varios días después, accedieron a la terminal y descubrieron que se habían hecho muchas transacciones en los días anteriores. Descubrieron que la terminal se conectaba a otra unidad parecida y tras una petición recibía una respuesta, entonces se iniciaba una larga serie de números y letras como password.

Los hackers grabaron esos datos y generaron cientos de transacciones a una cuenta ficticia que habían creado. Pero esta era sólo una prueba, ya que sólo sabían los datos de control de cada computadora.

Días después abrieron una cuenta en Suiza y otras seis en Estados Unidos, donde residían. Cada cuenta estaba registrada a un nombre diferente. Cada cuenta tenía una pequeña cantidad de dinero. Cuando llegó la noche, los hackers hicieron turno delante de la terminal respondiendo a los acuse de recibo. Al mediodía tenían cerca de $200,000 dólares en su cuenta de Suiza y al final de la semana, cada uno se llevo una gran cantidad de dólares.

El primer virus.

El primer virus informático apareció el 22 de octubre de 1987 (según Paul Mungo y su colega Bryan Clough). Este virus infectó cientos de disquetes. Descubrieron que el mensaje que se encontraba oculto en el virus, sólo mostraba un teléfono de contacto para solicitar una vacuna.

Este virus se llamó Brain. El virus Brain se esconde en el sector de arranque del disco y espera a que la computadora se ponga en marcha y lea las primeras pistas del disco. Entonces se carga a sí mismo en la memoria RAM, como si este fuera un programa de arranque común o BOOT.

El virus Brain tenía una densidad de 2,750 bytes, los cuales no cabían en el sector de arranque. El virus hacía dos cosas: colocar sus primeros 512 bytes en el sector de arranque y almacenar el resto de datos en otras seis pistas del resto del disco. De forma que siguiera una cadena.

Este virus resultaba inofensivo si el disco no estaba demasiado lleno, pero si no era así, podía borrar algunos datos importantes, cuando se rescribía en otras pistas del disco.

El Brain tenía un contador y trataba de infectar otro nuevo disquete cada cierto tiempo. Esto era lo que realmente hacia peligroso al Brain, en manos inexpertas. La misión de Brain era la de insertar la etiqueta de bienvenida y ejecutar un proceso automático de reescritura.

Kevin Mitnick.

La historia de Kevin comienza a los 16 años, cuando en 1980, rompió la seguridad administrativa del sistema informático del colegio donde estudiaba. Aquella vez sólo miró los archivos del sistema y no tocó nada.

En 1981, Kevin en compañía de unos amigos, penetró físicamente en las oficinas de COSMOS de Pacific Bell. Ésta era una base de datos de control de llamadas. Kevin y sus amigos robaron algunos manuales del sistema, las claves de seguridad, la combinación de las puertas de acceso al lugar y dañaron otros archivos.

Después de que los delatara la novia de uno de los amigos de Kevin, fueron condenados a tres meses en un centro de detención juvenil de los Ángeles y a un año de libertad provisional.

En 1982, Kevin entró de forma ilegal en un servidor del Ministerio de Defensa estadounidense y en aquella ocasión modificó el archivo de rastreo de llamadas, para no ser localizado.

En 1983, fue localizado y arrestado, tras entrar, a través de Arpanet, a las computadoras del Pentágono. Esta vez fue condenado a seis meses en un reformatorio. El hecho de haber entrado y romper las barreras del "Noth America Air Defense Command Computer" lo convirtió en el Cóndor y la nueva leyenda.

En 1988, Kevin estuvo observando el correo electrónico del departamento de seguridad de MCI y Digital. Con la ayuda de un amigo, Kevin penetró en el sistema y capturó 16 códigos de seguridad de ambas compañías. Pero de la computadora principal de Digital, Kevin se llevó consigo los archivos de un nuevo prototipo de seguridad de un sistema operativo, denominado VMS. Esto alertó a los ingenieros de Digital, que rápidamente se pusieron en contacto con el FBI. Esta vez Kevin cumplió un año de prisión por robo de software.

En 1992, Kevin comenzó a trabajar para una agencia de detectives, pero penetró en varios sistemas. El FBI determinó que Kevin era el responsable, pero esta vez escapó.

En 1994, Kevin se convierte en prófugo de la justicia. Como no puede dar su identidad en ninguna parte, Kevin obtiene una computadora portátil y un teléfono móvil, y es así como esquiva a la policía y al FBI.

Como *Phreaking*, Kevin era un especialista pero necesitaba algo más. Sabía que existía el peligro de ser detectado porque empleaba un teléfono móvil Motorola, los cuales poseen un software oculto que permite enviar una señal a la central para su localización. Pero Kevin conocía que los teléfonos OKI, permitían evitar lo anterior y sabía donde podría encontrar el software para ello.

El 25 de diciembre de 1994, Kevin había penetrado en la computadora de Tsutomu Shimomura, en busca del software de OKI. Este software era pirata, ya que Tsutomu era hacker antes que experto en seguridad.

El 24 de diciembre de 1994 Kevin se daba a la tarea de entrar en los sistemas de Tsutomu, que ese día estaba fuera de casa. Las tres computadoras de la casa de Tsutomu en San Diego, California, comenzaron a recibir una serie de instrucciones externas. Kevin trataba de averiguar qué relación tenían entre sí las tres computadoras que estaban encendidas ese día y pronto averiguó cual de las máquinas era el centro de la pequeña red local.

Se trataba de una SPARC que había sido detectada en tan sólo tres minutos. Recibía una solicitud de conexión desde una dirección falsa de Internet y la computadora contestaba con la respuesta adecuada de conexión con esa dirección.

Kevin envió otras 29 peticiones, con lo que consiguió bloquear la máquina con una ráfaga de datos rápidamente transmitidos. Otra de las SPARC recibió 20 solicitudes, las cuales reconoció, pero siempre recibió un mensaje de cancelación, con el fin de despistarla. Pero lo que realmente buscaba Kevin era capturar los datos obtenidos como respuesta de las SPARC. Estudió cada respuesta y dedujo que debía añadir 128,000 unidades al número de respuesta. De esta manera podía acceder a la tercer computadora. Entonces añadió un archivo oculto que le permitiría entrar libremente cada vez que lo solicitara, sin tantas complicaciones.

Kevin husmeó en el disco duro y encontró el software del OKI y otros archivos de seguridad que Tsutomu había desarrollado. Esto molestó realmente al japonés Tsutomu e inició una persecución contra Kevin, que culminó el 15 de febrero de 1995.

El sistema de codificación de videocrypt y el profesor ZAP.

Este caso le sucedió al grupo SKY y su sistema de codificación Videocrypt. El sistema Videocrypt se basaba en tecnología digital para la codificación del video. Este nuevo sistema se basaría en una tarjeta de acceso inteligente. Con lo que se podría activar y desactivar cada decodificador a voluntad. Además, el sistema digital de encriptación permitía trabajar con algoritmos complejos que necesitaban de claves secretas albergadas en el interior de la tarjeta electrónica.

Sin embargo, descubrieron que la orden de activación se definía como una tensión de control sobre el decodificador. De modo que bastaba con cortar una pista de cobre del circuito para eliminar la función de activación y desactivación del sistema.

Entró en acción la segunda fase de este sistema. Ahora, en lugar de ser una simple tensión de control, se convertiría en una palabra u octeto en forma de respuesta a partir de una palabra más larga. Dos claves, una pública y otra secreta se encargarían de descifrar la clave de acceso. Así, la clave pública se desenmascararía en el interior del decodificador, mientras que la clave secreta se revelaría en el interior de la tarjeta de acceso. Si se pretendía hacer un hackeo al sistema este sería por software, ya no por hardware como había sucedido anteriormente.

El algoritmo era complejo y utilizaba una palabra de control de varias decenas de bits. Lo peor era que esos códigos no eran repetitivos, porque se sabía que las tarjetas de acceso se basaban en el estándar de comunicación ISO 7816, y se podían leer las comunicaciones de dicha tarjeta con el decodificador a través de una interfaz programada. Se constataba que un sistema no podía trabajar con claves aleatorias.

Rider Shamir fue el encargado de crear un nuevo algoritmo que pondría en jaque a los hackers. El código se denominaba RSA y se creía más seguro que el estándar americano DES, un algoritmo que se permutaba 16 veces.

Un profesor motivado por la duda de uno de sus alumnos, se dedicó a estudiar la forma de revelar el algoritmo del sistema. El profesor desarrolló una interfaz con un pequeño programa para estudiar y leer lo que se avenía entre la tarjeta y el decodificador con la intención de enseñar a sus alumnos cómo funcionaba el protocolo ISO 7816. Además de los códigos de control comunes de este protocolo, habían otros códigos hexadecimales que variaban constantemente, pero pronto descubrió que ciertos códigos se repetían

esporádicamente y que si seguía con detenimiento la cadena de datos, estos se repetían asiduamente a lo largo de un periodo.

Un mes después, dio con la clave y tuvo la primer tarjeta electrónica basada en un microprocesador de Arizona Chip, un PIC 1654. El nivel de seguridad se denominaba nivel 6. Esta tarjeta cayó en manos de otros hackers. Pronto los códigos y tablas se difundieron con rapidez. Entonces, New Datacom cambió el nivel 6 al nivel 7, con pocas variaciones, pero el profesor dio de nuevo con la clave y creó las tablas que permitían cambiar el número secreto de la tarjeta, por lo tanto, un mismo algoritmo adoptaba formas diferentes en cualquier momento.

Cada tarjeta tenía un número de identificación, el cual se podía modificar vía aire y a través de software. Los PIC podían modificarse externamente y cada uno tenía un número clave de serie. Los ingenieros de New Datacom consiguieron algunas tarjetas piratas y encontraron una falla. Lo que hicieron fue modificar el software de la tarjeta para que respondiera de otra forma. La contramedida electrónica se llamó ECM, con la cual se anulaban las tarjetas piratas sin tener que cambiar los códigos continuamente.

Sin embargo, los piratas crearon un chip llamado Kentucky Fried Chip el cual permitía elegir la instrucción que daba autoridad para habilitar otro chip específico encargado de decodificar la señal de video. Esto duró más o menos un año hasta que los ingenieros de New Datacom modificaron el programa de dicho chip.

Surgió la tarjeta llamada Phoenix Hack la cual presentaba algunos problemas cuando llevaba algún tiempo insertada en el decodificador.

El profesor de informática, cuyo apodo es ZAP, tenía su nueva tarjeta basada en dos poderosos chips PIC 1684.

Algunas empresas seguían fabricando ***"cartones electrónicos"***. Ya que no todos los canales que estaban codificados con el sistema de codificación de Videocrypt, no trabajaban con el mismo código, todavía existían canales que funcionaban bajo el código 07 y el profesor ZAP vendió sus códigos con el nombre de SEASON 7 (este programa fue actualizándose hasta alcanzar la versión SEASON 13). Empresas tales como Megatek e Hi-Tech consiguieron colocar en el mercado miles de estas tarjetas con códigos 07.

Surgió un circuito llamado bloquer, el cual consistía en una interfaz electrónica, entre el decodificador y la tarjeta legal u oficial, mediante el cual el sistema se basaba en bloquear los códigos ECM de borrado de tarjeta. Además, los bloquers permitían activar tarjetas caducadas e impedían que se desactivaran desde el centro de control de abonados.

El sistema funcionó bien hasta que los ingenieros de New Datacom contra-atacaron con nuevos códigos ECM ***"Control de Medida Electrónica"*** para desactivar definitivamente las tarjetas legales. El sistema se basaba en una instrucción secreta que fundía el fusible de lectura de la tarjeta chip.

El capitán ZAP lanzó la nueva versión 09 que poseía códigos variables y tablas. El algoritmo seguía basándose en la norma RSA y sólo se había complicado en un octeto más de instrucción. Durante varias semanas, la tarjeta funcionó correctamente, pero New Datacom tenía preparada una nueva tarjeta oficial la cual tenía mucha memoria ROM interna y mucha más RAM.

Como era costumbre, los cambios de código se efectuaban el día de navidad. Cuando por fin llegó este día todas las tarjetas piratas reaccionaron de forma extraña, ya que sólo decodificaban por momentos y presentaban mensajes extraños en la pantalla del televisor. Debido a que esas tarjetas no poseían fusibles internos que desactivar y eran inmunes a los ECM, New Datacom decidió que la nueva versión debía ser cuasi-aleatoria y permitir modificar los códigos cada 48 horas.

Pero el profesor ZAP tenía lista una nueva tarjeta denominada **Card Mate** que estaba basada en un potente chip de Dallas DS 5002, además tenía más memoria interna y era reprogramable a través de un teclado al tacto.

Un año después, New Datacom decidió cambiar a la versión OA, por lo que sólo se tuvo que reprogramar las tarjetas Card Mate.

Canal de cine Filmnet.

Filmnet, un canal de cine las 24 horas, fue uno de los primeros canales de televisión vía Satélite que decidió codificar su señal el 1 de septiembre de 1986, con un sistema de cifrado basado en tecnología analógica.

La primera versión era similar a la empleada por SKY, al cual llamaron SATPAC. Este sistema de codificación sufrió cambios el 24 de diciembre de 1989, el 11 de mayo de 1990, en diciembre de 1990 y en enero y marzo de 1991.

Filmnet introdujo una codificación del audio digital que, con la llegada de potentes chips, hicieron posible su ruptura.

Otro caso fue el de Canal Plus de Francia que empleó un sistema de codificación llamado DISCRET 1, del cual la empresa inglesa Hi-Tech fabricó un millón de decodificadores piratas. Algo similar sucedió con el sistema SAVE de la BBC.

El Crack del código CSS.

El algoritmo de encriptación de los discos DVD fue descubierto por un miembro del grupo de hackers noruego, MoRE, "Master of Reverse Engineering": Jon Johansen, un estudiante de 15 años, quien descubrió en su computadora, que el sistema de protección del DVD podía romperse con un programa pequeño que había creado.

El programa DeCSS permite pasar el contenido de un DVD al disco duro de una computadora y reproducir la película con calidad perfecta. Este pequeño programa permite crear un duplicado desprotegido del contenido DVD en un disco virgen por medio de una grabadora.

El Crack del código regional.

El Crack de código regional se debe a la sucesión de los chips que permitían cargar discos piratas, en los Playstation. El microcontrolador 508 de microchip se empleaba para engañar la secuencia de arranque del disco. Tal como sucedía en los Playstation, la secuencia de arranque del disco, parte que contiene el código regional, era sustituido por varios ceros a fin de indicar al reproductor de la existencia de un disco universal.

Este crack es difícil de llevar a cabo, ya que se tiene que abrir el reproductor DVD, con lo que se pierde la garantía al momento de abrirlo. Sin embargo, en la red existen guías de cómo realizar esa tarea con éxito.

Los crackers han sacado los Firmwares, los cuales permiten modificar Reproductores DVD con y sin el chip 508.

Existe un crack por software que permite reproducir el contenido del DVD en la computadora, el cual consiste en renombrar un archivo DLL y, en otros casos, basta con parcharlos.

El Crack de Macrovision.

En octubre de 1988, la revista de electrónica Elektor, publicó lo que fue el primer decoder capaz de borrar la señal de anticopia de Macrovision. Se trataba de un circuito capaz de crear una ventana de captura, en la cual introducía nuevos niveles de negro capaces de sustituir los niveles positivos de la señal de anticopia de Macrovision. El decoder se basaba en un extractor de sincronismos, varios conmutadores digitales y un par de monoestables.

En 1993, un curioso de la electrónica que responde al apodo de OverrideSidek diseñó el decoder de Macrovision más rentable de los últimos años. El circuito se publicó en la revista Resistor.

En 1997, en la red existían varias páginas que muestran cómo decodificar el sistema de anticopia de Macrovision.

A finales de 1999, el crack de Macrovision se basa en el empleo de software, programas capaces de deshabilitar la función de Macrovision.

El Crack de Discret y Nagravision.

El Canal Plus, el primer canal de paga de Francia, adoptó el sistema de codificación DISCRET 1, el cual fue objeto de estudio en 1987. DISCRET tuvo una vida de sólo 6 años, la cual finalizó en 1990 con el DISCRET 12.

En 1994 surgió Nagravision, el cual estaba avalado por Andre Kudelski, uno de los mejores ingenieros de Europa. Pero a finales de 1998, se colocó en la red un software capaz de decodificar parte de la señal de Nagravision, el cual se llamó NagraDec83. Éste era capaz de desencriptar u ordenar, una imagen en Nagravision, en una computadora que tuviera una capturadora de Televisión.

El Crack de Save y la venta de Enigma.

El sistema SAVE de la BBC se estaba empleando en un canal hardcore. La empresa Hi-Tech llegó a fabricar tres millones de unidades para este sistema. LA BBC demandó a Hi-Tech, sin embargo, el Canal Hardcore no lo hizo. Los directivos de este canal pornográfico decidieron contratar los servicios del hacker, ya que la gente prefería adquirir un decoder pirata para ver películas pornográficas.

El sistema de codificación Enigma es similar al de Videocrypt. Nadie sacó el crack para este sistema. Cuando el canal pornográfico desapareció, los decodificadores de Enigma se

vendieron a otro canal hardcore llamado Adult Channel, el cual estaba decodificado con Videocrypt.

El crack de Irdeto Digital y Nokia 9600.

Los receptores Nokia 9600 y 9800 han sido elegidos por los hackers para experimentar con la televisión digital. El doctor OverFlow fue el primero en iniciar toda una línea de experimentos con este receptor digital. Su software Edit DVB, podía modificar la información de la ROM de este receptor de Nokia. Sin embargo, este software sólo permite modificar la estructura y presentación del menú OSD del receptor.

El Crack de Irdeto llega después y nadie sabe quien es el creador. Este Crack permitía reactivar la tarjeta original de Irdeto. El siguiente Crack de Irdeto emulaba perfectamente esta tarjeta.

Ataques a sitios Web.

En 1996, la página Web de Kriesgman (http://www.kriesgman.com/), una de las principales fábricas de pieles de Estados Unidos, fue hackeada, poniendo carteles y frases en defensa de los animales y la ecología.

En noviembre de 1996, la página de la Agencia Central de Inteligencia de los Estados Unidos (CIA) (http://www.odci.gov/cia) fue víctima de los hackers cuando ubicaron la frase "Welcome to the Central Stupidity Agency".

En 1997, se alteró el sitio de las famosas cantantes inglesas, Spice Girls (http://www.spicegirls.com), para protestar contra la cultura pop y el uso masivo de Internet.

La página Web del Ministerio de Justicia Local de Argentina fue intervenida por el grupo x-team, colocando una fotografía de José Luis Cabezas el mismo día que se cumplía un año de su asesinato. Debajo se encontraba un texto donde supuestamente los funcionarios le pedían perdón al pueblo por impedir constantemente el esclarecimiento del caso. La fotografía permaneció 24 horas hasta que la quitaron.

En diciembre de 1997, el sitio Web de la fuerza aérea de Estados Unidos, fue alterado por hackers, que incorporaron a la página principal una imagen pornográfica.

En julio de 1999 el sitio Web de Hillary Clinton fue hackeado. Sólo consistió en un redireccionamiento del URL, que hizo que quienes intentarán acceder al sitio web de Hillary Clinton fuesen llevados a la página creada por los simpatizantes de Rudolph Giuliani, pues ambos eran candidatos a la senaduría por Nueva York.

En agosto de 1999 el sitio web de Symantec fue alterado por hackers. La noticia causó revuelo, ya que Symantec es uno de los principales proveedores de software de seguridad y antivirus. Los hackers cambiaron la portada del sitio web corporativo con un texto en que su acción se reivindicaba como una victoria ("... we own your ass, Symantec").

Los piratas informáticos también lograron infiltrar los servidores de Symantec con un programa tipo "gusano", que automáticamente se propaga por sistemas interconectados y

que está en condiciones de causar daños similares a los virus. Aunque un portavoz de Symantec desmintió que los hackers hubieran logrado instalar un "gusano" en sus sistemas.

Ataques al Pentágono.

En 1996, el argentino Julio César Ardita penetró ilegalmente a la red del Pentágono de Estados Unidos mediante Internet. Fue condenado a cinco años de prisión y debió pagar una multa de 5,000 dólares.

En febrero de 1998 se informó que la red informática del Pentágono había estado expuesta a intensas interrupciones de grupos de hackers.

La Secretaría de Defensa de Estados Unidos señaló que los hackers en ningún momento tuvieron acceso a información clasificada, sino sólo a los registros de personal y sueldos.

Los ataques de MafiaBoy.

MafiaBoy es el apodo de un joven canadiense de 15 años que coordinó e inicio el mayor ataque a Internet. En febrero de 2001 realizó un bloqueo masivo de las páginas más importantes de EE.UU.: eBay, Amazon, CNN, Buy.com, Yahoo, entre otras.

MafiaBoy y su aliado Coolio, utilizaron el método "denegación de servicio" que consiste en bombardear los servidores atacados con peticiones falsas de información hasta colapsarlos. Con este método se paralizó la capacidad de respuesta, dejando colgado el servidor cuando se encuentra colapsado.

MafiaBoy fue detenido el 15 de Abril por la FBI, tras seguir algunas pistas que dejo en las computadoras de la Universidad de Santa Bárbara, después de enviar algunos correos, donde se burlaba de su hazaña.

1.8 ¿Qué es Estrategia?

No hay unanimidad sobre el origen de la palabra estrategia, sin embargo, la gran mayoría de los historiadores coincide en que se origina en la antigua Grecia y proviene de la palabra griega Strategus (Stratos=ejército y Agein=conductor) cuya acepción sería conductor de ejércitos o como muchos pensadores concordaban "el arte del general".

La mayoría de las definiciones de la palabra estrategia aportan un componente o matiz a la acepción diferente e importante, razón por la cual vamos a revisar algunas definiciones que se han formulado.
Otro interesante aporte lo entregó Von Der Goltz al establecer que: "La estrategia se define como la teoría con la que se conducen y se dirigen los ejércitos."[16]

"Pareciera que en este tercer cuarto del siglo XX se hubieran trastrocado todos los conceptos, valores y elementos clásicos de la conducción bélica, más aún diríamos que la guerra misma ha cambiado de naturaleza, que los conflictos armados son diferentes en sus formas y sus fines. La Guerra Fría, la guerra revolucionaria, la guerra nuclear y toda otra

[16] MONTT, Manuel. General del Ejército de Chile. La guerra, su conducción político-estratégica. 1970. p. 29.

forma de lucha parecieran haber desterrado las normas ortodoxas y clásicas de la estrategia."[17]

Para el Mariscal alemán Von Moltke, "La estrategia señala el mejor camino que conduce a la batalla, ella dice cuándo y dónde se debe combatir."[18]

De acuerdo con Shapiro las estrategias posibles para alcanzar los objetivos pueden ser muy diversas. Un mismo objetivo se puede conseguir a través de estrategias distintas y la misma estrategia no proporciona siempre los mismos resultados.

Para nuestros fines definiremos estrategia como:

El conjunto de reglas que aseguran una decisión óptima en cada momento.

La Estrategia, con el paso del tiempo, ha evolucionado desde una idea orientada exclusivamente a lo militar, hacia un concepto de mayor cobertura, en el que ha variado su campo semántico debido a los avances tecnológicos experimentados por los medios materiales.

Dentro del contexto de la seguridad informática, consideraremos estrategia como la dirección de la organización para prevenir o corregir la transferencia, modificación o destrucción no autorizada de la información.

[17] Ibid. p. 16.
[18] Ibib. p. 29.

Capítulo 2

Niveles de Seguridad Informática

2.1 Libro Naranja

La seguridad y confiabilidad de los sistemas de información es una parte que interesa a entidades gubernamentales, industriales, financieras, y en general a sectores que manejan información importante. Por esta razón, se tienen organismos que estudian el problema. Dentro del ámbito de los Estados Unidos de América se han formado grupos de trabajo alrededor del tema.

Las siglas NCSC surgen del *National Computer Security Center*, Centro de Seguridad para Computación a nivel Nacional en los Estado Unidos de América. Este centro se formó en 1981 con el propósito de proporcionar sistemas informáticos confiables para uso en misiones críticas y sensibles.

Este centro definió unos Criterios de Evaluación de Sistemas Informáticos Confiables (*Trusted Computer Systems Evaluation Criteria*, TCSEC), los cuales indican niveles de seguridad. La publicación de estos criterios se le conoce como el Libro Naranja (***Orange Book***), por el color de su portada. La referencia de esta obra es *Department of Defense Trusted Computer System Evaluation Criteria* December 1985, DOD 5200.28-STD.

Los TCSEC tienen por objetivo aplicar la política de seguridad del Departamento de Defensa estadounidense. Esta política se preocupa fundamentalmente del mantenimiento de la confidencialidad de la información clasificada a nivel nacional.

El Libro Naranja define cuatro extensas divisiones jerárquicas de seguridad, cada división consiste en una o más clases numeradas, entre más grande sea el número, se indica un mayor grado de seguridad. Cada clase de criterios cubre cuatro categorías de evaluación: políticas de seguridad, responsabilidad, confianza y documentación.

1) Políticas de Seguridad.

- **Control de Acceso Discrecional.**

  El Control de Acceso Discrecional (*Discretionary Access Control*, DAC) es un método para restringir el acceso a los archivos (y a otros objetos del sistema) basándose en la identidad de los usuarios y/o los grupos a los que pertenecen. EL DAC es el más común de los mecanismos de control de acceso que se encuentra en los sistemas.

- **Reutilización de Objetos.**

  La reutilización de objetos requiere la protección de archivos, memoria y otros objetos en un sistema auditado, debido a que pueden ser accedidas accidentalmente por usuarios que no tienen acceso autorizado a ellos. Las características de control de acceso de un sistema ordinario determinan quién puede y quién no puede acceder a archivos, dispositivos y otros objetos que han sido asignados a usuarios específicos. La reasignación de objetos requiere que las direcciones que aparecen en esos objetos sean reasignadas.

- **Etiquetas.**

  Las etiquetas y el control de acceso obligatorio son requerimientos separados de la política de seguridad, pero ambas funcionan de manera conjunta. Al iniciar en el

nivel B1, el libro naranja propone que cada sujeto (por ejemplo: usuario, proceso) y un objeto almacenado (por ejemplo: archivos, directorios, ventanas, socket) tengan una etiqueta sensitiva asociada a él. Una etiqueta sensitiva de usuario especifica el grado o nivel de confianza, asociado con ese usuario, las etiquetas de usuario sensitivas son usualmente llamadas como certificado de paso ó "*clearance*". Una etiqueta sensitiva de archivo especifica el nivel de confianza que un usuario puede ser capaz de tener al acceder a ese archivo.

- **Integridad de Etiquetas.**

  La integridad de etiquetas asegura que las etiquetas sensitivas asociadas con eventos y objetos tengan una representación exacta de los niveles de seguridad de estos eventos y objetos. Así una etiqueta sensitiva como TOP SECRET [VENUS] deberá estar asociada con un archivo TOP SECRET que contiene información acerca del planeta Venus.

- **Exportación de Información Etiquetada.**

  Un sistema confiable debe asegurar que la información es escrita por el sistema, que la información cuenta con mecanismos de protección asociados a ella. Dos formas de exportar información son asignar un nivel de seguridad a los dispositivos de salida y escribir etiquetas sensitivas en los datos. Los sistemas valorados, como B1 , en adelante deben proporcionar facilidades de exportación segura.

  Se definen dos tipos de dispositivos para exportar; multinivel y de nivel simple. Cada dispositivo de entrada/salida y canal de comunicaciones en un sistema debe de ser designado de uno o de otro tipo. Cualquier cambio a estas designaciones de dispositivos debe de ser capaz de ser auditado. Típicamente un administrador de sistemas designa dispositivos durante la instalación del sistema o durante su configuración.

- **Exportación de Dispositivos Multinivel.**

  Un dispositivo multinivel o un canal de comunicaciones multinivel es aquel con la capacidad de escribir información con un número diferente de niveles de seguridad. El sistema debe soportar una variedad de especificaciones de niveles de seguridad, desde la más baja (SIN CLASIFICACIÓN) hasta la más alta (ALTAMENTE SECRETA), permitiendo que un dato sea escrito en el dispositivo.

  Cuando se escribe la información en un dispositivo multinivel, se requiere que el sistema tenga alguna forma de asociar un nivel de seguridad a él. Los mecanismos pueden diferir para los diferentes sistemas y los diferentes tipos de dispositivos. Los archivos escritos a este dispositivo pueden tener etiquetas sensitivas agregadas a ellas (usualmente escritas en los encabezados del registro precediendo los datos del archivo). Todo esto para prevenir que un usuario desvíe los controles del sistema con una simple copia de un archivo sensitivo a otro de un sistema inseguro o dispositivo.

- **Exportación de Dispositivo de Nivel Único.**

  Un dispositivo de nivel único o un canal de comunicaciones de nivel único es capaz de escribir información con solo un nivel particular de seguridad. Usualmente las terminales, impresoras, dispositivos de cinta y puertos de comunicación están en la categoría de dispositivos de nivel único. El nivel que se especifica para un dispositivo depende usualmente de su localización física o de la seguridad inherente del tipo de dispositivo. Por ejemplo, la instalación de una red contempla varias impresoras en un número determinado de computadoras y oficinas. El administrador debe designar que esas impresoras tengan niveles sensitivos que correspondan al personal que tiene acceso a dichas impresoras.

- **Etiquetado de Salidas Legibles a la Persona.**

  Esto se refiere a los requerimientos de cómo se deben hacer las etiquetas para personas; éstas incluyen mapas, gráficas y otros indicadores. El administrador del sistema debe especificar la forma en que las etiquetas van a aparecer a la salida.

  Por lo regular, se requieren dos tipos de etiquetas. Primero, cada salida distinta debe ser etiquetada, al principio y al final con una etiqueta que represente con sensitividad general la salida. Si se esta imprimiendo se puede ver un "banner" al principio y final del archivo, mostrando claramente la etiqueta sensitiva del archivo. Segundo, cada página de la salida impresa deberá llevar en la parte superior, inferior o ambas, una etiqueta de sensitividad general o específica del contenido en esa página.

- **Etiquetas Sensitivas de Eventos.**

  Las etiquetas sensitivas de eventos requieren de estados donde el sistema pueda notificar a un determinado usuario de algún cambio en el nivel de seguridad, asociado con otro usuario durante una sesión interactiva. La idea de estas etiquetas es que un usuario siempre sepa el nivel de seguridad en el que se está trabajando.

- **Dispositivos Etiquetados.**

  Cada dispositivo físico debe tener asociado un nivel de seguridad en el sistema; éste puede ser multinivel, es decir, tener varios niveles de seguridad donde se debe especificar el nivel mínimo así como el máximo. Si tiene un solo nivel, entonces, el máximo y el mínimo son el mismo. Esto para reforzar las restricciones impuestas por el medio ambiente físico en donde el dispositivo se encuentre localizado.

- **Control de acceso obligatorio.**

  En el control de acceso obligatorio el sistema autoriza quién puede y quién no puede tener acceso a sus archivos y tiene restricciones en cuanto al manejo de dispositivos, etc. Es decir, pone el control de todos los accesos, como decisiones bajo el control del sistema.

2) Responsabilidad.

- **Identificación y Autenticación.**

  La identificación y la autenticación es una norma de seguridad básica en el libro naranja. Antes de poder realizar cualquier acción dentro del sistema, (como correr un programa, leer un archivo, etc.) se debe pasar por ese proceso.

  En la mayoría de los sistemas multiusuarios, este proceso se hace por medio del nombre de usuario (login), seguido de una contraseña (password). En el libro naranja se define que la contraseña debe estar protegida, pero no especifica cómo. Existe otra publicación en la cual se hace referencia a eso: *The Department of Defense Password Management Guideline*, publicado por el gobierno de Estados Unidos y también conocido como el **Libro Verde**.

  En el Libro Verde se definen tres aspectos fundamentales:

  1. Los usuarios deben ser capaces de cambiar sus contraseñas.
  2. Las contraseñas deben ser creadas por el sistema, más el realizado por el usuario.
  3. Deben existir reportes de auditoría, donde se guarden datos como fecha y hora del último acceso al sistema.

- **Rutas Seguras.**

  Una ruta segura proporciona un medio libre de errores, por el cual un usuario puede comunicarse con una Base de Computadoras Confiables *(Trusted Computing Base,* TCB*)* sin interactuar con el sistema a través de aplicaciones inseguras y capas del sistema operativo.

- **Auditoría.**

  Una auditoría es el registro, análisis y revisión de las actividades relacionadas con la seguridad de un sistema confiable. Consiste en revisar los eventos que pueden ser importantes para detectar un posible ataque al sistema.

  Entre estos eventos se encuentran:

  - Autenticaciones (exitosas y fallidas).
  - Accesos a sistemas remotos.
  - Operaciones con archivos: renombrar, borrar, abrir, etc.
  - Cambios en los privilegios.

  El revisar estos eventos es importante para poder detectar irregularidades en el sistema, como por ejemplo: un gran número de autenticaciones fallidas desde una misma terminal, o los repetitivos intentos de un usuario de tener accesos a archivos, a los cuales él no tiene acceso.

  Por eso cada vez que un evento auditable ocurre, se debe almacenar la siguiente información y en el siguiente orden:

- Fecha y hora de cada evento.
- Identificador único del usuario que ejecutó el evento.
- Tipo de evento.
- Si el evento fue exitoso o no.
- Origen de la petición (identificador de la terminal).
- Nombre de los objetos involucrados.
- Descripción y modificación a las bases de datos de seguridad.
- Niveles de seguridad de los usuarios y de los objetos.

Por lo tanto, la auditoría es una herramienta vital de la administración. Algunos proveedores proporcionan programas que te permiten llevar a cabo una auditoría, para eventos o archivos específicos.

3) Confianza.

- **Arquitectura del Sistema.**

El requerimiento de arquitectura del sistema tiene el objeto de diseñar un sistema para hacerlo lo más seguro posible, invulnerable.

Así, los sistemas de los niveles bajos (C1, B1 y hasta B2) no fueron necesariamente diseñados específicamente para seguridad; ellos soportan principios de diseño de hardware y sistema operativo, también como la habilidad de soportar características específicas que quizás son agregadas a estos sistemas. La mayoría de los diseños modernos de multiprocesamiento y sistemas multiusuarios siguen las claves de los principios de diseño necesarios para cumplir los requerimientos del libro naranja en los que la arquitectura del sistema se refiere al menos a C2 y B1, aunque estos principios no están necesariamente orientados a seguridad.

- **Integridad del Sistema.**

La integridad del sistema significa que el hardware y el firmware deben trabajar y ser probados para asegurar que trabajen adecuadamente. Para todos los niveles, el libro naranja establece las características de hardware y software que deben ser proporcionadas para ser usadas y periódicamente validadas para la correcta operación del hardware instalado y los elementos firmware del TCB.

La integridad del sistema es una meta de importancia vital para todos los desarrolladores de sistemas, y no sólo desarrolladores de sistemas seguros. Como ya se ha mencionado anteriormente, un elemento muy importante del sistema de seguridad es la habilidad de que el sistema funcione como se espera y permanecer en operación. Muchos vendedores miden los requerimientos de integridad del sistema, al proveer un juego de pruebas de integridad. El diagnóstico más substancial es hacer un programa calendarizado de periodos de mantenimiento preventivo.

- **Pruebas de Seguridad.**

El libro naranja tiene un interés substancial en probar las características de seguridad en los sistemas a evaluar. Las pruebas de seguridad aseguran que los

requerimientos están relacionados con los requerimientos de pruebas de documentación. El sistema desarrollado será probado para todas las características de seguridad, asegurando que el sistema trabaja como se describe en la documentación, y se documentan los resultados de las pruebas de estas características. El equipo de evaluación del NCSC está comprometido con sus pruebas.

Estos son los dos tipos básicos de pruebas de seguridad:

- Prueba de mecanismos y
- Prueba de interfaz.

La prueba de mecanismos significa probar los mecanismos de seguridad. Estos mecanismos incluyen: control de acceso discrecional, etiquetado, control de acceso obligatorio, identificación y autenticación, prueba de rutas y auditoría. La prueba de interfaz significa probar todas las rutinas del usuario que involucren funciones de seguridad.

- **Diseño de Especificaciones y Verificación.**

El diseño de especificaciones y la verificación requieren una comprobación de que la descripción del diseño para el sistema sea consistente con las políticas de seguridad del sistema.

A cada nivel de seguridad, empezando desde el B1 del Libro Naranja, corresponde un incremento del modelo formal (precisamente matemático) de las políticas del sistema de seguridad, que permite incrementar las pruebas de que el diseño del sistema es consistente con su modelo.

¿Qué es una prueba formal? Es un argumento matemático completo y convincente de que el sistema es seguro, o al menos de que el diseño del sistema lleva implementada una adecuada política de seguridad. Por ejemplo, si se demuestra matemáticamente bajo que condiciones existen ciertos sujetos (usuarios), que pueden acceder a cierto tipo de objetos (archivos) y se demuestra además que los usuarios no pueden engañar las condiciones de acceso.

- **Análisis de Canales Secretos.**

Un canal secreto es una ruta de información que no se usa ordinariamente para comunicaciones en un sistema por los mecanismos normales de seguridad del sistema: es una vía secreta para transportar información a otra persona o programa. Es el equivalente computacional de un espía que porta un periódico como una contraseña.

En teoría, cada pieza de información almacenada o procesada por un sistema computacional seguro es un potencial canal secreto.

Existen dos tipos de canales secretos: canales de almacenamiento y canales de temporización. Los canales de almacenamiento transportan información para cambiar datos almacenados en el sistema en alguna forma. Los canales de temporización transportan información que afecta el desempeño o modifica de

alguna forma el tiempo usado por los recursos del sistema en alguna forma medible.

- **Facilidad de la Administración de la Seguridad.**

  La facilidad de la administración de seguridad es la asignación de un individuo específico para administrar las funciones relacionadas con la seguridad de un sistema. La facilidad de administración de la seguridad está muy relacionada con el concepto de *privilegio mínimo*, un concepto tempranamente introducido en términos de arquitectura de sistemas. En el contexto de seguridad, el privilegio mínimo significa que el usuario de un sistema debe tener el menor número de permisos y la menor cantidad de tiempo – únicamente el necesario para desempeñar su trabajo. El concepto de administración está muy relacionado con la separación de obligaciones, la idea es asignar mejores piezas de seguridad relacionadas con tareas de algunas personas específicas y que ningún usuario tenga el control total de los mecanismos de seguridad del sistema, para que de ninguna forma un usuario pueda comprometer completamente al sistema.

- **Administración de Configuración.**

  La administración de configuraciones protege un sistema seguro mientras está siendo diseñado, desarrollado y mantenido. Involucra el identificar, controlar, contabilizar y auditar todos los cambios hechos en los lineamientos de TCB, incluyendo hardware, firmware y software; por ejemplo, cualquier cambio en el código, durante las fases de diseño, desarrollo y mantenimiento, así como la documentación, planes de pruebas y otras herramientas del sistema relacionadas y sus facilidades.

  La administración de configuraciones tiene varias metas. Primero, el control del mantenimiento del sistema durante su ciclo de vida, asegurando que el sistema es usado de la forma correcta e implementando las políticas de seguridad adecuadas. El "sistema adecuado" es el sistema que ha sido evaluado o que actualmente está siendo evaluado. En otras palabras, la administración de configuraciones previene de usar versiones obsoletas o nuevas, que no han sido probadas en el sistema o alguno de sus componentes.

  Segundo, hace posible regresar a versiones previas del sistema. Esto es importante si por ejemplo, un problema de seguridad es encontrado en una versión del sistema que no tenían en una versión anterior.

  Para cumplir los requerimientos de la administración de configuración, se necesita:

  - Asignar un identificador único para cada elemento configurable.
  - Desarrollar un plan de administración de la configuración.
  - Registrar todos los cambios de elementos de configuración (en línea y fuera de línea).
  - Establecer un tablero de control y configuraciones.

- **Recuperación Confiable.**

  La recuperación confiable asegura que la seguridad no ha sido violada cuando se "cae" un sistema o cuando cualquier otra falla del sistema ocurre. La recuperación confiable actualmente involucra dos actividades: prepararse ante una falla del sistema y recuperar el sistema.

  La principal responsabilidad en preparación es respaldar todos los archivos del sistema crítico con una base regular. El procedimiento de recuperación puede ser, esforzarse por restaurar sólo un día o dos de procesamiento de información.

  Si una falla inesperada ocurre, como una falla de disco duro o un corte de corriente eléctrica, se debe recuperar el sistema de acuerdo con ciertos procedimientos para asegurar la continuidad de la seguridad en el sistema. Este procedimiento también puede ser requerido, si se detecta un problema del sistema, como recursos perdidos, o una base de datos inconsistente o cualquier cosa que comprometa el sistema.

- **Distribución Confiable.**

  La distribución confiable protege un sistema seguro, mientras el sistema está siendo transportado al sitio del cliente. Este requerimiento sólo se tiene para el nivel A1. Este requerimiento tiene dos metas: protección y validación del lugar.

  La protección significa que el vendedor final (y durante el transporte del vendedor al cliente) se asegura que durante la distribución, el sistema llegue al lugar donde lo solicitó el cliente, exactamente, como fue evaluado antes de transportarse por el vendedor, ya que proporciona protección durante el empaque, transporte entre intermediarios hasta llegar al usuario final.

  La validación del lugar significa que el cliente final, con la distribución confiable, puede detectar falsificaciones del sistema o modificación del sistema.

4) Documentación.

- **Guía del Usuario de Características de Seguridad.**

  La Guía del Usuario de Características de Seguridad (*Security Features User's Guide*, SFUG) es un apunte ordinario, sin privilegios para todos los usuarios del sistema. En él se encuentran cosas que son necesarias para saber acerca de las características del sistema de seguridad y de cómo es que están reforzadas. Los temas típicos incluyen:

  - *Acceso al sistema seguro.* Cómo se debe introducir el login y el password, con que frecuencia debe de cambiarse, qué mensajes deben de verse y cómo deben de usarse estos mensajes para reforzar la seguridad del sistema.
  - *Protección de archivos y otro tipo de información.* Se debe de especificar una lista de control de acceso (o protecciones similares).
  - *Importar y exportar archivos.* Leer nuevos datos dentro del sistema confiable y como escribir datos de otros sistemas sin arriesgar la seguridad.

- **Facilidades del Manual de Seguridad.**

  Este documento es un apunte del administrador del sistema y/o administradores de seguridad. Habla sobre todas las cosas que se necesitan saber acerca de la configuración del sistema para ser seguro; reforzando el sistema de seguridad; interactuando con peticiones del usuario y haciendo que el sistema trabaje con las mejores ventajas. El Libro Naranja requiere que este documento contenga advertencias, acerca de las funciones y privilegios que deben ser controlados en sistemas seguros.

- **Documentación de Pruebas.**

  Para el Libro Naranja, la documentación de pruebas consiste en mostrar cómo los mecanismos de seguridad fueron probados, y los resultados de los mecanismos de seguridad con pruebas funcionales. El tener buena documentación de pruebas es generalmente sencillo, pero voluminoso. Es común que la documentación de pruebas para los sistemas C1 y C2 consista en varios volúmenes de descripción de pruebas y resultados.

- **Diseño de documentación.**

  Es un requerimiento formidable para todos los desarrolladores de sistemas. La idea de diseñar documentación es documentar internamente el sistema de (o lo más básico del TCB) hardware, firmware y software. El objetivo del diseño de documentación es que "la filosofía del fabricante sobre protección y... cómo esta filosofía es trasladada dentro del TCB". Una tarea clave que define los límites del sistema y distingue claramente entre cuales porciones del sistema son relevantemente seguras y cuales no.

  Las dos mayores metas del diseño de documentación son: probar al equipo de evaluación (que el sistema cumple con el criterio de evaluación) y auxiliar al equipo de diseño y desarrollo, para ayudar a definir las políticas del sistema de seguridad y hacer que las políticas se lleven a cabo durante la implementación.

A continuación describiremos cada uno de los Niveles de Seguridad del Libro Naranja con sus respectivas clases.

2.1.1 Nivel D (Protección Mínima)

Esta división contiene sólo una clase. Esta reservada para los sistemas que han sido evaluados, pero que no cumplen con los requisitos para una clase más alta de la evaluación. Es decir, si un sistema no cumple con ninguna categoría se clasifica como D, de ahí viene el nombre de mínima protección y por esa razón no se describen sus especificaciones.

2.1.2 Nivel C (Protección Discrecional)

Las clases en esta división proporcionan una protección discrecional (necesidad de identificación) y, a través de inclusión de capacidades de auditoría, exige la responsabilidad de los usuarios de las acciones que realiza.

La protección discrecional se aplica a una Base de Computadoras Confiables (TCB) con protección de objetos optativos (por ejemplo: archivo, directorio, dispositivos, etc.).

Clase C1: Protección de Seguridad Discrecional.

Las TCB de un sistema de la clase C1 deben cubrir los requisitos de seguridad discrecional proporcionando la separación de usuarios y de datos. Deben incorporar algún mecanismo de control y acreditación, así como la capacidad de hacer cumplir las restricciones de acceso de una base individual; es decir, garantizar de una forma convincente a los usuarios de que sus proyectos o información privada está protegida y evitar que otros usuarios accidentalmente puedan leer o destruir sus datos. Se supone que en el ambiente de la clase C1 existe cooperación entre los usuarios y además todos ellos procesan datos en el/los mismo(s) nivel(es) de sensitividad.

Los requisitos mínimos para los sistemas con asignación de la clase C1 son:

- Protección de archivos optativa, por ejemplo Control de Listas de Acceso (*Access Control Lists*, ACLs), Protección a Usuario/Grupo/Público.
- Protección de la contraseña y banco de datos seguro de autorizaciones (ADB).
- Protección del modo de operación del sistema.
- Verificación de Integridad del TCB.
- Documentación de Seguridad del Usuario.
- Documentación de Seguridad de la Administración de Sistemas.
- Documentación para Comprobación de la Seguridad.
- Diseño de documentación de TCB.
- Típicamente para usuarios en el mismo nivel de seguridad.

A continuación se muestran las características de esta clase, según el Libro Naranja (ver Tabla 2.1):

Clase C1

CATEGORÍA	DESCRIPCIÓN
Políticas de seguridad	
Control de acceso discrecional	La TCB deberá definirse y controlar el acceso entre usuarios registrados y objetos registrados (por ejemplo, archivos y programas), en el sistema de Procesamiento Automático de Datos(*Automatic Data Processing*, ADP). El mecanismo de ejecución (por ejemplo controles de usuario/grupo/público, control de listas de acceso) deberá permitir a los usuarios el especificar y controlar el compartir ciertos objetos a individuos registrados o grupos definidos o ambos.
Responsabilidad	
Identificación y autenticación	El TCB debe solicitar la identificación de los usuarios antes de empezar a ejecutar cualquier acción que el TCB deba de ejecutar. El TCB debe usar algún mecanismo de protección (passwords) para autenticar la identidad del usuario. El TCB debe proteger los datos de autenticación de manera que no puedan ser accedidos por usuarios no autorizados.

Confianza	
Arquitectura del sistema	EL TCB debe mantener un dominio para su propia ejecución que lo proteja de interferencia externa o falsificaciones (Ejemplo: para modificación de su código o estructura de datos). Los recursos controlados por el TCB pueden ser definidos en un subgrupo, así como los usuarios y objetos en el sistema ADP.
Integridad del sistema	Las características del hardware y/o el software deben ser proporcionadas para ser usadas y periódicamente validadas para su correcta operación, así como los elementos de hardware y firmware del TCB.
Pruebas de seguridad	Los mecanismos de seguridad del sistema ADP deberán ser probados y encontrados trabajando, y exigidos en la documentación del sistema. Las pruebas deberán ser hechas para asegurar que no hay caminos obvios para acceso de usuarios no autorizados o cualquier otra falla en el mecanismo de protección de la seguridad del TCB.
Documentación	
Guía del usuario sobre características de seguridad	Un resumen sencillo, capítulo o manual en la documentación del usuario, que describa los mecanismos de protección proporcionados por el TCB, lineamientos sobre su uso y cómo interactuar con otros.
Facilidades del manual de seguridad	Un direccionamiento manual por parte del administrador del sistema ADP, deberá presentar avisos sobre sus funciones y privilegios que deberá de controlar cuando ejecuta una instalación segura.
Pruebas de documentación	El desarrollador del sistema deberá proporcionar a los evaluadores un documento que describa el plan de pruebas, procedimientos de prueba que muestren como los mecanismos son probados, y los resultados de las pruebas funcionales de los mecanismos de seguridad.
Diseño de documentación	La documentación que proporcione una descripción de la filosofía del fabricante sobre protección deberá estar disponible, y una explicación de cómo esta filosofía es trasladada dentro.

Tabla 2.1. Características de la Clase C1 de acuerdo al Libro Naranja.

Clase C2: Protección de Acceso Controlado.

Este subnivel fue diseñado para solucionar las debilidades del C1. Cuenta con características adicionales que crean un ambiente de acceso controlado. Se debe llevar una auditoría de accesos e intentos fallidos de acceso a objetos. Tiene la capacidad de restringir aún más el que los usuarios ejecuten ciertos comandos o tengan acceso a ciertos archivos, permitir o denegar datos a usuarios en concreto, con base no sólo en los permisos, sino también en los niveles de autorización.

Requiere que se audite el sistema. Esta auditoría es utilizada para llevar registros de todas las acciones relacionadas con la seguridad, como las actividades efectuadas por el administrador del sistema y sus usuarios. La auditoría requiere de autenticación adicional para estar seguros de que la persona que ejecuta el comando es quien dice ser. Su mayor desventaja reside en los recursos adicionales requeridos por el procesador y el subsistema de discos.

Los datos de auditoría deben estar protegidos e incluir el uso de mecanismos de autenticación: operación con objetos, inicio de programas, borrado de objetos, acciones de

los operadores, administradores y para cada evento: fecha, hora, evento, usuario, estado del evento (*success* o *fail*), terminal, nombre del objeto, etc.
Los usuarios de un sistema C2 tienen la autorización para realizar algunas tareas de administración del sistema sin necesidad de la contraseña *root* (raíz). Permite llevar mejor las tareas relacionadas con la administración del sistema, ya que es cada usuario quien ejecuta el trabajo y no el administrador del sistema.

Los siguientes son requisitos mínimos para los sistemas con asignación de clase (C2):

- La protección de objetos puede estar con base al usuario, por ejemplo, de un ACL o una base de datos del administrador.
- La autorización para acceder sólo puede ser asignada por usuarios autorizados.
- Protección de reuso de objetos (por ejemplo, para evitar reasignación de permisos de seguridad de objetos borrados).
- Identificación obligatoria y procedimientos de autorización para los usuarios, por ejemplo, contraseñas.
- Auditoría de eventos de seguridad.
- Protección del modo de operación del sistema.
- Agrega protección para autorizaciones y auditoría de datos.
- Documentación de la información como C1 plus, al examinar la auditoría de la información.

A continuación se muestran las características de esta clase según el Libro Naranja (ver Tabla 2.2):

CLASE C2

CATEGORÍA Políticas de seguridad	DESCRIPCIÓN
Control de acceso discrecional	**Requerimientos adicionales.** Definición de grupos más específicamente. El mecanismo de ejecución debe proporcionar controles para limitar la propagación de permisos de acceso. El mecanismo de control de acceso discrecional deberá permitir, ya sea una acción de un usuario explícito o un default; proporciona que los objetos sean protegidos de accesos no autorizados. Este control de acceso debe ser capaz de incluir o excluir el acceso de usuarios. El permiso de acceso de un objeto para usuarios que ya no poseen el permiso de acceso, deberá ser asignado sólo por los usuarios autorizados.
Reutilización de Objetos	Todas las autorizaciones para la información contenida con un almacenamiento de objetos deberán ser revocadas previamente o con una asignación inicial, asignación o reasignación del tema desde el pool del TCB de los objetos no utilizados y almacenados. La información, incluyendo la representación encriptada de la información, producida por las acciones de un evento previo debe de estar disponible para cualquier evento que obtenga el acceso de un objeto que ha sido ya regresado al sistema.

Responsabilidad	
Identificación y autenticación	**Requerimientos adicionales.** El TCB debe ser capaz de reforzar las cuentas individuales al proporcionar la capacidad de identificación única a cada usuario individual ADP. El TCB debe también proporcionar la capacidad de asociar la identidad con toda acción audible elegida por esa persona.
Auditoría	El TCB debe ser capaz de crear, mantener y proteger de modificaciones, o acceso de usuarios no autorizados o destrucción de pistas de auditoría o accesos a objetos protegidos. La auditoría de datos debe ser protegida por el TCB de accesos de lectura o limitar a quien está autorizado para auditar los datos. El TCB debe ser capaz de registrar los siguientes tipos de eventos: Uso de mecanismos de identificación y autenticación, introducción de objetos en el espacio direccionable del usuario (apertura de archivos, inicialización de programas), eliminación de objetos, acciones tomadas por operadores de la computadora y administradores del sistema y/o administradores de la seguridad del sistema, y otros eventos relevantes del sistema. Para cada evento registrado, el registro de auditoría deberá identificar: fecha y hora del evento, y si el evento fue exitoso o falló. La identificación/autenticación de eventos que originan la petición (ID de la terminal) deberán ser incluidos en el registro de auditoría. El administrador de sistema ADP, debe ser capaz de seleccionar las acciones a auditar de uno o de varios usuarios basándose en la identidad individual.
Confianza	
Arquitectura del sistema	**Requerimientos adicionales.** El TCB debe aislar los recursos a ser protegidos de manera que los usuarios tengan control de acceso y requerimientos de auditoría.
Integridad del sistema	No se tienen requerimientos adicionales.
Pruebas de seguridad	**Requerimientos adicionales.** Las pruebas deberán también ser incluidas en la búsqueda de banderas obvias que puedan permitir una violación de recursos aislados, o que puedan permitir el acceso no autorizado de auditoría o autenticación de datos.
Documentación	
Guía del usuario sobre características de seguridad	No se tienen requerimientos adicionales.
Facilidades del manual de seguridad	**Requerimientos adicionales.** Los procedimientos para examinar y mantener los archivos de auditoría, así como las estructuras de los registros detallados de auditoría para cada tipo de evento auditable debe ser proporcionado.
Pruebas de documentación	No se tienen requerimientos adicionales.
Diseño de documentación	No se tienen requerimientos adicionales.

Tabla 2.2. Características de la Clase C2 de acuerdo al Libro Naranja.

2.1.3 Nivel B (Protección Obligatoria)

El Nivel B (Mandatory Protection, *Protección Obligatoria*) especifica que el sistema de protección del TCB debe ser obligatorio, no sólo discrecional.

La noción de un TCB que preserve la integridad de etiquetas de sensibilidad de la información y se utilice para hacer cumplir un conjunto de reglas obligatorias del control de acceso, es un requisito importante en esta división. Los sistemas en esta división deben llevar las etiquetas de sensibilidad en las estructuras de datos importantes del sistema. El desarrollador del sistema también debe proporcionar un modelo de política de seguridad en el cual se basa el TCB y equiparlo por medio de una serie de especificaciones. Evidentemente, debe ser proporcionada una demostración que sirva para aclarar el concepto del monitor de referencia y su forma de implementarlo.

Clase B1: Protección de Seguridad Etiquetada.

Los sistemas de la Clase B1 (Labeled Security Protection, *Protección de Seguridad Etiquetada*) requieren todas las características solicitadas para la Clase C2. Además, una declaración informal del modelo de la política de seguridad, de las etiquetas de los datos y del control de acceso obligatorio sobre los eventos y objetos nombrados debe estar presente. Debe existir la capacidad para etiquetar exactamente la información exportada. Cualquier defecto identificado al hacer las pruebas debe ser eliminado.

Los siguientes son los requisitos mínimos para los sistemas con asignación de grado de la Clase B1:

- Seguridad obligatoria y acceso por etiquetas a todos los objetos, por ejemplo: archivos, procesos, dispositivos, etc.
- Verificación de la Integridad de las etiquetas.
- Auditoría de objetos Etiquetados.
- Control de acceso obligatorio.
- Habilidad de especificar el nivel de seguridad impreso en salidas legibles al humano (por ejemplo: impresiones).

A continuación se muestran las características de esta clase, según el Libro Naranja (ver Tabla 2.3):

CLASE B1

CATEGORÍA Políticas de Seguridad	DESCRIPCIÓN
Control de acceso discrecional	No se tienen requerimientos adicionales.
Reutilización de Objetos	No se tienen requerimientos adicionales.
Etiquetas	Etiquetas sensitivas asociadas con cada evento y objeto almacenado bajo su control (por ejemplo: procesos, archivos, segmentos, dispositivos) deben ser mantenidos por el TCB. Estas etiquetas deberán ser utilizadas como las bases para las decisiones del control del acceso obligatorio. En orden de importancia de datos no etiquetados, el TCB debe solicitar y recibir de un usuario autorizado el nivel de seguridad de esos datos, y todas las acciones deberán ser auditadas por el TCB.

Integridad de Etiquetas	Las etiquetas sensitivas deberán representar con precisión los niveles de los eventos específicos u objetos con los que estos están asociados. Cuando son exportados por el TCB, las etiquetas sensitivas deberán precisar y representar sin ambigüedad las etiquetas internas y deberán estar asociadas con la información que esta siendo exportada.
Exportación de Información Etiquetada	El TCB deberá designar cada canal de comunicaciones y dispositivo de entrada/salida, ya sea como de un nivel sencillo o de multinivel. Cualquier cambio en esta designación deberá ser hecha manualmente y deberá ser auditable por el TCB. El TCB deberá mantener y ser capaz de auditar cualquier cambio en los niveles de seguridad o niveles asociados con un canal de comunicaciones o dispositivo de entrada/salida.
Exportación de Dispositivos Multinivel	Cuando el TCB exporta un objeto que es multinivel o un dispositivo de entrada / salida, la etiqueta sensitiva asociada con ese objeto también deberá ser exportada y permanecer residente en el mismo medio físico que la información exportada y deberá estar en la misma forma (por ejemplo, de forma legible a la máquina o en forma legible a la persona). Cuando el TCB exporta o importa un objeto sobre un canal de comunicación multinivel, el protocolo usado en ese canal deberá proporcionar una paridad que evite ambigüedad entre las etiquetas sensitivas y la información asociada que se está enviando o recibiendo.
Exportación de Dispositivos de Nivel Único	Los dispositivos de nivel único de canales de comunicaciones de entrada/salida no son requeridas para mantener las etiquetas sensibles de la información que procesan. De cualquier modo, el TCB debe incluir un mecanismo para que el TCB y un usuario autorizado fiable comunique y designe el nivel único de seguridad de la información importada o exportada vía canal de comunicaciones de nivel sencillo o dispositivo de entrada/salida.
Etiquetado de Salidas Legibles a la Persona	El administrador del sistema ADP debe ser capaz de especificar los nombres de las etiquetas imprimibles asociados con las etiquetas sensitivas exportables. El TCB debe marcar el inicio y el fin de todas las etiquetas sensitivas legibles a la persona que representen sensitivamente la salida. El TCB deberá, por omisión marcar el límite inferior y superior de cada página legible al hombre, compaginada de la salida impresa (por ejemplo, salidas de la impresora) con una etiqueta sensitiva legible al hombre que represente apropiadamente la sensitividad global de la salida o que represente apropiadamente la sensitividad de la información de cada página. Cualquier anulación de estas marcas por defecto deben ser auditables por el TCB.
Control de Acceso Obligatorio	El TCB debe reforzar las políticas del control de acceso obligatorio de todos los sujetos y objetos almacenados (procesos, archivos, dispositivos, etc.) A estos sujetos y objetos debe ser asignado una etiqueta sensitiva que sean una combinación de clasificación por nivel jerárquico y categorías no jerárquicas, y las etiquetas deberán ser usadas como la base de las decisiones para el control de acceso obligatorio El TCB debe ser capaz de soportar dos o más niveles de seguridad, los siguientes requerimientos deberán mantenerse para todos los accesos entre sujetos y objetos controlados por el TCB. Un sujeto puede leer un objeto solamente si la clasificación jerárquica del nivel de seguridad del sujeto, es menor o igual que la clasificación jerárquica de los niveles de seguridad del objeto y la categoría no jerárquica de los niveles de seguridad que se incluyen en todas las categorías no jerárquicas del nivel de seguridad del objeto. Un usuario puede escribir en un objeto solamente si la clasificación jerárquica del nivel de seguridad del sujeto es mayor o igual que la clasificación jerárquica de los niveles de seguridad del objeto y cumple con todas las categorías

	no jerárquicas de los niveles de seguridad que se incluyen en todas las categorías no jerárquicas del nivel de seguridad del objeto.
Responsabilidad	
Identificación y autenticación	**Requerimientos adicionales.** El TCB debe mantener los datos de autenticación que incluyen la información para verificar la identidad de los usuarios (password). Así como la información para detectar la autorización de usuarios individuales. Los datos deben ser usados por el TCB para autenticar la identidad de los usuarios y asegurar que el nivel de seguridad y la autorización de todos los usuarios externos al TCB puedan ser creados para actuar en nombre del usuario individual que se documenta por el pase y la autorización del tipo de usuario.
Auditoría	**Requerimientos adicionales.** El TCB también debe ser capaz de auditar cualquier sustitución de marcas de salida legibles al humano. Para eventos que introducen un objeto dentro del espacio direccionable del usuario y para borrar eventos de objetos, el registro de auditoría debe incluir el nombre de los objetos y el nivel de seguridad del objeto. El administrador de sistema ADP debe ser capaz de auditar selectivamente las acciones de algún o varios usuarios basándose en la identidad individual y/o nivel de seguridad de los objetos.
Confianza	
Arquitectura del Sistema	**Requerimientos adicionales.** El TCB debe mantener procesos aislados así como proporcionar distintas direcciones de espacio bajo su control.
Integridad del Sistema	No se tienen requerimientos adicionales.
Pruebas de Seguridad	**Requerimientos adicionales.** Los mecanismos de seguridad del sistema ADP deberán ser probados y encontrados trabajando con la documentación del sistema. Un equipo de individuos que entiendan completamente la implementación específica del TCB deberá diseñar documentación, código fuente y código objeto para el análisis completo y las pruebas. Estos objetivos deberán descubrir todo el diseño y la implementación de banderas que pudieran permitir a un sujeto externo al TCB el leer, cambiar o borrar datos normalmente denegados bajo políticas de seguridad discrecional u obligatorias reforzadas por el TCB, así como el asegurar que ningún sujeto (sin autorización para hacerlo) sea capaz de causar que el TCB entre en un estado tal que sea incapaz de responder a comunicaciones iniciadas por otros usuarios. Todas las banderas descubiertas deberán ser removidas o neutralizadas y el TCB vuelto a probar para demostrar que éstas han sido eliminadas y que nuevas banderas no han sido introducidas.
Diseño de Especificaciones y Configuración	Un modelo formal o informal de las políticas de seguridad soportadas por el TCB que deberá ser mantenido durante todo el ciclo de vida del sistema ADP y demostrar ser consistente con su axioma.
Documentación	
Guía del Usuario de Características de Seguridad	No se tienen requerimientos adicionales.
Facilidades del Manual de Seguridad	**Requerimientos adicionales.** El manual deberá describir las funciones del operador y del administrador relativas a la seguridad, al incluir los cambios de las características de seguridad para los usuarios.
Documentación de Pruebas	No se tienen requerimientos adicionales.

Diseño de Documentación	**Requerimientos adicionales.** Una descripción formal o informal del modelo de las políticas de seguridad reforzado por el TCB deberá estar disponible para dar una explicación de que es suficiente el reforzar las políticas de seguridad. El mecanismo de protección específica del TCB deberá ser identificable y una explicación que demuestre cómo éste mecanismo satisface el modelo.

Tabla 2.3. Características de la Clase B1 de acuerdo al Libro Naranja.

Clase B2: Protección Estructurada.

En los sistemas de Clase B2 (Estructured Protection, *Protección Estructurada*), los TCB deben estar basados en una documentación formal, clara y contar con un modelo de política de seguridad bien definido que requiera un control de acceso discrecional y obligatorio. Las imposiciones a los sistemas encontradas en la Clase B1 se deben extender a todos los eventos y objetos en sistemas ADP. Además, los canales secretos son direccionados. El TCB debe estar cuidadosamente estructurado en elementos de protección críticos y elementos de protección no críticos. La interfaz de TCB deberá estar bien definida; así como el diseño y la activación de la implementación del TCB le permiten ser sujeto de prueba y revisión más completa. Se consolidan los mecanismos de autenticación, el manejo de recursos seguros se proporciona en forma de ayuda para las funciones del administrador y del operador del sistema, y se imponen controles rigurosos de la administración de configuración. El sistema es relativamente resistente a la penetración.

Los siguientes son requisitos mínimos para los sistemas con asignación de grado de la Clase B2:

- Notificación de cambios del nivel de seguridad que afecten interactivamente a los usuarios.
- Etiquetas de dispositivos jerárquicas.
- Acceso obligatorio sobre todos los objetos y dispositivos.
- Rutas Confiables de comunicaciones entre usuario y sistema.
- Rastreo de los canales secretos de almacenamiento.
- Modo de operación del sistema más firme en multinivel en unidades independientes.
- Análisis de canales seguros.
- Comprobación de la seguridad mejorada.
- Modelos formales de TCB.
- Versión, actualización y análisis de parches y auditoría.

A continuación se muestran las características de esta clase, según el Libro Naranja (ver Tabla 2.4):

CLASE B2

CATEGORÍA	DESCRIPCIÓN
Políticas de Seguridad	
Control de acceso discrecional	No se tienen requerimientos adicionales.
Reutilización de Objetos	No se tienen requerimientos adicionales.
Etiquetas	**Requerimientos adicionales.** Las etiquetas sensitivas asociadas con cada recurso del sistema ADP (por ejemplo: eventos, objetos almacenados, ROM) que son directamente o indirectamente accedidos por eventos externos al TCB, debe ser mantenido por el TCB
Integridad de Etiquetas	No se tienen requerimientos adicionales.
Exportación de Información Etiquetada	No se tienen requerimientos adicionales.
Exportación de Dispositivos Multinivel	No se tienen requerimientos adicionales.
Exportación de Dispositivos de Nivel Unico	No se tienen requerimientos adicionales.
Etiquetado de Salidas Legibles a la Persona	No se tienen requerimientos adicionales.
Etiquetas Sensitivas de Eventos	El TCB debe notificar inmediatamente a la terminal del usuario de cada cambio en el nivel de seguridad asociado con ese usuario durante una sesión interactiva. La terminal de usuario debe de ser capaz de buscar el TCB cuando lo desee para desplegar un evento con etiqueta sensitiva.
Dispositivos Etiquetados	El TCB debe soportar la asignación de un nivel mínimo y máximo para todo dispositivo físico adjunto. Estos niveles de seguridad deben de ser usados por el TCB para reforzar las condiciones impuestas por el medio ambiente físico en cada uno de los dispositivos físicos localizados.
Control de Acceso Obligatorio	**Requerimientos adicionales.** El TCB debe reforzar las políticas del control de acceso obligatorio para todos los recursos (usuarios, objetos almacenados, dispositivos de entrada/salida) que sean accesibles directa o indirectamente por usuarios externos al TCB. Los requerimientos deberán mantenerse para todos los accesos entre todos los usuarios externos al TCB y todos los objetos accesibles directa o indirectamente por estos usuarios.
Responsabilidad	
Identificación y autenticación	No se tienen requerimientos adicionales.
Rutas Seguras	El TCB debe soportar una ruta segura de comunicaciones entre él y un usuario para su identificación y autenticación. La comunicación vía esta ruta, deberá ser iniciada exclusivamente por el usuario.
Auditoría	**Requerimientos adicionales.** El TCB debe ser capaz de auditar los eventos identificados que pueden ser usados en la explotación o cubierta de canales de almacenamiento.
Confianza	
	Nuevos Requerimientos. El TCB debe mantener un dominio para su propia ejecución de protecciones de interferencia externa o falsificaciones (por ejemplo, para modificación de su código o estructura de datos). El TCB debe mantener procesos aislados, así como proporcionar dirección de espacios distintos bajo su

Arquitectura del Sistema	control. El TCB debe estar estructurado internamente dentro de un módulo independiente bien definido. El módulo TCB debe ser diseñado bajo el principio de que los privilegios sean reforzados. Características de hardware, así como segmentación, debe ser usado para soportar lógicamente distinciones de objetos almacenados con atributos separados (nombrar, leer y escribir). La interfaz de usuario del TCB debe ser completamente definida y todos los elementos del TCB identificados.
Integridad del Sistema	No se tienen requerimientos adicionales.
Análisis de Canales Secretos	El sistema desarrollado deberá comportarse completamente, buscando la simulación de canales de almacenamiento y haciendo determinaciones (para las mediciones actuales o por estimaciones de ingeniería) o el máximo ancho de banda de cada canal identificado.
Facilidad de Administración de la Seguridad	El TCB debe soportar separadamente las funciones de administrador y operador.
Pruebas de Seguridad	**Requerimientos adicionales** El TCB deberá ser encontrado relativamente resistente a penetración Al probar todo deberá demostrarse que la implementación del TCB es consistente con la descripción de especificación de alto nivel.
Diseño de Especificaciones y Configuración	**Requerimientos adicionales.** Un modelo formal de la política de seguridad soportada por el TCB deberá ser mantenida durante todo el ciclo de vida del sistema ADP, que deberá proporcionar consistencia con su axioma. Especificación descriptiva de alto nivel (*Descriptive top-level specification*, DTLS) del TCB en términos de excepciones, mensajes de error y efectos. Este deberá demostrar ser una descripción exacta de la interfaz del TCB.
Administración de Configuración	Durante el desarrollo y mantenimiento del TCB, una administración de configuraciones deberá tomar lugar en el control de mantenimiento de los cambios en la especificación descriptiva de alto nivel y otros datos de diseño, documentación de implementación, código fuente, las versiones corridas del código objeto y las pruebas de correcciones y documentación. La administración de configuraciones del sistema deberá asegurar un mapeo consistente entre toda la documentación y el código asociado con las versiones actuales del TCB. Las herramientas deberán tenerse para generar una nueva versión del TCB desde el código fuente. También deberán estar disponibles las herramientas para hacer comparaciones de la nueva versión generada, con la versión previa del TCB en orden a determinar que sólo los cambios proyectados han sido hechos en el código que actualmente se está usando como la nueva versión del TCB.
Documentación	
Guía del Usuario de Características de Seguridad	No se tienen requerimientos adicionales.
Facilidades del Manual de Seguridad	**Requerimientos adicionales.** Los módulos del TCBN que contienen los mecanismos de validación de referencias deberán ser identificables. Los procedimientos para una operación segura de un nuevo TCB desde origen, después de modificarse por cualquier módulo en el TCB, deberá ser descrito.
Documentación de Pruebas	**Requerimientos adicionales.** Se deberá incluir los resultados de las pruebas de falta de efectividad de los métodos usados para reducir los anchos de banda de los canales secretos.
	Requerimientos adicionales. La interfaz entre los módulos del TCB deberán ser descritos. El modelo de políticas de seguridad deberá ser

Diseño de Documentación	formal y probado. La especificación descriptiva de alto nivel (DTLS) deberá ser mostrada en una descripción exacta de la interfaz del TCB. La documentación describirá como el TCB implementa el concepto de monitor de referencia y dar una explicación de porque es resistente a penetración, y no puede ser traspasado, y es correctamente implementado. La documentación deberá describir como el TCB se estructura para pruebas de instalación y reforzar los menores privilegios. Esta documentación deberá tambien presentar los resultados del análisis de los canales secretos y los intercambios involucrados al restringir los canales. Todos los eventos auditables que pueden ser usados en la explotación de conocer canales de almacenaje secretos, deberán ser identificados.

Tabla 2.4. Características de la Clase B2 de acuerdo al Libro Naranja.

Clase B3: Dominios de Seguridad.

En la Clase B3 (Security Domains, *Dominios de Seguridad*) los TCB deben satisfacer los requisitos de herramientas de monitoreo como un "monitor de referencia" que interviene en todos los accesos de usuarios a los objetos, a fin de ser comprobada, y que sea lo bastante pequeña para ser sujeta al análisis y pruebas. Al final, el TCB debe estar estructurado para excluir el código no esencial para aplicar la política de seguridad, mediante ingeniería de sistemas durante el diseño y la implementación del TCB, orientada hacia la reducción de su complejidad al mínimo.

Debe de contar también con un Administrador de Seguridad. Los mecanismos de auditoría se amplían para señalar acontecimientos relevantes de la seguridad, y se necesitan procedimientos de recuperación del sistema. El sistema es altamente resistente a la penetración.

Los siguientes son requisitos mínimos para los sistemas con asignación de un grado de Clase B3:

- ACL's adicionales basado en grupos e identificadores.
- Rutas de acceso confiables y autenticación.
- Análisis automático de la seguridad.
- Modelos más formales de TCB.
- Auditoría de eventos de seguridad.
- Recuperación confiable después de baja del sistema y documentación relevante.
- Cero defectos del diseño del TCB, y mínima ejecución de errores.

A continuación se muestran las características de esta clase, según el Libro Naranja (ver Tabla 2.5):

CLASE B3

CATEGORÍA	DESCRIPCIÓN
Políticas de Seguridad	
Control de acceso discrecional	**Requerimientos adicionales.** El mecanismo de ejecución debe de ser accedido mediante listas de control. El control de acceso debe ser capaz de especificar a cada objeto registrado, una lista de nombres de personas con sus respectivos modos de acceso a ese objeto. Además, para cada uno de los objetos registrados, de ser posible especificar una lista de los individuos registrados y una lista de los grupos o personas registradas con acceso denegado del grupo.
Reutilización de Objetos	No se tienen requerimientos adicionales.
Etiquetas	No se tienen requerimientos adicionales.
Integridad de Etiquetas	No se tienen requerimientos adicionales.
Exportación de Información Etiquetada	No se tienen requerimientos adicionales.
Exportación de Dispositivos Multinivel	No se tienen requerimientos adicionales.
Exportación de Dispositivos de Nivel Único	No se tienen requerimientos adicionales.
Etiquetado de Salidas Legibles a la Persona	No se tienen requerimientos adicionales.
Etiquetas Sensitivas de Eventos	No se tienen requerimientos adicionales.
Dispositivos Etiquetados	No se tienen requerimientos adicionales.
Control de Acceso Obligatorio	No se tienen requerimientos adicionales.
Responsabilidad	
Identificación y autenticación	No se tienen requerimientos adicionales.
Rutas Seguras	**Requerimientos adicionales.** El TCB debe soportar una ruta segura de comunicaciones entre él y los usuarios, para usarse cuando una conexión TCB a usuario es requerida (login, cambiar algún nivel de seguridad). Las comunicaciones vía ruta segura deben ser activadas exclusivamente por el usuario o el TCB y deben ser aisladas y libres de errores, así como distinguibles de otras conexiones.
Auditoría	**Requerimientos adicionales.** El TCB debe contar con un mecanismo, con la capacidad de monitorear las ocurrencias o acumulación de eventos de seguridad auditable que pueden indicar de una inminente violación a las políticas de seguridad. Este mecanismo deberá de ser capaz de notificar inmediatamente al administrador de seguridad cuando se excede el umbral, y si la acumulación de ocurrencias de eventos relevantes de seguridad continua, el sistema deberá tomar la última acción disolvente que termine con este evento.
Confianza	
Arquitectura del Sistema	**Requerimientos adicionales.** El TCB debe diseñar y estructurar el uso completo de un mecanismo de protección, conceptualmente simple con definición semántica precisa. Este mecanismo debe jugar un papel central en el reforzamiento de la estructura interna entre el TCB y el sistema. El TCB debe incorporar el uso significativo de capas, abstracción y ocultamiento de datos. Una aplicación de ingeniería de sistemas significativa debe ser directamente conducida minimizando la complejidad del TCB y excluyendo de los módulos del TCB los objetos que no presentan protección crítica.
Integridad del Sistema	No se tienen requerimientos adicionales.

Análisis de Canales Secretos	**Requerimientos adicionales.** Búsqueda de todos los canales simulados (almacenamiento y temporización).
Facilidad de Administración de la Seguridad	**Requerimientos adicionales.** Las funciones ejecutadas en el papel del administrador de seguridad deben ser identificadas. El Personal de Administración del sistema ADP, deberá ser capaz sólo de ejecutar funciones de administrador de seguridad después de tomar una acción auditable distinguible al asumir el papel de administrador de la seguridad en el sistema ADP. Las funciones que no son de seguridad que pueden ser ejecutadas por el papel de administrador de seguridad deberán limitarse estrictamente a lo más esencial para ejecutar la seguridad efectivamente.
Recuperación Confiable	Los procedimientos y/o mecanismos deberán ser proporcionados para asegurar que después de una falla del sistema ADP u otra discontinuidad, el sistema se recupere sin obtener un compromiso de protección.
Pruebas de Seguridad	**Requerimientos adicionales.** El TCB deberá ser encontrado resistente a penetraciones. Ninguna bandera de diseño y ninguna bandera de implementación sin correcciones, debe ser encontrada durante las pruebas y deberán ser razonablemente confidenciales las pocas que queden.
Diseño de Especificaciones y Configuración	**Requerimientos adicionales.** Un argumento convincente deberá ser proporcionado de que el DTLS es consistente con el modelo.
Administración de Configuración	No se tienen requerimientos adicionales.
Documentación	
Guía del Usuario de Características de Seguridad	No se tienen requerimientos adicionales.
Facilidades del Manual de Seguridad	**Requerimientos adicionales.** Se deberán incluir los procedimientos para asegurar que el sistema es inicialmente arrancado de un modo seguro. Los procedimientos deberán también estar incluidos en el compendio de operación del sistema de seguridad después de cualquier lapso de operación del sistema.
Documentación de Pruebas	No se tienen requerimientos adicionales.
Diseño de Documentación	**Requerimientos adicionales.** La implementación del TCB (hardware, firmware y software) deberá ser informalmente mostrada y ser consistente con el DTLS. Los elementos del DTLS deberán ser mostrados, usando técnicas.

Tabla 2.5. Características de la Clase B3 de acuerdo al Libro Naranja.

2.1.4 Nivel A (Protección Verificada)

Esta división se caracteriza por el uso de métodos formales para la verificación y por garantizar los controles de seguridad empleados en el sistema, que pueden proteger con eficacia la información clasificada, crítica o importante. Se requiere de una documentación amplia para demostrar que el sistema cumple con los requisitos de seguridad. Como en los niveles anteriores se debe cumplir con los requisitos del nivel anterior, en este caso nivel B3, más algunos adicionales.

Clase A1: Diseño Verificado.

La primera clase de este nivel es el A1 y se distingue de los demás sistemas por el análisis derivado de técnicas formales de especificación y verificación del diseño. Hay 5 criterios importantes para la verificación del diseño de la clase:

- Debe tener un modelo formal de la política de seguridad que esté identificado y documentado, en donde se incluya una prueba matemática de que el modelo es constante con sus axiomas y es suficiente para soportar la política de seguridad.

- Contar con una Especificación Formal de Alto Nivel (*Formal Top-Level Specification*, FTLS) del diseño, que incluya las definiciones abstractas de las funciones que el TCB realiza y de los mecanismos de la dotación física y/o de los firmware que se utilizan para usar dominios separados de ejecución.

- Se debe demostrar que el FTLS del TCB es constante y consistente con el modelo, por técnicas formales en lo posible (es decir, donde existen las herramientas de verificación) y las informales en otro caso.

- La implementación del FTLS debe mostrar informalmente que es consistente con el TCB, y expresar un mecanismo unificado de protección necesario para cumplir con la política de seguridad.

- Deben utilizarse técnicas de análisis formal para identificar y analizar los canales secretos, y se debe de justificar la continua existencia de canales secretos en el sistema.

A continuación se muestran las características de esta clase, según el Libro Naranja (ver Tabla 2.6):

Clase A1

CATEGORÍA	DESCRIPCIÓN
Políticas de Seguridad	
Control de acceso discrecional	No se tienen requerimientos adicionales.
Reutilización de Objetos	No se tienen requerimientos adicionales.
Etiquetas	No se tienen requerimientos adicionales.
Integridad de Etiquetas	No se tienen requerimientos adicionales.
Exportación de Información Etiquetada	No se tienen requerimientos adicionales.
Exportación de Dispositivos Multinivel	No se tienen requerimientos adicionales.
Exportación de Dispositivos de Nivel Único	No se tienen requerimientos adicionales.
Etiquetado de Salidas Legibles a la Persona	No se tienen requerimientos adicionales.
Etiquetas Sensitivas de Eventos	No se tienen requerimientos adicionales.
Dispositivos Etiquetados	No se tienen requerimientos adicionales.
Control de Acceso Obligatorio	No se tienen requerimientos adicionales.

Responsabilidad	
Identificación y autenticación	No se tienen requerimientos adicionales.
Rutas seguras	No se tienen requerimientos adicionales.
Auditoría	No se tienen requerimientos adicionales.
Confianza	
Arquitectura del Sistema	No se tienen requerimientos adicionales.
Integridad del Sistema	No se tienen requerimientos adicionales.
Pruebas de Seguridad	Las pruebas deberán demostrar que la implementación del TCB es consistente con la especificación formal de alto nivel. El manual u otros mapas del FTLS del código fuente pueden formar bases para las pruebas de penetración.
Diseño de Especificaciones y Verificación	Una especificación formal de alto nivel (FTLS) del TCB que deberá ser mantenido y descrito en término de excepciones, mensajes de error, componentes y efectos. Una combinación de pruebas formales e informales se deberá usar para mostrar que el FTLS es consistente con el modelo.
Análisis de Canales Secretos	Métodos formales deben ser usados en el análisis.
Facilidad de Administración de la Seguridad	No se tienen requerimientos adicionales.
Administración de Configuración	Durante el ciclo completo de vida durante el diseño, desarrollo, y mantenimiento del TCB, se deberá mantener un control formal de los cambios al sistema (hardware, software y firmware).
Recuperación Confiable	No se tienen requerimientos adicionales.
Distribución Confiable	Un sistema de control ADP confiable y facilidad de distribución deberá ser proporcionado, para mantener la integridad del mapeo entre los datos maestros que describen la versión actual del TCB y su copia en la versión actual. Se deberá hacer una prueba de la seguridad, en donde se pueda asegurar que el hardware, software y firmware distribuido se comporte exactamente como se especifica en las copias principales.
Documentación	
Guía del usuario sobre características de seguridad	No se tienen requerimientos adicionales.
Facilidades del Manual de Seguridad	No se tienen requerimientos adicionales.
Documentación de las Pruebas	Los resultados del mapeo entre las especificaciones formales de alto nivel y el código fuente del TCB deberán ser proporcionados.
Diseño de Documentación	La implementación del TCB debe mostrar informalmente que es consistente con el FTLS. Los elementos del FTLS deberán ser mostrados, usando técnicas de información, con su correspondiente elemento del TCB. Los mecanismos de hardware, firmware y software no compartidos con el FTLS pero estrictamente internos del TCB deberán ser claramente descritos.

Tabla 2.6. Características de la Clase A1 de acuerdo al Libro Naranja.

Ejemplos de Sistemas.

En la Tabla 2.7 se resumen los niveles de seguridad establecidos en el Libro Naranja, las clases que los integran, el nombre que recibe cada una de estas clases, así como ejemplos de algunos de los sistemas que han logrado ese grado.

NIVEL	CLASE	NOMBRE	EJEMPLO
D		Protección Mínima	
	D		Sistemas operativos básicos: MS-DOS
C		Protección Discrecional	
	C1	Protección de Seguridad Discrecional	IBM MVS/RACF Cualquier versión de UNIX ordinaria, que no ha sido enviada a una evaluación formal.
	C2	Protección de Acceso Controlado	Computer Asociates International: ACF/2/MVS Digital Equipment Corporation: VAX/VMS 4.3 HP MPE V/E
B		Protección Obligatoria	
	B1	Protección de seguridad por etiquetas	AT&T System V/MLS UNISIS OS 100 SecuryWare: CMW+ IBM MVS/ESA
	B2	Protección Estructurada	Honeywell Information System: Multics Trusted Information System XENIX
	B3	Protección por Dominios	Honeywell Federal System XTS-200
A		Protección Verificada	
	A1	Diseño verificado	Honeywell Information System SCOMP Boening Aerospace:SNS

Tabla 2.7. Ejemplos de los Niveles de Seguridad.

La Tabla 2.8 compara las clases de evaluación del Libro Naranja, mostrando las características requeridas para cada clase.

CATEGORÍAS	CLASES					
Políticas de Seguridad	C1	C2	B1	B2	B3	A1
Control de Acceso Discrecional						
Reutilización de Objetos						
Etiquetas						
Integridad de Etiquetas						
Exportación de Información Etiquetada						
Exportación de Dispositivos Multinivel						
Exportación de Dispositivos de Nivel Único						
Etiquetados de Salidas Legibles a la Persona						
Etiquetas Sensitivas de Eventos						
Dispositivos Etiquetados						
Control de Acceso Obligatorio						
Responsabilidad	C1	C2	B1	B2	B3	A1
Identificación y Autenticación						
Rutas Seguras						
Auditoría						
Confianza	C1	C2	B1	B2	B3	A1
Arquitectura del Sistema						
Integridad del Sistema						
Pruebas de Seguridad						
Diseño de Especificaciones y Verificación						
Análisis de Canales Secretos						
Facilidad de Administración de la Seguridad						
Administración de Configuración						
Recuperación Confiable						
Distribución Confiable						
Documentación	C1	C2	B1	B2	B3	A1
Guía del Usuario de Características de Seguridad						
Facilidades del Manual de Seguridad						
Documentación de Pruebas						
Diseño de Documentación						

Tabla 2.8. Características principales de las Clases de Seguridad del Libro Naranja.

Significado de las claves:

- No se requiere.
- Nuevo requerimiento para esta clase.
- Requerimiento mejorado para esta clase.
- No se tienen requerimientos adicionales para esta clase.

2.2 Criterios Comunes

El **TCSEC** (*Trusted Computer Security Evaluation Criteria or Orange Book* creado a mediados de los 80's) proveía niveles que requerían una funcionalidad de seguridad específica que era conveniente para un entorno específico. El **ITSEC** (*Information Technology Security Evaluation Criteria* por los gobiernos de Francia, Alemania, los Países Bajos y el Reino Unido), a principios de los 90's, proveía niveles de seguridad donde la funcionalidad del producto desarrollado se definía. Al final ambos probaron que no eran satisfactorios y las iniciativas se combinaron para producir un nuevo esquema. El nuevo esquema de evaluación de seguridad que reemplaza al TCSEC y al ITSEC, a finales de 1998, es llamado "Criterios Comunes para Evaluación de Seguridad de Tecnología de la Información" (*Common Criteria for Information Technology Security* - **CCITSE**) mejor conocido como **CC.**

El nuevo esquema fue originado con proyectos cooperativos que estaban relacionados con la Organización Internacional de Estándares (ISO). La versión 2.0 de CC tenía el mismo contenido que la Redacción Final del Comité (FCD) 15408, la cual fue llevada a votación por parte de la ISO en el verano de 1998.

CCITSE versión 2.1, aprobada en agosto de 1999, fue adoptada por (ISO) como "Tecnología de información – Técnicas de seguridad – Criterios de evaluación para la seguridad de IT" (ISO/IEC 15408) en diciembre de 1999.

En Octubre de 1998, Canadá, Francia, Alemania, el Reino Unido y los Estados Unidos firmaron un acuerdo de reconocimiento mutuo (MRA) de las evaluaciones basadas en los Criterios Comunes (CC). En mayo del 2000 un nuevo acuerdo de reconocimiento mutuo fue firmado, aquí se incluyó a Australia, Nueva Zelanda, Finlandia, Grecia, Italia, Holanda, Noruega y España. Este acuerdo es un paso adelante significativo para el gobierno y la industria en el área de los productos de Tecnología de la Información (IT) y los perfiles de protección de las evaluaciones de seguridad. El reconocimiento mutuo que este acuerdo provee significa que un certificado CC obtenido en un país es reconocido por los demás países firmantes.

La información contenida por los productos o sistemas IT es un recurso crítico que permite a las organizaciones tener éxito en su misión. El término *seguridad IT* es usado para prevenir y mitigar los riesgos de la seguridad, que es una de las principales preocupaciones de las organizaciones que tienen éxito.

Los CC son una norma internacional para evaluar la seguridad de los productos de tecnología de la información (IT) basados en los criterios europeos, norteamericanos y canadienses existentes para la evaluación de la seguridad de la IT, por ello, los resultados obtenidos al realizar una evaluación – la evaluación la realiza una autoridad específica del país – siguiendo los CC, son reconocidos internacionalmente. Además tienen como objetivos principales proporcionar protección a la información, como por ejemplo: no revelar secretos sin autorización, perder información por el uso y modificar la información.

Los CC pueden ser usados para seleccionar las medidas de seguridad IT apropiadas y que contengan criterios para la evaluación de los requerimientos de seguridad.

En la evaluación de las propiedades de seguridad de los productos, existen tres grupos que tienen interés general en la misma:

- **Consumidores TOE.-** Los CC dan a los *consumidores* - especialmente a grupos de consumidores y comunidades de interés - una ampliación independiente de la estructura condicionada al Perfil de Protección (PP) en la cual se expresan estos requerimientos especiales para las medidas de seguridad IT en una TOE (*Target of Evaluation*, Objetivo de la Evaluación).

- **Desarrolladores TOE.-** Los CC pretender apoyar a los *desarrolladores* en la preparación de sus productos o sistemas y brindar asistencia en la evaluación de sus productos o sistemas, así como en la identificación de los requerimientos de seguridad para que sean satisfechos por cada uno de sus productos o sistemas. Los CC pueden entonces ser usados para demandar que las TOE conformen sus requerimientos identificados por medio de funciones de seguridad especificadas y garantizando que serán evaluadas. Cada requisito de las TOE está contenido en una implementación dependiente de lo que está construido en las Metas de Seguridad (ST). Uno o más Perfiles de Protección (PP) pueden proporcionar los requerimientos de una amplia base de consumidores.

- **Evaluadores TOE.-** Los CC contienen criterios para ser usados por los evaluadores, cuando juzguen la conformación de los requerimientos de seguridad de las TOE. Los CC describen el conjunto de acciones generales que los evaluadores deben llevar a cabo y las funciones de seguridad sobre las cuales se ejecutarán estas acciones. Los CC no especifican los procedimientos a seguirse durante el desarrollo de estas acciones.

Uno de los elementos más importantes de los CC es el contexto de evaluación. En este sentido, para permitir llevar a cabo una comparación completa entre los resultados de evaluación, las evaluaciones podrían ser llevadas a cabo dentro de un marco de trabajo de un esquema de evaluación autoritario, debiendo estar conformado por los conjuntos de estándares, la calidad de los monitores de las evaluaciones y los evaluadores mismos.

La figura 2.1 representa los elementos más importantes que forman el contexto para las evaluaciones:

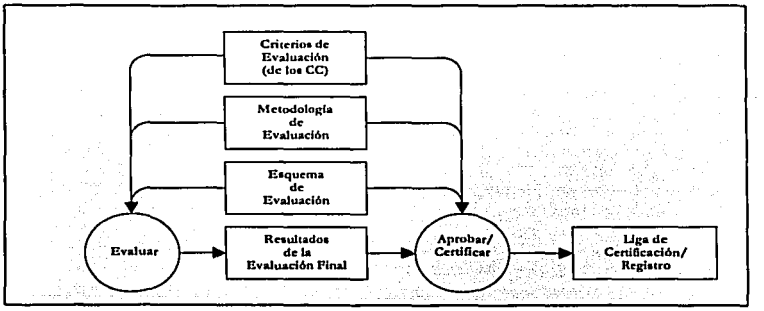


Figura 2.1. Contexto de Evaluación.

El esquema de evaluación, la metodología, y el proceso de certificación son responsabilidad de las autoridades de evaluación que administran esquemas de evaluación y están fuera del ámbito de los CC.

Bajo los CC, las clases de productos son evaluadas basándose en los puntos de los Perfiles de Protección (PP) que especifican los requerimientos funcionales de seguridad. Los PP deben ser desarrollados para aplicarse en los sistemas operativos, firewalls, tarjetas inteligentes y otros productos que se espera cuenten con requerimientos de seguridad. Los CC especifican una serie de evaluación de niveles de confianza (*Evaluation Assurance Levels* - EAL) para los productos evaluados. Un nivel alto de EAL especifica un nivel alto de confianza de que las funciones de seguridad del producto serán ejecutadas de manera correcta y efectiva. Para los consumidores y los desarrolladores de productos IT, los CC proveen un conjunto de criterios y están diseñados de tal manera que los aspectos de seguridad del producto IT pueden ser medidos de manera respetable, reproducible e independiente con la libertad de resultados favorables.

En una evaluación de CC un producto IT es evaluado contra un conjunto aprobado de criterios de evaluación de seguridad de la información. El conjunto de evaluación de seguridad de los CC puede estar acostumbrado a evaluar todo tipo de productos IT. Generalmente esto significa que para un producto IT específico, en una evaluación de CC, los siguientes aspectos se revisan:

- Si los requerimientos del producto son definidos correctamente.
- Si los requerimientos son implementados correctamente.
- Si el proceso de desarrollo y documentación del producto cumple con ciertos requerimientos.

Debido a que los CC son un medio para definir los recursos y la medida de los aspectos de la seguridad de los productos IT, proveen:

Un conjunto de criterios para las facilidades de prueba (llamadas facilidades de evaluación) para asegurar que dichas facilidades pueden ejecutar una prueba de seguridad bajo un sistema de calidad clara y definida.

Un marco para la especificación de funcionalidad que:

- Permite a los consumidores claramente especificar el problema de su seguridad.
- Permite a los desarrolladores claramente especificar su solución de seguridad.
- Permite a los consumidores comparar varias soluciones de seguridad para su problema.
- Permite a los evaluadores determinar sin equivocaciones qué es lo que un producto hace.

Un marco para la prueba de especificación que:

- Permite a los consumidores definir qué tan seguros están de querer saber si su producto es seguro.
- Permite a los desarrolladores saber anticipadamente qué entregas necesitan proveer y cuál debe ser el contenido de estas entregas.

- Permite a los evaluadores cumplir con las pruebas de una manera muy bien definida.

Organización de los Criterios Comunes

Los CC son presentados como un conjunto de diferentes partes pero relacionadas entre sí como se presenta a continuación:

1. **Parte 1. Introducción y modelo general.**- Es la introducción a los CC. Se definen los conceptos generales y los principios de la evaluación de seguridad IT y se presenta un modelo general de evaluación. La parte 1 además tiene la finalidad de expresar los objetivos de seguridad, para la selección y definición de los requerimientos de seguridad IT, y para escribir especificaciones de alto nivel para productos y sistemas. Adicionalmente, la utilidad de cada parte de los CC está descrita en términos de cada una de las metas del público en general.

2. **Parte 2. Requerimientos funcionales de seguridad.**- Establece un conjunto de componentes funcionales como una vía estándar de expresión de los requerimientos funcionales para las TOEs. La parte 2 cataloga un conjunto de componentes funcionales, familias, y clases.

3. **Parte 3. Requerimientos de garantía de seguridad.**- Establece un conjunto de componentes de garantía como una vía estándar de expresión de los requerimientos de garantía para las TOEs. La parte 3 cataloga el conjunto de componentes de garantía, familias y clases. La parte 3 define además los criterios de evaluación para los PPs y las STs, y presenta niveles de garantía de evaluación que definen la escala de CC predefinidos para garantizar la valoración para las TOEs, la cual es llamada Niveles de Garantía de Evaluación (EAL).

La siguiente tabla presenta, para las tres agrupaciones de público las metas clave, como las partes de los CC que serán de interés.

	Consumidores	Desarrolladores	Evaluadores
Parte 1	Se utiliza para conocer antecedentes y propósitos de referencia. Estructura guía para PPs.	Se utiliza para conocer antecedentes y como referencia para el desarrollo de requerimientos y formulación de especificaciones de seguridad para TOEs.	Se utiliza para conocer antecedentes y propósitos de referencia. Estructura guía para PPs y STs.
Parte 2	Se utiliza como guía y como referencia cuando es necesaria la formulación de informes de requerimientos para funciones de seguridad.	Se utiliza como referencia donde es necesaria la interpretación de informes de requerimientos funcionales y la formulación de especificaciones funcionales para TOEs.	Se utiliza como informe obligatorio de criterio de evaluación donde es necesaria se determina si una TOE efectivamente reúne las funciones de seguridad exigidas.
Parte 3	Se utiliza como guía cuando es necesaria la determinación de los niveles requeridos de garantía.	Se utiliza como referencia donde es necesaria la interpretación de informes de requerimientos de seguridad y la determinación de aproximaciones de garantía de las TOEs.	Se utiliza como informe obligatorio de criterio de evaluación donde se determina la garantía de las TOEs y donde se lleva a cabo la evaluación de PPs y STs.

Tabla 2.9 Mapa para los Criterios Comunes.

Perfiles de Protección y Metas de Seguridad.

Los Perfiles de Protección y Metas de Seguridad, conocidos como PP y ST, son elementos muy esenciales del armazón de los CC. Cuando se terminaron los documentos ST/PP eran muy similares. Sin embargo, sirven a diferentes roles en el proceso de evaluación:

- Un Perfil de Protección es un requerimiento que define un problema de seguridad general de un consumidor o grupo de consumidores. Básicamente un Perfil de Protección establece: esto es lo que se necesita.

- Una Meta de Seguridad es una especificación que define una solución general de un desarrollador para un problema de seguridad. Básicamente una Meta de Seguridad establece: Esto es lo que se ha construido o se construirá en el futuro.

En el mundo ideal, un consumidor escribe un Perfil de Protección reflejando su problema de seguridad y lo envía al mundo. Uno o más desarrolladores producen Metas de Seguridad reflejando su solución al problema y lo envían al consumidor. Basado en esto, el consumidor selecciona una de ellas y compra el sistema de ese desarrollador.

Beneficios

Los CC ofrecen varias ventajas tanto a los usuarios como a los desarrolladores de productos IT.

a) **Para los usuarios:** los CC proveen medios para comparar productos de varios desarrolladores – a través de la llamada Meta de Seguridad. Además, un esquema es provisto por usuarios que pueden especificar sus necesidades de seguridad de tal forma que los desarrolladores pueden entender de manera clara y sin ambigüedades – por medio de una lista de verificación de los requerimientos de seguridad resultantes en un perfil de protección. Al utilizar productos evaluados, un usuario incrementa su confiabilidad en la funcionalidad de seguridad de sus productos, porque una opinión experta independiente es dada sobre el producto de acuerdo a un conjunto de criterios internacionales y reconocidos.

b) **Para los desarrolladores:** los CC proveen medios para mostrar al mundo que se tiene un producto adecuado y seguro – ventajas competitivas del producto. Los CC proveen una guía de la información requerida exactamente, interpretación de requerimientos de seguridad y un armazón que especifica qué es lo que el producto provee en términos de seguridad. La opinión independiente y experta del producto es dada sobre un criterio público predefinido que indica lo bien organizados que están tanto el producto como el diseño.

Identificación de los factores de riesgo

Los siguientes párrafos explican los factores que deben ser tomados en cuenta. Para cada factor, los diferentes niveles de riesgo están definidos, por lo que la diferencia entre dos niveles adyacentes en cada factor representan un incremento (o decremento) comparable aproximado en riesgo. Los factores están definidos así que son de manera general independientes – un cambio en un factor no implica un cambio en otro factor. Estas propiedades permiten numerar los niveles de riesgo y combinarlos en la mayoría de los casos utilizando una suma.

Algunas veces el riesgo no puede ser cuantificado de manera precisa por ser abstracto. El esquema descrito posteriormente captura la intuición y experiencia de los practicantes de la seguridad de cómputo y es preferible simplemente establecer estas consideraciones aparte debido a que no están hechas de manera precisa.

a) **Capacidad de procesamiento local:** algunos sistemas tiene terminales sólo de recepción; los usuarios de estas terminales no tienen manera de entrar directamente a los comandos del sistema. Estas terminales representan un nivel de riesgo más bajo que las terminales que permiten la emisión y recepción de información. Al reemplazar una terminal interactiva con una función determinada por una terminal programable, una PC u otro dispositivo programable, introduciría un nivel muy alto de riesgo ya que el usuario puede programar su terminal para introducir los comandos por él. Un usuario que tiene acceso a un sistema de terminal de función determinada pero por la vía de una computadora anfitrión programable se considera que tiene la misma capacidad de procesamiento local que uno que utilizara una computadora personal como terminal. Los niveles de riesgo identificados para la capacidad de procesamiento local son:

   - Nivel 1: terminal de sólo recepción.
   - Nivel 2: terminal interactiva de función determinada.
   - Nivel 3: dispositivo programable (Acceso vía computadora personal o anfitrión programable).

b) **Ruta de comunicación:** la ruta de comunicación entre una terminal y el anfitrión puede afectar el riesgo del sistema. Una terminal que tiene una liga simple de recepción hacia su anfitrión vía red abastecedora y retransmisora posee menor riesgo que otra que se encuentra conectada vía liga dúplex abastecedora y retransmisora, ya que la ruta simple previene a los usuarios de las peticiones presentadas al sistema. Las terminales que están conectadas al anfitrión ya sea de forma directa, red de transporte largo de paquetes o a través de una LAN ofrecen un decremento en las posibilidades de penetración y mal uso sobre aquéllas que se encuentran conectadas sólo a través de una red abastecedora y retransmisora debido al incremento del ancho de banda y a la interacción más cercana anfitrión-terminal que permiten. Los niveles de riesgo identificados para la ruta de comunicación son:

   - Nivel 1: abastecimiento/retransmisión, sólo receptor.
   - Nivel 2: abastecimiento/retransmisión, emisor/receptor.
   - Nivel 3: interactiva, vía conexión directa, LAN, red de transporte largo de paquetes

c) **Capacidad del usuario:** a pesar del procesamiento local disponible a un usuario o la ruta de comunicación por la cual él tiene acceso a un anfitrión, si este anfitrión está programado sólo para proveer salidas predefinidas a pesar de las entradas que el usuario presenta, es menos arriesgado que un sistema que responda a las transacciones del usuario. El sistema que genera la cinta del indicador automático para una bolsa de acciones es menor en riesgo a las terminales que despliegan la

cinta, como un sistema interactivo electrónico de banco es a una máquina automatizada de cobro. Finalmente un sistema basado en la transacción es menos riesgoso para sus usuarios que un sistema que permita a sus usuarios capacidades de una completa programación. Los niveles de riesgo identificados para la capacidad del usuario son:

- Nivel 1: sólo salidas.
- Nivel 2: procesamiento de transacción.
- Nivel 3: programación completa.

d) **Entorno de desarrollo y mantenimiento:** un sistema que ha sido desarrollado y es mantenido por individuos bajo un control de configuración cerrada (entorno cerrado) debería plantear un riesgo menor que uno que no es desarrollado y mantenido de esta manera (entorno abierto). Esta distinción ha sido propuesta en la teoría del plan de aplicación. Parece razonable, pero algunos ejemplos de sistemas desarrollados y mantenidos de acuerdo a la definición propuesta como "entorno cerrado" han sido identificados fuera de la comunidad inteligente. Por simplicidad se asume que los sistemas son desarrollados y mantenidos en un entorno abierto.

e) **Exposición de datos:** Un sistema que tiene una gran disparidad entre el permiso del usuario de menor rango y la clasificación de los datos, presenta un proceso que se encuentra en más riesgo que otro que tenga una disparidad menor, de manera que la teoría del plan de aplicación propone un esquema para numerar y clasificar el rango de riesgo, al cual se le llama exposición de datos para distinguirlo de otros factores de riesgo. Los niveles de permisos se definen como:

- Nivel 0: no aclarados.
- Nivel 1: no aclarados, pero acceso autorizado a información delicada no clasificada.
- Nivel 2: permiso confidencial.
- Nivel 3: permiso secreta.
- Nivel 4: ultrasecreto/investigación de fondo.
- Nivel 5: ultrasecreto/investigación especial de fondo.
- Nivel 6: ultrasecreto/investigación especial de fondo, con autorización para una división.
- Nivel 7: ultrasecreto/investigación especial de fondo, con autorización para más de una división.

Los niveles de clasificación se numeran de la siguiente manera:

- Nivel 0: no clasificado.

- Nivel 1: información delicada no clasificada.
- Nivel 2: confidencial.
- Nivel 3: secreta.
- Nivel 4: secreta con una categoría.
- Nivel 5: ultrasecreta sin categorías o secreta con dos o más categorías.
- Nivel 6: ultrasecreta con una categoría.
- Nivel 7: ultrasecreta con dos o más categorías.

La exposición de datos es calculada como la diferencia entre el nivel del usuario menor de un sistema y el máximo nivel de los datos procesados por el sistema. Esto coloca un valor entre 0 (todos los usuarios certifican para todos los datos) y 7 (el sistema procesa los datos ultrasecretos con dos o más categorías y algunos usuarios no están certificados).

Aplicación de los factores de riesgo

Para un sistema en particular cada uno de los factores de riesgo necesita ser evaluado de manera que determine el riesgo total. Con menores excepciones, el riesgo del sistema es sencillamente la suma de los riesgos de los factores individuales de riesgo. Basándose en el riesgo del sistema y la exposición de datos, los requerimientos de seguridad pueden determinarse. En un sistema dado, las diferentes terminales pueden proveer diferentes funciones, guiados a diferentes niveles de riesgo, e imponiendo diferentes requerimientos de seguridad. Los requerimientos de seguridad para un sistema visto como un todo, deben estar determinados sobre la base de la parte más riesgosa.

Capítulo 3

Seguridad del Sistema

3.1 Seguridad Física

Normalmente se busca tener una gran seguridad en los sistemas informáticos a nivel lógico, es decir, con programas a través de la red. Pero se nos olvida que puede ser más sencillo tomar una cinta que contenga un respaldo de todo el equipo, que entrar por medios electrónicos a conseguir la información. Todo depende de la seguridad física que tengamos en nuestro sistema. Por seguridad física debemos entender todo aquello que nos lleva a proteger el hardware de nuestro sistema o acceso físico a él.

3.1.1 Protección del hardware

La protección del hardware depende directamente del lugar en el que se encuentre el sistema, por lo que es distinta en cada caso. Por eso, se trata un punto de partida y las cuestiones más importantes a considerar, pero no se puede dar una manera específica de proceder.

La manera más adecuada para comenzar, es por medio de un plan de seguridad física, el cual deberá incluir lo siguiente:

- Descripción de los activos físicos que se están protegiendo.
- Descripción de la zona donde se encuentran dichos activos.
- Descripción del perímetro de seguridad (frontera entre la zona segura y el resto del mundo).
- Amenazas de las que hay que protegerse.
- Defensas de seguridad y cómo pueden mejorarse.
- Costo estimado de las mejoras, costo de la información que se protege y probabilidad de que ocurra un ataque o accidente.

Dependiendo del tamaño de la empresa o institución, así como la importancia de la información, se puede usar desde el sentido común entre los administradores o responsables hasta contratar a un profesional para realizar el análisis.

3.1.1.1 Acceso físico

Un problema que nos encontramos al tratar de proteger una computadora, es que se tiene que usar continuamente, y hay un gran número de personas que deben tener acceso a ellas. Pero debe estar bien establecido qué personas tienen acceso a qué máquinas y existir un área en la cual estén las máquinas más importantes (servidores), en donde no haya acceso al público en general. Puesto que cualquier problema con un servidor puede afectar por completo la funcionalidad de todo nuestro sistema; puede ser algo tan sencillo como que alguien tropiece con un cable de alimentación. Riesgo que se puede correr con una máquina de escritorio de mediana importancia.

También se debe contemplar la posibilidad de que exista un robo, que se puede evitar con medidas relativamente sencillas, como que los equipos se fijen o se pongan siempre bajo llave las cintas de respaldo del sistema. Ante un robo planeado estas medidas no serán suficientes pero evitarán un robo ocasional, y de igual forma que en lo anterior se deberá hacer un estudio que relacione costo-beneficio para determinar si se debe poner una mayor seguridad. Colocando mecanismos más eficientes que pueden ir desde tarjetas inteligentes,

personal de seguridad, sistemas biométricos; pero por supuesto siempre repercutirá en el costo.
Al tomar un decisión sobre una de estas medidas se deben contemplar todas, puesto que puede ser que unas sean mejores que otras, en función de las necesidades específicas del lugar, o que algunas se hagan menos necesarias que otras, por ejemplo, aunque sean más caros los sistemas biométricos pueden hacer que se requiera mucho menos personal de seguridad.

Por último, debemos contemplar el sabotaje. Una de las cosas que es mas difícil de evitar es el sabotaje sobre todo cuando se trata de personal interno. En este tipo de ataque, lo que se busca es destruir equipo y/o información relevante, normalmente por una persona que se encuentra resentida o por otros intereses.

Se deben llevar a cabo algunas medidas de seguridad que ayudarán a evitar este tipo de situaciones:

- Al contratar nuevo personal, investigar los antecedentes de la persona en que se va a confiar equipo e información.
- Se debe buscar que cada persona tenga el mínimo de privilegios que le permitan realizar su trabajo.
- Deslindar responsabilidades, en donde cada persona tenga claro que le corresponde dentro de la política de seguridad.
- Auditorías, donde se revise que todo se está llevando a cabo de manera adecuada, así como los accesos que han tenido en un lapso de tiempo; también es importante que el personal esté enterado de que existen, como método disuasivo.

Todo esto nos lleva a recalcar la importancia de que ningún extraño tenga acceso físico al equipo de cómputo y al de red, al menos sin restricciones. Y que el personal interno tenga una cierta vigilancia, responsabilidades y precauciones.

3.1.1.2 Desastres Naturales

Se debe contemplar dentro de la seguridad física el daño que pueda recibir el hardware por desastres naturales, como puede ser un incendio, inundación, terremotos, etc. Esto depende de la ubicación, puesto que hay zonas que son mucho más propensas a ciertos desastres en específico.

Esto depende de la necesidad de buscar minimizar el riesgo, por ejemplo: si es un lugar propenso a temblores, no se debe colocar material pesado que pueda caer sobre el equipo, o si es una zona propensa a inundaciones poner el equipo a una altura en la que sea poco probable que a pesar de una eventualidad, esta sufra daño.

El equipo de cómputo no se caracteriza por tener un costo muy bajo y, perderlo puede tener graves repercusiones por lo que se deben contemplar opciones como: que piso y paredes sean contra fuego o las puertas selladas y contra agua; revisar los planes de contingencia que existan contra estos fenómenos, por ejemplo, en caso de un pequeño incendio en el que el fuego no dañe los equipos pudiera ser que el agua que se utilice para apagarlo, si lo haga.

Normalmente, es suficiente contar con las precauciones normales, pero bien planeadas; como tener extintores y que las personas que se encuentren ahí sepan usarlos, así como lugares de seguridad y salidas de emergencia.

3.2 Seguridad Lógica

La *seguridad lógica* consiste en la "aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo".

Los objetivos que se plantean serán:

1. Restringir el acceso a los programas y archivos.
2. Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
3. Asegurar que se estén utilizando los datos, archivos y programas correctos, y el procedimiento correcto.
4. Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.
5. Que existan los sistemas alternativos secundarios de transmisión entre diferentes puntos.
6. Que se disponga de pasos alternativos de emergencia para la transmisión de información.

3.2.1 Control de Acceso

El mecanismo de control de acceso se utiliza para autenticar las capacidades de una entidad para acceder a un recurso dado, se puede llevar a cabo en el origen o en un punto intermedio, y se encarga de asegurar que el emisor está autorizado a comunicarse con el receptor o a usar los recursos de comunicación.

3.2.1.1 Identificación y Autenticación

Se denomina *identificación* al momento en que el usuario se da a conocer en el sistema; y *autenticación* a la verificación que se realiza en el sistema sobre esta identificación.

Existen cuatro tipos de técnicas que permiten realizar la autenticación de la identidad del usuario, las cuales pueden ser utilizadas individualmente o combinadas:

1. Algo que solamente el individuo conoce: por ejemplo, una clave secreta de acceso, un número de identificación o NIP, etc.
2. Algo que la persona *posee*: por ejemplo, una tarjeta magnética.
3. Algo que el individuo *es* y que lo identifica unívocamente: por ejemplo, las huellas digitales o la voz.
4. Algo que el individuo es capaz de *hacer*: por ejemplo, los patrones de escritura.

3.2.1.2 Modalidad de Acceso

Se refiere al modo de acceso que se permite al usuario sobre los recursos y la información. Esta modalidad puede ser:

- **Lectura:** el usuario puede únicamente leer o visualizar la información, pero no puede alterarla. Debe considerarse que la información puede ser impresa o copiada.
- **Escritura:** permite agregar datos, modificar o borrar información.
- **Ejecución:** este acceso otorga al usuario el privilegio de ejecutar programas.
- **Borrado:** permite al usuario eliminar recursos del sistema (como programas, campos de datos o archivos). El borrado es considerado una forma de modificación.
- **Todas las anteriores.**

3.2.1.3 Control de acceso interno

3.2.1.3.1 Contraseñas (Passwords)

El control de acceso más común es la basada en el conocimiento. Permite el acceso a aquellas personas que puedan probar que conocen algo secreto, por lo común una contraseña.

Hay siete clasificaciones principales de contraseñas. Son:

1) *Contraseñas dadas por el usuario.*
2) *Contraseñas al azar generadas por el sistema.*
3) *Códigos de acceso generados al azar por el sistema.*
4) *Híbridas.*
5) *Frases de acceso.*
6) *Secuencias de preguntas y respuestas interactivas.*
7) *Predeterminadas por coordenadas por código.*

La mayoría de las contraseñas son de la clase "elígelas tú mismo" y debido a la mayor conciencia existente acerca de la seguridad, la mayoría de los programas actuales que piden contraseñas no aceptarán aquellas de extensión breve que el programa considere "hackeables" con demasiada facilidad, además de tomar otras medidas para proteger a los usuarios de su propia falta de creatividad.

Las contraseñas y los códigos al azar generados por el sistema pueden ser de varios tipos. La programación del sistema puede suministrar una secuencia totalmente al azar de letras, dígitos, símbolos de puntuación y extensión; que son determinados en el momento o pueden usarse límites en los procedimientos de generación, tales como cada código de acceso conforme a un formato fijo (como "abc-12345-defg") donde las letras y los números son generados al azar. Otras contraseñas generadas por la computadora pueden ser tomadas al azar de una lista de palabras o de sílabas sin sentido, suministradas por los autores del programa, creando así contraseñas como "nah.foop" o "tren-sol-bien".

La híbrida es en parte suministrada por el usuario, el resto es mediante cierto proceso al azar. Esto significa que si un usuario elige una contraseña muy fácil de adivinar, por

ejemplo: "secreto", la computadora le agregará alguna jerga incomprendible al final, formando una contraseña más segura "secreto/5rh11".

Las frases de acceso son buenas en el sentido que son largas y difíciles de adivinar, pero fáciles de recordar. Las frases pueden ser coherentes como "estábamos preocupados por eso", o pueden ser insensatas "pescados por nuestra nariz". Las frases de acceso se usan cuando el encargado de un lugar es muy propenso a la seguridad.

El sexto tipo de contraseña, las secuencias de preguntas y respuestas, exige que el usuario suministre respuestas a varias preguntas (por lo común personales). La computadora tendrá archivada las respuestas a muchas preguntas de este tipo y durante el login pedirá la respuesta de dos o tres de ellas.

Las contraseñas que están predeterminadas por coordenadas, generadas a través de códigos, comúnmente confían en algún artefacto externo, tal como las ruedas de código que se usan para impedir la piratería de software. En todo caso, un conjunto de prompts clave son presentados por la computadora, y se exige al usuario que ingrese las respuestas apropiadas. Con frecuencia este tipo de contraseñas se usa en un sistema con códigos de una sola vez.

Los códigos de una sola vez son contraseñas válidas para un solo acceso. A veces son empleadas en cuentas invitadas temporales para mostrar un sistema a clientes potenciales. Los códigos de una sola vez también pueden ser empleados por el sistema para permitir a los usuarios verdaderos hacer el login por primera vez; se espera entonces que los usuarios cambien la contraseña que se les suministró a una más segura, personal. En situaciones donde haya grupos de personas que tienen que hacer el login, pero deba mantenerse la seguridad, puede suministrarse una lista de códigos de una sola vez. Los usuarios extraen entonces un código por vez, dependiendo de códigos externos tales como la hora, la fecha o el día.

3.2.1.3.2 Encriptación

La encriptación es el método por el cual la información puede ser protegida a través de programas encargados de cifrarla, firmarla para identificar eficientemente al remitente, y cerrarla para que sólo pueda ser abierta nuevamente por quien tenga la clave apropiada, agregándose además métodos para corroborar la integridad de la información recibida, es decir, para validar que la información no haya sido modificada en el camino.

Encriptación es solamente una parte del campo de la seguridad informática llamado "**criptología**". La criptología se conforma de dos amplias áreas: la "**criptografía**" que se dedica a la construcción y operación de sistemas de seguridad informática; el "**criptoanálisis**" cuyo fin es desencriptar los criptogramas y acceder de manera ilegítima a la información contenida en los mensajes mediante ciertas técnicas con las que no es preciso conocer la clave de cifrado.

Criptografía simétrica.

Los métodos criptográficos tradicionales operan a partir de una palabra o frase llave, que sirve para codificar y decodificar información, el conocido password. Esta llave debe ser conocida por los extremos de la comunicación, por lo que el punto débil de este método es

justamente el proceso de difusión de la llave. El sistema *DES (Data Encription Standard)* representa el estándar de mayor difusión para los sistemas simétricos. Este método se puede apreciar en la figura 3.1.

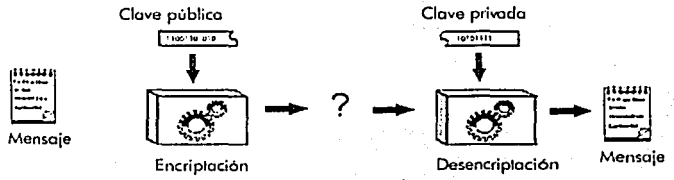


Figura 3.1. Criptografía simétrica.

Criptografía asimétrica.

Por el contrario, la criptología de clave pública (Kpu) consiste en poner a cada extremo de la comunicación un par de llaves, una pública que cualquiera puede solicitar y conocer, y otra privada (Kpr), cuya seguridad es fundamental para el éxito de la codificación. Las llaves son una secuencia bastante larga de caracteres y números, generadas por un procedimiento matemático.

Para enviar un mensaje a una persona, se codifica con la clave pública del destinatario. El sistema garantiza que el mensaje resultante sólo puede ser decodificado con la clave privada del destinatario (confidencialidad). Como se tiene la seguridad de la identidad del destinatario gracias a su clave pública, nos aseguramos que el mensaje va al sitio correcto (autenticación). Este método se muestra en la figura 3.2.

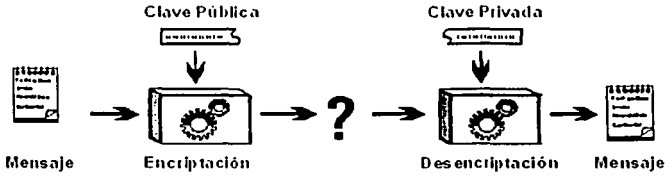


Figura 3.2. Criptografía asimétrica.

Para enviar un mensaje firmado, se genera una "firma digital" del mismo (con unos algoritmos matemáticos que proporcionan un resumen del mensaje), que se codifica con la clave privada del remitente. Posteriormente, el receptor puede utilizar la clave pública del remitente para verificar su origen; de esta forma se garantiza que el mensaje sólo puede ser

enviado por el remitente (no repudio), ya que él es el único que conoce su clave privada, como se muestra en la figura 3.3.

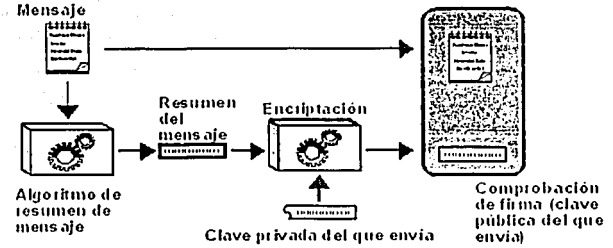


Figura 3.3. Como se envía un mensaje firmado.

Almacenamiento seguro.

PGP: Pretty Good Privacy.

El *software* PGP, desarrollado por el criptólogo estadounidense Phil Zimmermann, es mundialmente conocido como sistema de firma digital para correo electrónico. Aparte de esta función, PGP permite también el cifrado de archivos de forma convencional mediante criptografía simétrica. Esta faceta de PGP convierte al programa en una excelente herramienta para cifrar archivos que almacenamos en nuestro sistema; no es el mismo mecanismo que se emplea para cifrar un archivo que vamos a enviar por correo, algo que se hace utilizando la clave pública del destinatario, sino que es un método que no utiliza para nada los anillos de PGP, los userID o el cifrado asimétrico.

TCFS: Transparent Cryptographic File System.

TCFS es un *software* desarrollado en la Universidad de Salerno y disponible para sistemas Linux que proporciona una solución al problema de la privacidad en sistemas de archivos distribuidos como NFS: típicamente en estos entornos las comunicaciones se realizan en texto claro, con la enorme amenaza a la seguridad que esto implica. TCFS almacena los archivos cifrados, y son pasados a texto, antes de ser leídos; todo el proceso se realiza en la máquina cliente, por lo que las claves nunca son enviadas a través de la red.

La principal diferencia de TCFS con respecto a otros sistemas de archivos cifrados como CFS es que, mientras que éstos operan a nivel de aplicación, TCFS lo hace a nivel de núcleo, consiguiendo así una mayor transparencia y seguridad. Obviamente esto tiene un grave inconveniente: TCFS sólo está diseñado para funcionar dentro del núcleo de sistemas Linux, por lo que si nuestra red de Unix utiliza otro clon del sistema operativo, no podremos utilizar TCFS correctamente. No obstante, esta gran integración de los servicios de cifrado en el sistema de los archivos hace que el modelo sea transparente al usuario final.

Para utilizar TCFS necesitamos que la máquina que exporta directorios vía NFS ejecute el demonio *xattrd*; por su parte, los clientes han de ejecutar un núcleo compilado con soporte para TCFS. Además, el administrador de la máquina cliente ha de autorizar a los usuarios a que utilicen TCFS, generando una clave que cada uno de ellos utilizará para trabajar con los archivos cifrados; esto se consigue mediante *tcfsgenkey*, que genera una entrada para cada usuario en */etc/tcfspasswd*.

3.2.1.4 Control de Acceso Externo

3.2.1.4.1 Dispositivos de control de puertos

Estos dispositivos autorizan el acceso a un puerto determinado y pueden estar físicamente separados o incluidos en otro dispositivo de comunicaciones, como por ejemplo un módem.

3.2.1.4.2 Firewalls o Puertas de Seguridad

La conectividad de una red privada corporativa a redes como Internet hace necesario que haya mecanismos de seguridad que permitan un alto grado de confiabilidad y protección de la información, para ello una de las más típicas y eficaces formas existentes son los llamados *FIREWALLS* o barreras de protección, los cuales previenen los accesos indeseables hacia el interior de una red o a alguna porción de la misma.

Una red privada que lleva información sensitiva entre computadoras locales requiere de medidas de seguridad propias para proteger la privacidad e integridad del tráfico. Cuando tal red privada se conecta a otras redes, o cuando se permite acceso telefónico hacia el interior de la misma, los puntos de conexión remotos, líneas telefónicas y otras conexiones se convierten en extensiones de la red privada que deben ser protegidas apropiadamente. Por lo tanto, es necesario un sistema que provea mecanismos para reducir al máximo el riesgo de ataques externos que puedan causar pérdida de información o daños en la integridad de la red o ampliar las posibilidades de acceso no permitido; estos mecanismos deben garantizar fuertes procesos de autenticación de usuarios, control de acceso y protección de la integridad de datos sensibles en la red privada o conjunto de redes.

3.2.1.4.3 Acceso de Personal Contratado

Debido a que este tipo de personal, en general, presta servicios temporales, debe ponerse especial consideración en la política y administración de sus perfiles de acceso.

3.2.1.4.4 Accesos públicos

Para los sistemas de información consultados por el público en general, o los utilizados para distribuir o recibir información computarizada (mediante, por ejemplo, la distribución y recepción de formularios en soporte magnético, o la consulta y recepción de información a través de correo electrónico) deben tenerse en cuenta medidas especiales de seguridad, ya que se incrementa el riesgo y se dificulta su administración.

3.3 Seguridad del Sistema de Archivos

3.3.1 Sistema de Archivos

El término ***archivo*** se puede definir como un conjunto de datos con un nombre asociado. Los archivos suelen residir en dispositivos de almacenamiento secundario, tales como cintas, discos duros o disquetes. La razón de asignar un nombre a cada archivo es que de este modo tanto los usuarios como los programas pueden hacer referencia a los mismos de una forma lógica.

En un sistema Unix típico existen tres tipos básicos de archivos: archivos planos, directorios y archivos especiales (dispositivos). Los ***archivos planos*** son secuencias de *bytes* que *a priori* no poseen ni estructura interna ni contenido significante para el sistema: su significado depende de las aplicaciones que interpretan su contenido. Los ***directorios*** son archivos cuyo contenido son otros archivos de cualquier tipo (planos, más directorios, o archivos especiales). Y los ***archivos especiales*** son archivos que representan dispositivos del sistema; este último tipo se divide en dos grupos: los dispositivos orientados a carácter y los orientados a bloque. La principal diferencia entre ambos es la forma de realizar operaciones de entrada/salida: mientras que los dispositivos orientados a carácter las realizan *byte* a *byte* (esto es, carácter a carácter), los orientados a bloque las realizan en bloques de caracteres.

Un ***sistema de archivos*** es aquella parte del sistema responsable de la administración de los datos en dispositivos de almacenamiento secundario. El sistema de archivos debe proporcionar los medios necesarios para un almacenamiento seguro y privado de la información y, a la vez, la posibilidad de compartir esa información en caso de que el usuario lo desee.

Cada sistema Unix tiene su sistema de archivos nativo, por ejemplo: *ext3* en Linux (ver Apéndice I), UFS en Solaris o EFS en IRIS; por lo que para acceder a todos ellos de la misma forma, el núcleo de Unix incorpora una capa superior denominada VFS (*Virtual File System*) encargada de proporcionar un acceso uniforme a diferentes tipos de sistema de archivos.

Entre las características más relevantes del sistema de archivos de UNIX son:

- Los usuarios tienen la posibilidad de crear, modificar y borrar archivos y directorios.
- Cada archivo tiene definidos tres tipos de acceso diferentes: acceso de lectura [r], acceso de escritura [w] y acceso de ejecución [x]. A su vez, esos tres tipos de acceso pueden extenderse a la persona propietaria del archivo, al grupo al cual está adscrita dicha persona y al resto de los usuarios del sistema. Eso permite que los archivos puedan ser compartidos de forma controlada.
- Cada usuario puede estructurar sus archivos como desee, el núcleo de UNIX no impone restricción.
- UNIX proporciona la posibilidad de realizar copias de seguridad de todos y cada uno de los archivos para prevenir la pérdida de forma accidental o maliciosa de la información.

- Proporciona la posibilidad de cifrado y descifrado de información. Eso se puede hacer para que los datos sólo sean útiles a las personas que conozcan la clave de descifrado.
- El usuario tiene una visión de lógica de los datos, que es el sistema encargado de manipular correctamente los dispositivos y darle el soporte físico deseado a la información. El usuario no tiene que preocuparse por los dispositivos físicos, es el sistema el que se encarga de la forma en que se almacenan los datos en los dispositivos y de los medios físicos de transferencia de datos desde y hacia los mismos.

En UNIX los archivos están organizados en lo que se conoce como ***directorios***. Un directorio es un archivo especial que contiene información que permite localizar otros archivos. Los directorios pueden contener, a su vez, nuevos directorios, los cuales se denominan ***subdirectorios***. A la estructura resultante de esta organización se le conoce con el nombre de ***estructura en árbol invertido***. Un ejemplo de árbol de directorios UNIX se muestra en la figura 3.4.

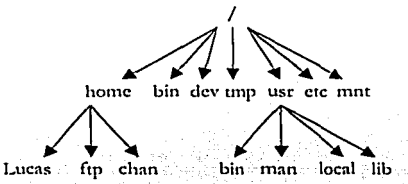


Figura 3.4. Esquema del árbol de directorios típicos de UNIX.

El sistema de archivos de UNIX tiene, para el usuario, una estructura en árbol invertido en el cual los archivos se agrupan en directorios. Todos los archivos y directorios dependen de un único directorio denominado directorio raíz o *root*, el cual se representan por el símbolo *slach "/"*.

Los archivos se identifican en la estructura de directorios por lo que se conoce como *pathname* o camino.

Algunos directorios interesantes en UNIX son:

- ***directorio raíz /***. Sólo hay una raíz en un sistema de archivos UNIX y se denota por el carácter "/". La raíz es el único directorio que no tiene directorio padre.
- ***/bin***. Contiene muchos de los comandos utilizados en UNIX. Normalmente, se encuentran los programas de uso más común para los usuarios.
- ***/usr***. Se derivan los diferentes directorios de trabajo de cada uno de los usuarios. este directorio contiene también archivos que posteriormente utilizan otros comandos de UNIX. Algunos subdirectorios importantes son:

- */usr/bin*: Contiene fundamentalmente los programas ejecutables que de alguna forma son mayores en tamaño y se utilizan menos frecuentemente que los comandos del directorio /bin.
- */usr/lib*: Contiene los archivos de biblioteca utilizados por los compiladores de lenguajes como FORTRAN, Pascal, C, etc. Estos archivos contienen básicamente funciones, en un formato específico, que pueden ser invocadas desde estos lenguajes.
- */usr/mail*: Es el subdirectorio de buzones. Toda la correspondencia se envía y se recibe aquí.
- */usr/man*: Contiene las páginas del manual en el disco de la computadora.
- */usr/local/bin* y */usr/contrib/bin*: Estos directorios son generalmente creados por el administrador del sistema para que contengan archivos ejecutables que no forman parte del UNIX estándar.

- */etc*. Este directorio contiene comandos y archivos de configuración empleados en la administración del sistema.
- */dev*. Este directorio contiene los archivos de dispositivo empleados para la comunicación con dispositivos periféricos, tales como cintas, impresoras, discos, etc.
- */home*. Contiene los directorios casa de los usuarios del sistema.
- */opt*. Semejante a /usr/local contiene programas adicionales.
- */mnt*. Punto sugerido para montar dispositivos removibles.
- */var*. Para almacenar archivos que varían su contenido con el transcurso del tiempo, como spools de impresora.
- */tmp*. Para las copias temporales.

3.3.2 Permisos de un Archivo

El sistema UNIX proporciona la posibilidad de proteger la información. Para ello, asocia a cada archivo una serie de derechos de acceso. En función de éstos, se determina qué es lo que cada usuario puede hacer con el archivo. Estos derechos se extienden a tres grupos de individuos: el ***propietario***, el ***grupo del propietario*** y los ***otros***. A su vez, estos grupos pueden tener diferentes posibilidades de acceso al archivo: para leer información del mismo, para escribir en él o para ejecutarlo, en el caso de que corresponda a un archivo ejecutable. Estos derechos aparecen como una secuencia de nueve caracteres **r**, **w**, **x** ó **-** .

Una **r** indica derecho de lectura, una **w** de escritura y la **x** de ejecución. El guión indica que el derecho correspondiente está desactivado. Estas secuencias de caracteres se agrupan de tres en tres. De izquierda a derecha tenemos que: los tres primeros caracteres corresponden con los derechos del propietario (*user*), los tres siguientes con los del grupo (*group*) y los tres últimos para los otros (*others*).

3.3.3 Bits SUID, SGID y sticky

El bit **SUID** significa "Set Users ID", fija la identificación del dueño y el programa se ejecuta con la identificación y los permisos del dueño. Es decir, el hecho de que un programa tenga este bit activo implica que cuando se ejecute dicho programa, este tomará como identificador de usuario el identificador del propietario. Si el propietario fuese el

administrador, entonces el programa se ejecutaría como si lo hubiese hecho el mismo administrador.

El bit **SGID** es análogo y significa "Set Group ID", es decir, 'Fijar la Identidad del Grupo'. Lo que provoca es que cuando un usuario ejecute un programa con el SGID activo, este se va a ejecutar con la identidad (y se supone, los privilegios) del grupo al que pertenece el archivo.

El **sticky bit** indica al núcleo de UNIX que el archivo es un programa con capacidad para que varios procesos compartan su código, y que este código se debe mantener en memoria aunque algunos de los procesos que lo utiliza deje de ejecutarse. Es decir, este bit, al contrario que los otros, en los que lo pueden activar el dueño, o cualquiera con permisos para ello, sólo lo puede activar *root*. Provoca que el programa al que se le aplica quede residente en memoria de forma que la próxima vez que sea llamado su carga sea más rápida. Cuando se le aplica a un directorio, impide que nadie más que su dueño pueda renombrar o borrar ningún archivo del mismo.

3.3.4 Atributos de un archivo

En el sistema de archivos *ext3* (*Second Extended File System*) de Linux existen ciertos atributos para los archivos que pueden ayudar a incrementar la seguridad de un sistema. Estos atributos son:

- **A** Don't update Atime
- **S** Synchronous updates (actualizaciones síncronas).
- **a** Append only (añadir sólo al final).
- **c** Compressed file (archivo comprimido).
- **i** Immutable file (archivo inmutable).
- **d** No Dump (no aplicable el comando *dump*).
- **s** Secure deletion (borrado seguro).
- **u** Undeletable file (archivo imborrable).

Definiremos algunos atributos:

El atributo **'a'** sobre un archivo indica que este sólo se puede abrir en modo escritura para añadir datos, pero nunca para eliminarlos.

El atributo **'i'** indica que el archivo está en modo inmutable. Esto quiere decir que no se podrá modificar el archivo (ni sobreescribirlo, ni borrarlo, ni añadir datos), ni tampoco enlazarlo. Se puede utilizar este bit para archivos que no se modifiquen frecuentemente en el sistema.

El atributo **'S'** indica al sistema operativo que debe realizar los cambios sobre el archivo de forma inmediata, y que no debe esperar al vaciado de buffer del sistema para registrar los cambios, de modo que por ejemplo, un corte de luz, no suponga pérdida de datos.

El atributo **'s'** sobre un archivo hace que los cambios sobre el archivo se escriban inmediatamente en el disco, en lugar de esperar el sync del sistema operativo. Aunque no es

lo habitual, bajo ciertas circunstancias un archivo de *log* puede perder información que aún no se haya volcado a disco.

3.3.5 Listas de Control de Acceso: ACL's

Las listas de control de acceso (ACL's, *Access Control Lists*) proveen de un nivel adicional de seguridad a los archivos extendiendo el clásico esquema de permisos en Unix: mientras que con estos últimos sólo podemos especificar permisos para los tres grupos de usuarios habituales (propietario, grupo y resto), las ACL's van a permitir asignar permisos a usuarios o grupos concretos; por ejemplo, se pueden otorgar ciertos permisos a dos usuarios sobre unos archivos sin necesidad de incluirlos en el mismo grupo. Este mecanismo está disponible en la mayoría de Unix (Solaris, AIX, HP-UX...), mientras que en otros que no lo proporcionan por defecto, como Linux, puede instalarse como un *software* adicional. A pesar de las agresivas campañas de *marketing* de alguna empresa, que justamente presumía de ofrecer este modelo de protección en sus *sistemas operativos* frente al 'arcaico' esquema utilizado en Unix, las listas de control de acceso existen en Unix desde hace más de diez años.

Las ACL's son de gran ayuda para el administrador de sistemas Unix, tanto para incrementar la seguridad como para facilitar ciertas tareas.

Capítulo 4

Políticas de Seguridad y Normatividad

En la actualidad es imposible hablar de un sistema cien por ciento seguro, debido a que el costo de la seguridad total es muy alto. Por eso las empresas, en general, asumen riesgos y deben optar entre perder un negocio o arriesgarse a la posibilidad de ser hackeadas.

La dependencia de las organizaciones en su información ha crecido al punto de ser considerada como uno de sus activos más importantes. A través del tiempo, las necesidades del intercambio electrónico de información han sido uno de los principales retos de cualquier organización. Como respuesta a dichas necesidades se establece una infraestructura que permita brindar los servicios necesarios a sus clientes, socios comerciales y empleados. Esta infraestructura se basa, principalmente, en el establecimiento de redes.

El principal objetivo informático de la organización es dar protección y seguridad a su información, para ello es necesario establecer las normas, políticas y estándares de seguridad para los sistemas distribuidos que procesan, almacenan y transmiten información, a fin de minimizar riesgos en su integridad, confidencialidad y disponibilidad. De esta manera se puede controlar todo un conjunto de vulnerabilidades, aunque no se logre la seguridad total.

Algunas organizaciones gubernamentales y no gubernamentales internacionales han desarrollado documentos, directrices y recomendaciones que orientan al uso adecuado de las nuevas tecnologías para obtener el mayor provecho y evitar el uso indebido de las mismas, lo cual puede ocasionar serios problemas en los bienes y servicios de las empresas en el mundo.

En este sentido, las *Políticas de Seguridad,* surgen como una herramienta organizacional para concienciar a cada uno de los miembros de una organización sobre la importancia y sensibilidad de la información y servicios críticos.

4.1 ¿Qué es una política de seguridad?

Antes de definir lo que es una política de seguridad, mencionaremos algunos conceptos que se aplican en las diversas definiciones de política de seguridad.

Decisión: elección de un curso de acción determinado entre varios posibles.
Política: definiciones establecidas por la dirección que determinan criterios generales a adoptar en distintas funciones y actividades donde se conocen las alternativas ante circunstancias repetidas.
Riesgo: proximidad o posibilidad de un daño, peligro. Cada uno de los imprevistos, hechos desafortunados, que pueden tener un efecto adverso.

Se debe tomar en cuenta que, proponer o identificar una política de seguridad requiere un alto compromiso con la organización, agudeza técnica para establecer fallas y debilidades, y constancia para renovar y actualizar dicha política en función del dinámico ambiente que rodea a las organizaciones modernas.

La Seguridad Informática no tiene una solución definitiva en estos momentos, porque esta es y será el resultado de la innovación tecnológica, a la par del avance tecnológico, por parte de aquellos que son los responsables de los sistemas.

A continuación, mencionaremos algunas definiciones de política de seguridad:

- "Una **Política de Seguridad** es un conjunto de requisitos definidos por los responsables de un sistema, que indica en términos generales qué está y qué no está permitido en el área de seguridad durante la operación general del sistema."[1]

- La RFC 1244 define **Política de Seguridad** como: "una declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requerirán."[2]

- "Una **Política de Seguridad** es una forma de comunicarse con los usuarios ... Siempre hay que tener en cuenta que la seguridad comienza y termina con personas."[3]

- "Una **Política de Seguridad** es aquella que fija los mecanismos y procedimientos que deben adoptar las empresas para salvaguardar sus sistemas y la información que estos contienen."[4]

De acuerdo con las definiciones anteriores, podemos concluir que:

*La **Política de Seguridad** es un conjunto de leyes, reglas y prácticas que regulan la manera de dirigir, proteger y distribuir recursos en una organización para poder llevar a cabo los objetivos de seguridad informática dentro de la misma.*

El conjunto de leyes, reglas y prácticas son los documentos en los que se describen, principalmente, la forma adecuada de uso de los recursos de un sistema de cómputo, las responsabilidades y derechos que tanto usuarios como administradores tienen y qué hacer ante un incidente de seguridad.

A través de las leyes, reglas y prácticas que reflejen las metas y situaciones de la organización, también reflejan los principios que se aplican en general, éstos son:

a) Responsabilidad individual: las personas son responsables de sus actos. El principio implica que la gente que está plenamente identificada debe estar consciente de sus actividades, debido a que sus acciones son registradas, guardadas y examinadas.

b) Autorización: son reglas explícitas acerca de quién y de qué manera puede utilizar los recursos.

c) Mínimo privilegio: la gente debe estar autorizada única y exclusivamente para acceder a los recursos que necesita para hacer su trabajo.

---

[1] HUERTA, Villalón Antonio. *Seguridad en Unix y Redes*[en línea]. Versión 2.1. Julio 2002. Capítulo 22. Gestión de la Seguridad. Disponible en: < http://www.rediris.es/cert/doc/unixsec/unixsec.pdf >[Consulta: 3 Mayo 2002].

[2] RFC 1244: Site Security Handbook. J. Reynolds – P. Holbrook. Julio 1991.

[3] SPAFFORD, Gene.(2000). "Manual de seguridad en redes" [en línea]. Argentina, ArCERT. Disponible en :< *http://www.arcert.gov.ar/webs/manual/manual_de_seguridad.pdf*> [Consulta : 7 Junio 2002]

[4] *Políticas de seguridad informática*[en línea]. Madrid, 9 Noviembre 2001. [Consulta: 5 Junio 2002]. Disponible en: < *http://www.delitosinformaticos.com/articulos/100530260583540.shtml*>

d) Separación de obligaciones: las funciones deben estar divididas entre las diferentes personas relacionadas a la misma actividad o función, con el fin de que ninguna persona cometa un fraude o ataque sin ser detectado. La separación de obligaciones funciona mejor cuando cada una de las personas involucradas tiene diferentes actividades y puntos de vista.

e) Auditoría: el trabajo y los resultados deben ser monitoreados durante su inicio y hasta después de ser terminado. Una revisión de los registros, donde se guardan las actividades, ayuda para realizar una reconstrucción de las acciones de cada individuo.

f) Redundancia: el principio de redundancia afecta al trabajo y a la información. Múltiples copias son guardadas con importantes registros y dichas copias son frecuentemente almacenadas en diferentes lugares.

g) Reducción de Riesgo: esta estrategia debe reducir el riesgo a un nivel aceptable, haciendo que el costo de la aplicación sea proporcional al riesgo.

Para poder llevar a cabo los objetivos de seguridad informática de la organización, las políticas de seguridad tienen que diseñarse de acuerdo a las características propias de cada organización.

La política define la seguridad de la información en el sistema central de la organización, por lo tanto, un sistema central es seguro si cumple con las políticas de seguridad impuestas para esa organización. La política especifica qué propiedades de seguridad el sistema debe proveer. De manera similar, la política define la seguridad informática para una organización, especificando tanto las propiedades del sistema como las responsabilidades de seguridad de las personas.

Una política de seguridad informática debe representar fielmente una política del mundo real y además debe interactuar con la política de recursos, por ejemplo, políticas en el manejo de bases de datos o de transacciones. En ella, se deben considerar las amenazas contra las computadoras, especificando cuáles son dichas amenazas y cómo contraatacarlas. Asimismo, debe ser expresada en un lenguaje en el que todas las personas involucradas (quienes crean la política, quienes la van a aplicar y quienes la van a cumplir) puedan entender.

Una política de seguridad puede ser **prohibitiva**, si todo lo que no está expresamente permitido está denegado, o **permisiva**, si todo lo que no está expresamente prohibido está permitido.

¿Por qué utilizar Políticas de Seguridad?

Existen muchos factores que justifican el establecimiento de políticas de seguridad para una organización en específico, pero los más determinantes son:

- Ayudan a la organización a darle valor a la información.
- Es una infraestructura desde la cual otras estrategias de protección pueden ser desarrolladas.
- Proveen unas claras y consistentes reglas para los usuarios de la red corporativa y su interacción con el entorno.
- Contribuyen a la efectividad y direccionan la protección total de la organización.

- Pueden ayudar a responder ante requerimientos legales.
- Ayudan a prevenir incidentes de seguridad.
- Proveen una guía cuando un incidente ocurre.
- Es una planeación estratégica del papel que juega la arquitectura de red al interior de la organización.
- Ayuda en la culturización de los usuarios para el uso de servicios de red e inculca el valor real que ellos representan.

Características de las Políticas de Seguridad.

Una política de seguridad es un plan elaborado de acuerdo con los objetivos generales de la organización y en el cual se ve reflejado el sentir corporativo acerca de los servicios y recursos que se desean proteger de manera efectiva y que representan activos importantes para el cumplimiento normal de la misión institucional. Por esto las políticas de seguridad deben cumplir con las siguientes características:

- Holísticas (cubrir todos los aspectos relacionados con las mismas).
- Claras (explícitas).
- Concisas (breves).
- Únicas.
- Estar siempre disponibles.
- Estar bien estructuradas.
- Se establecen como una guía, es decir, que sirvan de referencia.
- Ser escritas.
- Se pueden aplicar en cualquier momento a la mayoría de situaciones contempladas.
- Ser practicables y desarrollables.
- Se deben poder hacer cumplir.
- Ser consistentes con otras políticas organizacionales.
- Ser atemporales, lo cual implica que el tiempo en el que se aplica no debe influir en su eficacia y eficiencia.
- Deben ser cambiantes con la variación tecnológica.
- Mantenerse actualizadas.
- Darlas a conocer.
- Adecuarse a las necesidades y requerimientos de seguridad de la organización.
- Entendidas por los usuarios.
- Ser apoyadas por los directivos de la organización.

Elementos de una Política de Seguridad.

Cualquier política ha de contemplar seis elementos claves en la seguridad de un sistema informático:[5]

- **Disponibilidad**
  Es necesario garantizar que los recursos del sistema se encontrarán disponibles cuando se necesitan, especialmente la información crítica.

[5] Susan Peppard et al. *Unix Unleashed.* Sams Publishing, 1st edition, 1994.

- **Utilidad**
  Los recursos del sistema y la información manejada en el mismo, ha de ser útil para alguna función.

- **Integridad**
  La información del sistema ha de estar disponible tal y como se almacenó por un agente autorizado.

- **Autenticidad**
  El sistema ha de ser capaz de verificar la identidad de sus usuarios, y los usuarios la del sistema.

- **Confidencialidad**
  La información sólo ha de estar disponible para agentes autorizados, especialmente su propietario.

- **Posesión**
  Los propietarios de un sistema han de ser capaces de controlarlo en todo momento; perder este control en favor de un usuario malicioso compromete la seguridad del sistema hacia el resto de usuarios.

4.2 Responsabilidad de una Política de Seguridad

Un aspecto importante en torno a la política de seguridad de red es asegurar que todos saben cuál es su responsabilidad para mantener la seguridad, por lo tanto la política de seguridad debe poder garantizar que cada tipo de problema tiene a alguien que puede manejarlo de manera responsable. Así mismo, pueden existir varios niveles de responsabilidad asociados con una política de seguridad como son los de usuarios y administradores, que más adelante serán descritos.

4.3 Análisis de Riesgos

El **Análisis de Riesgos** implica responder a tres cuestiones básicas sobre la seguridad del sistema:

- ¿Qué queremos proteger?
- ¿Contra quién o qué lo queremos proteger?
- ¿Cómo lo queremos proteger?

Es el proceso de examinar los posibles riesgos y clasificarlos por nivel de severidad, esto involucra hacer decisiones costo-beneficio. No se debe llegar a una situación donde se gasta más para proteger aquello que es menos valioso.

En el análisis de los riesgos, es necesario determinar los siguientes factores:

- Estimación del riesgo de pérdida del recurso (R_i).
- Estimación de la importancia del recurso (W_i).

Como un paso hacia la cuantificación del riesgo de perder un recurso, es posible asignar un valor numérico. Por ejemplo, al riesgo (R_i) de perder un recurso, se le asigna un valor de cero a diez, donde cero, significa que no hay riesgo y diez es el riesgo más alto. De manera similar, a la importancia de un recurso (W_i) también se le puede asignar un valor de cero a diez, donde cero significa que no tiene importancia y diez es la importancia más alta.

La evaluación general del riesgo será entonces el producto del valor del riesgo y su importancia (también llamado el peso). Esto puede escribirse como:

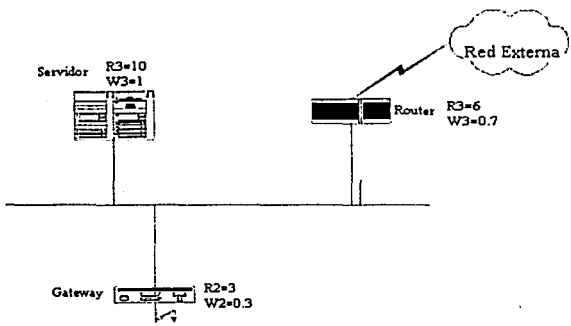
$$WR_i = R_i * W_i$$

Donde:

WR_i: es el peso del riesgo del recurso "i" (también lo podemos llamar ponderación).
R_i: es el riesgo del recurso "i".
W_i: es la importancia del recurso "i".

Ejemplo práctico[6]:

Supongamos una red simplificada con un router, un servidor y un bridge.



Los administradores de la red y de sistemas han producido las estimaciones siguientes para el riesgo y la importancia de cada uno de los dispositivos que forman nuestra red:
Como se ve, a cada uno de los componentes de sistema, se le ha asignado un cierto riesgo y una cierta importancia. Hay que destacar que estos valores son totalmente subjetivos, dependen exclusivamente de quien ó quienes están realizando la evaluación.
Tenemos, entonces:

Router:

$R_i = 6$
$W_i = 7$

[6] SPAFFORD, Gene. p. 64.

Bridge:

$R_2 = 6$
$W_2 = 3$

Servidor:

$R_3 = 10$
$W_3 = 10$

El cálculo de los riesgos evaluados, será, para cada dispositivo:

Router:

$WR_1 = R_1 * W_1 = 6 * 7 = 42$

Bridge:

$WR_2 = R_2 * W_2 = 6 * 3 = 18$

Servidor:

$WR_3 = R_3 * W_3 = 10 * 10 = 100$

La tabla que sigue a continuación, nos muestra cómo podríamos llevar a cabo esta tarea de una manera ordenada y los valores que contiene son los que hemos tratado:

Riesgo del Sistema		Riesgo (R_i)	Importancia (W_i)	Riesgo Evaluado ($R_i * W_i$)
Número	Nombre			
1	Router	6	7	42
2	Bridge	6	3	18
3	Servidor	10	10	100

Vemos que, en este caso, el recurso que debemos proteger más es el Servidor ya que su riesgo ponderado es muy alto. Por tanto, comenzaremos por buscar las probables causas que pueden provocar problemas con los servicios brindados por él.

Con la siguiente fórmula es posible calcular el riesgo general de los recursos de la red:

$$W_R = \frac{(R_1 * W_1 + R_2 * W_2 + \ldots + R_n * W_n)}{W_1 + W_2 + \ldots + W_n}$$

Otros factores que se deben de considerar para el análisis de riesgo de un recurso de red son su disponibilidad, su integridad y su carácter confidencial, los cuales pueden incorporarse a la fórmula para ser evaluados.

4.3.1 Identificación de recursos

Debemos identificar todos los recursos cuya integridad pueda ser amenazada de cualquier forma; el RFC 1244 define básicamente los siguientes:[7]

[7] Dave Curry et al. *RFC1244: Site Security Handbook.* Internet Activities Board, Julio 1991.

- *Hardware*
  Procesadores, tarjetas, teclados, terminales, estaciones de trabajo, computadoras personales, impresoras, unidades de disco, líneas de comunicación, servidores, *routers*. . .

- *Software*
  Códigos fuente y objeto, utilidades, programas de diagnóstico, sistemas operativos, programas de comunicación. . .

- *Información*
  En ejecución, almacenados en línea, almacenados fuera de línea, en comunicación, bases de datos. . .

- *Personas*
  Usuarios, operadores. . .

- *Documentación*
  De programas, hardware, sistemas, procedimientos de administración local.

- *Accesorios*
  Papel, cintas, tóners. . .

4.3.2 Identificación de amenazas

Se considerará todo aquello que constituya una amenaza en cualquiera de los siguientes rubros:

- ***Acceso no autorizado***: Utilizar recurso de cómputo sin previa autorización.
- ***Daño a la información***: Modificación o eliminación de la información en el sistema.
- ***Robo de información***: Acceso a cierta información sin previa autorización.
- ***Divulgación de la información***: Publicar detalles del sistema, como podrían ser las contraseñas, secretos, investigaciones, etc.
- ***Negación del servicio***: Obligar al sistema a negar recursos a usuarios legítimos.

4.3.3 Métodos de Protección

Después de que ya identificamos lo anterior, tenemos la pregunta de cómo protegemos ahora los recursos. Tal vez, ésta sea la pregunta más difícil de responder, pues, según el recurso del que se trate, será el modo de protegerlo.

Una aproximación acerca de cómo proteger los recursos de los problemas originados por el cliente interno consiste en la identificación del uso correcto de los mismos por parte de éstos.

Pero primero, deberemos saber quiénes son los que van a hacer uso de los recursos. Es decir, se debe contar, previamente, con un conocimiento cabal de todos los usuarios que tenemos en el sistema. Esta lista no es obligatoriamente individual, sino que puede ser, en

efecto, una lista por grupos de usuarios y sus necesidades en el sistema. Esta es, con seguridad, la práctica más extendida pues, definida la necesidad de un grupo de usuarios, lo más efectivo es englobarlos a todos en un mismo grupo.

Una vez identificados los usuarios (o grupos de usuarios), se puede realizar la determinación de los recursos de que harán uso y de los permisos que tendrán.

Hay que tener siempre presente que los riesgos se pueden minimizar, pero nunca eliminarlos completamente, por lo que sería recomendable planificar no sólo la prevención ante un problema sino también la recuperación si el mismo se produce; se suele hablar de medidas **proactivas** (aquellas que se toman para prevenir un problema) y medidas **reactivas** (aquellas que se toman cuando el daño se produce, para minimizar sus efectos).

4.4 Uso correcto de los recursos

El siguiente paso será el de proveer el uso aceptable del recurso. Las guías dependerán de la clase y por consiguiente de sus normas. La política que se desarrolle se llamará *política de uso aceptable* (PUA) para la red. Si el acceso a un recurso se restringe, deberá considerarse el nivel de acceso que tendrán las diferentes clases de usuarios. Las preguntas clave para el diseño de este tipo de políticas son:

- ¿Se permite irrumpir en cuentas ajenas?
- ¿Se permite adivinar contraseñas?
- ¿Se permite irrumpir el servicio?
- ¿Puede leerse un archivo ajeno cuyos permisos ante el sistema incluyen el de la lectura para todos?
- ¿Puede modificarse un archivo ajeno cuyos permisos ante el sistema incluyen el de escritura para todos?
- ¿Pueden los usuarios compartir sus cuentas?
- ¿Puede copiarse el software que no lo permita en su licencia?

La respuesta a todas estas preguntas debe ser **negativa.**

Existen dos enfoques: permisivo (todo lo que no este explícitamente prohibido está permitido) y prohibitivo (todo lo que no esté explícitamente permitido está prohibido). La elección dependerá del tipo de organización y el nivel de seguridad que esta requiera.

4.5 Determinar responsabilidades del usuario

Para la creación de políticas, en donde el usuario es el principal actor, se deben considerar algunos de los siguientes aspectos, con los cuales queden establecidos los lineamientos a seguir.

- Guías respecto al uso de recursos de red en caso de que los usuarios estén restringidos y cuáles son las restricciones.
- Lo que constituye abuso en los términos del uso de los recursos de red que afectan el desempeño del sistema y la red.
- ¿Podrán los usuarios compartir sus cuentas o permitir a otros utilizarlas?

- ¿Deberán los usuarios revelar sus contraseñas de manera temporal para permitir a quienes trabajan en un proyecto al acceso a sus cuentas?
- ¿Con qué frecuencia deberían cambiar sus contraseñas los usuarios y cualesquiera otras restricciones de contraseñas o requerimientos?
- ¿Son responsables los usuarios de brindar respaldo de sus datos o es responsabilidad del sistema?
- Consecuencias para los usuarios que divulgan información que podría ser propietaria.
- Una declaración sobre la privacidad de correo electrónico.
- Una política sobre comunicaciones electrónicas como falsificación de correo.

4.6 Determinar responsabilidades de los administradores del sistema

Cuando ocurren las amenazas a la seguridad de la red, el administrador del sistema podrá examinar los directorios y archivos privados del usuario para el diagnóstico del problema hasta cierto límite estipulado por la política del sistema de red. Las preguntas clave para diseñar las políticas de este tipo son:

- ¿Quién debe tener privilegios de administrador? Debe utilizarse el principio del mínimo privilegio: Proporcionar sólo los privilegios suficientes para ejecutar las tareas necesarias.
- ¿Cuáles son los derechos y responsabilidades de los administradores?
- ¿Pueden monitorear o leer los archivos de los usuarios?
- ¿Tienen derecho a examinar el tráfico de una máquina en específico?
- ¿Tienen derecho a examinar el tráfico de toda la red?
- ¿A qué grado pueden hacer uso de sus privilegios?
- ¿Qué tanto deberán respetar la privacidad de los usuarios?
- ¿Cómo deben resguardar su contraseña?
- ¿Cómo debe manejarse la información sensitiva?
- Debe evitarse que los usuarios almacenen información valiosa en sistemas poco seguros.

4.7 Detección y vigilancia de actividad no autorizada

4.7.1 Monitoreo del sistema

Esta garantiza un buen control de la red. Vigilar las actividades que se producen en el sistema y sus procesos, es una medida muy importante, ya que es difícil que un intruso ataque la primera vez que entra. Con esta medida de prevención podrían atraparse a la mayoría de los atacantes, si hay una persona controlando las entradas de las personas a la red y sus actividades.

4.8 Realización de la Política de Seguridad

Al realizar la Política de Seguridad se deberá tener en consideración los objetivos de la organización puesto que no se le puede dar el mismo enfoque para una Universidad que para un campo militar, y esto depende de los objetivos fundamentales de la organización.

Con base en el análisis de riesgos, delimitación de responsabilidades y auditorías consideradas necesarias, se lleva a cabo la Política de Seguridad, en donde debe quedar por escrito y en un lenguaje en el que para todas las personas involucradas sea entendible, el resultado de todo el análisis previo.

Una política debe contener los siguientes puntos:

- ✓ Ámbito de aplicación.
- ✓ Análisis de riesgos.
- ✓ Enunciados de políticas.
- ✓ Sanciones.
- ✓ Sección de uso ético de los recursos de cómputo.
- ✓ Sección de procedimientos para el manejo de incidentes.

En el diseño de políticas de seguridad, conviene seccionar el trabajo en diferentes políticas específicas a un campo (cuentas, contraseñas, control de acceso, uso adecuado, respaldos, correo electrónico, contabilidad del sistema, seguridad física, personal, etc.)

Políticas de cuentas: Establecen qué es una cuenta de usuario de un sistema de cómputo, cómo está conformada, a quién puede serle otorgada, quién es el encargado de asignarlas, cómo deben ser creadas y comunicadas. Algunos ejemplos de éstas son:

- ✓ Las cuentas deberán ser otorgadas exclusivamente a usuarios legítimos.
- ✓ Una cuenta deberá estar conformada por un nombre de usuario y su contraseña.
- ✓ El nombre deberá estar conformado por la primera letra del nombre y su apellido paterno.

Políticas de contraseñas: Son una de las políticas más importantes, ya que por lo general la contraseña es la única manera de identificarse ante el sistema y por tanto la única manera de defensa contra ataques. Estas establecen quien asignará la contraseña (longitud de la misma), qué formato debe tener y cómo será comunicada. Ejemplo:

- ✓ La longitud de las contraseñas deberá ser siempre verificada al momento de ser creada por el usuario, y debe contener al menos 7 caracteres.
- ✓ La contraseña elegida por el usuario no deberá ser una palabra de diccionario ni sencilla de adivinar, con secuencias conocidas de caracteres.

Políticas de control de acceso: Especifican cómo deben los usuarios acceder al sistema, desde dónde y de qué manera deben autenticarse. Ejemplo:

- ✓ Todos los usuarios deberán ingresar al sistema utilizando un programa que permita una comunicación segura y encriptada.
- ✓ Está prohibido acceder al sistema con una cuenta diferente de la propia, aún con la autorización del dueño de dicha cuenta.
- ✓ Si un usuario está fuera de su sitio de trabajo, debe conectarse a una máquina pública del sitio y, únicamente desde ésta, hacer la conexión a la computadora deseada.
- ✓ Al momento de conectarse el usuario al servidor se deberá desplegar la última fecha de ingreso al sistema, con lo cual se podrá detectar un ingreso no deseado al sistema.

Política de uso adecuado: Especifican lo que se considera un uso adecuado o inadecuado del sistema por parte de los usuarios, así como lo que está permitido y lo que no, dentro del sistema de cómputo. Para que el esquema de políticas de uso adecuado sea eficaz conviene realizar ciertas preguntas antes.

- ✓ ¿Se permite irrumpir en cuentas ajenas?
- ✓ ¿Se permite adivinar contraseñas?
- ✓ ¿Se permite interrumpir el servicio?
- ✓ ¿Puede leerse un archivo ajeno el cual tenga permisos para lectura para todos?
- ✓ ¿Puede modificarse un archivo que tenga los permisos para que cualquiera pueda modificarlo?
- ✓ ¿Pueden los usuarios compartir sus cuentas?
- ✓ ¿Puede copiarse el software que no lo permita su licencia?
- ✓ ¿Puede obtenerse una licencia para hackear?

Según el tipo de seguridad que se requiera se puede establecer que todo lo que no esté explícitamente permitido dentro de la política está prohibido o que todo lo que no esté prohibido estará permitido.

Después de ver esos puntos podemos ver algunos ejemplos:

- ✓ Queda estrictamente prohibido correr programas que busquen adivinar contraseñas.
- ✓ La cuenta de usuario es personal e intransferible, por lo cual no se permite que se comparta la cuenta con alguien más.
- ✓ Está prohibido hacer uso de programas que vulneren la seguridad del sistema de equipo de cómputo propio o ajeno.
- ✓ No se permite el uso de las computadoras con fines de lucro.

Política de respaldos: Especifican qué información deberá respaldarse, con qué periodicidad y en qué medio. Y en caso de ser necesario la manera en que deberá recobrarse la información.

Políticas de correo electrónico: Establece el uso adecuado como el inadecuado del servicio de correo electrónico, los derechos y obligaciones que el usuario debe hacer valer y cumplir al respecto. Ejemplos:

- ✓ El usuario es la única persona autorizada para leer su propio correo, a menos que él autorice que otra persona pueda leerlo o que su correo esté involucrado con un incidente de seguridad.
- ✓ No se deberá utilizar la cuenta de correo de la empresa para propósitos laborales ajenos a la empresa.

Políticas de contabilidad del sistema: Establecen los lineamientos bajo los cuales pueden ser monitoreadas las actividades de los usuarios del sistema de cómputo, así como la manera en que deben manejarse la contabilidad del sistema y el propósito de la misma. Ejemplos:

- ✓ Deberán ser registrados en bitácoras todos los comandos emitidos por todos los usuarios del sistema de cómputo.

- ✓ Cada semana deberá hacerse el corte de contabilidad del sistema cifrándose y respaldándose la información generada en un dispositivo de almacenamiento permanente.

Metodología del desarrollo.

Un esquema de políticas de seguridad debe llevar ciertos pasos para garantizar su funcionalidad y permanencia en la institución, por lo que se sugiere que se tengan en cuenta los siguientes pasos:

- ✓ *Preparación.*- La recopilación de todo tipo de material relacionado con cuestiones de seguridad en la organización: manuales de procedimientos, planes de contingencia, etc.
- ✓ *Redacción.*- Escribir las políticas de una manera clara, concisa y estructurada. Requiere de la labor de un equipo en que participen directivos, usuarios, administradores y abogados en caso de que sea necesario.
- ✓ *Edición.*- Reproducir las políticas de manera formal para ser sometidas a revisión y aprobación.
- ✓ *Aprobación.*- Probablemente, la parte más difícil, puesto que muchas personas se verán renuentes a aceptarlas, por lo que es fundamental el contar con el apoyo de las autoridades pertinentes.
- ✓ *Difusión.*- Dar a conocer las políticas a todo el personal mediante proyecciones de video, páginas WEB, correo electrónico, cartas compromiso, memos, pláticas informativas, etc.
- ✓ *Revisión.*- Las políticas son sometidas a revisión por un comité, que discutirá los comentarios emitidos por personas involucradas.

La política debe especificar al menos los siguientes puntos:

- ✓ ¿Quién tiene permisos para usar los recursos?
- ✓ ¿Quién esta autorizado a conceder acceso y a aprobar los usos?
- ✓ ¿Quién tiene privilegios de administración del sistema?
- ✓ ¿Qué hacer con la información confidencial?
- ✓ ¿Cuáles son los derechos y responsabilidades de los usuarios?[8]
- ✓ Manejo de la cuenta de los usuarios.
- ✓ Amenazas principales y forma de contrarrestarlas.
- ✓ ¿Qué hacer en caso de un ataque o una violación a la política de seguridad?
- ✓ Plan de auditoría.

Se deberá contemplar el seguimiento adecuado en el caso de una violación a la política e integridad de la información, así como saber cuáles son las autoridades adecuadas para denunciar un hecho dependiendo de lo que sucedió.

[8] Instituto Nacional de Estadística e Informática. *Seguridad en Redes de Datos* [en línea].Perú, 4 Abril 2000[Consulta:20 Junio 2000]. Disponible en: <http://www.inei.gob.pe/web/BiblioInei/ListaItemByTemaPalabra.asp?c=15&tt=Seguridad%20de%20la%20Informaci%C3%B3n>.p. 28.

4.9 Publicación y difusión de la política de seguridad

La publicación y difusión de la política de seguridad es una parte fundamental, porque aunque se haya realizado un eficiente análisis y por consiguiente una buena política, si no llega a los usuarios no servirá de nada.

Se debe concienciar a todos los involucrados, y primordialmente a las autoridades de la organización, tener el empuje necesario para llevarse a cabo, porque normalmente el implementar la política representa un mayor esfuerzo para las personas. En caso de que la organización ya se encuentre trabajando, en algunas ocasiones cuando se lleva mucho tiempo con un sistema las personas se acostumbran a la manera en que desarrollan su trabajo y es difícil que cambien sus hábitos por lo que el apoyo de las autoridades es imprescindible.

Por último, ya que se tiene todo el apoyo necesario, se busca o se debe elegir una o varias formas para distribuir la política de seguridad para que todos los usuarios las conozcan. Por ejemplo Internet, revistas, pancartas, etc. En el caso de los administradores y personal que estén involucrados directamente, será necesario discutirlas directamente e involucrarlos en la difusión de la misma.

Capítulo 5

Procedimientos

Los ***procedimientos*** indican el "cómo". Los procedimientos son los que nos permiten llevar a cabo las políticas.

5.1 Procedimientos preventivos

5.1.1 Monitoreo del sistema

Los servidores dedicados son máquinas especializadas en el funcionamiento de determinadas características o servicios en Internet. Cada uno de los servicios requiere que muchos procesos corran al mismo tiempo en el servidor.

Es muy posible tener cientos de procesos corriendo al mismo tiempo en un servidor. Un solo proceso que muere, puede generar que todos los usuarios se queden sin servicio. Mientras que el sistema operativo Linux es muy estable, errores de operaciones como: cgi, scripts, archivos de configuración incorrectos o instalaciones de software inadecuadas pueden generar problemas, y de vez en cuando puede colgar el sistema.

Para evitar lo anterior, se pueden tener procedimientos de verificación de accesos, de chequeo de tráfico de red, monitoreo de correo, monitoreo de conexiones activas, modificación de archivos, verificación de las máquinas de los usuarios, de monitoreo de los puertos.

- Procedimientos de verificación de accesos.

  Debe explicar la forma de realizar las auditorías de los archivos logísticos de ingresos a fin de detectar actividades anómalas. También debe detectar el tiempo entre la auditoría y cómo actuar en caso de detectar desviaciones.

  Normalmente, este trabajo es realizado por programas a los que se les dan normativas sobre qué y cómo comparar. *Scanean* archivos de "*log*" con diferentes fechas tomando en cuenta las reglas que se le han dado. Ante la detección de un desvío, generan reportes informando el mismo.

  En el procedimiento debe quedar perfectamente indicado quién es el responsable del mantenimiento de estos programas y cómo se actúa cuando se generan alarmas.

- Procedimiento para la verificación del tráfico en la red.

  Permite conocer el comportamiento del tráfico en la red, al detectar variaciones que pueden ser síntoma de mal uso de la misma.

  El procedimiento debe indicar el/los programas que se ejecuten, con qué intervalos, con qué reglas de trabajo, quién se encarga de procesar y/o monitorear los datos generados por ellos y cómo se actúa en consecuencia.

- Procedimiento para el monitoreo de los volúmenes de correo.

  Este procedimiento permite conocer los volúmenes del tráfico de correo o la cantidad de "mails" en tránsito. Dicho procedimiento se encuentra realizado por programas que llevan las estadísticas, generando reportes con la información pedida. El conocimiento

de esta información permite conocer, entre otras cosas, el uso de los medios de comunicación, y si el servidor está siendo objeto de un "spam".

Como en los casos anteriores, en el procedimiento debe estar de manera explícita quién es el encargado del mantenimiento y del análisis de los datos generados, y qué hacer cuando se detectan variaciones.

- Procedimientos para el monitoreo de conexiones activas.

  Este procedimiento se efectúa con el objeto de prevenir que algún usuario deje su terminal abierta y sea posible que alguien use su cuenta. El procedimiento es ejecutado por medio de programas que monitorean la actividad de las conexiones de usuarios.

  Cuando detecta que una terminal tiene cierto tiempo inactiva, cierra la conexión y genera un *log* con el acontecimiento.

- Procedimiento de modificación de archivos.

  Este procedimiento sirve para detectar la modificación no autorizada y la integridad de los archivos y, en muchos casos, permite la traza de las modificaciones realizadas. Al igual que en los casos anteriores, debe estar bien determinada la responsabilidad de quién es el encargado del seguimiento y de actuar en caso de alarmas.

- Procedimientos para la verificación de las máquinas de los usuarios.

  Este procedimiento permitirá encontrar programas que no deberían estar en las máquinas de los usuarios y que, por su carácter, pueden traer problemas de licencias y fuente potencial de virus. El procedimiento debe expresar claramente los métodos que se van a utilizar para la verificación, las acciones ante los desvíos y quién/quiénes lo llevarán a cabo.

- Procedimientos para el monitoreo de los puertos en la red.

  Este procedimiento permite saber qué puertos están habilitados en la red y, en algunos casos, verificar la seguridad de los mismos. El procedimiento deberá describir qué programas se deben ejecutar, con qué reglas, quién estará a cargo de llevarlo a cabo y qué hacer ante las desviaciones detectadas.

5.1.2 Revisión de bitácoras

Es muy importante que la información que viene de 'syslog' no haya sido comprometida. Un buen comienzo es hacer legibles y escribibles los archivos en '/var/log' sólo para un número limitado de usuarios.

Hay que revisar lo que se obtiene escrito ahí, especialmente bajo la facilidad 'auth'. Múltiples fallos de conexión, por ejemplo, pueden indicar un intento de asalto.

Dónde buscar el archivo de *log* dependerá de la distribución. En un sistema Linux que se conforma al "Linux Filesystem Standard", tal como RedHat, habrá de buscarse en '/var/log' y comprobar 'messages', 'mail.log' y otros.

Se puede averiguar hacia dónde se está conectando la distribución mirando en el archivo '/etc/syslog.conf'. Este es el archivo que le dice a 'syslogd' (el demonio de conexión de sistema) dónde registrar los diversos mensajes.

Si los archivos de *log* han sido estropeados, hay que ver si se puede determinar cuándo empezó el estropicio y qué tipo de cosas parecen estar estropeadas. ¿Hay grandes períodos de tiempo de los que no se puede responder? Una buena idea es comprobar las cintas de seguridad (si se tiene alguna) por si tienen archivos de *log* no estropeados.

Los archivos de *log* normalmente son modificados por el intruso para tapar sus huellas, pero aún así deben ser comprobados en busca de acontecimientos extraños. Se puede tener noticia de los intentos del intruso para lograr entrar, o de explotar un programa para obtener la cuenta del root. Se podrían ver también registros de entradas antes de que el intruso tenga tiempo de modificarlas.

Se debe separar la facilidad 'auth' de otros datos de *log*, incluyendo los intentos de cambio de usuarios usando 'su', los intentos de conexión y otra información de contabilidad del usuario.

Si es posible, se debe configurar 'syslog' para enviar una copia de los datos más importantes a un sistema seguro. Esto impedirá que un intruso encubra sus huellas borrando sus intentos de login, su, ftp, etc.

Finalmente, los archivos de *log* son mucho menos útiles cuando nadie los lee. Hay que tomarse algún tiempo de vez en cuando para mirar los archivos de 'log' y hacerse una idea de cual es el comportamiento que tienen en un día normal. Saber esto puede ayudar a notar las cosas inusuales.

5.1.3 Respaldos

Existen acontecimientos de los que puede resultar muy difícil protegerse como son los desastres naturales, y únicamente se podrá seguir una serie de pasos para evitar que su incidencia sea lo menor posible. La mejor solución es mantener un buen conjunto de copias de seguridad (respaldos) sobre toda la información necesaria del sistema. Hay que pensar que las copias de seguridad no sólo protegen de desastres naturales, sino también de los desastres que pueda ocasionar algún intruso en el sistema, de cualquier ataque a la disponibilidad o integridad de la información del sistema.

Si los datos tienen un tamaño inferior a 650Mb, puede ser una buena opción grabarlos en un CD, bien permanente (ya que es más difícil de falsificar con posterioridad, y si están almacenados de forma adecuada pueden durar mucho tiempo) o regrabable. Las cintas y otros medios sobre los que se puede escribir deberían protegerse tan pronto como se completa la copia y se verifica para evitar la falsificación. Hay que tener cuidado y almacenar la copia de seguridad en un sitio seguro. Una buena copia de seguridad da la posibilidad de restaurar el sistema.

Hay que insistir en la seguridad de las copias de seguridad. Si las copias de seguridad no están almacenadas en un sitio seguro, puede que el posible intruso no tenga necesidad de idear métodos sofisticados para obtenerla, sólo le basta con copiar o sustraer un CD.

¿Qué se debe respaldar?

Cada centro de cómputo tiene distintas necesidades y prioridades. Cada uno de ellos debe implementar un sistema de respaldos adecuado a sus políticas y necesidades. En general, se recomienda respaldar todo.

Características de las copias de seguridad.

Cuando se realice una copia de seguridad es conveniente seleccionar un método que garantice la conservación de las características de la información como son: derechos y permisos. Si se realiza una copia de seguridad de una forma o sobre un soporte que no contemple esta posibilidad, si tenemos que restaurar los datos sobre el sistema, el resultado sobre la seguridad y funcionalidad globales puede ser impredecible.

¿Cuándo se debe respaldar?

La periodicidad con la que se debe respaldar la información depende principalmente de su importancia y de qué tan a menudo cambie. Los directorios que suelen cambiar más frecuentemente, son los que almacenan información de los usuarios y su correo electrónico.

¿Se está respaldando bien?

Es de vital importancia revisar que los respaldos sean recuperables. Se recomienda hacer pruebas para verificar que la información efectivamente se puede restaurar.

Copiar las Bases de Datos del Sistema.

Existe cierta información del sistema que es imprescindible para su correcto funcionamiento. Es conveniente tener una copia de estos archivos en una ubicación segura. En particular, resulta conveniente tener una copia del contenido del directorio /etc. También hay que mantenerla en lugar seguro, ya que tiene copias de los archivos /etc/passwd y /etc/shadow, entre otros que puedan contener claves de usuarios que no están cifradas.

También en cada sistema se puede tener una base de datos de las aplicaciones que hay instaladas en el servidor. Cada distribución dispone de alguna herramienta que realiza el mantenimiento de la base de datos a la misma vez que instala o desinstala aplicaciones. La pérdida de esta base de datos haría perder el control sobre qué aplicaciones se tienen instaladas.

En muchas situaciones también será necesario tener copia de seguridad de los archivos de registro de incidencias, para tener constancia de las distintas actividades del sistema.

- Procedimientos para el resguardo de copias de seguridad

  Estos procedimientos deben indicar claramente dónde se deben guardar las copias de seguridad y los pasos a seguir en caso de problemas. Para lograr esto, deben estar identificados los roles de las personas que interactúan con el área, a fin de que cada uno sepa qué hacer ante la aparición de problemas.

5.1.4 Parches del sistema

Conforme pasa el tiempo, nuevos errores de programación se van encontrando en prácticamente todos los programas. Muchas veces, estos errores se ven reflejados en vulnerabilidades que pueden comprometer el sistema completo. Es por tanto, indispensable mantenerse al día con los parches.

El Red Hat Package Manager (RPM), es un sistema de gestión de paquetes que puede ser utilizado por cualquiera y funciona sobre la plataforma RedHat Linux como otras distribuciones de sistemas Linux y Unix. Red Hat, Inc. anima a otros distribuidores a tomar en consideración el uso de RPM para los propios productos. RPM puede distribuirse según los términos de la licencia GPL.

La instalación, la desinstalación y la actualización de los paquetes RPM son operaciones que requieren una sola línea de comandos. RPM contiene una base de datos de paquetes instalados y de sus archivos, que permitirá efectuar cualquier tipo de verificación y de consulta del sistema.

Durante la actualización de un paquete, RPM administra los archivos de configuración de manera que no se pierda su personalización - es una característica difícil de obtener con los paquetes del formato *.tar.gz*.

RPM proporciona un modo para producir automáticamente los paquetes que contienen la versión del software en código fuente y en versión compilada. El proceso de instalación del paquete se basa en un único archivo de configuración. La filosofía utilizada por RPM simplifica notablemente el mantenimiento de los paquetes y la creación automática de nuevas versiones.

Objetivos de RPM

Antes de utilizar RPM, puede ser útil una idea de cuales son los objetivos que se pretenden alcanzar.

Actualización.

> Con RPM se puede efectuar la actualización de paquetes únicos sin tener que reinstalar todo el sistema operativo. Cuando se encuentra una nueva versión de un sistema operativo basado en RPM (como por ejemplo, Red Hat Linux), no es necesario reinstalar todo el sistema operativo (como ocurriría con los sistemas operativos basados en otros sistemas de paquetes). RPM permite efectuar una actualización del sistema en tiempo real, de forma inteligente y completamente automática. Los archivos de configuración están protegidos durante las actualizaciones, de modo que no se pierde su personalización.

Consultas potentes y eficaces.

> RPM ha sido proyectado para tener potentes opciones de consultas. Se puede efectuar búsquedas a través de la base de datos para encontrar paquetes o también archivos solos. Se puede saber con gran facilidad a qué paquete pertenece un archivo, o bien su procedencia. Los archivos contenidos en un paquete RPM se encuentran en archivos comprimidos, con un encabezado binario personalizado

que ofrece importante información sobre el paquete mismo y sus contenidos, permitiéndole consultar a cada uno de los paquetes de manera fácil e inmediata.

Sistema de verificación.

Otra caracteristica importante es la capacidad de verificar los paquetes. Si se ha eliminado un archivo importante o algunos paquetes, simplemente se verifica el paquete. Se indicará cualquier anomalía. Si es necesario, se podrá reinstalar el paquete. Cada archivo de configuración que se haya modificado será protegido durante la fase de reinstalación.

Fuente original.

Un objetivo crucial es aquel que le permite el uso del código fuente originario del software, así como ha sido distribuido por los programadores. Con RPM se tiene la posibilidad de visualizar los códigos fuente originales junto a los recorridos y las instrucciones que han sido utilizadas. Esto es seguramente una gran ventaja por diversas razones. Ante todo, si es publicada una nueva versión de un programa, no tiene necesariamente que partir de cero para compilarlo. Se puede revisar la ruta para ver que es lo que se tiene que hacer. De este modo, todas las selecciones por defecto y todos los cambios ejecutados para "construir" debidamente el programa, son claramente visibles.

5.1.5 Información Actualizada

El mantener la información del sistema al día, no es una tarea sencilla, debido a que surgen nuevas herramientas de seguridad, una nueva versión del sistema operativo, etc. Sin embargo, existen diferentes medios por los cuáles la gente encargada de la seguridad del sistema, puede saber lo que ha sucedido, está ocurriendo u ocurrirá. Se cuenta con revistas, libros, periódicos, y uno de los medios que ofrece más información, el Internet.

5.1.5.1 Listas de correo

El correo electrónico es el medio predilecto de discusión de varios temas. La mayor parte de las conversaciones entre desarrolladores y usuarios del sistema operativo Linux se gestiona a través de varias ***listas de correo.***

Las ***listas de correo*** son una aplicación que envía automáticamente correo a un grupo determinado de usuarios. Son muy utilizadas para mantener informado a los miembros sobre las noticias de algún área de interés para ellos. Para estar dentro de la base de datos de una lista de correos normalmente es necesario suscribirse a la misma.

En la Tabla 5.1 se describe la clasificación de las listas de correo:

CON RESPECTO A:	LA LISTA SE PUEDE CLASIFICAR EN:
Forma de suscripción o alta	1. **Directa:** en donde todos los que se suscriben ingresan directamente. 2. **Indirecta:** en donde todos los que se suscriben, requieren de la aprobación del moderador.
Forma de remoción, desuscripción o baja	1. **Voluntaria:** Es cuando el suscripto decide apartarse de la lista. 2. **Involuntaria.** Aquí el moderador de la lista, en razón de considerar necesario el alejamiento de un suscripto, puede proceder a su remoción, ya sea transitoria o permanente, razón de una sanción o por haber concluido el período de suscripción.
Quienes pueden enviar correos	1. **Abierta:** Cualquiera que conozca la dirección de la lista. 2. **Cerrada:** Solamente los suscriptos. 3. **Cerrada al Moderador:** Solamente el moderador.
Distribución de los correos en la lista	**a) En cuanto a la distribución en sí:** 1. **Directa (Lista No Moderada).** Se envía el correo y llega a la lista. 2. **Indirecta (Lista Moderada).** Se envía el correo, el moderador lo aprueba, y se distribuye. **b) En cuanto al correo a distribuir:** 1. **Individual** (Cada correo es distribuido en forma propia) 2. **Colectiva** (Los correos son seleccionados, compilados y se les distribuye en forma de digesto(*obra jurídica*) o informe)

Respuesta del correo	La respuesta del correo que se distribuye a la lista puede ser dirigido: 1. A la Lista, por lo que es recibido por todos los suscriptos. 2. Al emisor, por lo que es recibido por quien envió el correo a la lista.

Tabla 5.1. Clasificación de las listas de correo.

Cabe resaltar que las listas de correo más comunes son:

- **Lista de correo moderada.**

  Lista de distribución en la cual los mensajes, antes de ser distribuidos, son filtrados manualmente por uno o más moderadores.

- **Lista de correo no moderada.**

  Lista de distribución en la cual los mensajes son enviados directamente a todos los inscritos, sin control por parte de moderadores.

Existen dos formas de suscribirse a una lista de correo:

- **Vía E-mail:**

  Para suscribirse a la lista de correo, simplemente se envía un mensaje con la palabra "subscribe" en el campo Subject:, el e-mail se deberá dirigir a la dirección de peticiones de esa lista.

  Para suscribirse al *digest*:

  El *digest* envía todos los mensajes de una sola vez, en un solo mensaje grande, en lugar de enviarlos uno por uno de manera individual. Para suscribirse al digest, se hace lo mismo que en el caso anterior.

- **Vía Web:**

  Usando un formulario del sitio.

Para desinscribirse de las listas de correo, se tienen dos alternativas:

- **Vía E-mail:**

  Para desinscribirse de la lista de correo, simplemente se envía un mensaje con la palabra "unsubscribe" en el campo Subject:, el e-mail se deberá dirigir a la dirección de peticiones de esa lista.

Para el *digest* se realiza de la misma forma.

- **Vía Web:**

  Usando un formulario del sitio.

A continuación mencionaremos algunas de las principales listas de correo:

LISTA	MANERA DE SUSCRIBIRSE	DESCRIPCIÓN
Bugtraq	Enviar un correo a: **listserv@lists.securityfocus.com** Indicando en el cuerpo del mensaje: **'subscribe bugtraq *nombre*'**	Es la lista de seguridad informática más importante que existe en la actualidad. Es imprescindible suscribirse, especialmente si se es administrador de Sistemas Unix. Se explican los problemas del sistema, su solución, su potencial, explotación por parte de un cracker. Análisis de vulnerabilidades y agujeros de seguridad, cómo explotarlos y cómo solucionarlos.
Best of Security	Enviar un correo a: **best-of-security-request@suburbia.net** Indicando en el cuerpo del mensaje: **'subscribe best-of-security'**	Lista con un gran volumen de tráfico donde se trata de sacar a la luz cualquier problema de seguridad en el mínimo tiempo posible, muchas veces con mensajes duplicados o reenvíos directos de otras listas; no es moderada.
Linux Security	Enviar un correo a: **linux-security-request@redhat.com** Indicando en el Subject: **'subscribe'**	Lista sin mucho tráfico en la que se tratan problemas de seguridad específicos de Linux.

Linux Alert	Enviar un correo a: **linux-alert-request@redhat.com** Indicando en el Subject: **'subscribe'**	Lista similar a la anterior, pero donde se envían problemas de seguridad urgentes (alertas) relativos a Linux. Generalmente, los mensajes sobre seguridad en Linux, pasan por bugtraq o Linux Security.
Computer Privacy Digest	Enviar un correo a: **comp-privacy-request@uwm.edu** Indicando en el cuerpo del mensaje: **'subscribe cpd'**	Lista moderada donde se tratan temas relacionados con la tecnología y la privacidad.
Computer Underground Digest	Enviar un correo a: **cu-digest-request@weber.ucsd.edu** Indicando en el cuerpo del mensaje: **'sub cudigest'**	En esta lista se trata cualquier tema relativo al *underground* informático.
Firewalls	Enviar un correo a: **majordomo@lists.gnac.net** Indicando en el cuerpo del mensaje: **'subscribe firewalls'**	En esta lista de correo se discuten temas relacionados con los firewalls y sus implicaciones de seguridad.
Intrusion Detection Systems	Enviar un correo a: **majordomo@uow.edu.au** Indicando en el cuerpo del mensaje: **'sub ids'**	Lista muy interesante, dedicada a discutir aspectos relativos a los sistemas de detección de intrusos. Algunos posibles tópicos son: técnicas usadas para detectar intrusos en sistemas y redes de cómputo; métodos usados por intrusos, políticas de sistemas de cómputo.

CERT	Enviar un correo a: **cert@cert.org** Indicando en el cuerpo del mensaje: **'I want to be on your mailing list'**	Lista del CERT, con muy poco tráfico. En general, poco útil, ya que cualquier problema de seguridad es tratado mucho antes en otros foros de discusión.
WWW Security	Enviar un correo a: **www-security-request@nsmx.rutgers.edu** Indicando en el cuerpo del mensaje: **'subscribe www-security *direccion_de_correo*'**	Lista moderada dedicada a la seguridad de los servidores Web.
Alert	Enviar un correo a: **mayordomo@iss.net** Indicando en el cuerpo del mensaje: **'subscribe alert'**	Lista moderada en la que se tratan vulnerabilidades, intrusiones, productos y herramientas de seguridad.
Risks	Enviar un correo a: **risks-request@csl.sri.com** Indicando en el cuerpo del mensaje: **'subscribe'**	Lista dedicada a la discusión de los riesgos que implican las nuevas tecnologías en la sociedad moderna.
University Info Security Forum	Enviar un correo a: **listserv@cuvmc.ais.columbia.edu** Indicando en el cuerpo del mensaje: **'subscribe uninfsec'**	Lista no moderada donde se trata cualquier tema relacionado con la seguridad informática en entornos de educación o I+D.
	Enviar un correo a: **majordomo@cs.yale.edu**	En esta lista se tratan temas relativos a la evaluación y evaluación legal de diferentes

Sneakers	Indicando en el cuerpo del mensaje: 'subscribe sneakers'	mecanismos de seguridad en redes, especialmente de firewalls.
Cypherpunks	Enviar un correo a: majordomo@toad.com Indicando en el cuerpo del mensaje: 'subscribe cypherpunks-unedited'	Lista con un gran volumen de mensajes dedicada a la discusión técnica de la privacidad personal en la red.
Cryptobytes	Enviar un correo a: majordomo@rsa.com Indicando en el cuerpo del mensaje: 'subscribe cryptobytes'	Lista sobre criptografía, de Cryptobytes (RSA), con un escaso volumen de mensajes.
Stegano-L	Enviar un correo a: stegano-l-request@as-node.jena.thur.de Indicando en el cuerpo del mensaje: 'sub stegano-l direccion_de_correo'	Lista dedicada a la esteganografía.
esCERT	Para suscribirse hay que visitar la siguiente dirección: http://listserv.rediris.es/archives/cert-es.html	Lista abierta y moderada de IrisCERT, en español, donde se tratan problemas de seguridad genéricos en redes y sistemas operativos.
Cripto Foro	Enviar un correo a: cripto_foro-request@fi.upm.es Indicando en el cuerpo del mensaje: 'subscribe cripto_foro'	Esta lista presenta un foro de discusión sobre temas relacionados con el cifrado de datos en España. No se suelen plantear dudas de carácter técnico, sino más bien se habla de conferencias, convenciones.

Hacking	Enviar un correo a: majordomo@argo.es Indicando en el cuerpo del mensaje: 'subscribe hacking'	Lista moderada de hacking en español.

Tabla 5.2. Listas de correo.

La Dirección General de Servicios de Cómputo Académico (DGSCA) de la UNAM a través del Departamento de Seguridad de Cómputo (DSC) administra listas de correo. En la Tabla 5.3 se mencionan algunas listas relacionadas con la seguridad:

LISTA	MANERA DE SUSCRIBIRSE	CORREO ELECTRÓNICO	DESCRIPCIÓN
Gasu	Visitar la siguiente dirección: http://www.seguridad.unam.mx/mailman/listinfo/gasu	Si desea enviar un mensaje a los miembros de la lista, escriba a: gasu@ds5000.seguridad.unam.mx	**Lista del Grupo de Administración y Seguridad en sistemas UNIX.** Dentro de esta lista se discute todo lo relacionado con seminarios GASU, tópicos de seguridad y administración de cualquier UNIX (IRIX, Linux, Debian, HP-UX, Solaris, FreeBSD, etc.). Lista cerrada.
Mx-Seguridad	Visitar la siguiente dirección: http://www.seguridad.unam.mx/mailman/listinfo/mx-seguridad	Si desea enviar un mensaje a los miembros de la lista, escriba a: mx-seguridad@ds5000.seguridad.unam.mx	**Lista de Tópicos de Seguridad en Cómputo.** Lista que discute los aspectos más importantes relativos a la seguridad en cómputo en nuestro país y a nivel mundial. En ella se podrán encontrar los tips, casos de seguridad que más impacto tienen en el campo de las Tecnologías de la Información. Lista cerrada.

Cert-avisos	Visitar la siguiente dirección: http://www.seguridad.unam.mx/mailman/listinfo/cert-avisos	Si desea enviar un mensaje a los miembros de la lista, escriba a: cert-avisos@www.seguridad.unam.mx.	**Lista de Boletines y Avisos del Departamento de Seguridad en Cómputo y UNAM-CERT.** Dentro de dicha lista se mantendrá información de los más de 110 Equipos de Respuesta a Incidentes de seguridad distribuidos en el mundo y del cual UNAM-CERT forma parte. Lista abierta.
Lassi	Visitar la siguiente dirección: http://www.seguridad.unam.mx/mailman/listinfo/lassi	Si desea enviar un mensaje a los miembros de la lista, escriba a: lassi@ds5000.seguridad.unam.mx.	Dentro de esta lista se discuten diversos tópicos relativos a los principios de una cultura de una buena Administración y Seguridad en todos los servicios que se configuran en los equipos UNIX. Lista cerrada.

Tabla 5.3. Listas de correo en la UNAM.

5.2 Procedimientos correctivos

5.2.1 Acciones cuando la seguridad ha sido violada

El enfoque que se ha venido trabajando, siempre es mejorar la seguridad y tratar de que nunca se llegue a situaciones correctivas; sin embargo, hablar de una seguridad perfecta o de los usuarios ideales es imposible, se debe contemplar qué hacer cuando se viole la seguridad.

5.2.1.1 Respuesta a las violaciones de la política

El incidente más sencillo que pueda ocurrir es una infracción a la política de la seguridad. Cuando suceda esto se debe investigar por que sucedió. La violación se puede deber a negligencia, error accidental, desconocimiento de la misma o falta de entendimiento de la misma; es importante determinar la causa para poder tomar las medidas adecuadas para que no vuelva a ocurrir.

En general, se puede definir que hacer en los siguientes pasos:

1. Investigar quién llevó a cabo esta violación.
2. Investigar cómo y por qué ocurrió esta violación.

3. Aplicar una acción correctiva (disciplinaria).
4. ¿Qué sucede si un usuario local viola las políticas de un sitio remoto?
5. Debe haber acciones a seguir bien definidas con respecto a los usuarios locales.
6. Debe estarse bien protegido en contra de posibles acciones desde el sitio remoto.

La violación de la política de seguridad normalmente se realiza por usuarios locales, los cuales tienen conocimientos de la misma por lo que las medidas disciplinarias normalmente serán internas.

5.2.1.2 Respuesta a un ataque al sistema

En caso de detectar un ataque que está actualmente en curso, primero se debe identificar el tipo de ataque: si es local o externo.

Si el ataque es local primero se debe verificar la identidad del atacante. No conviene sacar conclusiones precipitadas y culpar a alguien de atacar el sistema, cuando sólo puede que sea una negligencia a la hora de seleccionar una clave o abandonar abierta una consola. Hay que verificar el origen de la conexión, los registros del sistema y los procesos que tiene activos. Se tendrá que comprobar si son los habituales y qué es lo que se sale de lo normal. Después dirigirse a esa persona, por teléfono o personalmente, para preguntar qué está haciendo y pedir que cese en la actividad. Si no tiene una conexión activa y no tiene idea de lo que se está diciendo, habrá que profundizar en la investigación porque cabe la posibilidad de que alguien haya utilizado esa cuenta de forma ilegítima. Si reconoce el incidente, que le informe de los mecanismos que ha utilizado, las acciones que ha realizado y actúe en consecuencia.

Para el caso de que sea externo, existen dos estrategias de respuesta ante un incidente de seguridad:[1]

a) Proteger y proceder.
b) Perseguir y procesar.

La primera de estas estrategias, ***proteger y proceder***, se suele aplicar cuando la organización es muy vulnerable o el nivel de los atacantes es elevado; la filosofía es proteger de manera inmediata la red y los sistemas y restaurar su estado normal, de forma que los usuarios puedan seguir trabajando normalmente. Se busca desconectar el interfaz de red si es posible desde la cual esta atacando. Si no fuera posible desconectar el interfaz, deberíamos usar algún filtro para las conexiones procedentes de la dirección del atacante por medio de un programa. Evitando los paquetes procedentes de esa dirección. También se debe cerrar la cuenta del usuario e identificar qué procesos esta ejecutando para acabar con aquellos que puedan estar dañando al sistema. Seguramente será necesario interferir de forma activa las acciones del intruso para evitar más accesos, y analizar el daño causado.

La principal desventaja de esta estrategia es que el atacante se da cuenta rápidamente de que ha sido descubierto, y puede emprender acciones para no ser identificado, lo que incluso conduce al borrado de *logs* o de sistemas de archivos completos; incluso puede cambiar su estrategia de ataque a un nuevo método, y seguir comprometiendo al sistema. Sin embargo, esta estrategia también presenta una parte positiva: el bajo nivel de conocimientos de los atacantes en sistemas habituales hace que en muchas ocasiones se limiten a abandonar su

[1] Karanjit Siyan and Chris Hare. *Internet y seguridad en redes*. Prentice Hall, 1995.

ataque y dedicarse a probar suerte con otros sistemas menos protegidos en otras organizaciones.

Aunque, también se debe contemplar la posibilidad de que en los próximos minutos el atacante lo intente de nuevo, pero usando una cuenta diferente y/o una dirección diferente, por lo cual vale la pena estar alertas.

La segunda estrategia de respuesta, *perseguir y procesar*, adopta la filosofía de permitir al atacante proseguir sus actividades, pero de forma controlada y observada por los administradores, de la forma más discreta posible. Con esto, se intentan guardar pruebas para ser utilizadas en la segunda parte de la estrategia, la de acusación y procesamiento del atacante (ya sea ante la justicia o ante los responsables de la organización, si se trata de usuarios internos).

Evidentemente se corre el peligro de que el intruso descubra su monitorización y destruya completamente el sistema, así como que los resultados no se tengan en cuenta ante un tribunal debido a las artimañas legales que algunos abogados aprovechan; la parte positiva de esta estrategia es, aparte de la recolección de pruebas, que permite a los responsables conocer las actividades del atacante, qué vulnerabilidades de la organización ha aprovechado para atacarla, cómo se comporta una vez dentro, etc. De esta forma se puede aprovechar el ataque para reforzar los puntos débiles de los sistemas.

Es importante determinar un poco más acerca del ataque, como si se es el destino del ataque o sólo un punto intermedio, que dado el caso se deberá notificar al administrador del destino del ataque y conservar todas las pruebas existentes.

Una vez que el incidente ha terminado o bien se detectó cuando ya había ocurrido, se pueden tomar medidas más duraderas.

Se debe tratar de dejar el sistema mejor que como estaba antes de que ocurriera el incidente, puesto que se debe contemplar ahora la forma en que se atacó el sistema.

Se deberán analizar cuidadosamente los archivos de registro del sistema. En ellos debería haber una información valiosa para seguir la pista de las actividades del intruso en la máquina. Las causas más habituales son una mala configuración de algún servicio, un programa defectuoso o la negligencia de algún usuario con respecto a su clave de acceso. Hay que comprobar por los cauces más conocidos, que en el caso de Linux se pueden encontrar en la página recursos sobre seguridad bajo Linux.

Si no elimina al atacante, probablemente volverá. No sólo a la máquina, sino a cualquier otra de la red. Durante sus incursiones ha podido utilizar algún *sniffer* (programa que escucha el tráfico en la red), y disponer de información suficiente para tener acceso a otras máquinas locales.

Si sospecha que el atacante ha obtenido copias de los archivos importantes en el sistema, sería conveniente modificar las contraseñas de los usuarios. Si tiene distintos usuarios en la máquina, hay que obligarlos a cambiar su clave. En general, es preferible cambiar siempre las claves después de un incidente, una vez que se sepa que se hace de una forma segura.

Se necesita verificar si se han modificado las limitaciones de acceso a distintas herramientas de administración remota como *linuxconf*. Puede que el atacante trate de abrir alguna puerta trasera para continuar aprovechándose de las máquinas.

Por último, se debe hacer una revisión de las políticas y herramientas de seguridad después del ataque, considerando las siguientes preguntas:

¿Se tenía contemplado un ataque con esas características?
¿Son suficientes las medidas de seguridad actuales para ese tipo de ataque?
¿Cuál es el mayor daño que pudo haber causado?
¿Cuáles son las medidas pertinentes para minimizar el riesgo?

5.2.1.3 Organizaciones externas

También se debe analizar los enfoques legales para ver la posibilidad de llevar el incidente a otras instancias. El Código Penal Federal tiene un apartado de revelación de secretos y acceso ilícito a sistemas y equipos de informática (artículos 210 y 211), en donde especifica las sanciones por delitos informáticos dependiendo de lo que hizo el atacante o la institución afectada. Por ejemplo, en caso de que la organización afectada sea de carácter financiero las sanciones son más severas.

El proceso en caso de proceder legalmente empieza presentando una denuncia ante la autoridad competente. Esta autoridad decidirá si las acusaciones deberán ser investigadas y qué cargos (si los hay) se deben hacer.

En caso de que proceda la investigación se llevará a cabo una investigación en la cual será difícil encontrar al culpable, puesto que es poco probable que la actividad se repita, o si los responsables lo hicieron desde el extranjero puede resultar muy difícil llevarlos a un tribunal.

En México, se cuentan con algunas organizaciones encargadas de la seguridad informática, entre ellas se encuentran:

- **Instituto Nacional de Estadística, Geografía e Informática (INEGI)**

  El INEGI tiene la responsabilidad de coordinar los Sistemas Nacionales Estadísticos y de Información Geográfica de México, además de promover y orientar el desarrollo informático en el país.

  El INEGI fue creado por decreto presidencial el 25 de enero de 1983, e integró en su estructura a las direcciones generales de Estadística (instituida en 1882) y de Geografía (fundada en 1968), lo que la convierte en una Institución con gran tradición en captar, procesar y difundir información estadística y geográfica de México. Además, el INEGI cuenta con una infraestructura a nivel nacional, conformada por 10 direcciones regionales y 32 coordinaciones estatales, que le permite monitorear y atender requerimientos de información en las distintas zonas del país.

  Las principales direcciones con las que cuenta el INEGI son:

- Dirección General de Estadística.
- Dirección General de Contabilidad Nacional, Estudios Socioeconómicos y Precios.
- Dirección General de Geografía.
- Dirección General de Cartografía Catastral.
- Dirección General de Política Informática.
- Dirección General de Difusión.
- Coordinación Administrativa.

La Dirección General de Política Informática es la responsable de integrar y dar seguimiento al Programa de Desarrollo Informático de México. Por lo tanto, es la encargada de impulsar y fomentar el uso de la informática entre los diversos sectores del país, tanto a nivel nacional como entre los estados y municipios. Además, proporciona el apoyo de informática para todas las áreas del Instituto.

El INEGI tiene entre sus principales objetivos, orientar la política informática en la Administración Pública Federal; promover el mejor aprovechamiento de esta tecnología en las oficinas estatales y municipales; y además, administrar su propio parque informático para estar en posibilidad de satisfacer las demandas de información proveniente de los diversos sectores sociales.

El gran desarrollo registrado en las tecnologías de información ofrece ahora una gran versatilidad en el procesamiento, consulta y difusión de la información estadística y geográfica. Esto es particularmente relevante en nuestros días, cuando la propia dinámica de las sociedades genera significativos volúmenes de datos cuya oportuna disponibilidad resulta de suma utilidad para la toma de decisiones.

En atención a que el INEGI es la institución responsable de definir la política informática gubernamental, le corresponde también proporcionar asesoría en materia de adquisiciones y empleo de equipos de cómputo a las entidades públicas que así lo requieran.

Adicionalmente alienta y apoya la elaboración de los Programas Institucionales de Desarrollo Informático (PIDI) de las mismas entidades con el propósito de racionalizar y orientar el gasto en este rubro.

Asimismo, intensificó sus esfuerzos de intercambio de experiencias a nivel central y como resultado emprendió la creación del Comité de Autoridades en Informática de la Administración Pública (CAIAP): éste es un organismo de trabajo para la formulación concertada de lineamientos en el uso, aprovechamiento y desarrollo de las tecnologías de información en las entidades y dependencias de la Administración Pública Federal.

De igual manera, y con propósitos similares pero a nivel de las administraciones públicas estatales y municipales, participó en la creación del Comité de Informática de la Administración Pública Estatal y Municipal (CIAPEM).

Con miras a establecer una política integral, el INEGI ha convocado a destacados especialistas de los ámbitos público, privado, académico y social, y constituido el

Grupo Consultivo de Política Informática. Su participación ha sido destacada en la incorporación del tema de la informática al Plan Nacional de Desarrollo 1995-2000, como en el consecuente Programa de Desarrollo Informático, cuya elaboración estuvo a cargo del Instituto y tiene el propósito de fomentar el uso, aprovechamiento adecuado y desarrollo de la informática en los diversos sectores de la vida del país.

El INEGI efectúa también un monitoreo tecnológico, a nivel nacional e internacional, con el fin de detectar con oportunidad las innovaciones en equipos y desarrollo de programas para el procesamiento de la información, lo que facilita el análisis y el acceso a las nuevas tecnologías.

El PIDI impulsa la formación de recursos humanos en informática en los niveles: técnico, de licenciatura y postgrado. En el nivel de licenciatura, el INEGI ha participado de manera conjunta con la Asociación Nacional de Instituciones de Educación Informática (ANIEI), para la elaboración y difusión de modelos curriculares en carreras de informática y computación. En octubre de 1998, se creó el Consejo Nacional de Acreditación en Informática y Computación (CONAIC), organismo encargado de la acreditación de los programas de informática y computación a nivel nacional.

Con el propósito de elaborar diagnósticos sobre la situación de la informática en el país, realiza encuestas a nivel nacional y estatal sobre el tema. Entre ellas se pueden citar la Encuesta Estatal de Informática, la Encuesta Paraestatal en Informática y la Encuesta Nacional de Servicios Informáticos, en las cuales se tratan temas como:

El mercado informático

- El marco normativo.
- La política informática.
- La investigación nacional.
- El desarrollo de recursos humanos en informática.
- La situación de la cultura informática en México.

La computación primero y la informática después, entendiendo esta última como la convergencia de las tecnologías de computación, telecomunicaciones y administración, juegan un rol vital en las actividades del INEGI, permitiéndole cumplir con su misión de ofrecer el servicio público de información estadística y geográfica, así como promover el uso de la propia informática para contribuir al bienestar social y crecimiento económico y desarrollo democrático y por lo tanto, al fortalecimiento de México.

➢ **Grupo ASISA de México (GAMSA)**

El Grupo **ASISA** de México (GAMSA) nació de la conceptualización de una empresa que pudiera ofrecer nuevas alternativas en cuanto al servicio de consultoría, implementación y distribución de soluciones, dirigiendo éstos esfuerzos al mercado corporativo. **GAMSA** es una empresa líder en soluciones de seguridad (antivirus) y administración en México. Cuenta con 14 años de experiencia, la cual los ha llevado a proporcionar servicios a más de 30% de las empresas catalogadas como triple "A".

➢ **SekureIT**

SekureIT es una empresa mexicana joven, integrada por consultores con amplia experiencia en:

- Diseño, Implantación y Administración de Redes,
- Manejo de Herramientas de Seguridad Informática,
- Aplicaciones de Criptografía, etc.,

Además, de contar con **Capacitación Especializada** y actualización permanente en un área tan dinámica como lo es la seguridad informática.

La UNAM cuenta con organizaciones encargadas de la seguridad informática. Con la compra de la supercomputadora Cray YMP 4/464 en el año de 1991, el Departamento de Supercómputo de la DGSCA se preocupó por la seguridad, tanto de la supercomputadora, como del resto de las máquinas del departamento.

Con el transcurso del tiempo el número de máquinas del departamento fue aumentando, así como las actividades requeridas para poder mantener un buen nivel de seguridad en ellas. Por otro lado, cada vez se tenía más información de problemas de seguridad en la UNAM y en el resto del mundo. Dada la importancia y naturaleza de estos problemas, surgió la idea de formar un área dedicada a la seguridad en cómputo, cuyo rango de acción no se limitara al Departamento de Supercómputo, sino que atendiera las necesidades de la UNAM y difundiera a nivel nacional e internacional la cultura de la seguridad en cómputo.

En Agosto de 1995, se formó de manera oficial, lo que aquel entonces fue llamado, el ESC (Equipo de Seguridad en Cómputo) dirigido por el Ing. Diego Zamboni, quien había trabajado anteriormente en cuestiones de seguridad para el departamento de supercómputo y presentado, para obtener su título de Ingeniero, la tesis Proyecto UNAM/Cray de Seguridad en el Sistema Operativo Unix que involucra la formación de un grupo independiente para atender las necesidades de seguridad.

En su propuesta original el ESC perseguía los siguientes objetivos:

- Difundir información sobre seguridad en cómputo.
- Crear y difundir políticas de seguridad en cómputo.
- Ofrecer servicios de seguridad en cómputo.
- Ofrecer un servicio especial de respuesta a incidentes
- Crear, capacitar y promover grupos humanos dedicados a la seguridad en cómputo.
- Realizar investigación y desarrollo sobre seguridad en cómputo.

Debido a la labor tan importante que desempeñaba el ESC, sus actividades encaminadas a promover la cultura de la Seguridad en Cómputo aumentaron, por lo que se convirtió en el Departamento de Seguridad en Cómputo (DSC).

El departamento ha seguido creciendo para cumplir sus metas y se esta creando un organismo llamado UNAM-CERT (Equipo de Respuesta a Incidentes de Seguridad en Cómputo), que fue aprobado en el congreso celebrado en julio del 2000.

UNAM-CERT se encargará de proveer el servicio de respuesta a incidentes de seguridad en cómputo a sitios que han sido víctimas de algún "ataque", así como de publicar información respecto a vulnerabilidades de seguridad, alertas de la misma índole y realizar investigaciones de la amplia área del cómputo y así ayudar a mejorar la seguridad de los sitios. Este centro comienza operaciones a finales del mes de Noviembre del presente año (2002).

Además, el Departamento de Seguridad en Cómputo de la UNAM (DSC) organiza eventos como el Congreso de Seguridad en Cómputo 2002 que es el principal evento de Seguridad en Cómputo en América Latina, con el objetivo primordial de impulsar la cultura de Seguridad en Cómputo, así como también proporcionar los conocimientos y herramientas necesarias para mantener de forma íntegra la información.

Como es costumbre, el DSC/UNAM-CERT realizará una fuerte difusión del Día Internacional de la Seguridad en Cómputo México (DISC 2002) celebrado el día 30 de Noviembre de 2002 a través del Congreso de Seguridad en Cómputo 2002.

Debido a una iniciativa del Grupo de Interés Especial en Seguridad, Auditoría y Control (SIGSAC) de la *Association for Computing Machinery* (ACM), el DISC es celebrado desde 1998 en más de 40 países de forma simultánea. México ha participado oficialmente en el DISC desde 1994 a través del DSC/UNAM-CERT.

El Congreso de Seguridad en Cómputo actúa como un punto de encuentro de la comunidad de cómputo interesada en el área de seguridad, debido a que reúne a personalidades mundialmente reconocidas que han realizado grandes aportaciones al conocimiento de esta área y que utilizan este gran foro como plataforma de lanzamiento de sus investigaciones más recientes; también convocan a todos los puntos de contacto técnico de todos los proveedores de Internet (ISP), representantes de la Comisión de Biblioteca e Informática de la H. Cámara de Diputados e interesados en impulsar la Legislación en el rubro de Seguridad en Cómputo.

5.2.2 Plan de Contingencia

De acuerdo con el capítulo 4, al hablar de políticas de seguridad hay que contemplar tanto la prevención como la recuperación. Sin embargo, ningún sistema es completamente seguro, ya que pese a todas las medidas de seguridad puede ocurrir un desastre. De hecho los expertos en seguridad afirman "sutilmente" que hay que definir un ***Plan de Contingencia*** para "cuando falle el sistema", no "por si falla el sistema".

Definición de un Plan de Contingencia.

Algunas definiciones de Plan de Contingencia son las siguientes:

- "El plan de contingencias es una estrategia constituida por un conjunto de recursos ideados con el propósito de servir de respaldo, contando con una organización de emergencia y unos procedimientos de actuación encaminada a conseguir una restauración progresiva y ágil de los servicios de negocio efectuados por una paralización total o parcial de la capacidad operativa de la empresa.

Tal estrategia, puntualizada en un manual, es resultado de todo un proceso de análisis y definiciones que dan lugar a las metodologías. A su vez las metodologías existentes versan sobre el proceso necesario para obtener dicho plan."[2]

- "Un Plan de Contingencia de Seguridad Informática consiste en los pasos que se deben seguir, luego de un desastre, para recuperar; aunque sea en parte, la capacidad funcional del sistema aunque, y por lo general, constan de reemplazos de dichos sistemas."[3]

La primera definición menciona que cualquier empresa debe tener una estrategia en caso de una paralización operativa; mientras que la segunda definición es más particular, debido a que se enfoca a la Seguridad Informática, que en nuestro caso es la que nos interesa.

Pero ambas definiciones coinciden que un Plan de Contingencia debe ser capaz de reestablecer el correcto funcionamiento de la empresa o sistema y minimizar los daños.

De acuerdo con lo anterior podemos definir un ***Plan de Contingencia*** como:

"Conjunto de procedimientos que permiten recuperar y reestablecer el correcto funcionamiento del sistema en un tiempo mínimo después de que se haya producido el problema; considerando las acciones que se llevarán a cabo antes, durante y después del desastre, para tener el mínimo de pérdidas posibles."

El Plan de Contingencia implica un análisis de los posibles riesgos a los cuales pueden estar expuestos los equipos de cómputo y la información contenida en los diversos medios de almacenamiento.

Pese a todas las medidas de seguridad puede ocurrir un desastre, por tanto es necesario que el Plan de Contingencia incluya un Plan de Recuperación de Desastres, el cual tendrá como objetivo, restaurar el Servicio de Cómputo en forma rápida, eficiente y con el menor costo y pérdidas posibles.

Si bien es cierto que se pueden presentar diferentes niveles de daños, también se hace necesario presuponer que el daño ha sido total, con la finalidad de tener un Plan de Contingencia lo más completo posible.

Se pueden analizar dos ámbitos: el primero abarca las actividades que se deben realizar y los grupos de trabajo o responsables de operarlas; y el segundo, el control, esto es, las pruebas y verificaciones periódicas de que el Plan de Contingencia está operativo y actualizado.

Fases de un Plan de Contingencia.

Fase I. Análisis y Diseño.

Estudia la problemática, las necesidades de recursos, las alternativas de respaldo, y se analiza el costo/beneficio de las mismas. Esta es la fase más importante, pudiendo llegar al final de la misma, incluso a la conclusión de que no es viable o es muy costoso su

[2] Departamento de Auditoría Informática. (sin fecha). *Plan de Contingencias*[en línea]. DGSCA. Disponible en: < http://sistemas.dgsca.unam.mx/publica/pdf/Contingencias1.PDF > [Consulta: 1 Julio 2002].

[3] BORGHELLO, Cristian F. (2001). Capítulo 9. Políticas de Seguridad en Seguridad Informática [en línea]. Disponible en: < http://www.htmlweb.net/seguridad/seguridad.html> [Consulta: 3 Julio 2002].

seguimiento. En la forma de desarrollar esta fase, se diferencian las dos familias metodológicas. Estas son llamadas *Risk Analysis* y *Business Impact*.

Las *Risk Analysis* se basan en el estudio de los posibles riesgos desde el punto de vista de probabilidad de que los mismos sucedan. Aunque los registros de incidentes son escasos y poco fiables, aún así es más fácil encontrar este tipo de metodologías que las segundas.

Las *Business Impact*, se basan en el estudio del impacto (pérdida económica o de imagen que ocasiona la falta de algún recurso de los que soporta la actividad del negocio). Estas metodologías son más escasas, pero tienen grandes ventajas como es el mejor entendimiento del proceso o el menor empleo de tiempo de trabajo por ir más directamente al problema

Las tareas de esta fase en las distintas metodologías planteadas son las siguientes:

Risk Analysis	Business Impact
1. Identificación de amenazas. 2. Análisis de la probabilidad de materialización de la amenaza. 3. Selección de amenazas. 4. Identificación de entornos amenazados. 5. Identificación de servicios afectados. 6. Estimación del impacto económico por paralización de cada servicio. 7. Selección de los servicios a cubrir. 8. Selección final del ámbito del plan. 9. Identificación de alternativas para los entornos. 10. Selección de alternativas. 11. Diseño de estrategias de respaldo. 12. Selección de la estrategia de respaldo.	1. Identificación de servicios finales. 2. Análisis del impacto. En estas metodologías se evalúan los daños económicos y de imagen y otros aspectos no económicos. 3. Selección de servicios críticos. 4. Determinación de recursos de soporte. 5. Identificación de alternativas para entornos. 6. Selección de alternativas. 7. Diseño de estrategias globales de respaldo. 8. Selección de la estrategia global de respaldo.

Hay un factor importante a determinar en esta fase que es el *Time Frame* o tiempo que la organización puede asumir con paralización de la actividad operativa antes de incurrir en pérdidas significativas. Este factor marcará las estrategias de recuperación y se extraerá del análisis del impacto.

Fase II. Desarrollo de un plan.

Esta fase y la tercera son similares en todas las metodologías. En ella se desarrolla la estrategia seleccionada, implantándose hasta el final todas las acciones previstas. Se definen las distintas organizaciones de emergencia y se desarrollan los procedimientos de actuación generando así la documentación del plan.

Es en esta fase cuando se analiza la vuelta a la normalidad, dado que pasar de la situación normal a la alternativa debe concluirse con la reconstrucción de la situación inicial antes de la contingencia.

Fase III. Pruebas y mantenimiento.

En esta fase se definen las pruebas, sus características y sus ciclos, y se realiza la primera prueba como comprobación de todo el trabajo realizado, así como concienciar al personal implicado.

Asimismo, se define la estrategia de mantenimiento, la organización destinada a ello, y las normas y procedimientos necesarios para llevarlo a cabo.

Características de un Plan de Contingencia.

Un plan de contingencia debe contener:

1. **Aprobación.**

   El plan debe de ser aceptable para auditores internos; fuera de auditores, el director, clientes y proveedores.

2. **Flexibilidad.**

   El plan deberá ser especificado en guías, en lugar de relacionar los detalles a situaciones individuales del desastre.

3. **Mantenimiento.**

   Eludir detalles innecesarios de manera que el plan pueda ser fácilmente actualizado.

4. **Costo-Efectividad.**

   La planeación del proyecto deberá enfatizar en la necesidad de minimizar los costos del desarrollo del plan, respaldo redundante del procesamiento de la suscripción de honorarios, mantenimiento y costo de pruebas.

5. **Continuidad de la empresa.**

   El plan debe de asegurar la continuidad, durante un periodo de recuperación de desastres.

6. **Respuesta organizada.**

   El plan debe proporcionar una lista de verificación de salidas que necesitan atención inmediata que sigue al desastre. Asimismo, incluirá listas de números de teléfono y las direcciones de individuos para contactarlos.

7. **Responsabilidad.**

   A individuos específicos deberá asignárseles la responsabilidad de cada salida que requiera atención durante la Respuesta de Emergencia y el tiempo del periodo del procesamiento interno.

8. **Prueba.**

   La prueba con los usuarios para revisar los procedimientos de verificación de respaldo debe de realizar algo específico en los intervalos de tiempo. De tal forma, que el plan cuente con un estado de frecuencias de prueba y documente la metodología de prueba.

Características de un buen Plan de Contingencia.

- **Funcional** .- Desarrollado por los supervisores de primera línea.
- **Costo-Efectividad** .- En relación con baja probabilidad.
- **Flexibilidad** .- El mismo plan puede ser utilizado para cualquier desastre.
- **Fácil de mantener.**

Pero no basta con tener un manual cuyo título sea *Plan de Contingencia* o denominación similar, sino que es imprescindible conocer si funcionará con las garantías necesarias y cubre los requerimientos en un tiempo inferior al fijado y con una duración suficiente. El plan de contingencia inexcusablemente debe:

- Realizar un Análisis de Riesgos de Sistemas Críticos que determine la tolerancia de los sistemas.
- Establecer un Periodo Crítico de Recuperación en el cual los procesos deben ser reanudados antes de sufrir pérdidas significativas o irrecuperables.
- Realizar un Análisis de Aplicaciones Críticas por el que se establezcan las prioridades de Proceso.
- Determinar las prioridades de Proceso, por días del año, que indiquen cuáles son las Aplicaciones y Sistemas Críticos en el momento de ocurrir el desastre y el orden de proceso correcto.
- Establecer Objetivos de Recuperación que determinen el período de tiempo (horas, días, semanas) entre la declaración de Desastre y el momento en que el Centro Alternativo puede procesar las Aplicaciones Críticas.
- Designar, entre los distintos tipos existentes, un Centro Alternativo de Proceso de Datos.
- Asegurar la Capacidad de Comunicaciones.

- Asegurar la Capacidad de los Servicios de respaldos.

Algunas de las preguntas que pueden formularse al realizar una auditoría sobre este tipo de planes es:

- ¿Cómo está estructurado el Plan?
- ¿Es fácil de seguir el Plan en el caso de un desastre?
- ¿Indica el Plan, quién es el responsable de desarrollar tareas específicas?
- ¿Cómo se activa el plan en caso de un desastre?
- ¿Cómo están contenidos estos procedimientos de activación en los procedimientos de emergencia normales de la organización?
- ¿Han sido probados estos procedimientos en un test de desastre simulado?
- ¿Contiene el Plan, procedimientos que fijen los daños en las etapas iniciales de las Operaciones de Recuperación?
- ¿Incluye el Plan, procedimientos para trasladar el proceso desde el Centro Alternativo al Centro Restaurado o Nuevo?
- ¿Contiene el Plan, listados del Inventario del proceso de datos y hardware de comunicaciones, software, formularios preimpresos y stock de papel y accesorios?
- ¿Están actualizados los listados telefónicos del personal de recuperación, así como empleados del proceso de datos, alta dirección, usuarios finales, vendedores y proveedores?
- ¿Cómo esta contenido el plan?
- ¿Quién es el responsable de actualizar el plan?
- ¿Cuándo fue actualizado el plan?
- ¿Hay copias del plan distribuidas en otro lugar?

En la auditoría es necesario revisar si existe tal plan, si es completo y actualizado, si cubre los diferentes procesos, áreas y plataformas, o bien si existen planes diferentes según entornos, evaluar en todo caso su idoneidad, así como los resultados de las pruebas que se hayan realizado, y si permite garantizar razonablemente que en caso necesario, y a través de los medios alternativos, propios o contratados, podría permitir la reanudación de las operaciones en un tiempo inferior al fijado por los responsables del uso de las aplicaciones, que a veces son también los propietarios de las mismas, pero podrían no serlo.

Si las revisiones no aportan garantías suficientes se deben sugerir pruebas complementarias o hacer constar en el informe, incluso indicarlo en el apartado de limitaciones.

Es necesario verificar que la solución adoptada es adecuada: instalaciones propias, ajenas, compartidas, etc. Y que existe el contrato oportuno, si hay participación de otras entidades, aunque sean del mismo grupo o sector.

Dentro del rubro **crítico de las aplicaciones** se pueden distinguir las más críticas, con impacto muy alto en el negocio y sin alternativa, otras con alternativas, e incluso diferenciado si con costos altos o inferiores, y aquellas cuya interrupción, al menos en un número de días fijado, no tiene casi incidencia y habrá que distinguir qué tipos de consecuencias e impacto, en función del sector y entidad, y día del mes en que ocurriera el incidente, y tal vez la hora en algunos casos. Frente a lo que venía siendo la previsión de contingencias en estos años pasados, centrándose sólo en el *host* como un gran servidor, hoy en día, con la clara tendencia a **entornos distribuidos**, es necesario considerar también éstos en la previsión de las contingencias.

Debe existir un manual completo y exhaustivo relacionado con la continuidad, en el que se contemplen diferentes tipos de incidencias y a qué nivel se puede decidir, que se trata de una contingencia y de qué tipo.

En términos generales, el Plan de Contingencia deberá contener:

- **Objetivo del Plan de Contingencia:** Se deben indicar aquellos componentes de la función crítica que se pretenden cubrir frente a la contingencia considerada. Estos componentes pueden variar, así como su grado de cobertura para las distintas contingencias analizadas.

- **Criterio para la ejecución del Plan de Contingencia:** Condiciones bajo las cuales se considera que debe comenzar a aplicarse el Plan de Contingencia.

- **Tiempo esperado de duración del Plan de Contingencia:** Es el tiempo máximo que se puede continuar operando bajo estas condiciones de contingencia.

- **Roles, responsabilidad y autoridad:** Esto es clave para la buena marcha del Plan de Contingencia. Se debe determinar muy claramente, cuál es el papel de cada uno de los sectores de la organización ante la contingencia y cómo se alteran los procedimientos habituales para dar lugar a los procedimientos de contingencia.

- **Requerimientos de recursos:** Qué recursos se necesitan para operar en el modo contingencia y cuáles de los recursos habitualmente utilizados no se deben utilizar. Esto debe estar debidamente documentado y verificado lo más exhaustivamente posible.

- **Capacitación:** Otro aspecto importante es la capacitación al personal que debe intervenir en la contingencia, cuando ésta se presente. Es necesario que el personal involucrado sepa cómo se saca de servicio cualquier componente que, según el Plan de Contingencia, no debe seguir operando ante alguna falla; que pueda darse cuenta de qué debe hacer y que esté en capacidad de hacerlo cuando sea preciso. También debe tenerse en cuenta que en algún momento habrá de volver a la operación habitual; por lo tanto, deberán incluirse en el plan de mecanismos para volver a la operatoria anterior a la contingencia y el tiempo máximo que la función puede permanecer en estado de contingencia.

- **Implementación y Operación de los Planes de Contingencia:** Se desea que no haya que implementar los Planes de Contingencia, sin embargo, por si esto sucede, hay que estar preparado y tener instructivos claros para todas las tareas que deberían realizarse.

- **Reinstalación:** La contingencia como su nombre lo indica, no es una situación permanente. Por lo tanto, se deben prever mecanismos como para recuperar los datos de operación durante la contingencia, si es que son necesarios, y para aplicar las instrucciones necesarias para que las operaciones no sufran una interrupción traumática al terminar el periodo de contingencia.

Capítulo 6

Ética en la Informática

6.1 Definición de ética e informática

Al hablar de ética necesariamente tenemos que hablar de filosofía, pues pertenece a esta esfera del conocimiento. La acepción más conocida del vocablo "*ethos*" se presenta con Aristóteles donde se entendía como: temperamento, carácter, hábito, modo de ser. [1]

La ética:

- Es una disciplina filosófica.
- Su objetivo de estudio es la moral.
- Es normativa de la actividad humana en orden del bien.
- Es reflexiva, porque estudia los actos no como son, sino como deberían de ser.
- Es práctica, es decir, se enfoca al campo de acción humano.

La ética se define como: "principios directivos que orientan a las personas en cuanto a la concepción de la vida, el hombre, los juicios, los hechos y la moral." [2]

Es conveniente diferenciar la ética de la moral. La ética es una disciplina filosófica, la cual tiene como objetivo de estudio la moral, esto no quiere decir que la ética crea la moral, sino solamente reflexiona sobre ella.

"La moral se refiere a la conducta del hombre que obedece a unos criterios valorativos acerca del bien y el mal, mientras que la ética reflexiona acerca de tales criterios, así como de todo lo referente a la moralidad." [3]

"El término moral procede del latín "*mos*", que significa costumbre, hábito, en el sentido de conjunto de normas o reglas adquiridas por medio de hábito" [4]

Otro concepto importante es el de valor. Este no lo poseen los objetos por sí mismos, sino que estos lo adquieren gracias a su relación con el hombre como ser social.

Desde el punto de vista metafórico los valores según Emma Godoy, son como estrellas en el ancho firmamento de la libertad, hacia las cuales sólo pueden caminar a ellas por senderos infinitos, como el arte, la ciencia y la moral; el arte se dirige hacia la belleza; la ciencia hacia la verdad; la moral hacia el bien y a éstos se les denomina valores. [5]

Los reguladores de la moral influencian nuestra conducta.

- *Moral Social*, todo lo que la sociedad nos impone (religión, familia, educación, amistades y cultura).
- *Conciencia Moral*, principios morales de que todo ser humano es digno.
- *Leyes del Estado*, reglamentos impuestos por un gobierno, para el mejor funcionamiento de la sociedad.

---

[1] ESCOBAR Valenzuela, Gustavo. Ética. Cuarta edición. México, Editorial McGraw-Hill, 1999. 223 p.
[2] GARZA de Flores, Rosa María. Ética. México, Editorial Alambra, 1998. 296 p.
[3] Lozano V., Rodríguez. Ética. México, Pearson Educación, 1998. 243 p.
[4] ESCOBAR Valenzuela, Gustavo. p. 105.
[5] GODOY, Emma. *¿Qué son y para qué sirven los valores?* [en línea]. Disponible en: http://www.mty.itesm.mx/dhcs/centros/cvep/lecturas/ [Consulta: 15 Julio 2002]

El primero se refiere a todo aquello que se nos impone sin ninguna consecuencia legal en caso de infringirlos, el segundo apunta por los valores personales de cada individuo, y el tercero el que el Estado de Derecho fomenta.

Definición de informática.

La ***informática*** no está claramente definida dentro de nuestras instituciones académicas y menos como un estándar internacional.

Se puede buscar una definición general en la que informática sea descrita como una ciencia multidisciplinaria que estudia tanto la tecnología de la información (TI) en su relación con las actividades humanas administrativas y productivas y sus aplicaciones, así como las relaciones entre la información natural y la representativa, abstracta o artificial.

Es la ciencia de la información automatizada, todo aquello que tiene relación con el procesamiento de datos, utilizando las computadoras y/o los equipos de procesos automáticos de información.

Es la ciencia que se encarga de la automatización del manejo de la información.

6.2 Definiciones de la Ética Informática

La *Ética de la Informática* (EI) es una nueva disciplina que pretende abrirse campo dentro de las éticas aplicadas. El origen remoto de la EI está en la introducción cada vez más masiva de las computadoras en muchos ámbitos de nuestra vida social, cada vez más computarizada. Muchas profesiones reivindican para sí una ética particular con la cual pueden regirse ante los problemas morales específicos de esa profesión o actividad ocupacional. La existencia de la EI tiene como punto de partida el hecho de que las computadoras suponen problemas éticos particulares y por tanto distintos a otras tecnologías. En la profesión informática se quiere pasar de la simple aplicación de criterios éticos generales a la elaboración de una ética propia de la profesión. Los códigos éticos de asociaciones profesionales y de empresas de informática van en esta dirección.

El plantear una disciplina como la EI implica salir al paso de afirmaciones como "la ética no tiene nada que ver con las computadoras" o "no hay una ética especial para los informáticos". Realizar la primera afirmación supone no reconocer los dilemas éticos en las tareas del informático que son potenciados por el mismo desarrollo tecnológico. Contrarrestar la segunda afirmación, en cambio, supone demostrar que sí hay necesidad de una ética especial para los informáticos. Así como, otras ciencias y profesiones han tenido siglos para desarrollar conceptos éticos con los cuales tratar sus problemas (entre ellos, los provocados por las nuevas tecnologías), las tecnologías de la información llevan sólo unas pocas décadas de existencia para crear, como otras disciplinas lo han hecho, sus propios estándares éticos.

La definición más restrictiva de la EI es considerarla como la disciplina que analiza problemas éticos creados por la tecnología de las computadoras o también transformados o agravados por la misma, es decir, por las personas que utilizan los avances de las tecnologías de la información. Algunos de los autores se plantean si la cambiante sofisticación tecnológica plantea nuevos dilemas éticos o si las cuestiones éticas permanecen constantes.

Otras definiciones de la EI son mucho más amplias. No se reducen a un nuevo campo de ética aplicada sino que, por ejemplo, en Moor,[6] la EI es el análisis de la naturaleza y el impacto social de la tecnología informática y la correspondiente formulación y justificación de políticas para un uso ético de dicha tecnología. La EI estaría relacionada con los problemas conceptuales y los vacíos en las regulaciones que ha ocasionado la tecnología de la información. El problema es que hay una falta de reglamentación en cómo utilizar estas nuevas tecnologías que posibilitan nuevas actividades para las cuales no hay o no se perciben con nitidez principios de actuación claros. Las personas con responsabilidades en el área de diseño o gestión de sistemas de información cada vez han de tomar más decisiones sobre problemas que no se resuelven con lo legal y lo cuasi-legal (reglamentos, manuales de procedimiento de las empresas, etc.) sino que rozan lo ético mismo. La tarea de la EI es aportar guías de actuación cuando no hay reglamentación o cuando la existente es obsoleta. Al vacío de políticas se añade generalmente un problema de vacío conceptual. Por ello, la EI también ha de analizar y proponer una marco conceptual que sea adecuado para entender los dilemas éticos que ocasiona la informática.

Otra definición más general viene de Terrel Bynum, que basándose en Moor, define la EI como la disciplina que identifica y analiza los impactos de las tecnologías de la información en los valores humanos y sociales. Estos valores afectados son la salud, la riqueza, el trabajo, la libertad, la democracia, el conocimiento, la privacidad, la seguridad o la autorrealización personal. En este concepto de EI se quieren incluir términos, teorías y métodos de disciplinas como la ética aplicada, la sociología de las computadoras, la evaluación social de las tecnologías o el derecho informático.

Los que escriben sobre esta materia no tienen como objetivo adoctrinar o hacer proselitismo sobre una manera concreta de pensar tratando de transmitir un conjunto de valores concretos. La intención es incorporar una conciencia social relacionada con la tecnología informática y también ayudar a los informáticos a utilizar las computadoras no sólo con eficiencia sino con criterios éticos. El objetivo es tomar decisiones sobre temas tecnológicos de manera consistente, con la afirmación de los propios valores que uno profesa o con los derechos humanos en general.

Para ello esta disciplina se plantea varios objetivos intermedios. Por un lado, descubrir y articular dilemas éticos clave en informática. Determinar en qué medida son agravados, transformados o creados por la tecnología informática. Ante los dilemas éticos que ocasiona la informática, analizar y proponer un marco conceptual adecuado y formular principios de actuación para determinar qué hacer en las nuevas actividades ocasionadas por la informática en las que no se perciben con claridad líneas de actuación. Por último, siempre se pretende un análisis ético de casos realistas y significativos.

Para realizar lo anterior, la EI pretende tener en cuenta dos aspectos. Por un lado, utilizar la teoría ética para clarificar los dilemas éticos y detectar errores en el razonamiento ético. Por otro, colaborar con otras disciplinas en ese debate, siendo conscientes de los puntos de vista alternativos en las cuestiones referentes a valores y sabiendo discriminar en los distintos casos entre las consideraciones éticas y las técnicas.

Sin embargo, la EI puede ir más allá. No sólo proponer principios de actuación y ver qué valores son afectados, sino reconsiderar valores que son de hecho asumidos. Por ejemplo, el software supone un tipo de propiedad que no encaja perfectamente en el concepto de

[6] MOOR, James H. "What is Computer Ethics?", *Metaphilosophy*. Vol. 16, No. 4, October 1985. pp. 265-275.

propiedad tradicional. La EI puede analizar qué tipo de propiedad es el software, pero puede plantearse un debate más profundo preguntándose por qué ha de existir propiedad intelectual. Esto supone plantearse de manera nueva valores antiguos y reconsiderar su vigencia.

6.3 Códigos Deontológicos en Informática

La Deontología, del Griego *Deón* (deber) y *Logos* (razonamiento o ciencia): ***Ciencia del Deber***, es la disciplina que trata lo concerniente a los deberes que corresponden a ciertas situaciones personales y sociales.

Originada en las profesiones intelectuales de antiguo origen histórico (Derecho, Medicina) la Deontología, en particular, denota el conjunto de reglas y principios que rigen determinadas conductas de los profesionales, ejercidas o vinculadas, de cualquier manera, al ejercicio de la profesión y a la pertenencia, al respectivo grupo profesional.[7]

Las asociaciones de profesionales de informática y algunas empresas relacionadas con la informática han desarrollado códigos de conducta profesional. Estos códigos tienen distintas funciones:[8]

- Existan normas éticas para una profesión, esto quiere decir que un profesional, en este caso un técnico, no es sólo responsable de los aspectos técnicos del producto, sino también de las consecuencias económicas, sociológicas y culturales del mismo.
- Sirven como un instrumento flexible, como suplemento a las medidas legales y políticas, ya que éstas en general van muy lentas comparadas con la velocidad del desarrollo de las tecnologías de la información. Los códigos hacen de la ley su suplemento y sirven de ayuda a los cuerpos legislativos, administrativos y judiciales.
- Sirven como concientización pública, ya que crear unas normas así, hace al público consciente de los problemas y estimula un debate para designar responsabilidades.
- Estas normas tienen una función sociológica, ya que dan una identidad a los informáticos como grupo que piensa de una determinada manera; es símbolo de su estatus profesional y parte de su definición como profesionales.
- Estas normas sirven también como fuente de evaluación pública de una profesión y son una llamada a la responsabilidad que permiten que la sociedad sepa qué pasa en esa profesión; aumenta la reputación del profesional y la confianza del público.
- En las organizaciones internacionales, estas normas permiten armonizar legislaciones o criterios divergentes existentes (o ausentes, en su caso) en los países individuales.

Sin embargo, se critica a estas asociaciones que han realizado este tipo de códigos porque han trabajado poco por hacerlos cumplir, por imponer sanciones si no se cumplen o por comprobar si se aplican o si son relevantes o pertinentes. Hay códigos que no son conocidos por los miembros de sus asociaciones y menos por sus clientes. Tampoco se reinterpretan, es decir, que exceptuando las situaciones más obvias, que son a las que hacen referencia estos códigos, no se sabe casi nada de la ética de la mayoría de las acciones en las

[7] LEGA, Carlo. *Deontología de la profesión de Abogado.* Madrid, Editorial Civitas, 1976.
[8] HOLVAST, Jan. "Codes of Ethics: Discussion Paper" en INTERNATIONAL FEDERATION FOR INFORMATION PROCESSING (IFIP), *Ethics of Computing: Information Technology and Responsibility.* Madrid, 1992.

que se mueven los informáticos.[9] En general, también suelen faltar las medidas disciplinarias necesarias cuando las actividades de un miembro están en conflicto con la letra o el espíritu del código. También se critica que muchos códigos son el fruto del pensamiento tecnológico de los países desarrollados que no toman en cuenta las diferencias entre valores sociales y culturales.

En general, lo códigos no atienden a los grandes temas éticos de justicia que enfrentamos en nuestro tiempo: desigualdad económica, desempleo, pobreza, racismo, opresión del tercer mundo... La relación de estos problemas con las tecnologías de la información no es directa, ni unívoca ni de una forma en la que haya un consenso global pero al menos sí se admite que las computadoras y las telecomunicaciones, al ser ya parte de nuestra vida colectiva, pueden y deben aportar algo en estos problemas.[10]

El que las asociaciones de profesionales de informática busquen códigos de ética que les obliguen a un modo de actuar, tiene algo de positivo. Quiere decir que los técnicos se están haciendo conscientes de las consecuencias de su trabajo. Son los informáticos los que conocen en profundidad la naturaleza de los sistemas informáticos, la verdad sobre los sistemas de seguridad, los posibles daños por un mal uso del sistema y la verdadera intención de sus usuarios.

Para evitar confusiones sobre la relación entre la profesión y la sociedad hay que responder adecuadamente a:

- ¿A qué fin o bien sirve un informático?
- ¿Cómo es el proceso de toma de decisiones en la relaciones entre tu profesión y la finalidad a la que dices servir?

Los códigos son un paso en la concientización de las sociedades y organizaciones que quieren mejorar situaciones en las que los impactos sociales del desarrollo tecnológico no se tienen en cuenta. No tienen que duplicar lo que ya existe en la ley. La *ley* trata de la legalidad de las prácticas sociales, es normativa por definición y se impone con sanciones. Los *códigos*, en cambio, tratan del comportamiento según principios éticos, su normatividad es nada más mostrar una declaración de intenciones sobre la "misión" de una institución y la coerción real con que se imponen es pequeña, aunque en algunos casos se incluyen expulsiones de la asociación en cuestión. La ley es el acercamiento de más poder normativo y asigna con claridad los derechos, responsabilidades y deberes de cada uno.

6.4 Contenidos de la Ética Informática

Al no ser la Ética Informática una disciplina asentada, no hay unanimidad en los contenidos de esta. A continuación se indica una recopilación de temas y problemas que consideran algunos autores.[11]

---

[9] PARKER, Donn B., SWOPE, Susan y BAKER, Bruce N. *Ethical conflicts in information and computer science, technology, and business*, QED Information Sciences. MA (USA), Wellesley, 1990.

[10] BERLEUR, Jacques. "Final Remarks: Ethics, Self-Regulation and Democracy" en BERLEUR, Jacques y BRUNNSTEIN, Klaus (eds.): *Ethics of Computing. Codes, spaces for discussion and law*. London, Chapman & Hall, 1996. pp. 241-256.

[11] MOOR, James H. p. 107.

Existe una falta de control en los sistemas de información, se puede citar la continua proliferación de delitos informáticos en el mundo, los hackers o más conocidos piratas de la informática día tras día roban información permanentemente de las diferentes computadoras estatales e instalan virus informáticos para su posterior destrucción.

¿Qué podemos hacer para solucionar este problema?

Es difícil contestar a esta pregunta cuando se sabe que, los gobiernos del mundo y millones de hogares están sometidos al uso permanente de los sistemas de información y especialmente al uso de las redes informáticas como es el caso de la Red Internet.

Sólo una legislación fuertemente respetada por la ciudadanía, permitirá que se cumplan cada una de las normas establecidas al pie de la letra, posibilitaría tener algún tipo de control sobre este tipo, sumándole un cambio de actitud por parte de la sociedad, respetando el accionar de la misma.

- **Ética profesional en general.**

  Hace referencia a problemas que son comunes a otras actividades ocupacionales. Por un lado, están los criterios de la moral personal, entendiendo como tales los criterios, obligaciones y responsabilidades personales de los profesionales. Por otro lado, están los problemas internos de la empresa: relaciones jefe-empleado, lealtad organizacional, interés público (whistle blowing), el comercializar productos similares a los de tu jefe, etc.. Existen nuevos problemas que han sido creados o acentuados por las nuevas tecnologías: aumento de vigilancia en las oficinas automatizadas por medio del control del correo electrónico dentro de la empresa o de la información sobre el uso de la computadora que hace cada empleado, investigar en registros personales para detectar uso de drogas en los empleados, etc.. Por último, hay también problemas de ética que hacen referencia a prácticas comerciales incluyendo contratos, acuerdos y conflictos de interés, como, por ejemplo, proponer programas informáticos inferiores, comercializar software sabiendo que tiene errores (bugs), etc.

- **La utilización de la información.**

  En esta parte aparecen problemas relativos al uso no autorizado de los servicios informáticos o de la información contenida en ellos. Se plantean problemas de invasión de la privacidad, de falta de confidencialidad en la información, sobre todo de datos sensibles. Los esfuerzos por proteger la integridad y confidencialidad de la información chocan con la necesidad de información de las entidades públicas y privadas y los entornos académicos o de investigación, es decir, con su derecho a la libertad de información.

  Con respecto al mismo hecho de la información que existe en los distintos sistemas informáticos se plantean problemas concretos como pueden ser el uso de datos personales sin pedir permiso del sujeto, el hojear registros personales, el desarrollo de tarjetas de crédito inteligentes que almacenan información que no tiene que ver directamente con el crédito sin que lo sepan los titulares de las tarjetas, la definición de contenido apropiado o censura en los contenidos de la información (apologías de terrorismo, racismo, pornografía infantil...). Puede haber también injusticias o situaciones de inequidad en el mismo acceso a las redes de información.

- **Lo informático como nueva forma de bien o propiedad.**

  En esta parte se hace referencia al software informático como un bien que tiene características específicas. Los programas de computadora supone un tipo de propiedad de bien que no encaja fácilmente en los conceptos de propiedad de otros tipos de bienes. En principio parece que el problema podría subsumirse y reducirse a la protección de propiedad intelectual. Sin embargo, la pregunta que surge al plantearse la protección de software es, que es de hecho un programa. ¿Es un algoritmo o una idea, que no puede ser poseído por nadie porque pertenece al patrimonio cultural de la humanidad? ¿Es propiedad intelectual que puede ser poseída y protegida?

  De esta situación se generan nuevos problemas: posesión de propiedad, atribución, pirateo, plagio, derechos de autor, secretos industriales, derechos sobre productos, etc. Unido a esto están los problemas de cesión de software comercial, la producción de software nuevo a partir de un programa ya existente, la mejora de productos utilizando materiales registrados de la competencia, la reclamación de la propiedad de un software realizado por alguien en la universidad o en la empresa, etc.

- **Lo informático como instrumento de actos potencialmente dañinos.**

  Puede incluirse o no como un caso de la Ética Informática, debido a que los hechos informáticos pueden ser el medio o instrumento por medio del cual se cometen acciones que provocan daño a terceras personas. Los que proveen servicios informáticos y los que utilizan computadoras, datos y programas han de ser responsables de la integridad y conveniencia de los resultados de sus acciones. Aquí se pueden mencionar las consecuencias de los errores en datos y algoritmos, los problemas que se pueden causar por la falta de protección en la seguridad de sistemas con datos sensibles o que implican riesgos en la salud de clientes, los actos de terrorismo lógico, las acciones de fanáticos, el espionaje de datos, la introducción de virus y gusanos. En el fondo, se trata no sólo de luchar contra acciones expresamente dañinas, sino de fomentar una responsabilidad en las aplicaciones informáticas que pueden tener consecuencias controvertidas o que incluso pueden ser desconocidas.

- **Miedos y amenazas de la informática.**

  Aquí se analiza el punto de que las computadoras pueden ser máquinas pensantes o productoras de verdades absolutas e infalibles. Se trata de analizar las implicaciones de la llamada inteligencia artificial, las redes neuronales o el papel que están llamados a jugar los sistemas expertos de un tipo u otro.

  Un ejemplo, son los Sistemas de Decisión Informatizados (SDI), que forman parte de los mecanismos de decisión en muchas organizaciones privadas y públicas. Los beneficios de los SDI son claros: permiten tratar y gestionar la complejidad y la incertidumbre de manera racional, son eficientes y actúan según criterios consistentes. Sin embargo, también plantean problemas éticos. Por un lado, los referentes a los valores internos a los sistemas (por ejemplo, cómo gestionar los riesgos para la salud humana o cómo hacer equivalencias, si es que es justo, entre la vida humana y ciertas cantidades de dinero); por otro lado, posibles sesgos

escondidos en el proceso de toma de decisiones; por último, hasta qué punto son los diseñadores de estos sistemas responsables de los resultados de los mismos.[12]

- **Dimensiones sociales de la informática.**

  La informática ha contribuido en el desarrollo positivo de los medios de comunicación social. Las tecnologías de la información han hecho posible las comunicaciones instantáneas, el acumular y diseminar información y hechos como el turismo de masas. Sin embargo, al plantear cuestiones éticas, los autores se fijan más en aspectos problemáticos de la implantación de las tecnologías de la información que en sus logros positivos. Esto con el fin de buscar, desde una visión positiva hacia la técnica, cómo hacer que las consecuencias negativas de las nuevas tecnologías se transformen en positivas saliendo así del determinismo tecnológico en el cual la técnica es el fin y no el medio y el ser humano sirve a la técnica y no esta a las necesidades humanas.

Algunos valores en juego durante la implantación de las nuevas tecnologías son: la accesibilidad, la distribución equitativa, la justicia social, el trabajo autorrealizado, el crecimiento sostenido, etc. Como contribuciones problemáticas de las tecnologías de la información, está el papel que juegan en la globalización de la economía, las fusiones empresariales o en el aumento continuo del abismo entre los países desarrollados y en desarrollo. Dentro de las empresas hay también hechos que son muy afectados por la introducción de las tecnologías de la información: la reingeniería de procesos, racionalización de la gestión, con lo que lleva de pérdidas de puestos de trabajo, aumento de desigualdades, deshumanización y otros impactos en las condiciones de trabajo, la ultra competitividad, la distribución de poder, los cambios en los procesos de toma de decisiones, el problema de la centralización y descentralización. Otro aspecto problemático, más concreto, es el tema de las privatizaciones de los sistemas de telecomunicación y las alianzas de las empresas multinacionales de comunicaciones que ponen en cuestión lo que debería estar llamado a ser un "servicio universal". Aquí se originan problemas de acceso, de control, de participación, de la lucha entre intereses privados de lucro o el servicio a las mayorías, etc.

Algunas cuestiones pertenecen al nivel macro como la desigual distribución de información (ricos y pobres en información), el acceso desigual a los medios técnicos (incluyendo a las redes de información), el modo en el que la tecnología de la información refuerza la actual distribución de poder, la participación en las decisiones que afectarán a nuestras vidas en casa o en el trabajo, el control de las redes de información, la restricción de acceso de grupos o individuos que no tienen recursos para participar en un sistema dominado cada vez más por el mercado, el problema de la poca diversidad cultural de los sistemas y medios de información y comunicación que nos invaden. También existen análisis sobre otros efectos para la democracia, la privacidad y las libertades cívicas, los impactos en la sanidad, en la educación, en la cultura, en las familias, en el predominio del paradigma de la razón instrumental, etc.

[12] JOHNSON, Deborah G. y MULVEY, John M. "Accountability and Computer Decision Systems". *Communications of the ACM*, Diciembre 1995. Vol. 38, No. 12. pp. 58-64.

6.5 Situación actual de la Ética de la Informática

La proliferación de estudios existentes sobre la EI está teniendo repercusiones en la formación de los informáticos. Desde hace ya casi dos décadas, la asociación norteamericana ACM recomienda un curso de este tipo como parte de los programas de estudios de la carrera de informática. Sólo en las instituciones universitarias de EEUU se impartieron más de 400 cursos de EI en 1996, sobre un total de 300 un año antes. En el caso español, en algunos centros se está comenzado a impartir esta disciplina. En la revista *Computers and Society* se ha llevado a cabo durante varios números del año 1996 una recopilación bibliográfica de artículos y otras publicaciones relacionadas con la EI. Se puede decir que la situación actual de la EI es:

- No puede decirse que la naciente literatura de EI esté, en general, suficientemente asentada en las teorías éticas, ya sean clásicas o contemporáneas. Los términos clásicos que se utilizan en el análisis del comportamiento ético (por ejemplo, normas, consecuencias, colectividad, individuo, positivismo, fenomenología, etc.) no se tienen suficientemente en cuenta en esta reflexión de la EI. Sin embargo, algunos autores son excepción y sí analizan las distintas situaciones según teorías éticas concretas: Johnson y Berleur contrastan a veces puntos de vista consecuencialistas con kantianos; Holvast analiza el deontologismo, el consecuencialismo y lo que él llama el relativismo ético; Kling analiza con teorías de Rawls, Kant y de los utilitaristas el caso de control en el trabajo por medio de computadoras, etc.
- Mucha literatura existente tiene una orientación individualista. Se centra más en lo que tienen que hacer los empleados, directivos o diseñadores como personas individuales implicadas en las tecnologías de la información. Se habla menos de que es bueno o ético en cuanto a organizaciones, instituciones o corporaciones. Se dedica más tiempo a tratar sobre la elección moral del trabajador que a las elecciones de las organizaciones y sus gestores. Tampoco se dedica mucho espacio a los usos políticos de las tecnologías de la información o a consideraciones éticas sobre una sociedad intensiva en información. Falta una sistematización de la EI, indicando problemas, niveles de análisis, caminos recomendados. En este punto es una excepción la iniciativa ImpactCS, en la que un conjunto de expertos en impacto social y ética de la informática, quieren atender de manera sistemática a distintos niveles de reflexión en lo que respecta a esta disciplina.
- La literatura existente es más sociológica que ética; es menos prescriptiva o normativa que descriptiva. En general, no se ofrecen principios de actuación o respuestas a las preguntas "debe" (qué debería hacer yo como persona, que debería hacer yo y los míos como organización, qué normas sociales deberíamos promover, que leyes debemos tener...). El objetivo de la EI no es solamente proponer análisis sobre "sociología de la informática" o sobre la evaluación social de las tecnologías (technology assessment) sino ir algo más allá en el sentido de proporcionar medios racionales para tomar decisiones en temas en los que hay en juego valores humanos y dilemas éticos.

6.6 Códigos de ética

En México, existen algunos códigos de ética sobre todo en el ámbito periodístico, en el derecho y la medicina. Sin embargo, hay instituciones educativas y empresas que se preocupan por tener un código de ética; en cuanto a seguridad informática son muy pocos,

es por eso que en el capítulo 8, se propondrá un código de ética para la Unidad de Servicios de Cómputo Académico, el cual no sólo pueda aplicarse a la Unidad, sino también en la Facultad de Ingeniería.

Algunos de los códigos de ética que hacen referencia a la seguridad informática o a la informática, son los siguientes:

- Código de Ética del Ingeniero Mexicano (UMAI)
- Código de Ética de la IEEE.
- American Society for Industrial Security (ASIS)
- Código de Ética de la Asociación Mexicana de la Industria Publicitaria y Comercial en Internet, A. C. (AMIPCI)

Cada uno de estos códigos se encuentran en el Apéndice VII. En este documento también se anexa el código de ética universitario, como una muestra de que la UNAM se preocupa porque la gente que labora en ella esté comprometida a realizar su trabajo apegada a los principios establecidos en este código de ética.

Capítulo 7

Herramientas de Seguridad

7.1 Análisis de red

TCP-Wrappers

Este paquete contiene sin duda la herramienta de seguridad más utilizada en entornos Unix. *TCP Wrappers* permite monitorear y filtrar peticiones a diferentes servicios de red (*telnet, ftp, ssh, sendmail...*), pudiendo así restringir éstos a ciertas direcciones de máquina o de red, o bien a *hosts* que cumplan una característica determinada. Esta también se puede instalar desde los paquetes de instalación del sistema.

Este se ejecuta como un intermediario entre *inetd* y el servicio que *inetd* invoca y, filtra las conexiones basadas en la IP origen. Cuando se ejecuta una conexión a un puerto en particular, *inetd* le pasa la petición a tcpd, el cual verifica las reglas existentes (*/etc/hosts.all, /etc/hosts.deny*) para ver si la conexión es permitida. Si la conexión es permitida, pasa la petición al demonio apropiado, de no ser así, deniega la conexión.

Se puede encontrar en:

ftp://ftp.asc.unam.mx/Herramientas/Unix/TCP_Wrappers

Netlog

Este software de dominio público, diseñado por la Universidad de Texas, es una herramienta que genera trazas referentes a servicios basados en IP (TCP, UDP) e ICMP, así como tráfico en la red (los programas pueden ejecutarse en modo promiscuo) que pudiera ser "sospechoso" y que indicará un posible ataque a una máquina (por la naturaleza de ese tráfico).

El paquete está formado por el siguiente conjunto de programas:

- tcplogger

  Este programa escucha todos los servicios sobre TCP, dejando una traza de cada servicio en un archivo de trazas indicando: la hora, la máquina origen y el puerto de esa conexión.

- Udplogger

  Es semejante al anterior pero para los servicios sobre UDP. Los archivos que generan estas dos herramientas pueden ser útiles también para detectar ataques de tipo SATAN o ISS, ya que en los archivos de trazas se aprecian intentos de conexión muy cortos en el tiempo a puertos (tcp o udp) de forma consecutiva.

- Icmplogger

  Se encarga de trazar el tráfico de ***icmp***. Estos programas pueden guardar su información en ASCII o en formato binario, en este segundo caso el programa dispone de una herramienta (extract) que permite consultar los archivos de trazas dándole patrones de búsqueda, como pueden ser: tráfico desde una red concreta, intentos de conexión a puertos específicos, etc.

- **etherscan**

  Es una herramienta que monitorea la red buscando ciertos protocolos con actividad inusual, como pueden ser: conexiones **tftp** (en este caso si se han realizado con éxito, indica qué archivos se han llevado); comandos en el puerto de ***sendmail*** (25 tcp) como ***vrfy***, ***expn***, algunos comandos de ***rpc*** como ***rpcinfo***; peticiones al servidor de **NIS** (algunas herramientas utilizan este tipo de servidores para obtener el archivo de password, ejemplo: ypx); peticiones al demonio de ***mountd***, etc. Etherscan se ejecuta en modo promiscuo.

- **nstat**

  Esta herramienta, que originariamente fue diseñada para obtener estadísticas de uso de varios protocolos, se puede utilizar para detectar cambios en los patrones de uso de la red, que nos puedan hacer sospechar que algo raro está pasando en la misma. Esta herramienta viene acompañada por dos utilidades que nos permiten analizar la salida que origina ***nstat:*** **nsum, nload.** La primera de ellas nos da información de ciertos periodos de tiempo, el segundo es un programa awk que produce una salida que puede ser vista de forma gráfica por herramientas como **xvgr.**

Esta herramienta es muy útil para detectar ciertos tipos de ataques, como se ha reflejado anteriormente (con ***etherscan***), así como dar una idea de qué tipo de protocolos están viajando por la red. Además, tiene la ventaja que al estar en modo promiscuo, con sólo tenerlo en una máquina del segmento se puede tener monitoreado todo el segmento en el que esté conectada.

Se puede encontrar en:

ftp://ftp.asc.unam.mx/Herramientas/Unix/Monitor_Red/Netlog

argus

Es una herramienta de dominio público que permite auditar el tráfico **IP** que se produce en la red, mostrando todas las conexiones del tipo indicado que descubre. Este programa se ejecuta como un demonio y escucha directamente de la interfaz de red de la máquina, y su salida es mandada a un archivo de trazas o a otra máquina para ahí, ser leída. En la captura de paquetes IP se le puede especificar condiciones de filtrado como protocolos específicos, nombres de máquinas, etc.

A la hora de leer esa información se dispone de una herramienta que incluye el software (llamado ra) y que permite también realizar filtros de visualización. Una característica de esta herramienta es la posibilidad de filtrar paquetes de acuerdo a las listas de acceso de los routers **CISCO.** Por lo tanto, es posible decirle que capture aquellos paquetes que no cumplen las reglas de la lista de acceso definida para esa interfaz del router. Como en el caso anterior (***netlog***) es posible ejecutar el comando en modo promiscuo (si lo que se quiere es auditar todo el segmento). Este programa divide las transacciones en cuatro grupos: TCP, UDP/DNS, MBONE, ICMP.

Se encuentra disponible en:

ftp://ftp.andrew.cmu.edu/pub/argus/

cpm

La herramienta *Check Promiscuous Mode* es un pequeño programa realizado por la Universidad Carnegie Mellon, verifica la interfaz de red de la máquina descubriendo si está siendo utilizado en modo promiscuo (escuchando todo el tráfico de la red). Esta herramienta es muy útil, porque alerta de la posible existencia de un "*sniffer*" (olfateador) que intente capturar información en la red como pueden ser las palabras de paso. Este programa debería ser ejecutado de forma periódica para detectar lo antes posible el estado promiscuo en la placa de red. Una forma útil de utilizarlo es mandar el resultado vía correo electrónico.

tcpdump

Es un software de dominio público que imprime las cabeceras de los paquetes que pasan por una interfaz de red. Este programa es posible ejecutarlo en modo promiscuo con lo que se tendrá las cabeceras de los paquetes que viajan por la red. Tanto en la captura como en la visualización de la información es posible aplicar filtros por protocolo (**TCP, UDP, IP, ARP, RARP, ...**), puertos (en este caso el puerto puede ser un número o un nombre especificado en el archivo ***/etc/services***), direcciones fuente, direcciones destino, direcciones de red, así como realizar filtros con operadores (=, <, >, !=, and, not, ...). En la última versión es posible ver también los paquetes de datos. Es requerido para utilizar Courtney.

Se puede encontrar en:

ftp://ftp.asc.unam.mx/Herramientas/Unix/Monitor_Red/Tcpdump

Traceroute

Traceroute traza la ruta de paquetes IP tomados desde el sistema actual a un sistema remoto. *Traceroute* es una utilidad que registra la ruta desde el Internet, entre la computadora y una computadora destino especificada. *Traceroute* es una útil herramienta para entender o detectar donde están los problemas de la red Internet y para obtener información detallada de la red

Se puede encontrar en:

ftp://ftp.asc.unam.mx/Herramientas/Unix/Monitor_Red/Traceroute

rpcinfo

Es un comando incluido en todos los sistemas UNIX, *rpcinfo* hace una llamada RPC a un servidor de RPC (*portmap*) y reporta los servicios que encuentra. Es decir, realiza una petición al mapeador de puertos (*portmapper=portmap*) de una máquina en específico e imprime una lista de todos lo programas RPC registrados como activos. Este comando es capaz de listar los puertos TCP y UDP sólo si el mapeador de puertos está activo.

Para más información acerca del uso de este comando se deberá consultar la página del manual en su sistema:

$man rpcinfo <enter>

Netcat

Es una pequeña utilidad en UNIX que escribe y lee datos a través de una conexión de red usando los protocolos TCP o UDP. Es usado directamente o manejado por medio de otros programas o scripts, tiene un gran potencial para buscar errores y explorar una red, puesto que se puede hacer casi cualquier conexión. Su única limitante es que no cuenta con una explicación muy detallada de cómo funciona; en el archivo de ayuda vienen sólo algunos ejemplos muy elementales.

Pero tiene muchos posibles usos como:

- Bajar/Borrar/Ver/Escribir correo electrónico. La idea es poder usar el *netcat* para enviar correos usando directamente una conexión con el servidor smtp (o no necesariamente al mismo servidor).
- Identificación de sistemas y servidores. Se puede usar el *netcat* para averiguar que programa y que versión están usando para dar el servicio de páginas web.
- Realización de un sencillo chat, para 2 personas. Usando el *netcat* se puede establecer una conexión directa entre dos puertos de dos computadoras a través de Internet, de forma que se puede usar para emular un rudimentario chat entre dos personas.

Se puede encontrar en:

http://www.atstake.com/research/tools/index.html

Ident-Scan

Tiene la funcionalidad de obtener el nombre de usuario que es dueño del proceso correspondiente a un servicio activo a una máquina remota, sólo que para tener éxito es necesario que en la máquina objetivo esté en ejecución el demonio *identd*.

Este programa puede utilizarse para encontrar errores en la configuración de los servicios tales como: un servidor web ejecutándose con privilegios de *root* o cualquier otro tipo de demonio ejecutándose con el UID erróneo. Este programa toma como parámetros el nombre o la dirección IP de la máquina objetivo y también opcionalmente el rango de puertos a explorar en el orden de mayor a menor. Además, también obtiene el nombre del servicio encontrado basándose en la información de un archivo con formato e información similar al */etc/services*.

Su sitio es:

http://208.176.57.92/~daveg/projects/i-scan.html

Strobe

Es una herramienta que se puede usar para localizar y descubrir los puertos que están activos (escuchando) en una o varias máquinas remotas, utilizando una cantidad de proceso y ancho de banda tan mínimos como sean posibles.

Este programa utiliza el tipo de barrido de puertos TCP connect () e identifica exclusivamente puertos TCP activos. Es simple de utilizar y muy rápido, pero no tiene ninguna de las características que tienen los nuevos *scanners* de puertos.

Se puede obtener de:

ftp://suburbia.net/pub/

Nmap

Es una utilería para el *scanner* de grandes redes o de una sola máquina, la ventaja principal de *nmap* como *scanner* es que soporta diferentes tipos de protocolos como el TCP, UDP, ICMP. Antes de la existencia de este programa se tenía que tener muchos *scanners* y correrlos por separado.

Fue diseñado para permitir que los administradores sepan que servidores están activos y que servicios ofrecen. *Nmap* es muy versátil soporta diferentes técnicas de barrido como:

- Vainilla TCP connect().
- TCP SYN (half open).
- TCP FIN, Xmas, o NULL.
- TCP ftp proxy.
- SYN/FIN.
- TCP ACK.
- UDP raw.
- ICMP.
- TCP ping.
- Directo con RPC.
- Identificación remota del sistema operativo.

También utiliza un número variado de algoritmos, además de ser flexible a la especificación del *host* objetivo y el número de puertos, previsibilidad de la secuencia de los paquetes TCP, UDP o ICMP utilizados para hacer el barrido. La salida puede ser enviada a una terminal o a un archivo con un formato legible.

La última versión puede ser obtenida en:

http://www.insecure.org.nmap

Ethereal

Es una herramienta para realizar tareas de análisis de red.

Ethereal tiene las siguientes características:

- Disponible para Unix y Windows.
- La captura y despliegue de paquetes desde cualquier interfaz en Unix.
- También puede desplegar los paquetes capturados desde otras herramientas.

Ethereal también es un analizador de protocolos de red que permite que los datos del paquete sean vistos interactivamente en la red o de un archivo. Además, puede leer una captura ***noop*** y ***atmsnoop***.

Puede reconocer diferentes tipos de archivos y no es necesario decirle qué tipo de archivo es para que pueda interpretarlo. Utiliza GTK+, una librería que provee una interfaz de usuario gráfica, y *libpcap*, una librería para filtrar y capturar paquetes, también posee la posibilidad de ver la reconstrucción del fluido de una sesión TCP. Fácil uso y muy buena representación de los datos.

Su sitio es:

http://www.ethereal.com

Dsniff

Es una suite de poderosos sniffers para contraseñas y otra información. Incluye sofisticadas técnicas para evadir la protección de puentes (switch) en una red.

Dsniff permite explotar algunas de las fallas fundamentales de los protocolos de encriptación SSH y SSL. SSH y SSL son protocolos utilizados para proteger un alto número de tráfico de paquetes en la red, desde transacciones financieras con bancos en línea, hasta servidores que contienen información extremadamente valiosa.

Tanto SSH como SSL utilizan una "llave pública de encriptación". Es exactamente aquí donde se encuentran las vulnerabilidades. Ya desde las codificaciones de Hamilton, donde se hablaba de la posibilidad de la encriptación pública, se preveían estos problemas. Principalmente porque, cuando se realiza algún tipo de conexión, ya sea hacia un servidor confiable o cualquier otro sitio, se está en constante peligro, ya que las conexiones antes mencionadas, deben hacerse desde un medio público, una red heterogénea, como lo es Internet. Es aquí, en este punto, donde nada es seguro, donde, por un simple método se puede "engañar " al emisor y al receptor.

Esto en el caso de que nuestra información lleve un cifrado porque en otro caso es más vulnerable aún.

Se encuentra en:

http://monkey.org/~dugsong/dsniff/

Hping2

Hping2 es una utilidad de red capaz de enviar paquetes ICMP/UDP/TCP hechos a medida y mostrar las respuestas del objetivo como réplicas ICMP de ping. Maneja fragmentación y cuerpos del paquete de tamaños arbitrarios y puede ser utilizado para transferir archivos bajo los protocolos soportados. Utilizando *hping2*, puede: probar las reglas del firewall, realizar [spoofed] *scaneo* de puertos, realizar pruebas de red utilizando diferentes protocolos, tamaños de paquetes, TOS (tipo de servicio) y fragmentación, MTU, transferir archivos, auditar la pila TCP/IP, etc. *Hping* es una buena herramienta para adquirir conocimientos de TCP/IP.

Para más información revisar el sitio:

http://www.hping.org

Sniffit

Sniffit es una herramienta de monitoreo y *sniffer* que trabaja sobre diferentes plataformas Unix. Proporciona a un administrador información detallada sobre todo el tráfico que circula por el sistema, entregando el contenido del paquete en diferentes formatos (Hexadecimal, texto plano, etc.), y también le ofrece la posibilidad de neutralizarlo si se utiliza TOD (*Touch of Dead*), es decir, cerrar las conexiones que pasan a través de la máquina. Es software libre.

Se puede obtener de:

http://sniffit.rug.ac.be/~coder/sniffit/sniffit.html

Cheops-ng

Cheops-ng es una herramienta gráfica para el mapeo y supervisión de redes. Tiene funcionalidad de descubrimiento de *host*/red, detección del Sistema Operativo, y también hace un *scaneo* de puertos de cada computadora para determinar qué servicios están funcionando. Es conocido como la navaja del ejército suizo de las redes.

Su página oficial es:

http://cheops-ng.sourceforge.net.

Libnet

Libnet es un API que permite al programador construir paquetes de red. Provee una portable y simple interfaz para los paquetes a bajo nivel. *Libnet* esconde mucho el tedio al programar la creación de un paquete, haciendo muy sencillo los encabezados, orden de los bytes, administración del buffer, etc. Usando esta librería se pueden crear paquetes con mucho menos esfuerzo.

Para mayor información en el sitio:

http://www.packetfactory.net/libnet

IPTraf

Es una utilidad que utiliza una consola para ver las estadísticas de la red y que recopila recuentos de bytes y paquetes de las conexiones TCP, indicadores de actividad y estadísticas de la interfaz, interrupciones del tráfico de TCP/UDP y recuentos de bytes, paquetes de las estaciones de LAN. Además de la interfaz estándar (FDDI/Ethernet), puede monitorear el tráfico de SLIP PPP y RDSI. Si se utiliza Trinux, SUSE o Debian, es muy probable que *Iptraf* ya esté instalado. En caso contrario, puede obtenerlo en:

http://cebu.mozcom.com/riker/iptraf/about.html

iplog: icmplog, tcplog y udplog

Es un conjunto de tres utilidades que dan información sobre conexiones icmp, tcp y udp a través del demonio *syslog* usando la facilidad *daemon* y la prioridad info (para más información ver: *man syslogd; man syslog.conf*).

7.2 Auditoría

COPS

COPS (*Computer Oracle and Password System*) es un paquete clásico en la seguridad de UNIX. Es un conjunto de programas diseñados por la Universidad de Purdue que verifican ciertos aspectos del sistema operativo UNIX relacionados con la seguridad. Fue creado por Daniel Farmer y Eugene H. Spafford. Existen dos versiones de este paquete: una versión escrita en "sh" y "C" y otra versión escrita en "perl", aunque su funcionalidad es similar. Este programa es fácil de instalar y configurar y, se ejecuta en gran cantidad de plataformas UNIX. En el primer caso, se necesita un compilador de lenguaje C y un shell estándar (sh); en el segundo bastará con tener instalado el interprete de perl (versión 3.18 o superior). Entre las funcionalidades que tiene COPS destacan:

- Verificación de modos y permisos de los archivos, directorios y dispositivos.
- Palabras de paso pobres (en el caso que se tenga una herramienta como crack, se puede comentar la línea de verificación de palabras de paso).
- Verificación de contenido, formato y seguridad de los archivos de "*password*" y "*group*"
- Verificación de programas con root-SUID.
- Permisos de escritura sobre algunos archivos de usuario como "*.profile*" y "*.cshrc*"
- Configuración de ftp "anonymous".
- Verificación de algunos archivos del sistema como "*hosts.equiv*", montajes de NFS sin restricciones, "*ftpusers*", etc.

ISS

Es una herramienta de dominio público que revisa una serie de servicios para comprobar el nivel de seguridad que tiene esa máquina. *ISS* es capaz de verificar una dirección IP o un rango de direcciones IP (en este caso se indican dos direcciones IP e *ISS*, verificará todas las máquinas dentro de ese rango). El programa viene acompañado de dos utilidades que son: ypx y strobe; la primera permite la transferencia de mapas NIS a través de la red y la segunda revisa y describe todos los puertos TCP que tiene la máquina que verifica. Con la primera herramienta, es posible la transferencia de los archivos de "password" en aquellas máquinas que hayan sido configuradas como servidores de NIS.

ISS se puede ejecutar con varias opciones y la salida se deja en un archivo. Además, si ha podido traerse el archivo de "*password*" de la máquina revisada, creará un archivo aparte con la dirección IP de la máquina.

Se puede encontrar en:

ftp://coast.cs.purdue.edu/pub/tools/unix/iss

Para mayor información sobre ISS, visite:

http://www.cert.org/advisories/CA-93.14.Internet.Security.Scanner.html

Swatch

Swatch, Simple WATCHer Program, es un archivo de registro filtro/monitor fácilmente configurable. *Swatch* supervisa archivos de registro y actúa para filtrar hacia afuera datos no deseados y tomar uno o más usuarios, especificando acciones basadas en modelos del registro.

Swatch está disponible en:

ftp://ftp.stanford.edu/general/security-tools/swatch /

Tiger

Es un software desarrollado por la Universidad de Texas que está formado por un conjunto de shell scripts y código C que chequean el sistema para detectar problemas de seguridad de forma parecida a COPS. Una vez chequeado el sistema, se genera un archivo con toda la información recogida por el programa. *Tiger* dispone de una herramienta (*tigexp*) que recibe como parámetro dicho archivo y da una serie de explicaciones adicionales de cada línea que generó el programa anterior. El programa viene con un archivo de configuración donde es posible decirle qué tipo de revisión se quiere realizar (se pueden comentar las operaciones más lentas y ejecutar éstas de forma menos continua, mientras que las más rápidas pueden ser ejecutadas más frecuentemente). Entre la información que revisa el programa se tiene:

- Configuración del sistema.
- Sistemas de archivos.
- Archivos de configuración de usuario.
- Verificación de caminos de búsqueda.
- Verificación de cuentas.
- Verificación de alias.
- Comprueba la configuración de ftp "anonymous".
- Revisión de scripts de cron.
- NFS.
- Verificación de servicios en el archivo */etc/inetd.conf*
- Verificación de algunos archivos de usuario (*.netrc*, *.rhosts*, *.profile*, etc.)
- Comprobación de archivos binarios (firmas). Para poder revisar éstos, es necesario disponer de un archivo de firmas.

TARA

TARA (Tiger Analytical Research Assistant). Después de la creación del *Tiger* no se hicieron actualizaciones, por lo que con el tiempo fue quedando obsoleto, y Bod Todd en 1999 a partir del código de *Tiger* decidió generar un conjunto de scripts que siguieran verificando un sistema Unix en potenciales problemas de seguridad.

Con esto el *tiger* sufrió una reestructuración con la cual fuera más fácil su actualización por medio de bases de datos.

El programa verifica los siguientes puntos del sistema:

- Aliases
- *nisplus*
- *root*
- *ftp* anónimos
- *passwd*
- Permisos en cuentas
- *cron*
- *path*
- Grupos
- *rhost*
- *inetd*
- *sendmail*

Se puede obtener de:

http://www-arc.com/tara/

TripWire

Este software de dominio público desarrollado por el Departamento de Informática de la Universidad de Purdue, es una herramienta que comprueba la integridad de los sistemas de archivos, y ayuda al administrador a monitorear éstos frente a modificaciones no autorizadas. Esta herramienta avisa al administrador de cualquier cambio o alteración de archivos en la máquina (incluyendo binarios). El programa crea una base de datos con un identificador por cada archivo analizado, y puede ser comparado en cualquier momento el actual con el registrado en la base de datos, avisando ante cualquier alteración, eliminación o inclusión de un nuevo archivo en el sistema de archivos. La base datos está compuesta por una serie de datos como la fecha de la última modificación, propietario, permisos, etc.; con todo ello se crea una firma para cada archivo en la base de datos.

Esta herramienta debería ser ejecutada después de la instalación de la máquina, para tener una "foto" de los sistemas de archivos en ese momento, y puede ser actualizada cada vez que se añada algo nuevo. Dispone de un archivo de configuración que permite decidir qué parte del sistema de archivos va a ser introducida en la base de datos para su posterior comprobación.

Su sitio es:

http://www.tripwire.com

Nessus

Nessus es un auditor de seguridad muy completo para plataformas Linux, BSD, Solaris y otros sistemas. Fue desarrollado bajo la licencia GNU, es un proyecto de Renaud Deraison iniciado en abril de 1998, sus características principales son:

- *Libre*: Según el autor con la intención de que universidades, colegios, etc., puedan acceder a este tipo de software para protegerse de crackers o hackers.
- *Código abierto*: Por dos principales razones, una para que el código del mismo pueda ser analizado por cualquiera y de esta manera eliminar cualquier sospecha de que contenga troyanos, y la otra para promover la colaboración y participación de programadores independientes.
- *Facilidad de uso*: La seguridad no es una cosa sencilla de resolver en un sistema, de manera que *Nessus* pretende proveer una interfaz sencilla, cómoda, fácil de entender y eficaz para que se encuentre al alcance de cualquier administrador.
- *Nessus* es un programa que audita remotamente la red para detectar debilidades en nuestro sistema y su arquitectura consiste en un servidor y un cliente.
- Es multithreaded y esta basado en el uso de *"plugins"*, tiene una interfaz agradable hecha en GTK. Realiza actualmente más de 900 chequeos de seguridad remotos.
- Su capacidad de documentación es muy poderosa, genera reportes HTML, látex y texto ASCII y no sólo descubre las vulnerabilidades, sino que sugiere una solución para cada una de ellas.
- Comunicación encriptada (esto es, segura).
- Tiene un continuo desarrollo por comunidad de software libre, además de ser modular con multitud de pruebas.

Se puede obtener de:

http://www.nessus.org

SATAN

Security Analysis Tool for Auditing Networks (Herramienta de Análisis de la Seguridad para Auditar Redes). Es un software de dominio público creado por Dan Farmer que revisa máquinas conectadas en red y genera información sobre el tipo de máquina, qué servicios da cada máquina y avisa de algunos fallos de seguridad que tengan dichas máquinas. Una de las ventajas de *SATAN* frente a otros paquetes es que utiliza una interfaz de WWW (como Mosaic, Netscape, ...) y va

creando una base de datos de todas las máquinas revisadas y las va relacionando entre ellas (de forma que si encuentra una máquina insegura, y checa otra máquina que está relacionada con esta, automáticamente quedará marcada esta segunda también como insegura); además, tiene la posibilidad de poder revisar las máquinas con tres niveles ("light", normal y "heavy"). Una vez realizada la revisión de la máquina se genera una salida en formato html, y en el caso de encontrar fallos da una pequeña explicación sobre el fallo en concreto y si existe algún documento sobre ese fallo recogido en el CERT (advisory) tiene un enlace a ese documento, para que sobre la marcha pueda ser consultado. Además, en el caso que el fallo de seguridad sea debido a versiones antiguas de software da la posibilidad (mediante un enlace) de instalar una versión de ese software.

Algunos de los servicios verificados por *SATAN* son: finger, NFS, NIS, ftp, DNS, rexd; así como tipo de sistema operativo, versión de sendmail, etc. La base de datos generada por *SATAN* puede ser luego consultada por varios campos: tipo de sistema operativo, tipo de servicio (servidores de NIS, ftp, NFS, X, etc.).

SATAN ha sido diseñado como una herramienta de seguridad para ayudar a administradores de sistemas y redes, pero también puede ser utilizada para atacar a sistemas y descubrir la topología de la red de una organización (*SATAN* es capaz de revisar máquinas por subredes, con lo que quedan al descubierto todas las máquinas que se encuentran conectadas en dicha subred). Para poder compilar y ejecutar *SATAN* basta con poseer la versión 5 de perl y un visualizador de WWW.

Algunos de los fallos de seguridad que *SATAN* es capaz de detectar son:

- Acceso vía rexec.
- Vulnerabilidad en el sendmail.
- Acceso vía tftp.
- Accesos vía rsh.
- Acceso a servidores X no restringido.
- Exportar sistemas de archivos no restringido.
- Acceso a archivos de password vía NIS.

Se puede obtener más información en:

http://www.fish.com/satan

SAINT

Security Administrator's Integrated Network Tool. Una herramienta realmente útil en ciertas ocasiones es *Saint*, el sucesor de *Satan*, un *scanner* de seguridad de red, famoso por los medios de comunicación hace unos años (había serias preocupaciones de que los hackers acabaran con Internet haciendo uso de él). *Saint* produce una salida muy fácil de leer y entender, graduando por prioridad los problemas de seguridad (aunque no siempre de forma correcta) y también soporta módulos de *scaneo* añadidos, lo cual le hace muy flexible. Entre sus características está: el poder *scanear* a través de un firewall, tiene 4 niveles de seguridad (rojo, amarillo, café y verde) y despliega los resultados a través de una interfaz hecha en html.

Esta hecho para buscar agujeros de seguridad, por lo que es recomendable correrlo cada vez que se actualice la distribución.

Su sitio es:

http://www.wwdsi.com/saint

SARA

Security Auditor's Research Assistant (Asistente de Búsqueda del Auditor de Seguridad) es una herramienta de análisis de seguridad en sistemas tipo Unix de tercera generación, esta basada en el modelo de *Satan* que está cubierto en la licencia GNU.

Y tiene las siguientes características:

- Funciona encendido en la mayoría de las plataformas tipo Unix incluyendo OS X de MAC.
- Compila completamente con la especificación de la top 20 de SANS.
- *Scanner* remoto y facilidades del API.
- Fácilmente agrandable por medio de plug-in.
- Certificado SANS/ISTS.
- Soporta los estándares de CVE.
- Módulo de búsqueda por empresa.
- Modo standalone o de demonio.
- Licencia libre tipo *SATAN*.
- Actualizaciones dos veces al mes.
- Soporta el uso de extensiones.
- Trabaja de acuerdo con el modelo de *SATAN*.

Después de que se generaron las primeras herramientas de seguridad para analizar redes, empezaron a quedar obsoletas conforme pasaba el tiempo e hicieron falta actualizaciones, bajo este concepto nace *SARA* que tiene gran capacidad de análisis. Está siendo actualizado y además el escritor de reportes puede ser configurado de manera que de gran variedad de información.

Se puede obtener más información de *SARA* en:

http://www-arc.com/sara

Logcheck

Es parte del proyecto Abacus, un conjunto de herramientas de seguridad. Es un programa hecho para ayudar al procesamiento de los archivos *logfiles* generados por las demás herramientas en el proyecto Abacus. *Logcheck* puede detectar en esos archivos diferentes tipo de violaciones al sistema y avisar por correo electrónico.

Se puede obtener de:

http://www.psionic.com/products/logsentry.html

Merlin

Se trata de un programa desarrollado por CIAC que sirve de interfaz a otros programas de seguridad *(COPS, CRACK, tiger...)* a través de un navegador de WWW. *Merlin* permite que estas herramientas sean más sencillas de utilizar, así como en algunos casos extiende sus capacidades.

Se puede obtener en:

ftp://ciac.llnl.gov/pub/ciac/sectools/unix/merlin/

7.3 Contraseñas

anlpasswd

Es un programa de cambio de passwords (contraseñas) que impide que el usuario escoja passwords débiles. Se realizó en el Laboratorio Nacional de Argonne, escrito en su mayoría en Perl. Algunas de sus características son:

- Previene el uso de passwords débiles sustituyendo el *passwd, yppasswd.*
- Compara passwords usando un diccionario de reglas de passwords crackeadas.
- No es un cracker de passwords.

Algunas de las reglas estándar son:

- Número con espacios y espacios con números.
- Mayúsculas y minúsculas con espacios.
- Todo con minúsculas o mayúsculas.
- Combinar letras y números.
- Todas las combinaciones anteriores.

anlpasswd está disponible en:

ftp://info.mcs.anl.gov/pub/systems/
ftp://ftp.seguridad.unam.mx/Herramientas/Unix/Autenticacion/Anlpasswd/
ftp://ftp.cerias.purdue.edu/pub/tools/unix/pwdutils/anlpasswd/

Crack

Es un programa de "rompimiento" de passwords existente desarrollado por Alec D. Muffett. Intenta adivinar los passwords utilizando una serie de reglas configurables.

Está diseñado para identificación, por el estándar que conjeturan las técnicas, UNIX DES encripta passwords que se pueden encontrar en diccionarios extensamente disponibles.

Tradicionalmente el *Crack* permitió que cualquier usuario de un sistema crackeara el */etc/passwd* y determinara los passwords de otros usuarios (o de *root*) en el sistema. Los sistemas modernos requieren obtener acceso al */etc/shadow* para realizar esto.

Muchos administradores del sistema ejecutan el *Crack* como un sistema regular de procedimiento de administración y notifica a dueños de cuentas a quienes les han "crackeado" passwords. Por esta razón, sigue siendo una buena idea que los administradores del sistema corran un crack de vez en cuando para verificar que los usuarios tienen passwords fuertes.

Crack está disponible en:

http://www.users.dircon.co.uk/~crypto/
ftp://ftp.cerias.purdue.edu/pub/tools/unix/pwdutils/crack/

Cracklib

Es una biblioteca de funciones que pueden ser utilizadas para impedir que los usuarios elijan passwords que podrían ser adivinados por *Crack*.

Cracklib está disponible en:

http://www.users.dircon.co.uk/~crypto/
ftp://ftp.cerias.purdue.edu/pub/tools/unix/libs/cracklib/

passwd+

Matt Bishop autor de *passwd+*, ofrece las siguientes características:

- Capacidad extensa de loggin (*logeo*), incluyendo el loggin de cada sesión, cualquier tipo de errores, que los usuarios hayan cambiado sus passwords, que reglas el password no pudo satisfacer, y el éxito o la falla de un cambio de password.

- Especificación del número de caracteres significativos en el password (es decir, cuántos serán utilizados en la prueba).

Además, *passwd+* permite que se fije el mensaje de error que será mostrado cuando un usuario repite un paswword débil. Se debe utilizar esta funcionalidad para enseñar a los usuarios porqué sus opciones de password son malas.

Algunas de las reglas que proporciona *passwd+* son:

- Se prohíben el número de oficina, el teléfono de la oficina, el hostname y el dominio de nombres.
- Los passwords deben ser, por lo menos de *n* caracteres de largo.
- Los passwords deben ser una mezcla de casos.
- Se prohíben los passwords que aparecen en el diccionario.
- Se prohíben el nombre y apellidos (en cualquier orden).
- Se prohíbe el login.

Este programa de cambio de passwords que impide que el usuario escoja passwords débiles, basa el rechazo de passwords en un archivo de configuración que permite la utilización de expresiones

regulares, comparación con diccionarios o la ejecución de programas externos para examinar el password.

passwd+ está disponible en:

ftp://ftp.dartmouth.edu/pub/security/

shadow

El programa *shadow* de John F. Haugh, II, es un reemplazo para el login y el password que permiten a cualquier sistema utilizar archivos con passwords sombra (shadow password). Incluye ayuda para los archivos de passwords sombra, grupos de archivos sombra, archivos de passwords DBM, passwords de longitud doble y envejecimiento del password.

En el sistema operativo Linux, un archivo de passwords sombra es un archivo de sistema en el cual se almacena el password del usuario en forma encriptada, de modo que no esté disponible para la gente que intente entrar en el sistema. Ordinariamente, la información del usuario, incluyendo el password, se mantiene en un archivo del sistema llamado */etc/passwd*. El password de cada usuario se almacena de forma encriptada (generalmente, se realiza por medio de un algoritmo de encriptación).

En general, ***shadow*** es un paquete que permite a cualquier sistema hacer uso de *shadow passwords* (passwords sombra).

S/Key

S/Key es un sistema de Bellcore cuyos autores son: Phil Karn, Neil M. Haller, John S. Walden.

S/Key es un Sistema de Passwords One-Time (*de una sola vez* o *desechables*) que proporciona la autenticación sobre redes que están sujetas a ataques de eavesdropping/reply. La contraseña secreta del usuario nunca cruza la red durante la conexión, o cuando ejecuta otros comandos que requieren la autenticación tal como los comandos de UNIX *passwd* o *su*. No almacena dondequiera ninguna información secreta, incluyendo el *host* que es protegido y el algoritmo subyacente puede ser (y de hecho es) de conocimiento público.

En general, este sistema implementa passwords desechables para Unix. También incluye generadores de passwords desechables para PC's y MAC's.

Para obtener más información de *S/Key* se puede consultar la siguiente dirección:

ftp://thumper.bellcore.com/pub/nmh/docs/skey.txt

S/Key está disponible en:

ftp://thumper.bellcore.com/pub/nmh/

John the Ripper

John the Ripper es una utilidad activa para averiguar passwords. Su principal propósito es detectar passwords débiles en Unix. Una vez conseguido el archivo de passwd, este programa busca el password encriptado. Es un clásico que sigue siendo de gran utilidad y que todo administrador debería tener en cuenta para detectar cuentas con passwords débiles entre sus usuarios.

Actualmente está disponible para muchos Unix (11 son los que lo soportan, no contando las diferentes arquitecturas), DOS, Win32 y BeOS.

John the Ripper está disponible en:

http://www.openwall.com/john/

7.4 Autenticación

Kerberos

Kerberos es un sistema de autenticación para redes físicamente inseguras, basado en el modelo de distribución de llaves presentado por R.M. Needham y M.D. Schroeder. Permite a los elementos que intervienen en una comunicación identificarse entre sí y al mismo tiempo evitar "espionaje" en la red o ataques de repetición. También proporciona integridad en el flujo de datos (detección de modificaciones) y privacidad, utilizando sistemas criptográficos como DES. *Kerberos* tiene restricciones de exportación hacia fuera de los Estados Unidos.

El modelo de *Kerberos* está basado en un protocolo de autenticación a través de un servidor confiable (servidor *kerberos*), ya que este sistema considera que toda la red es una región de riesgo grande, excepto por este servidor. Trabaja proporcionando a los usuarios y a los servicios boletos que pueden usar para identificarse a sí mismos, además de llaves encriptadas secretas proporcionando cierta seguridad en la comunicación con los recursos de la red.

Gracias a que comparten una contraseña secreta (o llave) con el servidor *kerberos*, permite verificar que los mensajes del servidor *kerberos* son auténticos. Así en el servidor *kerberos*, los usuarios y los servicios pueden autenticarse.

Kerberos está disponible en:

http://consult.stanford.edu/afsinfo/kerberos.shtml
ftp://athena-dist.mit.edu/pub/kerberos/

pidentd

El demonio *pident* de Peter Eriksson, es una implementación del servidor de identificación de usuario descrito en RFC 1413, que permite averiguar la identidad del usuario que está solicitando un servicio remoto.

Se puede obtener en:

ftp://ftp.cerias.purdue.edu/pub/tools/unix/daemons/pidentd/servers/

ssh

Secure Shell (*ssh*) es un programa que permite realizar conexiones entre máquinas a través de una red abierta de forma segura, así como ejecutar programas en una máquina remota y copiar archivos de una máquina a otra. Tal y como se explica en el RFC de Secure Shell:

"SSH (Secure Shell) es un programa para conectarse a otros equipos a través de una red, para ejecutar comandos en una máquina remota y para mover archivos de una máquina a otra. Proporciona una exhaustiva autenticación y comunicaciones seguras en redes no seguras."

Ssh provee fuerte autenticación y comunicación segura sobre un canal inseguro y nace como un reemplazo a los comandos telnet, ftp, rlogin, rsh, y rcp, los cuales proporcionan gran flexibilidad en la administración de una red, pero sin embargo, presenta grandes riesgos en la seguridad de un sistema. Adicionalmente, *ssh* provee seguridad para conexiones de servicios X Windows y envío seguro de conexiones arbitrarias TCP.

Secure Shell admite varios algoritmos de cifrado entre los cuales se incluyen:

- Blowfish.
- 3DES.
- IDEA.
- RSA.

La ventaja más significativa de *ssh* es que no modifica mucho las rutinas. En todos los aspectos, iniciar una sesión de *ssh* es tan sencillo como (y similar a) iniciar una sesión de *telnet*. Tanto el intercambio de llaves, la autenticación, así como el posterior cifrado de sesiones son transparentes para los usuarios.

Entre los ataques más comunes que previene Secure Shell están:

- Sniffering(Captura de tráfico) .
- IP Spoofing.
- MACpoofing.
- DNS Spoofing.
- Telnet Hickjacking.
- ARP Spoofing.
- ARP Spoofing.
- IP Routing Spoofing.
- ICMP Spoofing.

Actualmente existen dos protocolos desarrollados sobre ssh: SSH1 y SSH2.

ssh está disponible en:

http://ftp.ssh.com/pub/ssh

OpenSSH

OpenSSH es una versión libre de los protocolos SSH/SecSH bajo licencia BSD y es totalmente compatible con los protocolos SSH1 y SSH2.

Debido a que OpenSSH rompe la barrera de los protocolos que ha causado confusión entre diversos sectores. Esta herramienta está siendo muy usada en distribuciones como Linux RedHat 7.x que ya la incluyen dentro de su sistema operativo.

OpenSSH es una sustitución segura de rlogin/rsh/rpc. Como se mencionó anteriormente, *OpenSSH* es derivado de la versión ssh de OpenBSDs, que es así mismo derivado del código *ssh* antes de que la licencia de *ssh* cambiara a no libre.

Hoy en día cualquier red que considere tener un poco de seguridad debería tener *OpenSSH* instalado, ya que le será imprescindible en sustitución a las altamente inseguras utilidades "r". Su fácil implementación y uso transparente hacen más que aconsejable su uso.

Sin embargo *OpenSSH* ha demostrado cierta inestabilidad, por lo que es altamente recomendable estar actualizando periódicamente el *OpenSSH* y estar al pendiente de vulnerabilidades presentadas.

OpenSSH está disponible en:

http://www.openssh.com/

7.5 Antiespionaje

swatch

Todd Atkins es autor de *swatch*. Este sistema permite monitorear los archivos de bitácoras del sistema y ejecutar acciones específicas en respuesta a ciertos patrones encontrados.

Swatch (Simple WATCHer Program) es un archivo de registro filtro/monitor fácilmente configurable. *Swatch* supervisa archivos de registro y actúa para filtrar hacia afuera datos no deseados y tomar uno o más usuarios especificando acciones basadas en modelos del registro.

Swatch está disponible en:

http://www.oit.ucsb.edu/~eta/swatch/

Courtney

Este software de dominio público sirve para identificar la máquina origen que intenta realizar ataques mediante herramientas de tipo *SATAN*. El programa es un script perl que trabaja conjuntamente con tcpdump. *Courtney* recibe entradas desde tcpdump y controla la presencia de peticiones a nuevos servicios del stack TCP/IP (las herramientas de este tipo realizan ataques, revisando de forma ordenada todos los puertos TCP y UDP que tiene el sistema, para poder ver qué servicios tiene instalados dicha máquina), si se detecta que se está produciendo una continua revisión de éstos puertos en un breve intervalo de tiempo, *Courtney* da un aviso. Este aviso se manda vía syslog.

Courtney puede generar dos tipos de alarmas dependiendo del ataque que se esté produciendo (normal o "heavy", las herramientas como *SATAN* dispone de distintos grados de revisión de la máquina).

Esta herramienta necesita el intérprete de **PERL** y el **tcpdump**.

Spar Show Process Accounting Records (Spar)

Su autor es Dough Schales. Es un programa que analiza y despliega los registros de contabilidad de procesos de un sistema Unix, de forma mucho más flexible que los programas estándar como *lastcomm*.

Está disponible en:

ftp://net.tamu.edu/pub/security/TAMU/

Watcher

Este paquete de Kenneth Ingham es una herramienta de monitoreo de sistemas expandible que verifica un número de comandos especificados por el usuario, analizando la salida, localizando elementos significativos y reportando éstos al administrador del sistema.

Está disponible en:

ftp://ftp.unm.edu/pub/unix/

Snort

Snort es un IDS (sistema de detección de intrusión). Funciona en cualquier plataforma capaz de usar *libpcap* que pueden ser utilizadas como sniffer/logger de sistema de detección de intrusos en redes de poca carga. Este último, se requiere para utilizar *snort*. *Snort* es capaz de analizar el tráfico IP y provee un *logging* muy fuerte. Se basa en scripts de reglas, es decir, que pueden vigilar lo que quieran. *Snort* llega con muchas reglas básicas: backdoor, ddos, finger, ftp. Estas reglas se definen en los archivos *snort-lib*.

Además, de ser un sniffer/logger de paquetes flexible para detectar ataques, sus principales características del *logging* están basadas en reglas que pueden ser representadas por búsqueda/concordancia del contenido, adicionalmente puede ser utilizado para detectar gran variedad de otros ataques y pruebas, como los buffer overflow, *scaneo* de puertos sigilosos, ataques CGI, SMB, y mucho más. *Snort* tiene la capacidad de alerta en tiempo real, con alertas enviadas a *syslog* a un archivo separada de "alerta", o incluso a una computadora Windows a través de Samba.

Snort es sin duda el mejor sniffer/logger que hay en estos momentos para pequeñas redes, el uso de reglas sencillas y el uso de fingerprint hace sencillo el detectar cualquier ataque que atente contra el sistema. Algunos de los detalles que tiene es la imposibilidad de *loggear* la dirección IP del atacante, aunque esto se puede solventar utilizando conjuntamente *tcpdump*.

Snort se encuentra disponible en:

http://www.snort.org/

Portsentry

El autor de *Portsentry* es Craig H. Rowland. Es un programa libre, utilizado para monitorear los puertos que se le indiquen que deben permanecer siempre inactivos. En caso de llegar una conexión a uno de ellos puede marcarlo en la bitácora del sistema, bloquear toda la comunicación con la máquina identificada como agresora y/o correr un comando externo.

Se recomienda visitar la siguiente dirección http://www.psionic.com/abacus/portsentry/ si no se tiene idea de que es el *scaneo* port/stealh antes de la instalación de *Portsentry*.

De otra manera, podrá fácilmente cerrar *hosts* que no desea (por ejemplo, su Servidor NFS o servidor de nombres).

Hunt

La principal meta del proyecto *HUNT* es desarrollar una herramienta para explotar las debilidades bien conocidas del protocolo de TCP/IP.

Es un sniffer avanzado de paquetes y de detección de intrusos en una conexión. *Hunt* es un programa para introducirse en una conexión, observar y resetear. *Hunt* es operativo en Ethernet y utilizado en su mayoría, para conexiones que pueden ser observadas a través de él. Por supuesto, es posible hacerlo con *hosts* en otros segmentos o *hosts* que están en switches ports.

Requerimientos del sistema	Linux 2.2, GlibC 2.1 con LinuxThreads, Ethernet
Medios probados	10/100Mb ethernet, Linux 2.0, Linux 2.1, 2.2, Solaris 2.5.1, NT4sp3/4, Win95, OSF1 V4.0D, HPUX 10.20, IRIX 6.2, pSOS BayNetworks 28115, 28200, 301 switches 3Com SuperStack II 3000, 1000 switches

Se puede obtener más información de *Hunt* en la siguiente dirección:

http://lin.fsid.cvut.cz/~kra/index.html#HUNT

scanlogd

Es una herramienta de detección del *scaneo* del puerto TCP, diseñada por Solar Designer para ilustrar varios ataques.

Detecta *scaneos* y *loggeos* al puerto TCP. Detecta los *scaneos* al puerto y escribe una línea por *scaneo* vía *syslog*. Si una dirección fuente envía múltiples paquetes a diversos puertos en un corto tiempo, el acontecimiento será registrado.
scanlogd está disponible en:

http://www.openwall.com/scanlogd/

NFR

NFR Security es el líder en soluciones de seguridad que detecta y responde a los ataques del ciberespacio. **NFR's Intrusion Management System** (*Sistema de Administración de Intrusos NFR*) va más allá del tradicional sistema de red o del sistema de detección de intrusos en la red, tiene una cobertura punto a punto en la línea del ataque - antes, durante, después, y en curso durante la exposición de este, detección de intrusos en la red, detección de intrusos en el *host*, investigación de los acontecimientos de seguridad y un rango de mecanismos de respuesta preactivos y reactivos.

Desde su fundación en 1996, *NFR* ha demostrado tener una compresión profunda dentro del mercado de detección de intrusos, y ha establecido una fuerte reputación en la innovación de productos y superioridad técnica. Está acreditada con varias "introducciones originales" en el campo incluyendo:

- Proporciona cerca de 500 firmas ataque.
- Publica firmas de ataque en código fuente para que el usuario las revise y modifique.
- Apoya a redes grandes.
- Proporciona un seguro, en la administración distribuida de sensores.
- Proporciona un sistema de prueba forzada que es fácil de instalar y mantener.

En la siguiente dirección se puede obtener más información acerca de *NFR*:

http://www.nfr.com/about/

Lids

LIDS es un sistema de detección/defensa en el kernel de Linux. El objetivo es proteger el sistema contra intrusiones de *root*, deshabilitando algunas llamadas al sistema en el mismo kernel. Si necesita alguna vez la administración del sistema, puede deshabilitar la protección *LIDS*.

Se comenta que es una gran herramienta, siempre y cuando no se hagan muy a menudo tareas administrativas.

Podemos destacar que *Lids* es:

- Parche del kernel y herramienta de administración para realzar la seguridad del kernel de Linux.

- Implementación de la referencia del monitoreo en el kernel.
- Control de Acceso Obligatorio en el núcleo.
- Proyecto activo con muchos hackers útiles.

Entre sus principales características están:

- Protección de archivos: nadie incluyendo *root* puede modificar los archivos protegidos-lids. El archivo puede ser ocultado.
- Proceso de protección: nadie incluyendo *root* puede matar al proceso protegido. El proceso puede ser ocultado.
- Control de Acceso con ACL's.
- Capacidad de uso para controlar el sistema entero.
- Alarma de seguridad del kernel.
- *Scanner* de puertos en el kernel.

En la siguiente dirección puede obtener mayor información sobre el Proyecto *Lids*:

http://www.be.lids.org/about.html

HostSentry

HostSentry es parte del Proyecto Abacus. Es una herramienta basada en la detección de intrusos que realiza la Detección de una Anomalía en la Conexión (LAD). Esta herramienta permite que los administradores observen la actividad sospechosa de una conexión y que respondan rápidamente a las cuentas comprometidas y al comportamiento inusual. HostSentry incorpora una base de datos dinámica y actualmente aprende el comportamiento de la conexión del usuario. Este comportamiento entonces es utilizado por las firmas modulares para detectar acontecimientos inusuales.

Sus principales características son:

- Detecta la actividad de un usuario inusual que se autenticó.
- Detecta la autenticación de dominios sospechosos.
- Detecta directorios de usuarios sospechosos.
- Detecta historia de comandos tecleados y los archivos de autenticación.
- Detectan los módulos de firmas de autenticación desconocidas.

En la siguiente dirección se puede obtener más información sobre hostsentry:

http://www.psionic.com/products/hostsentry.html

7.6 Anti-spam

Originalmente *'Spam'* se llamo al jamón con especias (Spiced Ham) producido por Hormel en 1926 como el primer producto de carne enlatada que no requería refrigeración. Esta característica hacía que estuviera en todas partes, incluyendo en los ejércitos americanos y rusos de la segunda guerra mundial. Tal vez, por esto se ha utilizado el término para calificar el correo electrónico no solicitado, y se ha convertido en una de las mayores molestias para las personas en la red.

El "*spam*" cuesta muy poco dinero a quien lo envía, porque la mayoría de los costos son pagados por los proveedores del sistema de Internet y los propios receptores del mensaje. La mayoría del "*spam*" es publicidad comercial, generalmente de productos o servicios de calidad dudosa, esquemas para hacerse rico rápido o para promocionar entradas a sitios de poca relevancia (generalmente, promocionando pornografía u otras propuestas ilegales).

Spam es la palabra que se utiliza para calificar el correo no solicitado enviado por Internet. La mayor razón para ser indeseable es que la mayoría de las personas conectadas a Internet no goza de una conexión que no les cueste, y adicionalmente reciben un cobro por uso del buzón. Por lo tanto, el envío indiscriminado de este tipo de correo ocasiona costos al lector, ya que utilizan tiempo y ancho de banda de las conexiones de Internet.

Cuando grandes cantidades de correo son dirigidas a o a través de un único sitio, este puede causar un cierre del servicio como causa de una pérdida de conexión a la red, caída del sistema o fallo de un servicio por causa de:

- Saturación de las conexiones.
- Uso de todos los recursos disponibles del sistema.
- Falta de espacio en el disco duro como consecuencia de la multitud de mensajes.
- Muchas veces el sistema pareciera perezoso (el e-mail es lento o no parece que sea enviado ni recibido), la razón puede ser que el sistema está intentando procesar un número alto de mensajes.

Un servidor de correos no sólo puede tener este problema de envío de correos masivos, sino también puede ser víctima de que lo utilicen para enviar virus o correos que han sido interceptados y modificados. Para evitar este tipo de problemas, se pueden emplear algunas herramientas como las siguientes:

SpamAssassin

El *SpamAssassin* es un filtro basado en scripts en Perl, que procesan los mensajes y detectan, en base a unas reglas bastantes complejas, si el mensaje es un *spam*. El resultado de filtrar los mensajes es un puntaje, que si supera determinado valor (5.0 por defecto) es considerado un *spam*.

Envía e-mails falsos que simulan un mensaje de error de dirección incorrecta lo que hace pensar a la compañía *Spam* que esa dirección no existe y por lo tanto, dejará de enviar mensajes a la dirección. Como no todas las veces se lo creen, entonces tiene otro sistema en el que la mete a una particular lista negra de direcciones, en la que ignorará automáticamente todos los mensajes con contenido molesto.

La mejor manera de hacerlo funcionar es arrancar el demonio *spamd* y comunicarse con él a través del *spamc*. De esta forma, se ahorra varios ciclos de CPU arrancando el Perl.

El paquete *SpamAssassin* instala los scripts de Perl y el demonio *spamd*. Por otro lado, el *spamc* provee el cliente (*spamc*) que se comunica con el *spamd*.

PGP

PGP (Pretty Good Privacy) como ya se había mencionado anteriormente, es un programa para cifrado del correo electrónico (y para todo tipo de información) que reúne tres características: es rápido, seguro y gratis.

Básicamente, *PGP* puede ofrecer dos cosas:

- Nadie leerá el correo electrónico (e-mail) salvo su destinatario. Es decir, tendrá "intimidad" mediante cifrado o encriptado de su mensaje.
- Nadie podrá suplantar su identidad en Internet y enviar mensajes trucados, así como retocar o alterar los originales.

PGP usa la tecnología conocida como criptografía de clave pública. Hace uso de dos claves para cifrar y descifrar el correo, una pública y otra privada. Ambas son complementarias, hermanas, ligadas por un complejo algoritmo informático y conociendo una, no se puede obtener la otra. Esta pareja de claves se generan una sola vez y sería lo primero que se haría para usar *PGP*. Virtualmente, sería imposible que dos personas tuvieran las mismas claves.

Ahora, lo que se hace es: por un lado distribuir ampliamente la clave pública, en las páginas WEB, en los servidores dedicados a tal fin, en la cuenta de trabajo (si se tiene); y por otro guardar celosamente la clave privada en la computadora, de manera que nadie pueda obtenerla, y en el caso de que la obtenga, para usarla, deberá conocer una clave secreta o "password" que sólo la conoce quien la distribuye y que no tendrá apuntada en ningún sitio.

Para escribir un mensaje cifrado, primero se deberá obtener la clave pública del destinatario (de cualquiera de las formas expuestas, por ejemplo, de su página WEB) y se encripta el mensaje con esa clave pública, que sólo será posible descifrar con su clave "hermana", la misma que el destinatario tiene protegida por un "password" que sólo él sabe.

Aunque, parezca un poco complicado, es una forma sencilla y muy potente de encriptar mensajes, tanto que el algoritmo matemático encargado de generar la pareja de claves pública y privada (inicialmente el RSA) ha sido fruto de innumerables problemas legales, dado que el *PGP* se escribió inicialmente en los USA, donde el software de criptografía se considera ilegal exportarlo, como el armamento estratégico.

Adicionalmente, con *PGP* se puede firmar digitalmente un mensaje, esto quiere decir que el destinatario puede comprobar si lo que le llega pertenece a su remitente y esta íntegro, es decir, no ha sido alterado en el camino. En este caso, el proceso es al revés, se encripta el mensaje con la clave privada y el destinatario lo abre con la clave pública (que deberá recogerla de alguno de los modos comentados), comprobando automáticamente la veracidad y la integridad del mensaje.

En estos momentos hay dos versiones disponibles: la 2.6.3 y la 5.0 (aunque acaba de salir la 5.53i para otras plataformas, para UNIX la ultima versión es la 5.0i, pero se está hablando ya de la 6.0i).

Mail Scanner

Mail Scanner es sistema anti-spammer y *scanner* de virus para el correo electrónico. Es capaz de detectar un gran número de tipos de correos electrónicos comerciales de publicidad (*spam*). No sólo posibilita el *scaneo* de virus conocidos, sino que también amplía su protección a los no conocidos,

revisando los archivos adjuntos o attachments y rechazando los que contengan una serie de patrones que MS tiene predeterminados como no aceptados. En los mencionados patrones, se destaca el de extensión de archivo, mediante el cual rechaza mails que contengan una serie de extensiones (por ejemplo. "txt,vbs").

Otra característica destacable es la posible desinfección de adjuntos en los mails (por ejemplo, un macro de Word) es automáticamente desinfectado y a continuación es enviado a su destino original. Es sencillo de instalar en un servidor, sin necesidad de cambiar la configuración inicial del programa al que se desea integrar. Soporta clientes sendmail y Exim MTAs, y antivirus comerciales como Sophos y McAfee, o gratuitos como F-Prot.

Otra de sus funciones básicas es el evitar los ataques de tipo DoS. Una herramienta muy útil para administradores de servidores de Internet bajo Linux.

7.7 Firewalls

Actualmente, hay mucho ruido alrededor de la palabra "*firewall*"; parte de esto es creado del lado corporativo, mientras otra parte se relaciona realmente con la funcionalidad de un *firewall.* El error de concepción más común es que los *firewalls* son un tipo de dispositivo mágico de seguridad en redes que pondrá fin a todas las preocupaciones de seguridad de un administrador. Esto no podría estar más alejado de la verdad; un *firewall* está diseñado para proveer servicios de IP avanzados como el filtrado de paquetes, redirección de puertos y traducción de direcciones de red. Un *firewall* bien configurado debe ser parte de toda red segura. Simplemente no es lo único que hay por saber de seguridad en redes.

Es clara la intención inicial del uso del *firewall*, pero adicionalmente permite obtener ventajas en campos que van más allá de la seguridad como tal; entre otras se pueden mencionar las siguientes:

- Es un punto centralizado para las decisiones de seguridad.
- Puede reforzar la política de seguridad.
- Puede rastrear la actividad Internet eficientemente.
- Limita la revelación de su red al público.

Algunas de las debilidades de los *firewalls* son:

- No protege de usuarios internos maliciosos.
- No puede proteger contra conexiones que no pasan a través de él.
- No tiene un esquema de protección para cada nueva amenaza.
- No puede proteger contra virus.

Cuando se habla a cerca del diseño e implementación de arquitecturas de *firewalls,* es necesario clarificar una serie de términos para describir los componentes de la arquitectura, algunos de ellos son:

Screening Router: Es un componente básico de la mayoría de *firewalls,* puede ser un enrutador comercial o un enrutador basado en un servidor con alguna clase de software para filtrado de paquetes. Típicamente, tienen la habilidad de bloquear tráfico entre redes o máquinas específicas a nivel de puerto IP. Algunos *firewalls* consisten solamente en un *Screening router*, entre una red privada e Internet.

Es muy usado para la implementación de filtrado de paquetes, en la cual se permiten o bloquean ciertos tipos de paquetes para reflejar la política de seguridad corporativa, el esquema de diseño se muestra en la figura 7.1.

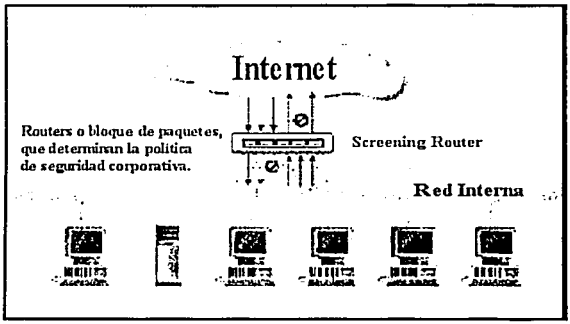


Figura 7.1. Esquema de diseño *Screening Router*.

Bastion Host: Es un sistema identificado por el administrador del *firewall* como un punto crítico en el sistema de seguridad de la red, generalmente tienen algún grado de extra protección.

Dual Homed Gateway: Algunos *firewalls* son implementados sin un *Screening Router* colocando una máquina de cara a la red interna por un lado y a Internet por el otro (2 interfaz de red) y deshabilitando el TCP/IP *forwarding*. De esta manera, las computadoras de la red privada se pueden comunicar con el *gateway*, así como los de Internet también, pero el tráfico directo entre las redes no es posible. La figura 7.2 muestra como es el esquema más común para implementaciones a través de *Dual Homed Gateway* o *Dual Homed Host*, como se puede ver, por definición un *Dual Homed Gateway* es un *Bastion Host*.

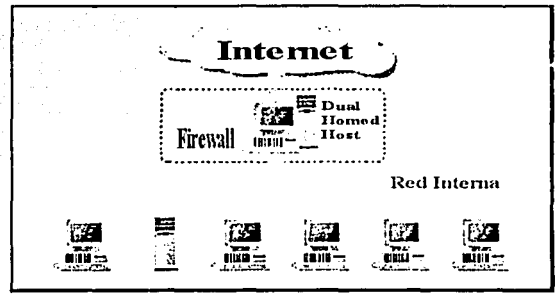


Figura 7.2. Esquema de diseño *Dual Homed Gateway*.

Screened Host Gateway: Es quizás la configuración más común de *firewall*, es implementada usando un *Bastion Host* y un *Screening Router*. Usualmente, el *Bastión Host* está ubicado en la red privada y el *Screening Router* está configurado de tal forma que el *Bastion Host* es el único sistema en la red privada que se puede alcanzar desde Internet. A menudo, el *Screening Router* es configurado para evitar tráfico hacia el *Bastion Host* en puertos específicos permitiendo a un número reducido de servicios comunicarse con él.

La figura 7.3 muestra un esquema típico del *Screened Host Gateway*.

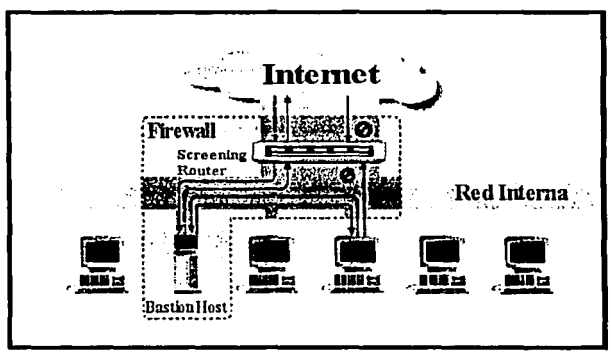


Figura 7.3. Esquema de diseño *Screenes Host Gateway*.

Screened Subnet: En algunas implementaciones para *firewalls* se crea una subred aparte, situada entre Internet y la red privada. Típicamente, esta red es aislada usando *Screening router*, lo cual permite

implantar niveles de filtramiento de paquetes variable. Generalmente una *Screened Subnet* es configurada de tal forma que tanto las máquinas de la red privada y de Internet tienen acceso a los que componen esta subred *(Screened Subnet)*, pero el tráfico a través de la *Screened Subnet* no es permitido. La figura 7.4 muestra el esquema típico para este tipo de implementación.

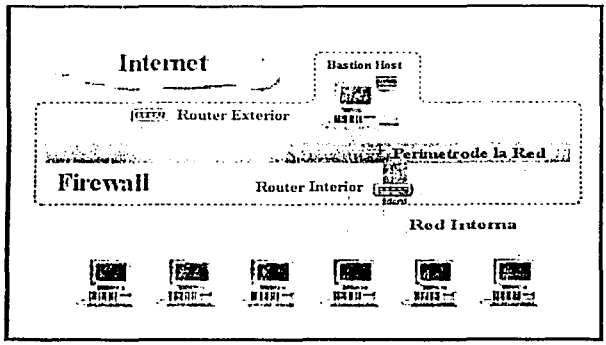


Figura 7.4. Esquema de diseño *Screened Subnet.*

Application Level Gateway: También es conocido como *Proxy Gateway.* Son reflectores o "Proveedores" de servicios específicos, los cuales operan la mayoría de las veces a nivel de aplicación de usuarios más que a nivel de protocolo. Generalmente, estos servicios de "reflexión o pasada", cuando están ejecutándose en un *firewall* son puntos importantes para la totalidad de la seguridad de la red. Los servicios *proxy* son más o menos transparentes entre los usuarios de la red interna y un servicio de la red externa, en vez de "hablar" directamente cada uno "habla" a un *proxy.* Para el usuario, un servidor proxy presenta la ilusión de que el contacto ha sido hecho directamente con el servidor remoto. La configuración típica se muestra en la figura 7.5.

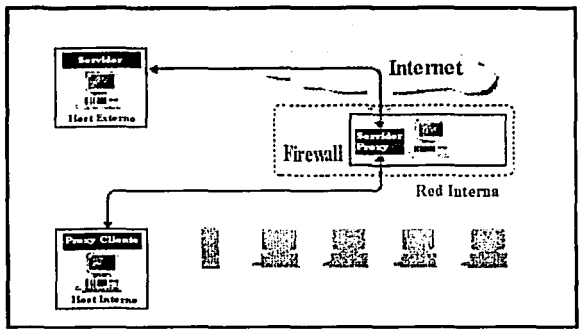


Figura 7.5. Esquema de diseño *Application Level Gateway*.

En general, no se puede hablar de cuál método es el mejor, ya que existen muchos factores para determinar cuál es el mejor *firewall* para una situación específica, entre otros, los factores más influyentes son: costos, política corporativa de seguridad, tecnologías de red existentes, políticas al interior de la organización; todos éstos pueden prevalecer sobre la consideración técnica justificada para adoptar una plataforma de *firewall* concreta.

Los dos principales usos de un *firewall* son:

- Filtrar paquetes

  Un filtro de paquetes, o packet filter, es un sistema, de software o hardware embebido de firmware, que valiéndose de la lectura de los headers de cada paquete, realiza un "*accept*" (aceptación del paquete), "*reject*" (descarte del paquete, informando de dónde vino), o un "*deny*" (descarte del paquete, sin dejar huellas).

  Lo más interesante de todo, es que *Linux*, con su sencillez, posee la capacidad de realizar filtrado de paquetes en su propio kernel, así como un gran conjunto de acciones a desarrollar con los mismos. En Linux dependiendo de la versión del kernel se tienen distintas herramientas como son:

  - *ipfwadm.* La utilidad **ipfwadm** (el administrador del *firewall* de IP) es la herramienta que se utiliza para construir las reglas del firewall para todos los núcleos anteriores al 2.2.0. La sintaxis de las órdenes puede resultar muy confusa. La utilidad **ipfwadm** se incluye en la mayoría de las distribuciones modernas de Linux, aunque quizás no por defecto.
  - *ipchains.* Al igual que la utilidad **ipfwadm**, la utilidad **ipchains** puede resultar algo desconcertante al principio. Proporciona toda la flexibilidad de **ipfwadm** con una sintaxis simplificada, y además proporciona un mecanismo de "encadenamiento" que le permite gestionar múltiples conjuntos de reglas y enlazarlas conjuntamente. La orden **ipchains** aparece en la mayoría de las distribuciones de Linux basadas en los núcleos 2.2.

- *iptables.* La sintaxis de la utilidad **iptables** es bastante similar a la de **ipchains.** Los cambios consisten en mejoras y en el resultado del rediseño de la herramienta para que sea extensible a través de librerías dinámicas. La utilidad **iptables** se incluye en el paquete de código fuente de *netfilter.* También estará incluido en cualquier distribución basada en la serie de núcleos 2.4.

Una de las implementaciones más comunes de *firewalls* (y muy buena para propósitos educativos) es una máquina que hace NAT (*Network Address Translation*, traducción de direcciones de red) y actúa como una puerta de acceso a Internet para pequeñas redes. Esta tiene una funcionalidad similar a la que ofrece Linux a través de IPMASQ, pero es muy diferente en términos de configuración e implementación.

IP-Masquerading posibilita la conexión de varias computadoras a Internet usando una máquina Linux con solo una IP pública. Esto quiere decir, que se puede conectar una red privada a Internet y el proveedor de Internet creerá que sólo se tiene una computadora conectada.

➢ Servicio de Proxy

Los servidores proxy son un invento que permite el acceso directo a Internet detrás de un firewall. Funcionan abriendo un socket en el servidor y permitiendo la comunicación con Internet a través de él.

Capítulo 8

Implantación de Medidas de Seguridad en la Unidad de Servicios de Cómputo Académico

8.1 UNICA

La Unidad de Servicios de Cómputo Académico (UNICA) es una dependencia de la Secretaría General de la Facultad de Ingeniería, cuya finalidad principal es la de proporcionar, en el ámbito institucional, los servicios de apoyo en cómputo que la comunidad de la Facultad requiere, recursos de cómputo comerciales y de alta especialización que el avance de la educación, el desarrollo de la informática y el ejercicio profesional demanden.

La misión de UNICA es mantener el liderazgo y estar a la vanguardia en cómputo tanto dentro de la Facultad de Ingeniería como en el entorno universitario.

En UNICA, el objetivo principal es cumplir con los requerimientos de los usuarios en el área de cómputo, teniendo como meta elevar la calidad de sus productos y servicios, para ello se compromete en un proceso de mejora continua.

Los objetivos generales de UNICA son:

- Proporcionar a nivel institucional los servicios de apoyo en cómputo que los alumnos de la Facultad requieren para la realización y cumplimiento eficaz de sus tareas sustantivas.
- Apoyar a la Secretaría General en las actividades que involucren institucionalmente a la Facultad de Ingeniería.
- Proporcionar Servicios de cómputo de calidad a la comunidad de la Facultad de Ingeniería.
- Desarrollar sistemas de información en apoyo a las actividades académicas.
- Formar recursos humanos de calidad no sólo en el área de cómputo sino también en su vida profesional a través del Programa de formación de becarios UNICA.
- Proporcionar asesoría especializada en tópicos de cómputo a la comunidad de la Facultad de Ingeniería.
- Desarrollar material didáctico.
- Investigar y desarrollar nuevas tecnologías que favorezcan que la Facultad se mantenga a la vanguardia en cuanto a cómputo se refiere.
- Implementar y dar mantenimiento de la red de cómputo de la Facultad de Ingeniería.
- Apoyar en el soporte técnico a Secretarías y Divisiones de Facultad de Ingeniería.
- Mantener la operación de los servidores de aplicaciones (correo, bases de datos, WEB) que utilizan los usuarios para el desarrollo de sus funciones.
- Mantener la seguridad de la información.

La estructura organizativa de UNICA se muestra en la figura 8.1, en ella se observa al Departamento de Redes y Operación de Servidores, que es el responsable de la administración, operación, mantenimiento y seguridad de la red de comunicación de la Facultad y de la intercomunicación de la red central de la UNAM; así como del desarrollo e implementación de proyectos para la expansión del servicio.

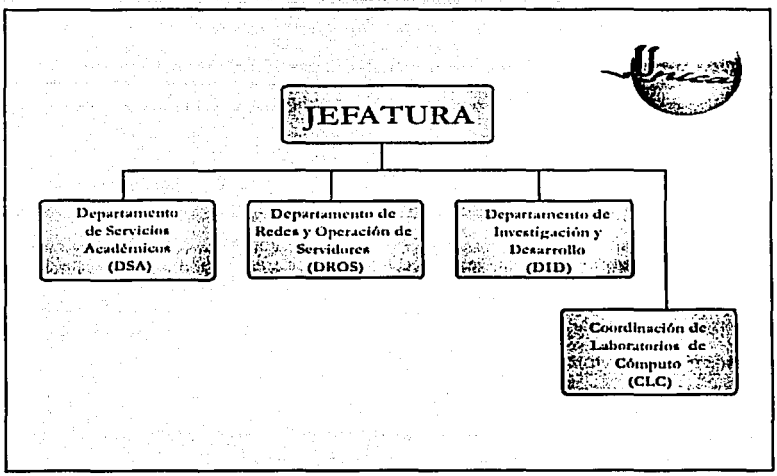


Figura 8.1. Estructura organizativa de UNICA.

Las principales actividades y funciones que realiza el Departamento de Redes y Operación de Servidores son:

Área Unix

- ✓ Mantenimiento a los servidores UNIX (LINUX, SOLARIS, HP-UX) en sus cuatro principales funciones:

  1) Usuario.
  2) Monitoreo.
  3) Seguridad.
  4) Aplicación.

- ✓ Instalación y levantamiento de servidores UNIX.
- ✓ Actualización de las versiones de Sistema Operativo, así como de las aplicaciones con las que cuentan estos servidores.
- ✓ Verificar la integridad y seguridad de la información, evitando posibles ataques.
- ✓ Mantenimiento de la Base de Datos Postgres.

  1) Levantamiento de las Bases.
  2) Creación de Usuarios.

- ✓ Respaldos periódicos de los servidores de misión críticos.
- ✓ Asesoría a Usuarios.
- ✓ Cuentas de Correo: Altas, bajas y cambios de cuentas de correo electrónico, en cancun.fi-a.unam.mx.
- ✓ Monitoreo.- Verificar que los servicios electrónicos que los servidores proporcionan se encuentren activos.
- ✓ Elaboración de pequeños manuales de uso de servicios.
- ✓ Coordinación y logística para eventos de informática (pláticas, conferencias, talleres, etc.).
- ✓ Elaboración de informes solicitados.

Funciones en la Web principal de la Facultad de Ingeniería:

- ✓ Mantener la operación física del servidor Web.
- ✓ Instalar, mantener y actualizar el sistema operativo del servidor
- ✓ Instalar, mantener y actualizar el software de administración del Web.
- ✓ Implementar la Seguridad del Sitio Web y el Sistema Operativo, así como la revisión de bitácoras.
- ✓ Instalar las aplicaciones requeridas para la operación del sitio Web.
- ✓ Realizar los respaldos del servidor Web.
- ✓ Asesorar técnicamente a las áreas de la Facultad en tópicos relacionados con la Web.
- ✓ Proponer nuevas innovaciones de tecnología para crear servicios del Web para el beneficio de la Facultad (como el caso del Webmail y SSH web)

Incidentes de Seguridad

- ✓ Apoyo al responsable de administración en red.
- ✓ Atender llamados de reportes del equipo de cómputo de la DGSCA.
- ✓ Distribuir los reportes a las áreas solicitadas.
- ✓ Verificar que los reportes se atiendan.

Redes

- ✓ Asesoría de conectividad a través de cableado estructurado para voz y datos en las diversas áreas de la Facultad.
- ✓ Monitoreo del tráfico de la red de datos.
- ✓ Instalación y administración de equipos activos de la red.
- ✓ Instalación y administración del protocolo TCP/IP (Direcciones públicas y privadas).
- ✓ Soporte técnico a los usuarios de la infraestructura de la red de cómputo.
- ✓ Capacitación al personal de apoyo sobre tecnología de telecomunicaciones.
- ✓ Participación en proyectos en cómputo y telecomunicaciones de Secretaría General.

Soporte Técnico y plataforma Windows

- ✓ Instalación de sistemas operativos a computadoras personales.
- ✓ Instalación y configuración de software de aplicación.
- ✓ Asesorías técnicas en uso y manejo de software.

- ✓ Instalación y mantenimiento de servicios de impresión en red.
- ✓ Instalación de software para correo electrónico y conexión a Internet.
- ✓ Control de préstamo de software al personal de la Secretaría General.
- ✓ Mantenimiento a los servidores Windows (WNT , Windows 2000 Server) en sus cuatro principales funciones:

  1) Usuario.
  2) Monitoreo.
  3) Seguridad.
  4) Aplicación.

- ✓ Instalación y levantamiento de servidores Windows (WNT, profesional, W2000 server).
- ✓ Actualización de las versiones de Sistema Operativo, así como de las aplicaciones con las que cuentan estos servidores.
- ✓ Verificar la integridad y seguridad de la información, evitando posibles ataques.
- ✓ Creación de Usuarios.
- ✓ Respaldos periódicos de los servidores de misión crítica.
- ✓ Asesoría a Usuarios.
- ✓ Monitoreo.- Verificar que los servicios electrónicos que los servidores proporcionan se encuentren activos.
- ✓ Elaboración de informes solicitados.

Otras Actividades

- ✓ Proponer, actualizar, modificar la normatividad del web de la Facultad de Ingeniería y políticas de cómputo.
- ✓ Coordinar el Subcomité de Administradores y fungir como el área que administra la red de Cómputo General ante DGSCA
- ✓ Coordinar el subcomité de administradores de red de cómputo.

Por otra parte, en UNICA existen varios servidores que trabajan con el sistema operativo Linux Red Hat, los cuales serán descritos en el Análisis de Riesgos.

8.2 Análisis de Riesgos

Como se había mencionado en el Capítulo 4, el análisis de riesgos es uno de los aspectos más importantes, ya que a partir de éste se va a definir qué recursos de nuestra red necesitan ser protegidos contra cualquier amenaza.

Por esta razón, el objetivo de UNICA es proteger tanto los dispositivos (computadoras, servidores, switch, hub's, etc.), así como la información que le ha sido confiada. Esta última es la que nos interesa proteger, debido a que puede ser uno de los activos favoritos de los hackers, crackers o cualquier otro delincuente informático ansioso de hacer de las suyas.

En relación a la seguridad de los sistemas, la situación en que se encontraba UNICA, presentó la siguiente problemática y situaciones:

- Inexistencia de políticas de seguridad enfocadas a: cuentas de usuarios, contraseñas, control de acceso, uso adecuado del sistema, respaldos, correo electrónico, etc. Las cuales puedan ser aplicadas en UNICA.
- Cuentas de usuarios, las cuales:
  - Ya no se utilizaban, pero seguían presentes en el archivo */etc/password* o aunque no existía en ese archivo, existía su *home*.
  - Las contraseñas son fáciles de adivinar.
- Algunos usuarios mientras se ausentan, dejan sus sesiones abiertas sin protección alguna.
- Inexistencia de un firewall.
- No se contaba con un detector de intrusos.
- No existían procedimientos para restablecer el funcionamiento de un servidor, durante y después de un incidente.
- No se contaba con un antivirus para los correos de entrada/salida.
- No se contaba con un área de seguridad.
- No existían medidas de seguridad física robustas. Debido a la zona geográfica en la que se encuentra la Unidad, la posibilidad de que ocurra un terremoto o una inundación es mínima, pero se destaca la necesidad de crear medidas que reduzcan el riesgo de incendios. Además, se tiene la necesidad de un mayor control del equipo, debido al robo que se ha efectuado en la Unidad.

Tomando en cuenta lo anterior, comenzaremos por evaluar el riesgo de los recursos de la red UNICA, la cual cuenta con la siguiente estructura:

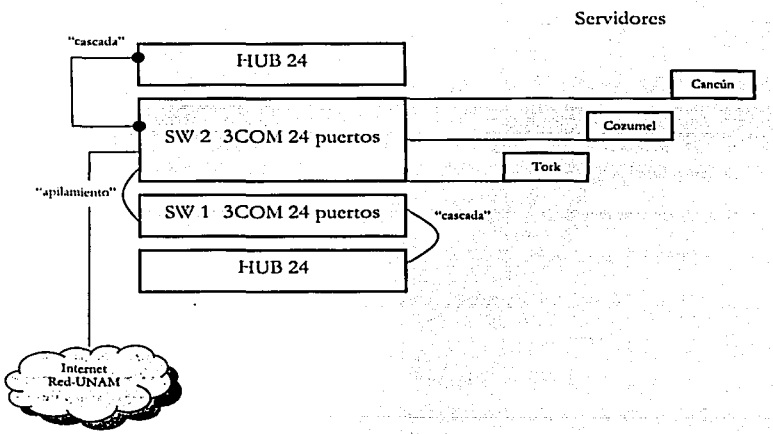


Figura 8.2. Red UNICA.

Como se puede observar en la figura anterior, UNICA cuenta con dos *switches* "apilados" conectados en cascada con dos *hubs*. Del *switch* 2 están conectados tres servidores: Cancun, Cozumel y Tork, los cuales proporcionan diferentes servicios a la comunidad de la Facultad de Ingeniería, éstos se describen brevemente a continuación:

- *Servidor Cancun.*- Proporciona el servicio de correo electrónico y de *ssh* por Web, guarda toda la información de los usuarios, cuenta con NIS (*Network Information Services*) y NFS (*Network File System*), a pesar de que no es el servidor de Web tiene este servicio por contar con el sistema de inscripciones de uso de las salas.

- *Servidor Cozumel.*- Es el servidor Web, el cual cuenta con php y el manejador de bases de datos Postgres. Además, los usuarios pueden hacer su página Web y solicitar que resida en Cozumel, siempre y cuando cumplan con el reglamento del Web.

- *Servidor Tork.*- Es el servidor de Bases de Datos (utiliza el manejador de bases de datos Postgres), proporcionando este servicio a aquellos usuarios que requieren tener una cuenta para poder hacer uso de la base de datos. Además, en él residen la mayoría de las aplicaciones desarrolladas en UNICA como:

  - SCOSU (Sistema de Control de Salas de UNICA).
  - SICC (Sistema de Inscripciones y Control de Cursos).
  - SICI (Sistema de Control de Inventarios).
  - SECC (Sistema de Encuestas de Cursos de Cómputo).

Para calcular el peso del riesgo del recurso, utilizaremos la fórmula vista en el capítulo 4:

$$WR_i = R_i * W_i$$

Donde:

WR_i: es el peso del riesgo del recurso "i" (también lo podemos llamar ponderación).

R_i: es el riesgo del recurso "i".

W_i: es la importancia del recurso "i".

Se ha hecho una estimación del riesgo y la importancia de los recursos de la red UNICA, recordando que éstos valores son totalmente subjetivos, ya que dependen de quien o quienes estén realizando la evaluación.

La siguiente tabla muestra cada uno de los valores de los recursos, así como el riesgo evaluado:

Recurso del sistema		Riesgo (R_i)	Importancia (W_i)	Riesgo Evaluado ($R_i * W_i$)
Número	Nombre			
1	Hub 1	3	4	12
2	Hub 2	3	5	15
3	Switch 1	3	7	21
4	Switch 2	3	7	21
5	Servidor Cancun	9	10	90
6	Servidor Cozumel	6	9	54
7	Servidor Tork	7	9	63

Tabla 8.1. Evaluación del riesgo de la red UNICA.

Los valores que se asignaron tanto para el riesgo como para la importancia se hicieron considerando lo siguiente:

- Tanto los hub's como los switches se encuentran en un lugar bajo llave, en el cual sólo los responsables de ese equipo tienen acceso. Además, se les da el mantenimiento necesario, por lo que el riesgo de pérdida del recurso es mínimo. En cuanto a su importancia, cabe resaltar que la de los hub's es menor a la de los switches, porque en éstos últimos se encuentran conectados los servidores que prestan diferentes servicios a la comunidad de la Facultad de Ingeniería.
- El riesgo de perder al servidor Cancun es alto por toda la información que maneja, de ahí que su importancia también sea alta. Hay que considerar que son diferentes tipos de usuarios los que constantemente se conectan a él para hacer uso de servicios como el correo electrónico.
- El riesgo de perder al servidor Cozumel no es tan alto, pero su importancia sí lo es, debido a que es el servidor Web y en él se encuentra no sólo la página de la Facultad de Ingeniería, sino aplicaciones de usuarios. Además, se cuenta con un servidor de respaldo que ante una "baja" de su servicio entra en operación en 10 minutos.
- El riesgo de perder al servidor Tork es más alto que el del servidor Cozumel, debido a que es el servidor de Bases de Datos, donde muchas aplicaciones desarrolladas en UNICA hacen uso de él.

De acuerdo con la tabla, el recurso que más debe protegerse es el servidor Cancun, ya que su riesgo evaluado es el más alto. Por lo tanto, hay que buscar cuáles son las causas probables que pueden provocar problemas con los servicios brindados por él.

Calculando el riesgo general de los recursos de la red UNICA, tenemos que:

$$\Pi'_R = \frac{12 + 15 + 21 + 21 + 90 + 54 + 63}{4 + 5 + 7 + 7 + 10 + 9 + 9}$$

$$\Pi'_R = 5.41$$

Podemos observar que el riesgo total de la red UNICA es de menos de 6 puntos sobre 10, pero esto no quiere decir que no existan problemas, ya que hay que recordar que los riesgos evaluados son mayores en los servidores.

Hemos identificado que los servidores son los recursos cuya integridad está amenazada, lo cual puede influir en UNICA, por lo tanto es necesario identificar las amenazas a las que están expuestos.

Como se mencionó en el capítulo 1 existen diferentes tipos de amenaza como: acceso no autorizado; daño, robo o divulgación de la información; errores en el sistema, en la red; la falta de la seguridad física y las que suelen ser las más comunes, las humanas.

Por esta razón, es indispensable que se tenga una lista de las amenazas para ayudar principalmente a los administradores de la seguridad a identificar los distintos métodos, herramientas y técnicas de ataque que se pueden utilizar. Es importante que los administradores actualicen constantemente sus conocimientos en esta área, ya que los nuevos métodos, herramientas y técnicas para sabotear las medidas de seguridad evolucionan de forma continua.

Una de las cosas más difíciles es cómo se van a proteger esos recursos, puesto que el modo de protegerlo dependerá del recurso que se trate.

Hemos visto que los usuarios de la comunidad de la Facultad de Ingeniería son quienes utilizan los servidores dependiendo de las actividades que tengan, por lo que actualmente los administradores los tienen identificados por grupos de usuarios de acuerdo a las necesidades que presentan. Algunos grupos son: *profesorrs* (académicos de la Facultad de Ingeniería); *ssocial* (usuarios que realizan el servicio social en las salas de cómputo de UNICA); *prebes* (usuarios que entran al Plan de Formación de Becarios de UNICA); *civil, minas, electronico, computacion, telecom, geofisica, geologia, industrial, mecanica, mecanic-elec, petrolero, topografo,* éstos grupos hacen referencia a cada una de las carreras de la Facultad de Ingeniería; *posgrado* (usuarios que están realizando su posgrado); *tesista* (usuarios que se encuentran realizando su tesis); entre otros.

Debido a que ya se tienen identificados a los usuarios, se pueden determinar tanto los recursos que utilizarán, como los permisos que tendrán.

Por todo lo anterior, se ha recurrido a implantar políticas de seguridad, procedimientos, reglamentos, plan de contingencia y un código de ética; ya que si bien existen un reglamento

para el acceso a las salas de cómputo de UNICA y un reglamento de Web, no son suficientes para hacer frente a cualquier delito informático.

Sin embargo, los administradores han realizado algunas acciones que han permitido que la seguridad de los sistemas no sea tan vulnerable, por ejemplo:

- Quitar permisos a algunos comandos que permitirían a los usuarios obtener información del sistema que sólo debe conocer *root*, como son: *console helper, wall, chroot,chfn,chsh,chgrp,chpasswd,cc, perl,gcc,nmap, ypcat, make, rpcinfo, vmstat, free, mount, umount, netrport, pub, slocate, traceroute, traceroute6, gnome-pty-helper,utempter, pig6, change, gpasswd, newgrp, at, rpc, rlogin, rsh, crontab, mc, cons.saber, pt_chown, ssh-keysign, userhelper, usernetctl, pwdb_chkpwd, unix_ch pwd, suexec, ifconfig, ifup, ifdown, tcpdump, ismod, lsattr, chattr, route, iname, mysql, arch.*
- Cambiar el ftp por el comando *scp* cuando se trabaja en Linux. En Windows se tiene el Secure File Transfer Client.

Pero lo anterior no es suficiente, porque los administradores de la seguridad de UNICA se enfrentan constantemente a usuarios que no hacen un buen uso de los servicios o que intentan romper la seguridad de los servidores, principalmente de Cancun, debido a que no existe un documento en el cual se les informe de la sanción que tendrían por realizar ese tipo de ilícito. Proponemos unas políticas de seguridad que tratan de cubrir esta amenaza, mencionando también las sanciones a las que se harían acreedores todos aquellos que intenten hackear/crackear los servidores.

Con el propósito de que UNICA ofrezca un excelente servicio, lo mismo que cada una de las personas que la integran, se propone un código de ética con la finalidad de contribuir a un mejor desempeño tanto personal como laboral.

Uno de los temas principales es la ubicación del área de seguridad informática dentro del organigrama de UNICA, ya que una mala ubicación de esta puede causar conflictos o retrasar las actividades.

Finalmente, se propone un Plan de Contingencias para el servidor Cancun por ser uno de los más vulnerables a ser atacado por toda la información que en él se encuentra y por los servicios que ofrece a la comunidad de la Facultad de Ingeniería; asimismo, se contará con procedimientos preventivos y correctivos, que ayudarán considerablemente cuando se tenga una amenaza contra el sistema.

Aún con todas estas medidas de seguridad, estamos conscientes de que los riegos siempre estarán presentes, pues no se pueden eliminar completamente. Sin embargo, de esta manera podemos estar preparados para cualquier tipo de ataque, actuando de manera rápida para solucionar el problema.

8.3 Organigrama del Departamento de Redes y Operación de Servidores

De acuerdo con el Análisis de Riesgos se vio la necesidad de crear un área de seguridad y se propone el organigrama para el Departamento de Redes y Operación de Servidores, como se muestra en la figura 8.3, con el que será más fácil y eficiente realizar las diversas tareas de dicho departamento.

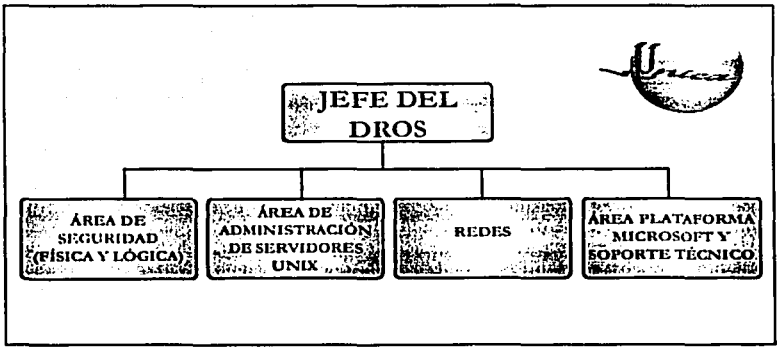


Figura 8.3. Organigrama del Departamento de Redes y Operación de Servidores.

A grandes rasgos, según el organigrama anterior, las funciones que realizarían serían las siguientes:

Jefe del DROS. Es el responsable de mantener y vigilar las actividades del DROS, es decir, la administración, operación, mantenimiento y seguridad de la red de comunicación de la Facultad de Ingeniería y de la intercomunicación con la red central de la UNAM.

Área de Administración de Servidores UNIX. Será la responsable de que el servidor de correo, el servidor de web y el servidor de base de datos proporcionen dichos servicios de manera eficiente.

Área de Seguridad.

- **Física.** Realizará un monitoreo diario de las instalaciones de UNICA para verificar la integridad y ubicación del equipo, mediante un formato (Ver Apéndice II) llevará el control del todos los movimientos que se tengan que realizar con el equipo de cómputo; realizará un inventario del equipo de cómputo de acuerdo al número de inventario de la UNAM; tendrá las llaves de los equipos; se coordinará con el área de mantenimiento para que pueda verificar que una vez que dicha área haya terminado de realizar el mantenimiento al equipo, este se encuentre con todos sus componentes;

capacitará e informará a todo el personal de UNICA sobre los procedimientos y medidas que hay que llevar a cabo antes y durante un sismo o un incendio, además de estar investigando más medidas de seguridad física.

- **Lógica.** Proteger los sistemas informáticos ante posibles amenazas, desarrollar, promocionar y actualizar las políticas en conjunto con el Área de Seguridad Física y el Área de Administración de Servidores; desarrollar e implementar el Plan de Seguridad; monitorear día a día la implementación y el uso de los mecanismos de seguridad de la información; coordinar investigaciones de incidentes de seguridad informática; revisar los *logs* de auditoría y sistemas de detección de intrusos; participar en los proyectos informáticos de UNICA para agregar consideraciones de seguridad informática e investigar nuevas herramientas de seguridad que sean necesarias para los servicios que proporciona UNICA.

8.4 Medidas de seguridad física

Dentro de nuestro caso de estudio, UNICA, y de acuerdo al análisis de riesgos en contra de desastres naturales, se obtuvo que se deben tener medidas contra un incendio por lo cual se hace la siguiente propuesta.

Propuesta contra incendio.

Debido a la localización y terreno en el cual se encuentra UNICA y a la naturaleza misma del área se proponen medidas necesarias para prevenir un incendio.

Medidas básicas contra un incendio:

- ✓ Contar con extintores adecuados en la sala. Para la Unidad se proponen que sean de: espuma y de CO_2. El primero cubre y humedece la materia inflamada (papel, madera, tela, etc.). El segundo es excelente para material eléctrico, debido a que no es conductor, no deja residuos y no deteriora; pero el uso de bióxido de carbono, debe reservarse, por el efecto letal que tiene sobre los seres humanos. Anteriormente se usaba el gas halón en lugar del CO_2; el halón es un gas inodoro, no nocivo para la salud y no afecta a los equipos de cómputo, también crea una atmósfera inerte y se dispesa muy rápidamente. Actualmente se estudia por situaciones de posible contaminación ambiental o efectos sobre la capa de ozono y por ello se prefiere el uso del CO_2.

- ✓ Deben ubicarse sufientes extintores portátiles de CO_2, tanto en la sala de cómputo como en el local del sistema de fuerza ininterrumpible en lugares estratégicos.

- ✓ Capacitar al personal encargado de la sala, en su uso.

- ✓ Contar con salidas de emergencia, así como con letreros que indiquen donde se encuentran.

- ✓ Un dispositivo manual de emergencia para cortar el sistema eléctrico y el aire acondicionado deberá instalarse en cada salida de la sala de cómputo.

- ✓ Las paredes del área del equipo de cómputo deben ser de material incombustible. Si el área del equipo de cómputo tiene una o más paredes exteriores adyacentes a un edificio que sea susceptible de incendio, la instalación de ventanas irrompibles mejorará la seguridad.

- ✓ El techo falso debe de ser de material incombustible o resistente al fuego.

- ✓ Todas las canalizaciones y materiales aislantes deben ser de materiales incombustibles y que no desprendan polvo.

- ✓ El piso falso instalado sobre el piso real debe ser incombustible. Se debe contemplar la posibilidad de poner un recubrimiento al piso, pared y plafón de material antiestático disipativo (AD). Es revestimiento pensado para la industria como por ejemplo: el ensamble de componentes eléctricos, electrónicos, salas de cómputo, áreas donde exista el potencial de riesgo de flamas o explosiones por el tipo de materiales manejados dentro de los propios procesos. Este material permite la aspersión de la flama en caso de incendio, es decir, aunque es inflamable no propaga la flama.

- ✓ El techo de la sala y el área de almacenamiento de discos y cintas magnéticos deben ser impermeables.

- ✓ Debe preverse un sistema de drenaje en el piso firme.

- ✓ Los detectores de fuego y humo se deben colocar cuidadosamente en relación con los aparatos de aire acondicionado, ya que los conductores de este pueden difundir el calor o el humo y no permitir que se active el detector.

- ✓ El detector de humo que se elija debe ser capaz de detectar los distintos tipos de gases que desprendan los cuerpos en combustión. Algunos no detectan el humo o el vapor que proviene del plástico quemado que se usa como aislante en electricidad y, en consecuencia, los incendios producidos por un corto circuito tal vez no se detecten.

- ✓ Los detectores de humo y de temperatura se deben instalar en la sala de cómputo, junto a las áreas de oficina y dentro del perímetro físico de las instalaciones.

- ✓ Es necesario colocar detectores de humo y temperatura bajo el piso y en los canales del aire acondicionado.

- ✓ Instalación eléctrica en paneles y conductores eléctricos. Para reducir el riesgo de que ocurra un incendio eléctrico y se propague, la instalación debe estar colocada en paneles y conductores resistentes al fuego. Estos conductores generalmente incluyen un piso levantado del cuarto de cómputo contra fuego.

Propuesta para una buena administración del equipo.

En cuanto a tener un mejor control del equipo y evitar el extravío, desperdicio o robo del mismo, se proponen las siguientes medidas que forman parte del área de seguridad (física). Cuando se refiera al responsable en los siguientes puntos, se hará referencia a la persona asignada del área de seguridad (física) del organigrama que se muestra en la figura 8.3.

- ✓ El responsable deberá contar con una relación del equipo que existe en la unidad en el que se especifique tanto las características del equipo, así como el lugar donde se encuentra.
- ✓ Fijar el equipo, así como cerrarlos con llave, de manera que no sea posible moverlo.
- ✓ Todo espacio que contenga equipo de cómputo debe estar cerrado con llave y no contar con algún lugar de fácil acceso (como una ventila).
- ✓ El responsable deberá realizar una revisión diaria para verificar la integridad física de los equipos, así como una mensual, acompañado del coordinador; estas revisiones se realizarán de manera aleatoria y se deberá reportar cualquier anomalía (equipo abierto, fuera de su lugar, etc.).
- ✓ Para poder mover cualquier equipo de lugar se deberá tener la autorización por escrito del responsable.
- ✓ Para dar mantenimiento y/o corrección de cualquier equipo se deberá contar con la autorización por escrito del responsable.
- ✓ A las salas de cómputo sólo podrán ingresar las personas que hayan dado de alta su cuenta y a los cubículos sólo el personal que trabaje ahí. En caso de tener un visitante por ningún motivo se puede quedar solo y es responsabilidad de la persona que le dio acceso al área, cualquier falta que el visitante cometa.
- ✓ Cuidar que los accesos de entrada física (puertas, ventanas, paredes de vidrio, ventilación, pared falsa, etc.) existentes en áreas de cómputo, no estén expuestos a violación accidental o intencional.
- ✓ En el momento de encontrar que cualquiera de estas disposiciones no se ha cumplido avisar inmediatamente al responsable.
- ✓ Las medidas de seguridad física con respecto al buen uso del equipo se encuentran en el apartado 3 de las Políticas de UNICA.

8.5 Políticas de la Unidad de Servicios de Cómputo Académico

INTRODUCCIÓN

Este documento representa una propuesta de política de alcances institucionales que permita crear y establecer una educación y una filosofía sobre la postura que en materia de seguridad en cómputo debe tener la institución respecto a las amenazas que lo rodean.

Esta propuesta de política define ciertos lineamientos que establecen un límite entre lo que está permitido a los usuarios dentro de la institución y fuera de ella y lo que no está, esto es con el propósito de proteger la información almacenada en los sistemas y el acceso a los mismos.

El *principio básico de seguridad* es "Lo que no se permite expresamente, está prohibido".

La tecnología tiene la capacidad para abrir las puertas a un vasto mundo de recursos de información, así como de personas: a cualquier estudiante o miembro de la comunidad universitaria con una conexión a Internet. Las oportunidades que tenemos con esta conectividad son casi ilimitadas, mas no así los recursos computacionales y de conectividad disponibles. Este nuevo mundo virtual al que tenemos acceso requiere de reglas y precauciones, para asegurar un uso óptimo y correcto de los recursos. En este sentido, la Unidad de Servicios de Cómputo Académico (UNICA) cree firmemente en que el desarrollo de políticas que sean bien entendidas, que circulen ampliamente y que sean efectivamente implementadas, conllevará a hacer de la red UNICA e Internet un ambiente seguro y productivo para estudiantes y miembros en general de la comunidad universitaria.

Se trata entonces de presentar lo que se conoce como **Políticas y Reglamentos para el Uso Aceptable** (en inglés AUP) para los recursos computacionales y de conectividad presentes en la red UNICA. Estas políticas establecen, entre otras cosas, el comportamiento esperado de los miembros de la comunidad universitaria hacia diferentes servicios de información (e-mail, WWW, etc.) y las reglas en cuanto al uso adecuado de recursos físicos.

La política de seguridad en cómputo de UNICA se define bajo dos premisas :

1. Como medida correctiva en solución a los problemas de seguridad en cómputo que han ocurrido en la institución y de los que actualmente son motivo potencial de incidentes de seguridad.
2. Como medida preventiva de nuevos ataques que si bien no han ocurrido se desean evitar hasta el mayor grado posible.

1.- Usuarios Autorizados

1.1.- El objetivo de la red de comunicaciones e información de UNICA es proporcionar los servicios de apoyo en cómputo para cumplir con la función académica e investigadora de la Facultad de Ingeniería. Dentro de este marco, la universidad permite el uso de la red UNICA a:

a) Miembros vigentes de la comunidad de la Facultad de Ingeniería que hayan realizado su trámite de registro.

b) La comunidad universitaria que realice actividades académicas y de investigación legítimas, que hayan realizado su trámite de registro con previa autorización del Jefe de UNICA.

1.2.- El uso de la red UNICA por individuos u organizaciones que no sean parte del personal, estudiantes o afiliados legítimos*(b)*, no está permitido.

2.- Seguridad Física

a) Mantener las computadoras alejadas del fuego, humo, polvo y temperaturas extremas.
b) Colocarlas fuera del alcance de rayos solares, vibraciones, insectos, ruido eléctrico, agua, etc.
c) Se prohíbe el consumo de alimentos y bebidas cerca de las computadoras.
d) El acceso a los servidores será restringido, las puertas deberán contar con chapas.
e) Los lugares en donde se encuentre el equipo de cómputo contará con instalaciones eléctricas adecuadas y en particular los servidores deberán tener no-breaks.
f) Las salas de cómputo deberán tener extintores y el personal deberá estar capacitado para su uso.
g) Las salas de cómputo deberán contar mínimo con una salida de emergencia.
h) Mantener el equipo de cómputo en un entorno limpio y sin humedad. Además, asegurarse de que la superficie sobre la que se encuentra sea lisa y firme.
i) No colocar ningún objeto encima del equipo que cubra los orificios de ventilación del monitor o del CPU.
j) Evitar que los interruptores u otros controladores se mojen, ya que la humedad puede dañar alguno de estos elementos y provocar averías eléctricas.
k) Verificar que el interruptor de voltaje a la PC esté en la posición adecuada (115VAC).
l) Se deberán colocar los cables de alimentación de manera que no sean pisados o aplastados al colocar otras cosas encima o contra ellos.
m) No se sobrecargarán los toma corrientes de pared, reguladores, nobreaks, etc.
n) En caso de falla del equipo, reportarlo inmediatamente al responsable del Área de Seguridad (física) o al Jefe del DROS.
o) No se intentará la reparación de cualquier equipo de cómputo sin la autorización del responsable del Área de Seguridad (física).
p) No se debe insertar ningún objeto a través de las aberturas del equipo.
q) Si se cuenta con un no-break, se debe conectar únicamente la computadora.
r) Apagar los equipos personales cuando abandone temporal o definitivamente el área de trabajo.
s) El CPU no deberá estar conectado directamente a líneas de corriente no regulada; asimismo, no conectarlo junto con impresoras láser para no provocar variación de voltaje en la fuente de poder.

3.- Del control de acceso

3.1.- Del acceso a áreas críticas.

a) El acceso a áreas críticas será restringido sólo al personal del Departamento de Redes y Operación de Servidores (DROS).
b) Los accesos a las áreas críticas deberán de ser clasificados de común acuerdo entre el jefe de UNICA y el comité de seguridad del DROS.
c) Bajo condiciones de emergencia o de situaciones de urgencia manifiesta, el acceso a las áreas de servicio crítico estará sujeto a las que especifiquen las autoridades superiores de UNICA.

3.2.- Del control de acceso al equipo de cómputo.

a) Todos y cada uno de los equipos son asignados a un responsable, por lo que es de su competencia hacer buen uso de los mismos.
b) Las áreas donde se tiene equipo de propósito general cuya misión es crítica estarán sujetas a los requerimientos que UNICA emita.

3.3.- Del control de acceso local a la red.

a) Los administradores son responsables de proporcionar a los usuarios el acceso a los recursos informáticos con aplicaciones que permitan una comunicación segura y encriptada.
b) El Departamento de Servicios Académicos es el responsable de difundir el reglamento para las salas de cómputo de UNICA.
c) Dado el carácter personal del acceso a la Red UNICA, el DROS verificará el uso responsable, de acuerdo al reglamento para las salas de cómputo de UNICA.
d) Todo el equipo de cómputo que esté o sea conectado a la Red UNICA, o aquellas que en forma autónoma se tengan y que sean propiedad de la institución, deben sujetarse a éstas políticas.

3.4.- De control de acceso remoto.

a) Los usuarios que se conecten remotamente lo harán con aplicaciones que permitan una comunicación segura y encriptada
b) El acceso a Internet en la Facultad de Ingeniería debe hacerse desde una estación debidamente registrada y/o autorizada por el grupo de Servicios de Redes. Dicho de otra forma, la computadora debe estar registrada dentro del DNS (*Domain Name Server*) primario de la universidad y estar localizado con una dirección IP legítima.
c) Todos los administradores que den un servicio de acceso remoto deberán contar con aplicaciones que permitan una comunicación segura y encriptada.

3.5.- De acceso a los sistemas administrativos.

a) Tendrá acceso a los sistemas administrativos sólo el personal de UNICA que es responsable de los servidores.

b) El manejo de información administrativa que se considere de uso restringido deberá ser cifrada con el objeto de garantizar su integridad.
c) El control de acceso a cada sistema de información de UNICA será determinado por el DROS.

3.6.- De cuentas de acceso

3.6.1.- Creación de una cuenta.

a) Las cuentas deben ser otorgadas únicamente a usuarios autorizados.
b) Una cuenta está conformada por un nombre de usuario y su respectiva contraseña.
c) La asignación de cuentas será realizada por el administrador del servidor.
d) La longitud de una contraseña deberá siempre ser verificada de manera automática al ser construida por el administrador/usuario. Todas las contraseñas deberán contar con al menos seis caracteres.
e) Está prohibido que los usuarios construyan contraseñas compuestas de algunos caracteres constantes y otros que cambien de manera predecible y sean fáciles de adivinar.

3.6.2.- Uso autorizado.

a) Las cuentas de ingreso a los sistemas y los recursos de cómputo son propiedad de UNICA y se usarán exclusivamente para actividades relacionadas con la Institución.
b) El usuario tiene la obligación de revisar el Manual de Usuario (Ver Apéndice III) para el uso del sistema que le será entregado una vez que su cuenta sea creada.
c) El uso de la red UNICA para ganancias y actividades financieras, no relacionadas con las actividades normales de la Universidad, es catalogado como una práctica inaceptable.
d) Las cuentas en los sistemas son estrictamente personales e intransferibles.

3.6.3.- Tiempo de uso de las cuentas.

a) Se prohíbe dejar sesiones abiertas sin control alguno.
b) La cuenta de un empleado de UNICA, será removida del servidor siempre y cuando sea necesario o el Jefe del DROS lo indique.
c) Todos los datos encontrados en la cuenta de un estudiante de la Facultad de Ingeniería, serán removidos al inicio del siguiente semestre del calendario académico. Estudiantes dados de baja académica o que se han retirado por cuenta propia tendrán sus cuentas eliminadas al momento de la fecha efectiva de expulsión o retiro.
d) Las cuentas de estudiantes de Post-Grado, tesistas o servicio social serán removidas al semestre siguiente de la fecha efectiva de culminación de su programa académico. Cuando se trate de la expulsión o retiro del estudiante, la cuenta será eliminada al momento de la fecha efectiva de expulsión o retiro.

4.- Sobre el sistema y servicios de red

4.1.- Utilización de los recursos de la red.

a) Los recursos disponibles a través de la red UNICA serán de uso exclusivo para asuntos relacionados con las actividades sustantivas de la misma.
b) El DROS es el responsable de emitir y dar seguimiento al Reglamento para las salas de cómputo de UNICA.
c) Corresponde al DROS administrar, mantener y actualizar la infraestructura de la Red UNICA.
d) Dado el carácter confidencial que involucra el correo electrónico, los administradores podrán tener acceso a él con la autorización del Jefe del DROS, solamente cuando ponga en riesgo la seguridad del sistema.
e) Está prohibido enviar correos conteniendo injurias y malas palabras.
f) Está prohibido enviar correos sin remitente y sin asunto.
g) Está prohibido enviar por correo: virus, archivos o información que ponga en peligro la seguridad del sistema.
h) Está prohibido enviar correos SPAM.
i) Está prohibido enviar correos haciéndose pasar por otra persona.
j) Está prohibido enviar correos electrónicos a los contactos de otros usuarios sin autorización expresa.

4.2.- Servicios de Red.

a) No se pueden utilizar los servicios de comunicación para intimidar, insultar o molestar a otros.
b) Se prohíbe el uso de herramientas de hardware o software para realizar monitoreo de la red a aquellos usuarios no autorizados, a menos que se compruebe que es para uso académico.
c) Está prohibido a los usuarios tener acceso remoto a computadoras que no se le hayan designado explícitamente.
d) No es permitido explotar huecos de seguridad, hacer uso programas o accesos no autorizados que alteren la consistencia o que dañen cualquier sistema de cómputo.

4.3.- Administración de Seguridad.

a) La configuración de los sistemas debe ser estándar y revisada cada 6 meses.
b) Se debe proveer la instalación de un sistema de passwords, cuyo mecanismo impida el reuso de los mismos y obligue al usuario al cambio periódico y la elección de passwords únicos y robustos.
c) Los passwords deberán cambiarse máximo cada seis meses.
d) Se debe restringir el uso de los recursos del sistema y de la red, restricción de directorios, permisos y programas para ser ejecutados por los usuarios.
e) Si el usuario cambia los permisos de sus archivos será su responsabilidad, si se comprometen por tener permisos incorrectos.
f) Todas las computadoras personales deben tener un sistema antivirus para proteger la información almacenada en los discos.

g) Debido a que UNICA se esforzará en mantener la privacidad de las comunicaciones personales, el DROS monitoreará la carga de tráfico de la red y cuando sea necesario tomará acción para proteger la integridad y operatividad de sus redes. Además, UNICA:

- Realizará estadísticas de utilización de computadoras basado en direcciones IP, protocolos de red y tipo de aplicación.

h) En caso de que los sistemas se encuentren comprometidos, el usuario tiene la obligación de cambiar su password y colaborar en lo que sea necesario. Si por alguna razón se percata de cualquier hueco, falla de seguridad o inconsistencia en cualquier sistema de cómputo está obligado a reportarlo a los administradores del mismo.

5.- Administración de los sistemas de cómputo

5.1.- Administración General de Cómputo.

a) El DROS será encargado de suministrar medidas de seguridad razonables contra la intrusión o daños a la información almacenada en los sistemas, como la instalación de cualquier herramienta, dispositivo o versión de software que refuerce la seguridad de los sistemas. Sin embargo, debido a la amplitud y constante innovación de los mecanismos de ataque, no se garantiza una seguridad total.
b) El DROS debe estar pendiente de la instalación de cualquier parche de software que refuerce la seguridad de los sistemas de cómputo de UNICA.

5.2.- Administradores de Sistemas/Servidores.

a) La instalación del software se hará únicamente por los administradores.
b) El administrador debe mantener informado al jefe del DROS de cada software adquirido e instalado.
c) Cada máquina debe estar registrada en el patrón único de control de equipo de cómputo y red de UNICA.
d) El administrador debe auditar periódicamente los sistemas y los servicios de red, para verificar que no existen archivos no autorizados, configuraciones inválidas o permisos extra que pongan en riesgo la seguridad de la información.
e) Los incidentes de seguridad deben ser reportados en el formato de control de incidentes de seguridad (Ver Apéndice IV) y enviados al jefe del DROS, junto con cualquier experiencia o información que ayude a fortalecer la seguridad de los sistemas de cómputo.
f) Los administradores de cómputo deben realizar la instalación o adaptación de sus sistemas de cómputo que en materia de seguridad se requiera.
g) Es responsabilidad del administrador revisar periódicamente las bitácoras de los sistemas a su cargo.
h) Está estrictamente prohibido borrar el archivo *.bash_history* o modificar cualquier variable de ambiente que esté relacionada con la modificación de este archivo, en la cuenta de usuario que tiene cada administrador en el sistema.

i) Si el administrador encuentra a un usuario ejecutando comandos fuera de lo común o no permitidos, debe guardar en un archivo el registro y posteriormente auditar la cuenta del usuario.

6.- Respaldos

6.1.- Usuario.

a) Para reforzar la seguridad de la información de la cuenta, el usuario deberá hacer respaldos de su información dependiendo de la importancia y frecuencia del cambio de la misma.

6.2.- Administrador.

a) Los administradores deben hacer respaldos mensuales de la información de los servidores que tengan a su cargo, siempre y cuando se cuente con dispositivos de respaldo.
b) La información respaldada deberá ser almacenada en un lugar seguro y diferente del lugar donde estan los servidores.
c) Deberá mantenerse una versión reciente de los archivos más importantes del sistema.
d) En el momento en que la información respalda deje de ser útil a UNICA, dicha información deberá ser borrada antes de deshacerse del medio.

7- Del equipo

7.1.- Del mantenimiento de equipo de cómputo.

a) Al DROS le corresponde la coordinación del mantenimiento preventivo y correctivo de los equipos, la conservación de su instalación, la verificación de la seguridad física, y su acondicionamiento específico a que tenga lugar.
b) En el caso de los equipos atendidos por terceros, el DROS vigilará el correcto funcionamiento del equipo.
c) El personal técnico de apoyo interno de los departamentos académicos se apegará a los requerimientos establecidos en las políticas que el DROS emita.

7.2.- De la actualización del equipo.

a) Todo el equipo de cómputo (computadoras personales, estaciones de trabajo, y demás relacionados) que sean propiedad de UNICA, debe procurarse sea actualizado tendiendo a conservar e incrementar la calidad del servicio que presta, mediante la mejora sustantiva de su desempeño.

7.3.- De la reubicación del equipo de cómputo.

a) La reubicación del equipo de cómputo se realizará de acuerdo a las disposiciones de cada Jefe de Departamento de UNICA.

b) En caso de existir personal técnico de apoyo de los departamentos académicos, este notificará de los cambios tanto físicos como de software de red que realice al DROS, y en su caso si cambiara de responsable (el equipo) al DID y al DROS. Notificando también los cambios de equipo inventariado (cambio de monitores, de impresoras etc.).
c) El equipo de cómputo a reubicar que sea de UNICA o bien externo se hará únicamente bajo la autorización del responsable, contando el lugar a donde se hará la ubicación con los medios necesarios para la instalación del equipo.

8.- Del Software

8.1.- De la adquisición de software.

a) De acuerdo a los objetivos globales de UNICA, se deberá propiciar la adquisición y asesoramiento en cuanto a software de vanguardia.
b) En cuanto a la paquetería sin costo deberá respetarse la propiedad intelectual intrínseca del autor.
c) UNICA promoverá y propiciará que la adquisición de software de dominio público provenga de sitios oficiales y seguros.
d) DROS deberá promover el uso de sistemas que redunden en la independencia de la institución con los proveedores.

8.2.- De la instalación de software.

a) El DROS es responsable de brindar asesoría y supervisión para la instalación de software informático.
b) La instalación de software que desde el punto de vista del DROS pudiera poner en riesgo los recursos de la institución, no está permitida.
c) Con el propósito de proteger la integridad de los sistemas informáticos, es imprescindible que todos y cada uno de los equipos involucrados dispongan de software de seguridad (antivirus, vacunas, privilegios de acceso y otros que se apliquen).
d) La protección lógica de los sistemas corresponde a quienes en un principio se les asigna y les compete notificar cualquier movimiento al DID.

8.3.- De la actualización del software.

a) La adquisición y actualización de software para equipo especializado de cómputo se llevará a cabo de acuerdo a los requerimientos de cada departamento de UNICA.
b) Corresponde al jefe UNICA autorizar cualquier adquisición y actualización del software.
c) Las actualizaciones de software de uso común o más generalizado se llevarán a cabo de acuerdo al plan de actualización desarrollado por el DROS.

8.4.- Del software propiedad de la institución.

a) Los datos, las bases de datos, la información generada por el personal y los recursos informáticos de la institución deben estar resguardados.

b) El Jefe del DROS administrará los diferentes tipos de licencias de software y vigilará su vigencia en concordancia con la licencia informática.

8.5.- Sobre el uso de software académico.

a) Cualquier software que requiera ser instalado para trabajar sobre la Red UNICA deberá ser evaluado por el área que el Jefe del DROS designe.
b) Todo el software propiedad de la institución deberá ser usado exclusivamente para asuntos relacionados con las actividades de la institución.

9.- Uso responsable de los recursos de cómputo

a) No dañar, substraer o hacer mal uso de los recursos de cómputo y red de UNICA.
b) Por ningún motivo resetear, desconectar periféricos o provocar interrupciones eléctricas en cualquier equipo de cómputo si no es responsable directo del equipo.
c) A ningún miembro de la comunidad universitaria, le será permitido interceptar, leer, copiar o modificar datos electrónicos privados (ya sea en tránsito a través de la red o almacenados dentro de una computadora) sin el consentimiento escrito del propietario legítimo.
d) No instalar o ejecutar programas de juegos en las computadoras.
e) Está estrictamente prohibido ejecutar programas que intenten adivinar las contraseñas o que exploten la vulnerabilidad del sistema a menos de que sea de carácter académico y bajo la autorización del área de seguridad de UNICA.
f) Los recursos de cómputo que le son asignados al personal de UNICA no pueden ser usados por visitas ni para fines personales.

10.- De supervisión y evaluación

a) El DROS propiciará la conformación de un grupo especializado en auditoría de sistemas de cómputo y sistemas de información.
b) Corresponderá al área de seguridad realizar las auditorías internas.
c) Las auditorías de cada actividad donde se involucren aspectos de seguridad lógica y física deberán realizarse periódicamente por el DROS.
d) Los sistemas considerados críticos, deberán estar bajo monitoreo permanente.

11.- Uso de direcciones IP

El área Responsable de representar a la Facultad de Ingeniería ante DGSCA es Secretaría General.

- El administrador de red deberá contar con un registro de sus direcciones IP utilizadas.
- El formato que utilizará para registrar su información está contenido en el Apéndice V.
- Ningún área puede hacer uso de una dirección IP que no le corresponda, sin autorización expresa y escrita del administrador del área en cuestión.
- Ningún usuario final podrá hacer modificaciones en la configuración de su dirección IP asignada al equipo de su responsabilidad.

- En el campus de C.U. no se permite el uso de servidores de DHCP con Direcciones IP homologadas.
- No se permiten utilizar en subredes de una zona, rangos de otras zonas. Por ejemplo, en la zona A utilizar rangos de la zona C.
- Cada equipo que se incorpore a la red Internet deberá tener autorización del administrador de red del área en cuestión.
- Si se realiza un cambio de tarjeta de red se deberá de informar del reemplazo y de la dirección física asociada a la IP, al administrador de red.
- Se permite DHCP con rango de direcciones privadas 192.168.X.X pero su asignación deberá de controlarse únicamente a los equipos asignados al área.
- Las direcciones IP que podrán otorgarse serán homologadas o privadas. Las homologadas sólo serán otorgadas si se justifican su uso y disponibilidad. Para asignar una dirección IP deberá de justificarse su autorización y solicitarla al administrador o responsable de cómputo para su autorización.
- El administrador de red podrá realizar reasignaciones de los rangos de las direcciones IP homologadas y privadas para un mejor desempeño de la red.
- El administrador de red y el representante ante comité de cómputo son los únicos autorizados en solicitar dar de alta nombres canónicos de hosts, alias, mail Exchangers al Administrador General de la Red.

12.- Generales

a) Debido al carácter confidencial de la información, el personal de UNICA deberá de conducirse de acuerdo al código de ética, políticas y procedimientos establecidos.

13.- Sanciones

A los usuarios que quebranten estas políticas se les aplicarán las siguientes sanciones:

Todas las acciones en las que se comprometa la seguridad de la Red UNICA y que no estén previstas en estas políticas, deberán ser revisadas por el jefe de UNICA y el Jefe del DROS para dictar una resolución sujetándose al estado de derecho.

En casos que involucren alegada actividad fraudulenta, UNICA puede, a discreción del jefe de UNICA, suspender los privilegios de acceso en espera de los procedimientos legales.

En caso de que llegará a ocurrir un incidente grave como los siguientes:

- Obtener el privilegio de root o administrador del sistema, sin que se le haya otorgado explícitamente.
- Borrar, modificar Información.
- Difundir información confidencial.
- Copiar información confidencial.
- Ejecución de programas para obtener privilegios y que sean exitosos
- Violar correos de cuentas ajenas.

- Un incidente donde este involucrado un administrador de sistema u trabajador de la UNAM.
- Modificar Configuraciones de Switches y ruteadores sin ser responsables del equipo.
- Daño físico intencional a los medios de comunicación de la red, como fibra óptica, UTP, Switches,hubs, ruteadores, transceivers.

Se reportará al Departamento de Seguridad de la DGSCA y se seguirán los procedimientos establecidos por ellos para recabar las pruebas que demuestren que se ha vulnerado el sistema, mientras tanto la(s) cuenta(s) involucradas se deshabilitarán hasta que se deslinden responsabilidades sobre el incidente ocurrido.

Violación del punto	Sanción
2	La sanción la aplicará el Jefe de UNICA de acuerdo al daño que haya ocasionado.
3.1	Llamada de atención por el Jefe de UNICA o el Jefe del DROS. **Reincidencia:** Si es profesor, académico, trabajador o becarios de UNICA, el Jefe de UNICA decidirá a su criterio la sanción.
3.2 inciso a	Llamada de atención por el Jefe de UNICA o la sanción que el considere de acuerdo al caso.
3.3	Llamada de atención por el Jefe del DROS. **Reincidencia**: el Jefe de UNICA aplicará la sanción.
3.4	Llamada de atención por el Jefe del DROS. **Reincidencia**: el Jefe de UNICA aplicará la sanción.
3.5	Llamada de atención por el Jefe del DROS. **Reincidencia**: el Jefe de UNICA aplicará la sanción.
3.6.1 inciso a,b,c y d	Llamada de atención por el Jefe del DROS. **Reincidencia**: el Jefe de UNICA aplicará la sanción.
3.6.1 inciso e	Llamada de atención por el Jefe del DROS. **Reincidencia**: Suspensión del servicio por un dia y si volviera a reincidir se le suspederá por un mes.
3.6.2 inciso a	Suspensión del servicio por una semana **Reincidencia**: Suspensión del servicio por un mes
3.6.2 inciso c	Suspensión del servicio por un mes **Reincidencia**: Suspensión del servicio por tres meses.
3.6.2 inciso d	Llamada de atención por el Jefe del DROS y suspensión del servicio por dos semanas a las personas involucradas. **Reincidencia**: Suspensión del servicio por un mes.
3.6.3	Llamada de atención por el Jefe del DROS. **Reincidencia**: el Jefe de UNICA aplicará la sanción.

4.1 inciso a,b y c	Llamada de atención por el Jefe del DROS. **Reincidencia**: el Jefe de UNICA aplicará la sanción.
4.1 inciso d	Quitar los passwords de administrador al o los administradores involucrados y el Jefe delDROS decidirá que sanción tendrá.
4.1 inciso e,f,g,h,i y j	Suspensión del servicio de correo por una semana. **Reincidencia**: suspensión del servicio por tres meses.
4.2 inciso a	Suspensión del servicio por un mes. **Reincidencia**: suspensión del servicio por un semestre.
4.2 inciso b	Llamada de atención por el Jefe del DROS. **Reincidencia**: el Jefe de UNICA aplicará la sanción de acuerdo a su criterio.
4.2 inciso c	Llamada de atención por el Jefe del DROS. **Reincidencia**: el Jefe de UNICA aplicará la sanción de acuerdo a su criterio.
4.2 inciso d	Si es un alumno se le suspendará el servicio por semestre. Si es el caso de un académico, investigador, trabajador se hará una carta de "extrañamiento" dirigida al Jefe de División o Secretaría.
4.3	Llamada de atención por el Jefe del DROS. **Reincidencia**: el Jefe de UNICA aplicará la sanción.
5	Llamada de atención por el Jefe del DROS. **Reincidencia**: el Jefe de UNICA aplicará la sanción.
6.2	Llamada de atención por el Jefe del DROS. **Reincidencia**: el Jefe de UNICA aplicará la sanción.
9 inciso a	Suspensión del servicio por un semestre y en caso de ser personal que labora en la unidad el Jefe de UNICA decidirá la sanción.
9 inciso a	Si no se causo ningún daño grave al equipo el Jefe de UNICA le llamará la atención. En caso de haber causado algun daño grave al equipo el Jefe de UNICA decidirá que sanción aplicar.
9 inciso c	En caso de ser un alumno se le suspenderá el servicio de 6 meses a un año. Si es un administrador se le quitaran privilegios de administrador y el Jefe de UNICA decidirá si puede continuar administrando el sistema. Si es el caso de un académico, investigador, trabajador se hará una carta de "extrañamiento" dirigida al Jefe de División o Secretaría.
9 inciso d	Si es un alumno el Jefe del DROS le llamará la atención. Si es el caso de persona(s) que laboran en la Unidad, el Jefe de UNICA decidirá la sanción.

9 inciso e	Si es un alumno se le suspenderá el servicio un semestre. Si es el caso de persona(s) que laboran en la unidad el Jefe de UNICA decidirá la sanción. Si es el caso de un académico, investigador, trabajador se hará una carta de "extrañamiento" dirigida al Jefe de División o Secretaría.
9 inciso f	Llamada de atención por el Jefe inmediato de la persona(s) involucrada(s) o por el Jefe de UNICA.
11	Cualquier violación por parte de algún administrador de red, académico u investigador en la política de uso de direcciones IP, se hará una carta de "extrañamiento" dirigida al Jefe de División o Secretaría.

8.6 Herramientas de seguridad

De acuerdo con las diferentes herramientas de seguridad que se mencionaron en el Capítulo 7, consideramos que las siguientes cumplen con los requerimientos suficientes para hacer que el sistema no sea tan vulnerable a cualquier ataque.

A continuación, se presentan las bitácoras de instalación de las herramientas de seguridad que se implantaron.

Tripwire

Justificación.

Tripwire es excelente para los administradores de sistemas que requieren tanto de facilidades para detección de intrusos como de control de daños para sus servidores puesto que verifica la consistencia de archivos y directorios de sistema críticos identificando todos los cambios hechos a ellos. Si Tripwire detecta que uno de los archivos monitoreados ha sido cambiado, lo notifica al administrador del sistema vía correo electrónico. También puede fácilmente identificar los archivos que son modificados, agregados o eliminados, lo que hace ágil el proceso de recuperación luego de una entrada forzada pues mantiene el número de archivos que deben ser restaurados a un mínimo.

Instalación.

La forma más fácil de instalar Tripwire es instalando el RPM de Tripwire, escribiendo el comando siguiente como usuario root:

[root@maquina]# rpm –ivh tripwire-2.3.1-17.i386.rpm

Después de haber instalado el RPM Tripwire, realizamos los siguientes pasos para inicializar el software:

Modificar el archivo "/etc/tripwire/twcfg.txt" en el que se puede alterar la localización de los archivos Tripwire, personalizar los parámetros del e-mail o el nivel de detalles para los informes.

Modificar "/etc/tripwire/twpol.txt" este archivo de política permite darse cuenta de las aplicaciones específicas, de los archivos y de los directorios del sistema. La modificación del archivo de política aumenta la utilidad de los informes de Tripwire minimizando los avisos falsos para los archivos y programas que no está usando y añade funcionalidad como por ejemplo las notificaciones en forma de e-mail.

Correr el siguiente script el cual debe de tener permisos de ejecución. Durante la ejecución pedirá contraseñas del sitio y local. Estas contraseñas son usadas para generar llaves criptográficas para la protección de los archivos Tripwire. El script luego crea y firma estos archivos.

[root@maquina]# /etc/tripwire/twinstall.sh

The Tripwire site and local passphrases are used to sign a variety of files, such as the configuration, policy, and database files.

Passphrases should be at least 8 characters in length and contain both letters and numbers.

See the Tripwire manual for more information.

Creating key files...

(When selecting a passphrase, keep in mind that good passphrases typically have upper and lower case letters, digits and punctuation marks, and are at least 8 characters in length.)

Enter the site keyfile passphrase:
Verify the site keyfile passphrase:
Generating key (this may take several minutes)...Key generation complete.
(When selecting a passphrase, keep in mind that good passphrases typically have upper and lower case letters, digits and punctuation marks, and are at least 8 characters in length.)

Enter the local keyfile passphrase:
Verify the local keyfile passphrase:
Generating key (this may take several minutes)...Key generation complete.

Signing configuration file...
Please enter your site passphrase:
Wrote configuration file: /etc/tripwire/tw.cfg
A clear-text version of the Tripwire configuration file
/etc/tripwire/twcfg.txt
has been preserved for your inspection. It is recommended
that you delete this file manually after you have examined it.

Signing policy file...
Please enter your site passphrase:
Wrote policy file: /etc/tripwire/tw.pol
A clear-text version of the Tripwire policy file
/etc/tripwire/twpol.txt
has been preserved for your inspection. This implements
a minimal policy, intended only to test essential
Tripwire functionality. You should edit the policy file
to describe your system, and then use twadmin to generate
a new signed copy of the Tripwire policy.

Una vez encriptados los archivos de configuración, de política, la base de datos y los archivos de informe, Tripwire los protege de los intrusos que no conocen las contraseñas locales ni de los sitios. Esto siginifica que aunque un intruso obtenga al acceso de root al sistema, no podrá alterar los archivos Tripwire para enmascararse.

Es importante recalcar que una vez encriptados y firmados, no se puede cambiar el nombre ni mover los archivos de configuración y de políticas generados con el script twinstall.sh.

Se inicializa la base de datos Tripwire, de la siguiente manera:

[root@maquina]#/usr/sbin/tripwire –init

Please enter your local passphrase:

Parsing policy file: /etc/tripwire/tw.pol

Generating the database...

*** Processing Unix File System ***

Wrote database file: /var/lib/tripwire/xelha.twd

The database was successfully generated.

Por defecto, el RPM Tripwire añade un script de la shell llamado tripwire-check al directorio /etc/cron.daily/. Este script ejecuta automáticamente un control de integridad una vez al día.

Se puede ejecutar un control de integridad de Tripwire en cualquier momento mediante el comando:

```
[root@maquina]# /usr/sbin/tripwire --check

Parsing policy file: /etc/tripwire/tw.pol

*** Processing Unix File System ***

Performing integrity check...

Wrote report file: /var/lib/tripwire/report/maquina-20030922-135609.twr

Tripwire(R) 2.3.0 Integrity Check Report

Report generated by:        root

Report created on:          lun 22 sep 2003 13:56:09 CDT

Database last updated on:   Never

=============================================================
Report Summary:
=============================================================
Host name:                  maquina
Host IP address:            127.0.0.1
Host ID:                    None
Policy file used:           /etc/tripwire/tw.pol
Configuration file used:    /etc/tripwire/tw.cfg
Database file used:         /var/lib/tripwire/maquina.twd
Command line used:          /usr/sbin/tripwire --check

=============================================================
Rule Summary:
=============================================================

-------------------------------------------------------------

 Section: Unix File System

-------------------------------------------------------------

 Rule Name                 Severity Level   Added   Removed  Modified

 ---------                 --------------   -----   -------  --------
```

El comando twprint -m r mostrará los contenidos de un informe Tripwire en texto plano. Uno debe especificar cual archivo de informe mostrar, de la siguiente manera:

```
[root@maquina]# /usr/sbin/twprint -m r --twrfile /var/lib/tripwire/report/<name>.twr
```

BITÁCORA DE INSTALACIÓN

Nessus

Justificación.

Nessus es un *scanner* remoto de la seguridad en un equipo, como ya lo habíamos mencionado antes, es de distribución libre y es considerado como el mejor de su tipo por ser el que detecta mayor número de problemas. Es por eso que se recomienda que una vez que el servidor esté listo para funcionar, se busquen huecos en la seguridad con esta herramienta.

Instalación.

No es necesario que se instale en el servidor, se puede instalar en otra máquina con sistema operativo tipo UNIX. Este programa esta dividido en dos partes un cliente y un servidor. Para instalarlo lo primero que se debe de hacer es descargarlo de la siguiente dirección: www.nessus.org.

Existen diferentes formas para instalarlo una de las más sencillas es descargar el archivo (nessus-installer.sh) que es un paquete que se auto instala con sólo ejecutar el siguiente comando:

```
[root@maquina]# sh nessus-installer.sh
```

Esto pedirá alguna información referente a la computadora donde residirá y las carpetas donde se instalará.

Una vez instalado, por default deja dentro de la carpeta */usr/local/sbin* los programas del servidor y dentro de */usr/local/bin* los del cliente. Y ahora se procede a crear una cuenta con lo siguiente:

```
[root@maquina]# /usr/local/sbin/nessus-adduser

Login : usuario
Password : contraseña
Authentification type ([pass] | [cert] ): pass
Now enter the rules for this user, and hit ctrl-D once you are done :
(the user can have an empty rule set)

Login          : usuario
Pssword        : contraseña
Authentification : pass
Rules          :

Is that ok (y/n) ? [y] y

user added.
```

¿Cualquier duda o información más detallada? con el comando ***nessus-adduser*** se puede consultar la ayuda con:

```
$ man nessus-adduser.
```

Posteriormente, se puede configurar el demonio *nessus* con el idioma, entre otras cosas, en el archivo /usr/local/etc/nessus/nessusd.conf. Una vez hecho esto, ya se puede levantar el servidor con:

```
[root@maquina]# /usr/local/sbin/nessusd –D.
```

Por último, se ejecuta el cliente ***nessus,*** lo cual abrirá una interfaz gráfica. El cliente y el servidor pueden trabajar en una misma máquina o en diferentes. En el cliente se proporciona el *host* y el puerto de donde se está corriendo el demonio ***nessusd***; adicionalmente login y contraseña de un usuario válido para ese servidor, para autentificarse con el botón de login. Como lo muestra la figura 8.3.

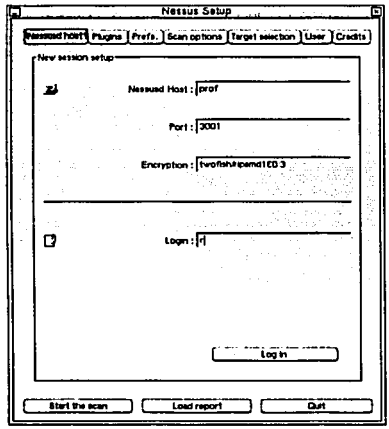


Figura 8.3. Cliente Nessus.

Una vez conectado, se puede establecer diferentes tipos, tanto de *scaneo* como de preferencias en la pestaña de prefs como lo muestra la figura 8.4.

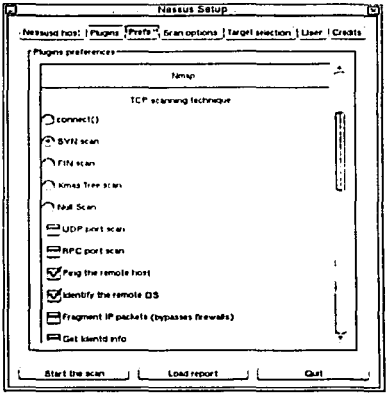


Figura 8.4. Configurando el tipo de análisis.

Se debe seleccionar el equipo al que se le va realizar el análisis por medio de la pestaña target selection, donde se colocará en target el *host* (o IP) de la máquina. Como lo muestra la figura 8.5.

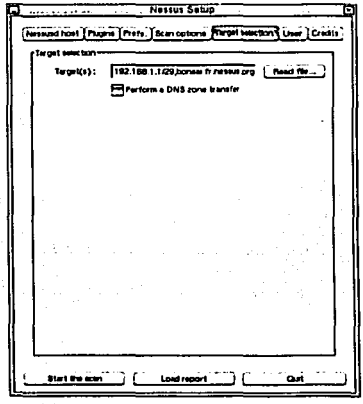


Figura 8.5. Estableciendo el objetivo.

Una vez realizado esto, se está listo para iniciar el *scaneo* con el botón de **start the scan**; empezará el *scaneo* con una barra de progreso, se puede poner más de un objetivo, separándolos por coma en **target**.

Cuando ha concluido, *Nessus* presenta un reporte con lo encontrado, que incluye: el problema, una pequeña descripción, una clasificación del la importancia del problema y una solución.

A grandes rasgos es el funcionamiento del programa aunque se pueden configurar varias cosas como el reporte, el tipo de análisis, se pueden conectar diferentes clientes con un solo servidor de *Nessus*, etc.

BITÁCORA DE INSTALACIÓN

Snort

Justificación.

Snort es un sistema de detección de intrusos en tiempo real y basado en red muy potente. Este sistema sigue el planteamiento de colocar una máquina con una interfaz en modo promiscuo que monitorea el tráfico que circula por la red, de este modo *Snort* busca patrones que hagan presagiar que se está desencadenando un ataque sobre la red que este monitorea.

Instalación.

Se descarga el programa *snort* de http://www.snort.org y la instalación se hace con los siguientes pasos:

```
[root@maquina]# cp snort-stable-snapshot.tar.gz  /usr/src/redhat/SOURCES
[root@maquina]# cd /usr/src/redhat/SOURCES
[root@maquina]# tar –zxvf snort-stable-snapshot.tar.gz
[root@maquina]# cd /usr/src/redhat/SOURCES/snort-stable
[root@maquina]# ./configure
[root@maquina]# make
[root@maquina]# make install
```

Una vez instalado, se definen las reglas con las cuales va detectar y avisar cuando el programa se encuentre auditando.

La reglas que tiene el *snort* por default se bajan del archivo snortrules.tar.gz de http://www.snort.org/dl/snapshots/ y se pueden ir actualizando; *snort* también permite configurar reglas propias.

Para instalarlo se siguen los siguientes pasos:

```
$ mkdir /etc/snort
$ cp snortrules.tar.gz to /etc/snort
$ tar –zxvf snortrules.tar.gz
$ cd /etc/snort/rules
```

```
$ mv * ../
$ cd ..
$ rmdir rules
$ vi snort.conf
$ mkdir /var/log/snort
```

En el archivo snort.conf se puede configurar todo lo referente al trabajo de *snort*, lugar donde buscará las reglas, donde pondrá los archivos de salida o incluso se puede configurar para que la salida la dé una base de datos (mysql, postgresql, etc.).

Dentro del archivo se modifican las siguientes líneas:

```
var RULE_PATH ../rules
por
var RULE_PATH /etc/snort
```

Donde la parte final es la ruta absoluta en donde están las reglas.

Una vez configurado todo para ejecutarlo, se usa:

```
[root@maquina]# /usr/local/bin/snort -i eth1 –D -c /etc/snort/snort.conf
 -i  se selecciona la interfaz sobre la cual se va correr el programa.
-D para correr como demonio y que ponga las alertas en el archivo /var/log/snort/alert.
-c  se selecciona el archivo del cual va tomar la configuración.
```

El resultado lo pone en archivos dentro de la carpeta */var/log/snort*. Para activarlo de manera automática al iniciar el sistema se puede crear un script, que se coloca en la carpeta */etc/rc.d/init.d*, existe un script ya hecho en la página de *snort*.

BITÁCORA DE INSTALACIÓN

John the Ripper v 1.6

Justificación.

John the Ripper es uno de los crackeadores de passwords más conocidos; además, tiene la ventaja de que puede desencriptar una mayor cantidad de passwords que otros crackeadores como el Crack, Cracker Jack, entre otros.

Es recomendable ejecutar *John the Ripper* en otra máquina que no sea el servidor, debido a que el tiempo que se tarda en resolver los passwords encriptados depende tanto de las características de la máquina como del tamaño del archivo.

Instalación.

A continuación se explica cómo realizar la compilación e instalación de John the Ripper v 1.6 bajo Linux:

- Descargar el programa de Internet.

```
[root@maquina root]# mkdir /root/sistema/john
[root@maquina root]# cd /root/sistema/john
[root@maquina john]# wget "http://www.openwall.com/john/john-1.6.tar.gz"
```

- Descomprimir y desempaquetar el archivo john-1.6.tar.gz.

```
[root@maquina john]# cd /usr/src
[root@maquina src]# tar -zxvf /root/sistema/john-1.6.tar.gz
[root@maquina src]# cd john-1.6/src
[root@maquina src]# make
To build John the Ripper, type:
        make SYSTEM
where SYSTEM can be one of the following:
linux-x86-any-elf       Linux, x86, ELF binaries
linux-x86-mmx-elf       Linux, x86 with MMX, ELF binaries
linux-x86-k6-elf        Linux, AMD K6, ELF binaries
linux-x86-any-a.out     Linux, x86, a.out binaries
linux-alpha             Linux, Alpha
linux-sparc             Linux, SPARC
freebsd-x86-any-a.out   FreeBSD, x86, a.out binaries
freebsd-x86-k6-a.out    FreeBSD, AMD K6, a.out binaries
freebsd-x86-any-elf     FreeBSD, x86, ELF binaries
freebsd-x86-mmx-elf     FreeBSD, x86 with MMX, ELF binaries
freebsd-x86-k6-elf      FreeBSD, AMD K6, ELF binaries
openbsd-x86-any         OpenBSD, x86
openbsd-x86-k6          OpenBSD, AMD K6
solaris-sparc-gcc       Solaris, SPARC, gcc
solaris-sparc-v8-cc     Solaris, SPARC V8, cc
solaris-sparc-v9-cc     Solaris, SPARC V9, cc
solaris-x86-any         Solaris, x86, gcc
solaris-x86-k6          Solaris, AMD K6, gcc
digital-alpha-cc        Digital UNIX, Alpha, cc
aix-ppc-cc              AIX, PowerPC, cc
hpux-pa-risc-gcc        HP-UX, PA-RISC, gcc
hpux-pa-risc-cc         HP-UX, PA-RISC, cc
irix-mips32-cc          IRIX, MIPS 32-bit, cc
irix-mips64-cc          IRIX, MIPS 64-bit, cc
dos-djgpp-x86-any       DOS, DJGPP 2.x, x86
dos-djgpp-x86-mmx       DOS, DJGPP 2.x, x86 with MMX
dos-djgpp-x86-k6        DOS, DJGPP 2.x, AMD K6
win32-cygwin-x86-any    Win32, Cygwin, x86
win32-cygwin-x86-mmx    Win32, Cygwin, x86 with MMX
win32-cygwin-x86-k6     Win32, Cygwin, AMD K6
generic                 Any other UNIX system with gcc
```

- Seleccionar linux-x86-any-elf como sistema(esto es en la mayoría de los casos), pero se pueden forzar optimizaciones para i686:

  En este caso, se haría lo siguiente:

  ```
  [root@maquina src]# vi Makefile
  ```

  Sustituimos este párrafo:

  ```
  linux-x86-any-elf:
  $(LN) x86-any.h arch.h
  $(MAKE) $(PROJ)
  JOHN_OBJS="$(JOHN_OBJS) x86.o"
  CFLAGS="$(CFLAGS) -m486"
  ```

  Por este otro:

  ```
  linux-x86-any-elf:
  $(LN) x86-any.h arch.h
  $(MAKE) $(PROJ)
  JOHN_OBJS="$(JOHN_OBJS) x86.o"
  CFLAGS="$(CFLAGS) -mcpu=i686 -march=i686"
  ```

  Si selecciona como sistema la opción linux-x86-any-elf, entonces sería:

  ```
  [root@maquina src]# make linux-x86-any-elf
  ```

- El ejecutable ha quedado en /usr/src/john-1.6/run/john, ahora sigue la instalación.

  ```
  [root@maquina src]# mv -f /usr/src/john-1.6/run/john /sbin
  [root@maquina src]# chown root:root /sbin/john
  [root@maquina src]# chmod 700 /sbin/john
  ```

- En la siguiente documentación se encuentra más información del programa.

  ```
  [root@maquina src]# more /usr/src/john-1.6/doc/README
  [root@maquina src]# more /usr/src/john-1.6/doc/CONFIG
  ```

Ejecutando John the Ripper.

- Realizar una copia del archivo john.ini.

  ```
  [root@maquina src]# cp /usr/src/john-1.6/run/john.ini /root/john.ini
  [root@maquina src]# cd /root
  ```

- Realizar una copia del archivo /etc/passwd.

  ```
  [root@maquina src]# cp /etc/passwd /root/passwd
  [root@maquina src]# chmod 600 /root/passwd
  ```

[root@maquina src]# chown root:root /root/passwd

- Ejecutar el john para ver sus posibilidades.

[root@maquina root]# john

John the Ripper Version 1.6 Copyright (c) 1996-98 by Solar Designer

Usage: john [OPTIONS] [PASSWORD-FILES]

-single	"single crack" mode
-wordfile:FILE -stdin	wordlist mode, read words from FILE or stdin
-rules	enable rules for wordlist mode
-incremental[:MODE]	incremental mode [using section MODE]
-external:MODE	external mode or word filter
-stdout[:LENGTH]	no cracking, just write words to stdout
-restore[:FILE]	restore an interrupted session [from FILE]
-session:FILE	set session file name to FILE
-status[:FILE]	print status of a session [from FILE]
-makechars:FILE	make a charset, FILE will be overwritten
-show	show cracked passwords
-test	perform a benchmark
-users:[-]LOGIN|UID[,..]	load this (these) user(s) only
-groups:[-]GID[,..]	load users of this (these) group(s) only
-shells:[-]SHELL[,..]	load users with this (these) shell(s) only
-salts:[-]COUNT	load salts with at least COUNT passwords only
-format:NAME	force ciphertext format NAME (DES/BSDI/MD5/BF/AFS/LM)
-savemem:LEVEL	enable memory saving, at LEVEL 1..3

- Ejecutando el john en modo single.

Este modo es rápido y en ocasiones eficaz, obtiene la información del usuario para obtener su password.

[root@maquina root]# john -single /root/passwd

Si se obtiene un resultado como este:

Loaded 0 passwords, exiting...

significa que el sistema tiene el paquete shadow passwords activado. En tal caso, se tendrán que exportar las claves encriptadas del archivo /etc/shadow al formato del /etc/passwd:

* Con RedHat 6.x

[root@maquina src]# pwunconv
[root@maquina src]# cp /etc/passwd /root/passwd
[root@maquina src]# pwconv

* Con otras distribuciones

```
[root@maquina src]# unshadow /etc/passwd /etc/shadow > /root/passwd

[root@maquina src]# chmod 600 /root/passwd
[root@maquina src]# chown root:root /root/passwd
[root@maquina src]# john -single /root/passwd
```

Después de unos minutos, se obtendrá un resultado como el que sigue:

```
Loaded 7 passwords with 7 different salts (FreeBSD MD5 [32/32])
pepe          (prueba)
guesses: 1  time: 0:00:00:02 100%  c/s: 2233  trying: root1969
```

En este caso del ejemplo, se ha logrado averiguar una contraseña de 7 cuentas (un 100% del total de las del sistema).

- Ejecutando el john en modo word list.

Este modo puede ser más efectivo que el anterior, porque al utilizar un diccionario puede ofrecer más contraseñas resueltas.

```
[root@maquina root]# john -w:diccionario.txt -rules passwd
Loaded 6 passwords with 6 different salts (FreeBSD MD5 [32/32])
mio           (juli)
holita        (luisito)
guesses: 2  time: 0:00:00:00 100%  c/s: 979  trying: Aaaaaaing
```

En este caso se hace uso de un diccionario "diccionario.txt", un archivo de texto plano con el siguiente aspecto:

```
mio
holita
aaadddd
aadavis
aaaaaaa
aa
aame
...
```

de tal manera que John the Ripper intenta construir contraseñas a partir de las palabras del diccionario. Mientras más palabras tenga el diccionario, más efectiva será la búsqueda. Un buen diccionario tiene palabras en los idiomas más conocidos: Español, Inglés, Francés, Alemán, entre otros.

- Ejecutando el john en modo incremental.

Este es el modo más potente para crackear passwords, usa todas las posibles combinaciones de caracteres, se puede elegir entre números o letras.

Los comandos para este modo son:

:all	Todas las letras, número y caracteres especiales.
:digits	Sólo números.
:alpha	Sólo letras.

Por ejemplo:

[root@maquina root]# john –incremental:all passwd

o

[root@maquina root]# john –i passwd

[root@maquina root]# john –i:digits passwd
[root@maquina root]# john –i:alpha passwd

- Revisar los passwords que han sido crackeados.

Para ver los passwords que John the Ripper ha crackeado se utiliza el comando *–show*:

[root@maquina root]# john –show passwd
pepe:prueba:500:500::/home/aver/pepe:/bin/bash
luisito:holita:503:501::/home/aver/luisito:/bin/bash
julimio:504:501::/home/aver/juli:/bin/bash

3 passwords cracked, 4 left

- Reanudar el crackeo.

Muchas veces cuando se crackean los passwords se puede llevar mucho más tiempo del que se pensaba, para ello se utiliza la opción *-restore*.

Por ejemplo:

[root@maquina root]# john -i passwd
Loaded 4 passwords with 4 different salts (FreeBSD MD5 [32/32])
guesses: 0 time: 0:00:08:01 c/s: 1754 trying: matrotal
Session aborted

Se ha parado el programa con Ctrl + C. Podría pensarse que hay que volver a empezar desde cero, pero no es así, ya que para eso nos sirve el archivo *restore* que se ha generado en el sistema.

[root@maquina root]# john –restore

o

[root@maquina root]# john –re

- Ejecutando el john en modo test.

  El tiempo de desencriptado varía según la máquina, así como del sistema operativo y del tipo de encriptado que utilice. Para ver la velocidad de cada uno de los distintos sistemas se usa la opción *–test*.

  [root@maquina root]# john –test
  Benchmarking: Standard DES [24/32 4K]... DONE
  Many salts: 87142 c/s real, 87845 c/s virtual
  Only one salt: 81305 c/s real, 82126 c/s virtual

  Benchmarking: BSDI DES (x725) [24/32 4K]... DONE
  Many salts: 2867 c/s real, 2913 c/s virtual
  Only one salt: 2360 c/s real, 2463 c/s virtual

  Benchmarking: FreeBSD MD5 [32/32]... DONE
  Raw: 1890 c/s real, 1917 c/s virtual

  Benchmarking: OpenBSD Blowfish (x32) [32/32]... DONE
  Raw: 114 c/s real, 115 c/s virtual

  Benchmarking: Kerberos AFS DES [24/32 4K]... DONE
  Short: 77209 c/s real, 78624 c/s virtual
  Long: 204083 c/s real, 208248 c/s virtual

  Benchmarking: NT LM DES [24/32 4K]... DONE
  Raw: 552076 c/s real, 566813 c/s virtual

BITÁCORA DE INSTALACIÓN

Portsentry

Justificación

Portsentry tiene la ventaja de que sirve para detectar el barrido de puertos a través del monitoreo de los puertos no usados en el sistema. Una vez que el atacante realiza un intento de conexión a los puertos no usados, ***Portsentry*** es alertado y tiene la habilidad de ejecutar algunos comandos en respuesta al barrido de puertos (ipf, ipfwadm, ipchanins, iptables, o usar los tcp_wrappers (hosts.allow y hosts.deny)). Los comandos que serán ejecutados al momento en que portsentry 'reaccionará' a un barrido de puertos, son especificados por el administrador en el archivo de configuración.

Debido a que cualquier comando puede ser usado en respuesta al barrido de puertos, los más útiles pueden ser los comandos que permitan bloquear el envío de cualquier paquete desde la máquina del atacante, negando así la entrada del tráfico proveniente de esa dirección IP.

La violación y la acción correspondiente son detectadas y realizadas por portsentry y son registradas a través del sistema de bitácoras (syslog).

Instalación

A continuación se explica cómo realizar la compilación e instalación del *Portsentry* bajo Linux:

- Descargar el programa de Internet.

  [root@maquina root]# mkdir /root/portsentry
  [root@maquina root]# cd /root/portsentry
  [root@maquina portsentry]# wget " http://www.psionic.com/abacus/portsentry/portsentry-1.1.tar.gz"

- Descomprimir y desempaquetar el archivo portsentry-1.1.tar.gz.

  [root@maquina portsentry]# cd /usr/local
  [root@maquina local]# tar -zxvf /root/portsentry/portsentry-1.1.tar.gz

- Cambiarse al directorio portsentry-1.1.

  [root@maquina local]# cd portsentry-1.1
  [root@maquina portsentry-1.1]# ls

CHANGES	portsentry.c	portsentry_io.c	README.COMPAT
CREDITS	portsentry.conf	portsentry_io.h	README.install
ignore.csh	portsentry_config.h	portsentry_tcpip.h	README.methods
LICENSE	portsentry.h	portsentry_util.c	README.stealth
Makefile	portsentry.ignore	portsentry_util.h	

- Editar el archivo portsentry.conf.

  [root@maquina portsentry-1.1]# vi portsentry.conf

  La configuración de este archivo conserva las siguientes líneas:

```
# Use these if you just want to be aware:
TCP_PORTS="1,11,15,79,111,119,143,540,635,1080,1524,2000,5742,6667,12345,12346,20034,276
65,31337,32771,32772,32773,32774,40421,49724,54320"
UDP_PORTS="1,7,9,69,161,162,513,635,640,641,700,37444,34555,31335,32770,32771,32772,3277
3,32774,31337,54321"

# On many Linux systems you cannot bind above port 61000. This is because
# these ports are used as part of IP masquerading. I don't recommend you
# bind over this number of ports. Realistically: I DON'T RECOMMEND YOU MONITOR
# OVER 1024 PORTS AS YOUR FALSE ALARM RATE WILL ALMOST CERTAINLY RISE.
You've been
# warned! Don't write me if you have have a problem because I'll only tell
# you to RTFM and don't run above the first 1024 ports.
#
#
ADVANCED_PORTS_TCP="1024"
ADVANCED_PORTS_UDP="1024"
```

Reemplazar las siguientes líneas, que permiten excluir algunos puertos:

```
# Default TCP ident and NetBIOS service
ADVANCED_EXCLUDE_TCP="113,139"
# Default UDP route (RIP), NetBIOS, bootp broadcasts.
ADVANCED_EXCLUDE_UDP="520,138,137,67"
```

Por:

```
# Default TCP ident and NetBIOS service
ADVANCED_EXCLUDE_TCP="113,139,143,109,110,995,993,443,21,80,23"
# Default UDP route (RIP), NetBIOS, bootp broadcasts.
ADVANCED_EXCLUDE_UDP="520,138,137,67,143,109,110,995,993,443,53,21,80,23"
```

Conservar las siguientes líneas:

```
####################
# Ignore Options #
####################
# These options allow you to enable automatic response
# options for UDP/TCP. This is useful if you just want
# warnings for connections, but don't want to react for
# a particular protocol (i.e. you want to block TCP, but
# not UDP). To prevent a possible Denial of service attack
# against UDP and stealth scan detection for TCP, you may
# want to disable blocking, but leave the warning enabled.
# I personally would wait for this to become a problem before
# doing though as most attackers really aren't doing this.
# The third option allows you to run just the external command
# in case of a scan to have a pager script or such execute
# but not drop the route. This may be useful for some admins
# who want to block TCP, but only want pager/e-mail warnings
# on UDP, etc.
#
#
# 0 = Do not block UDP/TCP scans.
# 1 = Block UDP/TCP scans.
# 2 = Run external command only (KILL_RUN_CMD)

BLOCK_UDP="1"
BLOCK_TCP="1"
```

Descomentar la siguiente línea:

```
# Newer versions of Linux support the reject flag now. This
# is cleaner than the above option.
KILL_ROUTE="/sbin/route add -host $TARGET$ reject"
```

- Editar el archivo portsentry.ignore.

```
[root@maquina portsentry-1.1]# vi portsentry.ignore
```

Puede configurar este archivo para declarar los *hosts* que serán ignorados por *Portsentry*.

- Compilar *Portsentry*. Al ejecutar el comando *"make"* aparecen los nombres de los sistemas soportados, por lo tanto es necesario elegir el sistema operativo adecuado al compilar.

```
[root@maquina portsentry-1.1]# make
Usage: make <systype>
<systype> is one of: linux, debian-linux, bsd, solaris, hpux, hpux-gcc,
freebsd, osx, openbsd, netbsd, bsdi, aix, osf, irix, generic

This code requires snprintf()/vsnprintf() system calls
to work. If you run a modern OS it should work on
your system with 'make generic'. If you get it to
work on an unlisted OS please write us with the
changes.

Install: make install

NOTE: This will install the package in this
      directory: /usr/local/psionic

Edit the makefile if you wish to change these paths.
Any existing files will be overwritten.
```

```
[root@maquina portsentry-1.1]# make linux
SYSTYPE=linux
Making
cc -O -Wall -DLINUX -DSUPPORT_STEALTH -o ./portsentry ./portsentry.c \
      ./portsentry_io.c ./portsentry_util.c
```

- Ejecutar el comando *"make install"* para instalar *Portsentry* en el sistema.

```
[root@maquina portsentry-1.1]# make install
```

- *Portsentry* queda instalado en el siguiente directorio:

```
[root@maquina portsentry-1.1]# cd /usr/local/psionic/portsentry
[root@maquina portsentry]# ls
portsentry portsentry.conf portsentry.ignore
```

- Operando *Portsentry* en modo avanzado.

En el modo avanzado, *Portsentry* no abre ningún puerto, sino que le pide al kernel que le notifique si llega alguna petición a algún puerto menor al especificado en las opciones **ADVANCED_PORTS_TCP** y **ADVANCED_PORTS_UDP**. La ventaja de este modo es que los puertos aparentemente no estarán escuchando dado que no están realmente abiertos.

```
[root@maquina portsentry]# /usr/local/psionic/portsentry/portsentry –atcp
[root@maquina portsentry]# /usr/local/psionic/portsentry/portsentry –audp
```

- Existen varias manera de ver si el *Portsentry* se está ejecutando, algunas son:

  - Viendo los procesos que están corriendo.

```
[root@maquina portsentry]# ps auxw | grep portsentry
root     3687  0.0  0.3  1380  464 ?        S    15:32   0:00
/usr/local/psionic/portsentry/portsentry –atcp
root     3689  0.0  0.5  1648  716 ?        S    15:32   0:00
/usr/local/psionic/portsentry/portsentry –audp
```

  - Portsentry además de generar bitácoras en el sitio donde fue instalado, utiliza *syslog* para reportar toda la información generada por la ejecución del programa. El administrador puede acceder a esta información en el archivo "*messages*" o donde se lo haya especificado en el *syslogd.conf*.

```
[root@maquina portsentry]# vi /var/log/messages
Jan 10 15:32:21 linux4 portsentry[3687]: adminalert: PortSentry is now active and listening.
Jan 10 15:32:26 linux4 portsentry[3688]: adminalert: Psionic PortSentry 1.1 is starting.
Jan 10 15:32:26 linux4 portsentry[3689]: adminalert: Advanced mode will monitor first
1024 ports
Jan 10 15:32:26 linux4 portsentry[3689]: adminalert: Advanced mode will manually exclude
port: 520
Jan 10 15:32:26 linux4 portsentry[3689]: adminalert: Advanced mode will manually exclude
port: 138
...
```

  - Ejecutando el comando *netstat –nap* el sistema reportará los puertos que está escuchando.

```
[root@maquina portsentry]# netstat -nap
raw      0      0 0.0.0.0:6           0.0.0.0:*           7          3687/portsentry
raw      0      0 0.0.0.0:17          0.0.0.0:*           7          3689/portsentry
```

BITÁCORA DE INSTALACIÓN

scanlogd

Justificación

Scanlogd permite detectar *scaneos* y *loggeos* al puerto TCP. Cuando detecta los *scaneos* al puerto, escribe una línea por *scaneo* vía *syslog*. Lo interesante de esta herramienta es que no utiliza demasiada memoria.

Instalación

A continuación se explica cómo realizar la instalación de *scanlogd*:

- Descargar el programa de Internet.

```
[root@maquina root]# mkdir /root/scanlogd
[root@maquina root]# cd /root/scanlogd
[root@maquina scanlogd]# wget "ftp://rpmfind.net/linux/Madeinlinux/distro/
                              4.0SE/cdtree/cd2/madeinlinux/RPMS/scanlogd-2.2-
                              1.5.i386.rpm"
```

- Instalación del rpm.

```
[root@maquina scanlogd]# cd /etc/init.d
[root@maquina init.d]# rpm –ivh /root/scanlogd/scanlogd-2.2-1.5.i386.rpm
```

- Editar el archivo /etc/syslog.conf

```
[root@maquina init.d]# vi /etc/syslog.conf
```

Se agrega en el archivo la siguiente línea:

```
# Detector de scaneos al puerto TCP
daemon.alert                    /var/log/alert
```

- Editar el archivo /etc/rc.d/rc.local

```
[root@maquina init.d]#  vi /etc/rc.d/rc.local
```

Se agrega la siguiente línea:

```
/etc/init.d/scanlogd
```

- Cuando se realiza un *scaneo* a la máquina se registra en el archivo *alert* que se encuentra en */var/log/*
- Si se borra el archivo *alert*, se debe de reinicar el demonio *syslog*.

```
[root@maquina init.d]#  /etc/init.d/syslog restart
```

BITÁCORA DE INSTALACIÓN

Antivirus MailScanner con F-prot

Justificación

Debido a que MailScanner procesa cada mensaje que se recibe en el servidor antes de colocarlo en el archivo correspondiente al buzón del usuario de correo, es una herramienta muy útil para los administradores de servidores Web bajo Linux. Además, si encontrara cualquier tipo de virus, eliminaría el archivo adjunto y daría aviso al emisor, al destinatario y al postmaster.

Instalación

A continuación se explica cómo realizar la compilación e instalación de *MailScanner*, junto con *F-Prot*, que es el más potente de los antivirus gratuitos para Linux:

- Se descarga el archivo de antivirus gratuito *F-Prot* de Internet. Para más información se puede consultar la siguiente dirección: http://linux.bankhacker.com/software/F-Prot+Antivirus+for+Linux/

  [root@maquina]# mkdir /root/antivirus
  [root@maquina]# cd /root/antivirus
  [root@maquina antivirus]# wget "ftp://ftp.f-prot.com/pub/fp-linux_beta.tar.gz"

- Descomprimir y desempaquetar el archivo fp-linux_beta.tar.gz

  [root@maquina]# cd /usr/local/
  [root@maquina local]# tar -zxvf /root/antivirus/fp-linux_beta.tar.gz

- Realizar las siguientes ligas.

  [root@maquina local]# ln -fs /usr/local/fp-linux_311b_beta /usr/local/f-prot
  [root@maquina local]# ln -fs /usr/local/f-prot/f-prot.sh /usr/local/bin/f-prot

- Cambiar permisos.

  [root@maquina local]# chmod +x /usr/local/f-prot/f-prot*

- Descargar de Internet el *MailScanner*.

  [root@maquina]# cd /root/antivirus
  [root@maquina antivirus]# wget
  "http://www.sng.ecs.soton.ac.uk/mailscanner/files/MailScanner-3.12-4.tar"

- Desempaquetar el archivo MailScanner-3.12-4.tar.

  [root@maquina]# cd /usr/local/
  [root@maquina local]# tar -xvf /root/antivirus/MailScanner-3.12-4.tar

- Configurar el sendmail.

  [root@maquina local]# cd /var/spool
  [root@maquina spool]# mkdir mqueue.in
  [root@maquina spool]# chown root mqueue.in
  [root@maquina spool]# chgrp bin mqueue.in
  [root@maquina spool]# chmod 750 mqueue.in
  [root@maquina spool]# cp -f /etc/rc.d/init.d/sendmail /etc/rc.d/init.d/sendmail.old
  [root@maquina spool]# vi /etc/rc.d/init.d/sendmail
  Se busca en el archivo la cadena:

  "sendmail -bd -q15m"

o

"daemon /usr/sbin/sendmail $(["$DAEMON" = yes] && echo -bd) $([-n "$QUEUE"] && echo -q$QUEUE)"

Y se reemplaza por:

"sendmail -bd -ODeliveryMode=queueonly -OQueueDirectory=/var/spool/mqueue.in ; sendmail -q15m"

o

"daemon /usr/sbin/sendmail -bd -ODeliveryMode=queueonly -
OQueueDirectory=/var/spool/mqueue.in ;
daemon /usr/sbin/sendmail $(["$DAEMON" = yes] && echo -bd) $([-n "$QUEUE"] && echo -q$QUEUE)"

El archivo queda de la siguiente manera:

#daemon /usr/sbin/sendmail -bd -ODeliveryMode=queueonly -
OQueueDirectory=/var/spool/mqueue.in ; daemon /usr/sbin/sendmail $(["$DAEMON" = yes] && echo -bd) $([-n "$QUEUE"] && echo -q$QUEUE)

sendmail -bd -ODeliveryMode=queueonly -OQueueDirectory=/var/spool/mqueue.in ; sendmail -q15m

#daemon /usr/sbin/sendmail -bd -ODeliveryMode=queueonly –
OQueueDirectory=/var/spool/mqueue.in

Salvar los cambios en el archivo

- Reiniciar el sendmail.

[root@maquina spool]# /etc/init.d/sendmail stop
[root@maquina spool]# /etc/init.d/sendmail start

- Se instalan los módulos de perl necesarios.

  - IO-stringy

[root@maquina]# cd /root/antivirus
[root@maquina antivirus]# wget "http://www.cpan.org/authors/id/ERYQ/IO-stringy-2.108.tar.gz"
[root@maquina antivirus]# cd /usr/src/
[root@maquina src]# tar –zxvf /root/antivirus/IO-stringy-2.108.tar.gz
[root@maquina src]# cd /usr/src/IO-stringy-2.108/
[root@maquina IO-stringy-2.108]# perl Makefile.PL
[root@maquina IO-stringy-2.108]# make
[root@maquina IO-stringy-2.108]# make test
[root@maquina IO-stringy-2.108]# make install

➢ MIME-Base64

```
[root@maquina]# cd /root/antivirus
[root@maquina antivirus]# wget "http://www.cpan.org/authors/id/GAAS/MIME-Base64-2.12.tar.gz"
[root@maquina antivirus]# cd /usr/src/
[root@maquina src]# tar –zxvf /root/antivirus/MIME-Base64-2.12.tar.gz
[root@maquina src]# cd /usr/src/MIME-Base64-2.12/
[root@maquina MIME-Base64-2.12 ]# perl Makefile.PL
[root@maquina MIME-Base64-2.12]# make
[root@maquina MIME-Base64-2.12]# make test
[root@maquina MIME-Base64-2.12]# make install
```

➢ MailTools

```
[root@maquina]# cd /root/antivirus
[root@maquina antivirus]# wget
"http://www.cpan.org/authors/id/M/MA/MARKOV/MailTools-1.43.tar.gz"
[root@maquina antivirus]# cd /usr/src/
[root@maquina src]# tar –zxvf /root/antivirus/MailTools-1.43.tar.gz
[root@maquina src]# cd /usr/src/MailTools-1.43/
[root@maquina MailTools-1.43]# perl Makefile.PL
[root@maquina MailTools-1.43]# make
[root@maquina MailTools-1.43]# make test
[root@maquina MailTools-1.43]# make install
```

➢ File-Spec

```
[root@maquina]# cd /root/antivirus
[root@maquina antivirus]# wget "http://www.cpan.org/authors/id/R/RB/RBS/File-Spec-0.82.tar.gz"
[root@maquina antivirus]# cd /usr/src/
[root@maquina src]# tar –zxvf /root/antivirus/File-Spec-0.82.tar.gz
[root@maquina src]# cd /usr/src/File-Spec-0.82/
[root@maquina File-Spec-0.82]# perl Makefile.PL
[root@maquina File-Spec-0.82]# make
[root@maquina File-Spec-0.82]# make test
[root@maquina File-Spec-0.82]# make install
```

➢ Mime-tools

```
[root@maquina]# cd /root/antivirus
[root@maquina antivirus]# wget "http://www.cpan.org/authors/id/ERYQ/MIME-tools-5.411a.tar.gz"
[root@maquina antivirus]# cd /usr/src/
[root@maquina src]# tar –zxvf /root/antivirus/MIME-tools-5.411a.tar.gz
[root@maquina src]# cd /usr/src/MIME-tools-5.411/
[root@maquina MIME-tools-5.411]# perl Makefile.PL
[root@maquina MIME-tools-5.411]# make
[root@maquina MIME-tools-5.411]# make test
[root@maquina MIME-tools-5.411]# make install
```

- Instalar el decodificador TNEF, que se encarga de transcribir los archivos en formato RTF.

```
[root@maquina MIME-tools-5.411]# cd /usr/src
[root@maquina src]# tar -zxvf /usr/local/MailScanner-3.12-4/mailscanner/bin/tnef-
1.1.1+sizelimit.tar.gz
[root@maquina src]# ln -sf tnef-1.1.1+sizelimit tnef-1.1
[root@maquina src]# cd tnef-1.1
[root@maquina src]# ./configure
[root@maquina src]# make
[root@maquina src]# mv /usr/local/MailScanner-3.12-4/mailscanner/bin/tnef
/usr/local/MailScanner-3.12-4/mailscanner/bin/tnef.old
[root@maquina src]# cp src/tnef /usr/local/MailScanner-3.12-4/mailscanner/bin/tnef
```

- Configurar el *MailScanner.*

```
[root@maquina src]# cd /usr/local/MailScanner-3.12-4/mailscanner/etc/
[root@maquina etc]# rm -f mailscanner.conf
[root@maquina etc]# ln -fs mailscanner.conf.linux mailscanner.conf
```

Reemplazar "/opt/MailScanner" por "/usr/local/MailScanner-3.12-4/mailscanner/" en los siguientes archivos:

```
[root@maquina etc]# cd /usr/local/MailScanner-3.12-4/mailscanner/bin
[root@maquina bin]# vi check_mailscanner
```

Reemplazar las siguientes líneas:

```
virusdir=/opt/mailscanner/bin
config=/opt/mailscanner/etc/mailscanner.conf
```

Por :

```
virusdir=/opt/mailscanner/bin
config=/usr/local/MailScanner-3.12-4/mailscanner/etc/mailscanner.conf
```

```
[root@maquina bin]# vi config.pl
```

Reemplazar la siguiente línea:

```
my $prefix = '/opt/mailscanner';
```

Por:

```
my $prefix = '/usr/local/MailScanner-3.12-4/mailscanner';
```

```
[root@maquina bin]# cd ../etc/
[root@maquina etc]#  vi mailscanner.conf
```

Reemplazar la siguiente línea :

```
Virus Scanner      = sophos
```

Por :

Virus Scanner = f-prot

Y

Sweep = /opt/sophos/bin/sophoswrapper

Por

Sweep = /usr/local/MailScanner-3.12-4/f-prot/f-protwrapper

- Ligas de programas del sistema.

```
[root@maquina etc]# ln -sf /bin/ps /usr/bin/ps
[root@maquina etc]# ln -sf /bin/fgrep /usr/bin/fgrep
[root@maquina etc]# ln -sf /bin/grep /usr/bin/grep
[root@maquina etc]# ln -sf /bin/sed /usr/bin/sed
```

- Generar algunos directorios que requiere el *MailScanner.*

```
[root@maquina etc]# mkdir /var/spool/MailScanner/
[root@maquina etc]# mkdir /var/spool/MailScanner/quarantine/
[root@maquina etc]# mkdir /var/spool/MailScanner/incoming/
```

- Otras ligas necesarias son:

```
[root@maquina etc]# ln -sf /usr/local/MailScanner-3.12-4/mailscanner
/usr/local/MailScanner

[root@maquina etc]# ln -sf /usr/local/MailScanner-3.12-4/mailscanner/etc/filename.rules.conf
/usr/local/MailScanner-3.12-4/mailscanner/etc/filename.rules

[root@maquina etc]# ]# ln -sf /usr/local/MailScanner-3.12-
4/mailscanner/etc/sender.virus.report.txt /usr/local/MailScanner-3.12-
4/mailscanner/etc/sender.report.txt
```

- Realizar un cron para poder asegurar que el *MailScanner* está funcionando siempre.

```
# 18/05/2000 JKF Ensure my e-mail virus scanner is still running

0,20,40 * * * * [ -x /usr/local/MailScanner-3.12-4/mailscanner/bin/check_mailscanner ]&&
/usr/local/MailScanner-3.12-4/mailscanner/bin/check_mailscanner >/dev/null 2>&1
```

- Para verificar que se está ejecutando correctamente el *MailScanner*, se puede descargar de la siguiente dirección: http://www.eicar.org/anti_virus_test_file.htm, un archivo.zip (http://www.eicar.org/download/eicar_com.zip) con un virus inofensivo, para examinar el sistema, se envía por correo. Si todo funciona bien, el mensaje será devuelto y se dará aviso al emisor, al destinatario y al postmaster.

- Para actualizar el antivirus se realiza lo siguiente:

```
[root@maquina]# cd /root/antivirus
[root@maquina antivirus]# wget --passive-ftp ftp://ftp.f-prot.com/pub/fp-def.zip
[root@maquina antivirus]# wget --passive-ftp ftp://ftp.f-prot.com/pub/macrdef2.zip
[root@maquina antivirus]# unzip fp-def.zip
[root@maquina antivirus]# unzip macrdef2.zip
[root@maquina antivirus]# mv –f SIGN* MACRO* /usr/local/f-prot
[root@maquina antivirus]# 0,20,40 * * * * | -x /usr/local/MailScanner-3.12-
4/mailscanner/bin/check_mailscanner |&& /usr/local/MailScanner-3.12-
4/mailscanner/bin/check_mailscanner >/dev/null 2>&1
[root@maquina antivirus]# /etc/init.d/sendmail stop
[root@maquina antivirus]# /etc/init.d/sendmail start
```

BITÁCORA DE INSTALACIÓN

Iptables

Justificación.

Como lo hemos mencionado **iptables** es el software que permite filtrar los paquetes, es decir mira la cabecera de los paquetes para ver si deben pasar, decidiéndolo al instante. Con esta herramienta podremos permitir ciertos tipos de tráfico y desactivar otros, en nuestro caso particular realizamos un script para permitir pings, tráfico DNS, conexiones por medio del Secure Shell (ssh), servicio de correo electrónico, servicio Network File System (NFS) y Network Information System (NIS), servicio de Web seguro y base de datos MySQL, que son los servicios que presta la Unidad de Servicios de Cómputo Académico a la comunidad de la Facultad de Ingeniería.

Instalación.

Primero se comprueba que estén instalados los módulos iptable_filter y ip_tables.

[root@maquina]# /sbin/lsmod

Después se corre el script que activará las reglas de filtrado de paquetes llamado iptables.bash.

[root@maquina]# ./iptables.bash

El contenido del script iptables.bash es el siguiente:

```
[root@maquina]# more iptables.bash
#Establecemos las politicas por defecto
# Explicacion: hay 3 politicas forward (reenvio), output (salidas)
# e input (entradas)
# Resultado: nada entra, todo sale y nada se reenvia
/sbin/iptables -P FORWARD DROP
/sbin/iptables -P OUTPUT ACCEPT
```

```
/sbin/iptables -P INPUT DROP

# Aqui establecemos las entradas (input) permitidas
# Dejamos pasar todo el trafico local (dentro de tu LAN)
/sbin/iptables -A INPUT -i lo -p all -j ACCEPT

#Permitimos realizar pings
# 0 - Respuesta de Eco (Respuesta a un ping)
# 8 - Solicitar un Eco (solicitar ping)

#/sbin/iptables -A INPUT -p icmp --icmp-type 8 -j ACCEPT
#/sbin/iptables -A INPUT -p icmp --icmp-type 0 -j ACCEPT

/sbin/iptables -A INPUT -p icmp -j ACCEPT

# Permitimos el trafico dns (DNS) - El servidor de nombres
# ESTABLISHED El paquete seleccionado se asocia con otros paquetes en una conexion establecida
# RELATED El paquete seleccionado esta iniciando una nueva conexion en  algun punto de la
conexion existente

/sbin/iptables -A INPUT -p tcp --dport 53  -m state --state ESTABLISHED,RELATED -j ACCEPT
/sbin/iptables -A INPUT -p udp --dport 53 -m state --state ESTABLISHED,RELATED -j ACCEPT

# Permitimos el trafico ssh (Secure Shell Daemon)
# NEW El paquete seleccionado o bien esta creando una nueva conexion o bien  forma parte de una
# conexion de dos caminos que antes no habia sido vista.

/sbin/iptables -A INPUT -p tcp -i eth0 -m state --state NEW,ESTABLISHED,RELATED --dport 22
-j ACCEPT
/sbin/iptables -A INPUT -p udp -i eth0 -m state --state NEW,ESTABLISHED,RELATED --dport 22
-j ACCEPT

/sbin/iptables -A INPUT -p tcp --dport 1024:  -j ACCEPT
/sbin/iptables -A INPUT -p udp --dport 1024:  -j ACCEPT
# Acepto paquetes de conexiones ya establecidas

/sbin/iptables -A INPUT -p TCP -m state --state RELATED  -j ACCEPT

# Rechazamos paquetes de conexiones nuevas

/sbin/iptables -A INPUT -i eth0 -m state --state INVALID -j DROP

# Rechazamos paquetes de forwarding de conexiones no establecidas

/sbin/iptables -A FORWARD -i eth0 -m state --state INVALID -j DROP

#No permitir la entrada de paquetes que provienen de ip's virtuales
#Rechazar paquetes provenientes de una red privada clase A
/sbin/iptables -A INPUT  -i eth0 -s 10.0.0.0/8 -j DROP
#Rechazar paquetes provenientes de una red privada clase B
/sbin/iptables -A INPUT  -i eth0 -s 172.16.0.0/12 -j DROP
#Rechazar paquetes provenientes de una red privada clase C
```

```
/sbin/iptables -A INPUT  -i eth0 -s 192.168.0.0/16 -j DROP
#Rechazar paquetes provenientes de una red multicast clase D
/sbin/iptables -A INPUT -i eth0 -s 224.0.0.0/4 -j DROP
#Rechazar paquetes provenientes de una red privada clase E
/sbin/iptables -A INPUT -i eth0 -s 240.0.0.0/5 -j DROP

# Anti-flooding o inundacion de tramas SYN.

/sbin/iptables -N syn-flood
/sbin/iptables -A INPUT -i eth0 -p tcp --syn -j syn-flood
/sbin/iptables -A syn-flood -m limit --limit 1/s --limit-burst 4 -j RETURN
/sbin/iptables -A syn-flood -j DROP

# Abrimos para SMTP

/sbin/iptables -A INPUT -p tcp -s 0.0.0.0/0 --dport 25 -j ACCEPT
/sbin/iptables -A INPUT -p udp -s 0.0.0.0/0 --dport 25 -j ACCEPT
#Permitimos trafico hp-alarm-mgr

/sbin/iptables -A INPUT -p tcp --dport 783 -j ACCEPT

# Permitimos el trafico pop3
/sbin/iptables -A INPUT -p tcp -s 132.248.54.0/24 --dport 110 -j ACCEPT
/sbin/iptables -A INPUT -p tcp -s 132.248.52.0/24 --dport 110 -j ACCEPT
/sbin/iptables -A INPUT -p tcp -s 132.248.139.0/24 --dport 110 -j ACCEPT
/sbin/iptables -A INPUT -p udp -s 132.248.54.0/24 --dport 110 -j ACCEPT
/sbin/iptables -A INPUT -p udp -s 132.248.52.0/24 --dport 110 -j ACCEPT
/sbin/iptables -A INPUT -p udp  -s 132.248.139.0/24 --dport 110 -j ACCEPT

# Permitimos el trafico imap

/sbin/iptables -A INPUT -p tcp -s 127.0.0.1 --dport 143 -j ACCEPT
#/sbin/iptables -A INPUT -p udp -s 132.248.52.0/24 --dport 143 -j ACCEPT

# Permitimos el trafico mysql
/sbin/iptables -A INPUT -p tcp -s 127.0.0.1 --dport 3306 -j ACCEPT
#/sbin/iptables -A INPUT -p udp -s 127.0.0.1 --dport 3306 -j ACCEPT

# Permitimos el trafico https
/sbin/iptables -A INPUT -p tcp --dport 443 -j ACCEPT
#/sbin/iptables -A INPUT -p udp --dport 443 -j ACCEPT

#Pertimos el trafico pop3pw

/sbin/iptables -A INPUT -p tcp -s 127.0.0.1 --dport 106 -j ACCEPT
#/sbin/iptables -A INPUT -p udp -s 127.0.0.1 --dport 106 -j ACCEPT
```

8.7 Procedimientos Preventivos y Correctivos

8.7.1 Procedimientos Preventivos

Consideraciones Generales.

- Aplicación de parches de seguridad.
- "Tomar una foto del sistema LIMPIO" (md5, cops-crc.chk, tripwire).
- Bloqueo de puertos.

Uno de los métodos más recomendados para la prevención al barrido (*Scaneo*) de puertos es la desactivación de servicios que no se encuentren en uso en el sistema. El problema principal del barrido de puertos es que los principales servicios menores al puerto 1024 o mejor conocidos como puertos privilegiados son vulnerables a diversos tipos de ataques.

Es importante saber para qué sirve cada puerto y el servicio que proporciona, para sólo tener los puertos abiertos para los servicios que ofrece el servidor , ya que se recomienda que ante menos servicios menores serán las probabilidades de intrusión en el sistema. En seguida se enumeran el número de puerto y el servicio que proporciona dicho puerto.

- Echo (7/tcp, udp) Se utiliza únicamente para depuración.
- systat (11/tcp/udp) Muestra información acerca del servidor, información tal como usuarios conectados, carga del sistema, procesos en funcionamiento, etc.
- chargen (19/tcp, udp) Se utiliza únicamente para depuración.
- telnet (23/tcp, udp) Muy Vulnerable. Se sugiere utilizar en su lugar otras soluciones como SSH.
- smtp (25/tcp, udp) Históricamente la mayoría de las entradas en los servidores han venido a través de este puerto. Se debe FILTRAR este puerto y mantener SIEMPRE la última versión estable conocida de cualquier programa de correo, especialmente si se trabaja con sendmail.
- time (37/tcp, udp) Devuelve la hora del sistema en un formato legible por la máquina (4 bytes mas o menos).
- nameserver (42/tcp, udp) Si dispone de una red privada, debe instalar un servidor de nombres para ella. Bloquee el acceso a dicho servidor desde el exterior, y utilice siempre la última versión de BIND para resolver nombres.
- tftp (69/tcp, udp) Falta de autentificación. Usado en el pasado principalmente bajo el protocolo UDP.

- private dialout (75/tcp, udp) [RFC1700] Recomendamos deshabilitarlo, usado internamente.
- finger (79/tcp, udp) Puede obtenerse información acerca de usuarios concretos, información que puede utilizarse para adivinar claves de acceso.
- http (80/tcp, udp) Puerto usado para el servidor Web. Conviene redirigir el acceso a un puerto no privilegiado en máquinas UNIX.
- npp (92/tcp, udp) [Network Printing Protocol] Impresión remota vía red.
- objcall (94/tcp, udp) [Tivoli Object Dispatcher] Utilizado por la herramienta de Gestión de redes Tivoli.
- sunrpc (111/tcp,udp) Especialmente peligroso sobre UDP. Usado en servicios NFS.
- auth (113/tcp,udp) Usado para la autentificación de usuarios (puede utilizarse para realizar un portscan).
- ntp (123/tcp,udp) [Network Time Protocol] Se utiliza para sincronizar los relojes de las máquinas de una subred.
- netbios (137, 138, 139/tcp, udp) Según los RFC2001 y 2002 NetBIOS es capaz de funcionar correctamente a pesar de que se estén enviando bloques de datos con información errónea o corrompida.
- snmp (161/tcp, udp) Se puede obtener mucha información a través de este servicio, como por ejemplo: el estado de la interfaz de red, conexiones concurrentes en la máquina, etc.
- snmp-trap (162/tcp, udp) A través de este puerto se realizan solicitudes que pueden cambiar la configuración del servidor.
- irc (194/tcp, udp) Generalmente, conviene bloquear los puertos 6666, 6667 y 6668 ya que son a los que se enganchan los servidores de IRC.
- exec (512/tcp) Ejecuta órdenes en estaciones remotas. Hace uso de los comandos 'r' (rexec, rcp, rlogin).
- biff (512/udp) Notifica de la llegada de correo.
- login (513/tcp) rlogin. (ver exec).
- who (513/udp) Muestra quien está utilizando el servidor remoto.
- cmd (514/tcp) Similar a exec (512/tcp.)

- syslog (514/udp) Maneja las bitácoras y eventos del sistema.
- printer (515/tcp,udp).
- router (520/tcp,udp) Local routing process.
- ingreslock (1524/tcp) En la mayoría de los Unix se puede encontrar esta entrada en */etc/services*. Ya que está dado de alta y es un puerto no privilegiado es un buen lugar para una puerta trasera (no sería la primera vez que ocurre).

➢ Cuando la máquina inicialice, verificar que sólo los demonios necesarios estén activados. A continuación se muestra una lista de los más comunes:

- **anacron.** Ejecuta comandos con frecuencia de días.
- **Apmd.** Este demonio sólo es necesario en Laptops para las funciones Apm y en X Window proporciona información acerca de la batería. Si se utiliza una PC de escritorio, este servicio será innecesario.
- **Arpwath.** Guarda información de ethernet/ip para notificar al *syslog*.
- **atd.** Ejecuta los comandos necesarios para reiniciar los procesos atorados.
- **autofs.** El demonio *autofs* es capaz de montar y desmontar automáticamente sistemas de archivos locales y remotos, liberándonos de hacerlo manualmente mediante la orden mount y umount.
- **chargen y chargen-udp.** Es un generador de caracteres servido internamente por *inetd*, que se utiliza sobre todo para comprobar el estado de las conexiones en la red; cuando alguien accede a este servicio simplemente ve en su terminal una secuencia de caracteres ASCII que se repite indefinidamente.
- **crond.** Demonio de *crontab*, para lanzar trabajos a intervalos regulares de tiempo.
- **daytime y daytime-udp.** El servicio daytime, asociado al puerto 13, tanto TCP como UDP, es un servicio interno de xinetd (esto es, no hay un programa externo que lo sirva, el propio xinetd se encarga de ello); al recibir una conexión a este puerto, el sistema mostrará la fecha y la hora, en un formato similar al resultado del comando *date*. No es un servicio básico por lo que se recomienda cerrarlo. Debe activar xinetd para usar este servicio.
- **echo y echo-udp.** Este servicio lo único que hace es un eco, envía de vuelta todo lo que recibe.
- **finger.** Permite que otras máquinas hagan un finger a la nuestra. Debe activar xinetd para usar este servicio.
- **gpm.** Es el demonio que se encarga del ratón cuando se trabaja en modo de texto. Si el sistema utiliza X Window, o bien se considera innecesario utilizar el ratón en el modo de texto, este servicio será innecesario.
- **identd.** Controla el servidor de identificación de usuario
- **ipchains.** Administración de IP firewall con ipchains.
- **iptables.** Administración de IP firewall con iptables.
- **keytable.** Controla la carga del teclado.
- **kotalk.** Versión de talk de KDE. Debe activar xinetd para usar este servicio.
- **kudzu.** Controla y prueba el hardware.

- lpd. Es el demonio que se encarga de la impresión a través del comando «*lpr*». Si la computadora no utilizara una impresora, este servicio será completamente innecesario.
- **mountd,nettfs,nfs.** Estos demonios son necesarios si se desea un servidor de sistema de archivos (NFS). Si la computadora no estuviera conectada a una red local, estos servicios serán innecesarios.
- **netfs.** Controla el montaje de NFS, SMB, NCP (NetWare).
- **network.** Controla la interfaz de red.
- **nfs.** Controla el montaje de los archivos de sistema NFS.
- **nfslock.** Controla el bloqueo de archivo NFS.
- **ntalk.** Controla el servicio de ntalk. Debe activar xinetd para usar este servicio.
- **ntpd.** Es el demonio NTPv4.
- **portmap.** Soporte para la invocación de procedimientos remotos RPC(Remote Procedure Call).
- **random.** Controla la generación de números aleatorios.
- **rawdivices.** Maneja algunos dispositivos físicos.
- **rexec.**
- **rhnsd.**
- **rlogin.** Inicia una sesión remota por medio del comando rlogin. Debe activar xinetd para usar este servicio.
- **rsh.** Inicia un shell remoto. Debe activar xinetd para usar este servicio.
- **rsync.**
- **sendmail.** Controla los servicios de envío de correo.
- **servers.**
- **services.**
- **sgi_fam.**
- **snmpd.** Controla el demonio Simple Network Management Protocol (SNMP).
- **snmptrapd.** Se trata de un agente que procesa las alertas de otros agentes. Para ello permanece escuchando en el puerto 162 (udp), cuando recibe una alerta por este puerto procede a guardarla en el registro (syslog). Sin embargo, también puede ser configurado para utilizar programas externos en el tratamiento de las alertas.
- **sshd.** Demonio del OpenSSH.
- **syslog.** Inicia y detiene los servicios System Logging.
- **talk.** Controla las comunicaciones con usuarios remotos. Debe activar xinetd para usar este servicio.
- **telnet.** Permite conexiones remotas. Debe activar xinetd para usar este servicio.
- **time.**
- **time-udp.**
- **vncserver**
- **xinetd.** Inicia y detiene el servicio xinetd.
- **yppasswd.** Controla el servidor YP password.
- **ypserv.** Controla los servicios de Network Information. Este debe correr en el servidor NIS.
- **ypxfrd.**

➢ Realizar respaldos de los archivos de configuración: /etc/passwd, /etc/hosts, /etc/hosts.deny, /etc/hosts.allow, en disquetes o cd room.

- Realizar respaldos periódicamente.

Para realizar un respaldo completo del filesystem /users con una densidad BPI a la unidad de cinta y que grabará este evento al archivo /etc/dumpdates, se debe utilizar el siguiente comando:

```
[root@servidor_1 root]#dump 0udf 327670 /dev/st0 /users
```

El siguiente comando respaldaría todos los archivos que hayan cambiado desde el último respaldo nivel 2,1, ó 0 :

```
[root@servidor_1 root]#dump 3udf 327670 /dev/st0 /users
```

Para poder hacer respaldo a través de la red, se utilizará el comando *rdump*. Pero se debe de poder configurar la máquina destino (donde se grabará el respaldo) para que admita conexiones sin password de la máquina origen para la cuenta de *root*. Es suficiente con configurar el archivo *.rhosts* para este propósito y cuando se acabe el respaldo quitar el archivo por seguridad. Además habilitar los servicios de rlogin y rsh.

Para respaldar un filesystem del servidor_2 a cinta en el servidor_1, se haría lo siguiente:

1. Editar el archivo *.rhosts*

```
[root@servidor_1 root]#vi .rhosts
servidor_2.fi-c.unam.mx root
```

2. Habilitar los servicios de *rlogin* y *rsh*.

```
[root@servidor_1 root]# vi /etc/xinetd.d/rsh
# default: on
# description: The rshd server is the server for the rcmd(3) routine and, \
#       consequently, for the rsh(1) program.  The server provides \
#       remote execution facilities with authentication based on \
#       privileged port numbers from trusted hosts.
service shell
{
    disable = no
    socket_type         = stream
    wait                = no
    user                = root
    log_on_success      += USERID
    log_on_failure      += USERID
    server              = /usr/sbin/in.rshd
}

[root@servidor_1 root]# vi /etc/xinetd.d/rlogin
# default: on
# description: rlogind is the server for the rlogin(1) program.  The server \
#       provides a remote login facility with authentication based on \
```

```
#       privileged port numbers from trusted hosts.
service login
{
    disable = no
    socket_type          = stream
    wait                 = no
    user                 = root
    log_on_success       += USERID
    log_on_failure       += USERID
    server               = /usr/sbin/in.rlogind
}
```

3. Reiniciar el servicio *xinetd*.

   ```
   [root@servidor_1 root]# /etc/init.d/xinetd restart
   ```

4. Realizar el respaldo.

   ```
   [root@servidor_2 root]# rdump 0udf 327670 servidor_1.fi-a.unam.mx:/dev/st0 /home
   ```

5. Regresar a su estado original el archivo *.rhosts* y los servicios rlogin y rsh

A cada una de las cintas hay que etiquetarlas y ponerles los siguiente datos:

- Nombre del servidor.
- Nombre del filesystem que se respaldo.
- Número de cintas que se emplearon, por ejemplo, si sólo se ocupó una, se pone 1/1.
- Comando con el que se hizo el respaldo.
- Fecha del respaldo.

- Considerar la instalación de un firewall.
- Educación de usuarios y administradores.
- Instalar y configurar herramientas de seguridad tales como ssh, logdaemon, PGP, S/key, Opie, IPsec, tripwire, COPS, TCP-Wrappers, Tiger, Swatch, syslogd, syslog-ng, etc.
- Reducir el uso de programas como telnet y ftp y sustituirlos paulatinamente por ssh, scp y sftp, respectivamente.
- Usar contraseñas seguras (fuertes).
- Evitar el uso de mecanismos de confianza entre máquinas y/o usuarios.

- Utilizar sistemas de detección de intrusos académicos o comerciales (como Network Flight Recorder).
- Recompilar syslogd para leer un archivo de configuración diferente a /etc/syslog.conf y enviar las bitácoras a un servidor remoto (de preferencia que este servidor sea dedicado).
- Desarrollar e implementar políticas de seguridad.
- Si no se necesitan, desinstalar compiladores.
- Activar sólo los puertos, cuentas y servicios de red realmente necesarios y configurarlos adecuadamente.
- En su caso, configurar de manera segura el servidor de FTP anónimo.
- Asegurarse de tener las últimas versiones de sendmail, ftpd, BIND, httpd, fingerd, herramientas de seguridad, qpopper, majordomo, etc.
- Revisar constantemente y de manera impredecible las bitácoras del sistema y las generadas por las herramientas de seguridad instaladas.

Seguridad Física.

1. Cerrar con llave los CPU.
2. Se puede usar el BIOS para impedir que los atacantes reinicien el equipo y manipulen el sistema Linux:
   - Si el BIOS de la PC lo permite, poner una contraseña de inicio. Esto no proporciona mucha seguridad, pero podría ser un buen elemento disuasorio.
   - Leer el manual de BIOS, muchos BIOS de x86 también permiten especificar otras diversas configuraciones de seguridad buenas.

   Nota: Si el equipo es un servidor y se establece una contraseña de inicio, el equipo no se iniciará sin atención. Se necesitará ir y poner la contraseña en el caso de un fallo de energía.
3. Los distintos cargadores de inicio de Linux pueden tener también un juego de contraseña de inicio.
   - LILO, por ejemplo, tiene password y restricted; password requiere siempre la contraseña en el momento del inicio, mientras que restricted requiere una contraseña para inicio, sólo si se especifican algunas opciones (tales como single) en el indicador de LILO .
   - Estas contraseñas meramente retrasarán al atacante resuelto. No impedirán a alguien iniciar desde un floppy y montar la partición de root. Si se va a usar seguridad junto

con el cargador de inicio, se podría también desactivar el inicio desde un floppy en el BIOS de la computadora y proteger el BIOS con contraseña.

4. Si se va a dejar la máquina por un momento, es bueno poder "bloquear" la consola para que nadie emplee la cuenta o mire el trabajo. Dos programas que hacen esto son: xlock y vlock.

   - xlock es un cierre X de presentación en pantalla. Debe estar incluido en todas las distribuciones de Linux que soporten X. En general, se puede ejecutar xlock desde cualquier terminal X de la consola y se bloqueará la pantalla, y requerirá la contraseña para abrirse.
   - vlock es un programa simple que permite cerrar algunas o todas las consolas virtuales en el sistema Linux. Puede cerrar sólo aquella en la que se está trabajando o todas. Si sólo se cierra una, otros pueden entrar y usar la consola; no podrán usar la consola virtual hasta que se abra para ello, también requerirá la contraseña.

   Bloquear la consola impedirá a alguien entrometerse en el trabajo, pero desde luego no le impedirá reiniciar el equipo o estropear de otro modo el trabajo. Tampoco le impedirá acceder a al equipo desde otro equipo en la red y causar problemas.

   Lo más importante es que no impide a alguien desconectar completamente el Sistema X Window, ir al indicador de conexión de una consola virtual normal, o al VC desde el cual se arrancó el X11, suspenderlo y así obtener los privilegios. Por esta razón, se debería considerar usarlo sólo bajo control de xdm.

Crear Nuevas Cuentas.

1. Darles la cantidad mínima de privilegios que necesiten.

2. Ser consciente desde cuándo/dónde se conectan.
3. Asegurarse de remover las cuentas inactivas.

4. El uso del mismo ID de usuario en todos los computadoras y redes es aconsejable para facilitar el mantenimiento del recuento, así como para permitir un análisis más fácil de los datos de *log*.

5. La creación de ID de usuario de grupo debería estar absolutamente prohibida. Las cuentas de usuario también proporcionan transparencia y esto no es posible con cuentas de grupo.

6. El formato de las cuentas de los usuarios para los servidores es el siguiente:
   CCPMNDD

   donde

   CC son dos letras según la carrera que estén cursando, de acuerdo a la siguiente tabla:

CARRERA	CÓDIGO
Ingeniería Civil	ci
Ingeniería en Minas y Metalurgista	mm
Ingeniería Eléctrica Electrónica	ee
Ingeniería en Computación	co
Ingeniería en Telecomunicaciones	te
Ingeniería Geofísica	gf
Ingeniería Geología	gl
Ingeniería Industrial	id
Ingeniería Mecánica	mc
Ingeniería Mecánica Eléctrica	me
Ingeniería Petrolera	pt
Ingeniería Topográfica y Geodésica	tg
Posgrado	po
Tesista	ts

P inicial del apellido paterno.
M inicial del apellido materno.
N inicial del nombre o del primer nombre en caso de que sean dos.
DD son dos dígitos, los cuales se van aumentando en el caso de que coincidan las iniciales, por default es el 00.

Ejemplo:

comfg00 El usuario Gabriela Martínez Fuentes estudia la carrera de Ingeniería Computación y es el primer usuario con esa secuencia de caracteres.

Seguridad de Root.

1. Al realizar algún comando complejo, ejecutarlo primero en modo no destructivo. Especialmente los comandos que usen comodines: por ejemplo, si se quiere hacer "rm foo*.bak", primero hacer "ls foo*.bak" y asegurarse que se van a borrar los archivos correctos.

2. Proporcionar a los usuarios un alias por defecto para que el comando rm les pida confirmación para el borrado de archivos.

3. Convertirse en root sólo para hacer tareas específicas. Si se está intentando planificar cómo hacer algo, volver al shell de usuario normal hasta que se esté *seguro* de lo que necesita ser hecho por root.

4. La variable de entorno PATH es muy importante para el usuario root, ya que en ella se especifican los directorios en los que el shell busca los programas.

   - Limitar el PATH para el usuario root tanto como sea posible y no incluir que significa "el directorio actual".
   - No tener directorios escribibles en el PATH de búsqueda, dado que esto puede permitir a los atacantes modificar o poner nuevos binarios, permitiéndoles ejecutar como root ese comando, la próxima vez que se ejecute.

5. Nunca usar como root el conjunto de herramientas rlogin/rsh/rexec (las llamadas utilidades-r). Están sujetas a muchos tipos de ataques y es absolutamente peligroso ejecutarlas como root. De preferencia no crear un archivo .rhosts para el root, si es necesario, eliminarlo una vez que se termine de ocupar.

6. El archivo /etc/securetty contiene una lista de terminales desde los que puede conectarse root. Por defecto (con Linux Red Hat) esto se pone sólo para las consolas virtuales locales (vtys). Hay que tener mucho cuidado al añadir cualquier otra cosa a este archivo. Se tendría que ser capaz de conectarse remotamente como cuenta de usuario regular y entonces hacer su si se necesita (empleando ssh u otro canal encriptado), así que no hay necesidad de conectarse directamente como root.

7. Actuar despacio y de forma meditada cuando se ejecutan programas como root. Las acciones podrían afectar aún muchas cosas.

Seguridad de archivos y del sistema de archivos.

1. Nunca debe haber una excusa para que los usuarios ejecuten programas SUID/SGID desde sus directorios home.

   - Usar la opción nosuid en /etc/fstab para particiones que sean escribibles por otros que no sean root.
   - También se puede usar nodev y noexec sobre particiones home de usuarios, así como /var, prohibiendo de este modo la ejecución de programas y la creación de dispositivos de carácter o de bloque, que de todos modos nunca serían necesarios.

2. Si se está exportando un sistema de archivos usando NFS, asegurarse de configurar /etc/exports con el acceso más restrictivo posible. Esto significa no usar comodines, no permitir acceso de escritura de root y exportar archivos de sólo lectura, siempre que sea posible.

3. Configurar el umask de creación de archivos de usuarios para que sean tan restrictivos como sea posible. Normalmente, las configuraciones de umask incluyen 022, 027 y 077 (que es el más restrictivo).

4. Si se están montando sistemas de archivos usando un sistema de archivos de red tal como NFS, configurar /etc/exports con restricciones adecuadas. Normalmente, es deseable usar 'nodev', 'nosuid' y, quizás 'noexec'.

5. Poner límites al sistema de archivos en vez de dejarlo ilimitado como viene por defecto. Se pueden controlar los límites por usuario usando el módulo PAM de límites de recursos y /etc/pam.d/limits.conf. Por ejemplo, los límites para el grupo usuarios podrían parecerse a esto:

```
@users    hard core   0
@users    hard nproc  50
@users    hard rss    5000
```

   Esto significa prohibir la creación de archivos core, restringir el número de procesos a 50 y restringir el uso de memoria por usuario a 5M.

6. Los archivos /var/log/wtmp y /var/run/utmp contienen los registros de conexión de todos los usuarios del sistema. Debe mantenerse su integridad porque pueden usarse para determinar cuándo y desde dónde ha entrado un usuario (o un intruso potencial) en el sistema. Estos archivos también deben tener permisos 644 sin afectar a la operación normal del sistema.

7. El bit inmutable puede usarse para impedir borrar o sobrescribir accidentalmente un archivo que debe ser protegido. También impide que alguien cree un enlace simbólico al archivo (tales enlaces simbólicos han sido la fuente de ataques incluyendo borrar /etc/passwd o /etc/shadow).

8. Encontrar todos los programas SUID/SGID del sistema y mantener un registro de lo que son, para estar consciente de cualquier cambio que pudiera indicar que hay un intruso potencial. Usar el siguiente comando para encontrar todos los programas SUID/SGID en el sistema:

```
root# find / -type f \( -perm -04000 -o -perm -02000 \)
```

9. Se pueden quitar los permisos SUID o SGID a un programa sospechoso con chmod, después cambiarlo de nuevo si se cree que es absolutamente necesario.

10. Los archivos escribibles por todo el mundo, particularmente los archivos de sistema, pueden ser un agujero de seguridad, si un cracker logra acceso al sistema y los modifica. Además, los directorios escribibles por todos, son peligrosos, dado que permiten a un cracker añadir o borrar archivos a su antojo. Para localizar todos los archivos escribibles por todos en el sistema, usar el siguiente comando:

```
root# find / -perm -2 ! -type l -ls
```

    y asegurarse de que se sabe por qué esos archivos son escribibles. En el curso normal de la operación, diversos archivos serán escribibles por todos, incluyendo algunos

desde /dev, y enlaces simbólicos, así el ! -type l que excluye a éstos del comando previo find.

11. Los archivos sin propietario también pueden ser un indicio de que un intruso ha accedido al sistema. Para localizar en el sistema los archivos sin propietario, o que no pertenezcan a ningún grupo, es con el comando:

```
root# find / -nouser -o -nogroup -print
```

12. Encontrar archivos .rhosts es una de las tareas regulares de la administración del sistema, puesto que estos archivos no deben estar permitidos en el sistema, un cracker sólo necesita una cuenta insegura para, potencialmente, lograr acceso a toda la red. Para localizar todos los archivos .rhosts en el sistema, es con el siguiente comando:

```
root# find /home -name .rhosts –print
```

13. Antes de cambiar los permisos sobre cualquier archivo del sistema, asegurarse de que se entiende lo que se está haciendo. Nunca cambiar los permisos sobre un archivo porque parezca el modo más fácil de lograr que las cosas funcionen. Determinar siempre por qué el archivo tiene ese permiso, antes de cambiarlo.

14. Los archivos de configuración del sistema (normalmente en /etc) están usualmente en modo 640 (-rw-r-----) y el dueño es root. Nunca dejar los archivos de sistema escribibles, por un grupo o por cualquiera. Algunos archivos de configuración, incluyendo /etc/shadow, sólo deben ser legibles por el root y los directorios en /etc al menos no deben ser accesibles a otros.

Detección de intrusos.

1. Mantener la calma.
2. Revisar bitácoras.

Las bitácoras son una gran ventaja, pero con frecuencia son ignoradas. A continuación se mencionará como sacar sólo la información necesaria de estas bitácoras.

1. Lo primero que se debe hacer es un plan.

   - Enseguida se define qué es lo que se quiere conocer.
   - Determinar qué información se necesita de las bitácoras

2. El segundo paso es identificar qué bitácoras contienen esa información.

   - Revisar los accesos a la cuenta comprometida (utilizando last).
   - Revisión de Archivos de Bitácoras:

     - syslog.
     - messages.

- maillog.
- xferlog.
- secure.

En diversas ocasiones los intrusos modifican las bitácoras, por lo que no se puede confiar totalmente, en la lectura de las mismas.

Bitácora /var/log/messages ó /var/adm/messages

En esta bitácora se pueden identificar ataques del tipo bufferoverflow por varios tipos de ataques como *mountd*. Se pueden ver cosas similares en la bitácora maillog (se pueden ver ataques como *imapd*).

Un ataque de bufferoverflow puede aparecer de la siguiente manera:

Apr 14 04:20:51 mozart mountd[6688]: Unauthorized access by NFS client 192.168.11.200.
Apr 14 04:20:51 mozart syslogd: Cannot glue message parts together
Apr 14 04:20:51 mozart mountd[6688]: Blocked attempt of 192.168.11.200 to mount
~P~P~P~P~P~P~P~P~P~P~P~P
~P~P~P~P~P~P~P~P~P~P~P~P
~P~P~P~P~P~P~P~P~P~P~P~P
~P~P~P~P~P~
P~P~P~P~P~P~P~P~P~P~P~P~
P~P~P~P~P~P~P~P~P~P~P~P~
P~P~P~P~P~P~P~P~P~P~P~P~
P~P~P~P~P~
P~P~P~P~P~P~P~P~P~P~P~P~
P~P~P~P~P~P~P~P~P~P~P~P~
P~P~P~P~P~P~P~P~P~P~P~P~
P~P~P~P~P~
P~P~P~P~P~P~P~P~P~P~P~P~
P~P~P~P~P~P~P~P~P~P~P~P~
P~P~P~P~P~P~P~P~P~P~P~P~
P~P~P~P~P~P
P~P~P~P~P~P~P~P~P~P~P~P~
P~P~P~P~P~P~P~P~P~P~P~P~
P~P~P~P~P~P~P~P~P~P~P~P~
P~P~P~P~P~P
P~P~P3Ù3À°^Í~@3Ò3À~KÚ°^
Fí~@þÂuô1À°^Bí~@~EÂubëb^
V¬<ýt^FþÂt^Këö°0þÈ~HFÿëì^°^
B~
I^FþÈ~IF^D°^F~IF^H°f1ÛþÂ~I
ñí~@~I^F°^Bf~IF^L°*f~IF^N~
MF^L~IF^D1À~IF^P°^P~IF^H°

```
ñþÃÍ~@°^A~ÍF^D°f^DÍ~@ë^D
ëLëR1À~ÍF^D~ÍF^H°ñþÃÍ~@~
HÃ°?1Ë Í~@°?þÁÍ~@°?þÁÍ~@,.
bin@~
I^F,.sh!@~ÍF^D1À~ÍF^G~Iv^H
~ÍF^L°^K~Ió~MN^H~MV^LÍ~
@1À°^A1ÚÍ~@ëÈÿÿÿÿÿÿPrivet
ADMcrew~P(-^E^H(-^E^H(-
^E^H(-^E^H(-^E^H (-^E^H(-
^E^H(-^E^H(Apr 14 04:20:51
mozart ^H(-^E^H(-^E^H(-^E^H(-
^E^H(-^E^H(-^E^H(-^E^H (-
^E^H(-^E^H(-^E^H(-^
E^H(-^E^H-^E^H(-^E^H(-
^E^H(-^E^H(-^E^H(-^E^H(-
^E^H (-^E^H(-^E^H(-^E^H(-^E
^H(-^E^H-^E^H(-^E^H(-^E^H(-
^E^H(-^E^H(-^E^ H (-^E^H(-
^E^H(-^E^H(-^E^H(-^E
^H(-^E^H(-^E
```

Cuando aparezca algo similar significará que alguien ha intentado explotar una vulnerabilidad del *automount* del sistema. Es difícil determinar si fue exitoso o no.

Una forma de saber si lo logró, es viendo si hay conexiones de lugares remotos al sistema. Otra forma de ver si tuvieron éxito es buscando cuentas como "moof", "rewt", "crack0" o "w0rm" ó algunas otras, que se hayan agregado recientemente al sistema, específicamente al /etc/passwd.

Estas cuentas con UID 0, son agregadas por algunos scripts de explotación comunes. Una vez que está adentro, lo más común es que limpien las bitácoras e instalen troyanos para las bitácoras. De aquí en adelante, ya no se recibirán bitácoras provenientes del sistema.

También en esta bitácora se puede ver, si se ha sido rastreado (*scaneado*) recientemente. Se puede dar cuenta si encuentra algo parecido a lo siguiente:

> Apr 14 21:08:58 mozart imapd[11682]: ttloop: peer died: Invalid or incomplete multibyte or wide character

> Apr 14 21:03:12 mozart ftpd[11688]: FTP session closed

Bitácora /var/log/xferlog ó /var/adm/xferlog

Si el sistema comprometido tiene servicio de FTP, en este archivo se encontrarán todos los procesos ejecutados del FTP.

Examinar que tipo de herramientas y software ha introducido al sistema el intruso y que archivos nuevos se encuentran dentro de su home o en el sistema completo.

Bitácora /var/log/maillog

También en esta bitácora se puede ver si ha sido rastreado y se puede encontrar algo similar a lo siguiente:

```
Apr 14 21:01:58 mozart imapd[11667]:
command stream end of file, while reading
line user=??? Host=[192.168.11.200]
Apr 14 21:01:58 mozart ipop3d[11668]: No
such file or directory while reading line
user=??? Host=[192.168.11.200]
Apr 14 21:02:05 mozart sendmail[11675]:
NOQUEUE:[192.168.11.200]:expn root
```

Bitácora /var/log/secure

En este archivo se puede buscar por intentos de conexiones repetidas intentando entrar por diversos servicios, si aparecen intentos de conexiones como:

```
Apr 14 19:18:56 mozart in.telnetd[11634]:
connect from 192.168.11.200
Apr 14 19:18:56 mozart imapd[11635]:
connect from 192.168.11.200
Apr 14 19:18:56 mozart in.fingerd[11637]:
connect from 192.168.11.200
Apr 14 19:18:56 mozart ipop3d[11638]:
connect from 192.168.11.200
Apr 14 19:18:56 mozart in.telnetd[11639]:
connect from 192.168.11.200
Apr 14 19:18:56 mozart in.ftpd[11640]:
connect from 192.168.11.200
```

Se puede notar que el sistema ha sido rastreado por la dirección que aparece.

3. Buscar archivos ocultos.

Buscar aquellos archivos que empiecen con un '.'(punto), pero revisar exhaustivamente todos los archivos ocultos, estos no aparecen con un simple *ls*, se utilizan para esconder herramientas para romper la seguridad del sistema, por ejemplo, un programa crack o también contener el /etc/passwd del sistema o de otros sistemas a los que ha entrado el intruso.

Muchos intrusos suelen crear directorios ocultos utilizando nombres como '...'(punto-punto-punto), '..''(punto-punto), '..^g'(punto-punto control+g). También se dan casos en los cuales utiliza nombres como '.x' o hasta '.mail'.

- Buscar archivos ocultos o inusuales en el sistema (.*).

```
find / -name ".*" -print
```

- Buscar programas adivinadores de contraseñas (crack, John The Ripper, Cracker Jack, Hades, etc.)

```
find / -name \( -name "*crack*"-o -name  "*Crack* \) –print
```

4. Buscar archivos SETUID.

Se debe buscar cuidadosamente archivos SETUID o SETGID (especialmente, los que pertenecen a root). Para eso se puede utilizar, el comando find.

- find / -group wheel -perm –2000 print
- find / -user root -perm -4000 -print -xdev
- ncheck -s /dev/rsd0g

Este último comando 'ncheck' permite buscar archivos SETUID por particiones.

5. Revisar archivos binarios.

Buscar archivos que contengan caballos de troya en los archivos binarios. Esta es una de las tareas principales de un intruso cuando ha comprometido la seguridad de un servidor. Una lista de los posibles binarios, generalmente más usados y preferidos por los intrusos, pero no completa, que se pueden sustituir es la siguiente:

Login	Ls	su
Find	telnet	du
Df	Netstat	ifconfig
Libc	sync	w, who

También hay herramientas que se pueden utilizar para detectar estos troyanos, por otro lado, los intrusos también tiene herramientas como son los conocidos rootkits.

6. Examinar los archivos que son ejecutados por "cron" y "at".

Algunos intrusos depositan puertas traseras, mejor conocidas como backdoors, que les permitan volver al sistema aunque se les niegue el acceso al mismo.

Hay que asegurarse que todos los archivos son nuestros y que no tiene permisos de escritura.

7. Buscar Sniffers (capturadores de red).

Se tienen que buscar sniffers, ya que esta es una de las opciones favoritas y más utilizadas por los intrusos, los usan para capturar todo el tráfico de la red, incluyendo las sesiones de ftp y telnet a otros sistemas.

- Buscar sniffers (linsniff, esniff, solsniff, sunsniff, sniffit, etc.)

```
find / -name "*sniff*" -print
```

De este modo puede obtener cuentas de usuarios (logins) y passwords. Se puede ver el sistema en modo promiscuo en /var/log/messages , pero no debe pasar mucho tiempo, después de que el sistema fue comprometido, por ejemplo en Linux se vería de la siguiente forma :

```
Apr 27 17:03:38 mozart
kernel:eth0:Setting
promiscuous mode

Apr 27 17:03:43 mozart
kernel:eth0:Setting
promiscuous mode
```

Algunos de los sniffers más conocidos son los siguientes:

- linsniff666.c
- sunsniff.c
- esniff.c
- sniffit
- solsniff.c

8. Examinar el archivo /etc/inetd.conf.

Hay que buscar en especial entradas que ejecuten un shell (por ejemplo: /bin/sh o /bin/csh) y comprobar que todos los programas son legítimos y no troyanos.

De igual forma hay que revisar los demonios de los programas como telnet, ftp y todos los servicios que preste la máquina.

9. Buscar alteraciones en el sistema y en los archivos.

En especial hay que buscar entradas con el signo '+' o servidores de máquinas no apropiados en archivos como /etc/host.equiv, /etc/hosts.lpd y en todos los archivos .rhost del sistema, con especial interés los de root, uucp y ftp. Estos archivos no deberían tener atributo de escritura.

10. Examinar los equipos del área local.

    Hay que buscar indicios de que la red ha sido comprometida. En particular aquellos equipos que compartan NIS+ o NFS o aquellos sistemas listados en el /etc/hosts.equiv. Lógicamente, revisar también los sistemas que los usuarios comparten mediante el acceso del .rhosts.

11. Examinar el archivo /etc/passwd.

    Hay que buscar alteraciones en las cuentas de los usuarios o la creación de nuevas cuentas, especialmente aquellas con UID 0, las que no tienen password, etc. Otra cosa que hará el intruso es obtener la tabla de passwords, a la cual le correrá un programa para buscar passwords débiles y así obtener mas cuentas para entrar al sistema.

12. Utilizar el comando finger

    Ejecutando el comando 'finger' se intentará sacar información del intruso y de dónde provino la intrusión, por ejemplo:

    - finger @intruso.net
    - finger intruso@intruso.net

    Si se tiene suerte se puede sacar información de la máquina de la cual provino la intrusión.

8.7.2 Procedimientos durante el ataque

Si el intruso se encuentra en el sistema.

Algunos de los consejos más comunes para llevar a cabo si se detecta a un intruso en sesión son:

- Asegurarse de tener respaldos recientes y en buen estado.
- Ignorarlo, tratar de hablar con él (write, talk) o monitorear sus actividades (tcpdump, snoop).
- Sacarlo del sistema (matar sus procesos, cambiar su contraseña, desconectar la máquina de la red, tirar los servicios de red, apagar la máquina).

```
ps [-fea | aux] | grep cuenta_intruso | grep -v grep | xargs kill –9
```

- Rastrearlo usando los comandos who, w, last, lastcomm, netstat, whois, nslookup, finger, telnet, strings /var/adm/lastlog, /var/adm*, obtener información del ruteador, examinar los archivos de historia ($HOME/.history, $HOME.sh_history),etc.
- Si existe un teléfono de contacto, llamar al encargado y hacerle saber el problema. (NO USAR E-MAIL, a menos que sea la única opción, en cuyo caso se deberá ser discreto).
- Contactar a otros administradores involucrados y dar aviso.

- Levantar el reporte de incidente.
- Contactar a un organismo de seguridad (DGSCA), si se amerita.

8.7.3 Procedimientos Correctivos

Detectar Compromisos de Seguridad Física.

1. Comprobar cuándo fue reiniciado el equipo. Dado que Linux es un sistema operativo (SO) robusto y estable, las únicas veces que el equipo debe reiniciarse es cuando *uno* lo desmonta para mejoras en el SO, cambios de hardware o cosas así. Si el equipo ha sido reiniciado, eso puede ser un signo de que un intruso lo ha puesto en peligro. Muchos de los modos en que el equipo puede verse comprometido requieren que el intruso reinicie o apague el equipo.
2. Comprobar los signos de intrusión. Aunque muchos intrusos limpian las huellas de su presencia de los *logs*, es una buena idea comprobarlos todos y anotar cualquier discrepancia.
3. Almacenar los datos de *log* en un lugar seguro, tal como un servidor dedicado a *log* dentro en la red bien protegida. Una vez que el equipo ha estado comprometido, los datos de *log* serán de poca utilidad, porque lo más probable es que también hayan sido modificados por el intruso.
4. Algunas cosas a comprobar en los *logs*:

   - *Logs* cortos o incompletos.
   - *Logs* que contengan registros de fecha extraños.
   - *Logs* con permisos o propietarios incorrectos.
   - Registros de reinicios de servicios.
   - *Logs* perdidos.
   - Entradas *su* o *logins* desde sitios extraños.

El Compromiso de Seguridad ya ha ocurrido.

1. Cerrar el "Agujero".
   - Si se es capaz de determinar qué medios usó el atacante para entrar al sistema, se debe intentar cerrar ese "agujero".
   - Comprobar todos los archivos de *log*, hacer una visita a las listas y páginas de seguridad y ver si hay nuevos exploits comunes que se puedan arreglar. Red Hat no tiene todavía separadas sus mejoras de seguridad de sus mejoras de fallos, pero las erratas de la distribución están disponibles en http://www.redhat.com/errata

2. Evaluar el Daño.

   - Lo primero es evaluar el daño. ¿Qué ha estado comprometido? Ejecutar un chequeo de integridad con Tripwire o buscar en todos sus datos importantes.
   - Se puede considerar salvar los archivos de configuración y luego limpiar el disco y reinstalar, restaurando entonces los archivos de usuario y los archivos

de configuración desde las copias de seguridad. Esto asegurará que se tiene un sistema nuevo y limpio. Si se tienen que hacer las copias de seguridad a partir del sistema comprometido, se tiene que ser especialmente cuidadoso con todos los binarios que se restauren, dado que pueden ser caballos troyanos puestos ahí por el intruso.

- La re-instalación debe considerarse obligatoria cuando el intruso ha obtenido acceso de root. Además, se debe mantener cualquier evidencia que haya, por lo que se puede tener un disco libre en un sitio seguro.
- Luego se debe ver, cuánto tiempo hace que sucedió el compromiso y si las copias de seguridad mantienen algún trabajo dañado.

3. Copias.

   - Si el sistema está comprometido, se pueden restaurar los datos que se necesiten a partir de las copias de seguridad. Por supuesto, algún dato es valioso también para el atacante y no lo destruirá, sino que lo robará y tendrá sus propias copias; pero al menos aún se tienen los datos.
   - Comprobar las diversas copias de seguridad realizadas anteriormente antes de restaurar un archivo que ha sido estropeado. ¡El intruso podría haber comprometido los archivos hace mucho tiempo y se pudieron haber hecho con éxito muchas copias de seguridad de un archivo comprometido!

Cuando ocurre un robo de equipo.

1. No tocar nada, revisar lo que hace falta.

2. Realizar un oficio dirigido al Secretario Administrativo de la Facultad de Ingeniería indicando las características del equipo de cómputo robado y las condiciones en las que se encontró el lugar.

3. Se anexarán copias para:

   - Jefe de la Unidad de Servicios de Cómputo Académico.
   - Secretario General de la Facultad de Ingeniería.
   - Jefe del Departamento Jurídico.
   - Jefe del Departamento de Servicios Escolares.

8.8 Plan de Contingencia

La Unidad de Servicios de Cómputo Académico (UNICA), considera que la información es el patrimonio principal de toda Institución, por lo que se deben aplicar medidas de seguridad para protegerla y estar preparados para afrontar contingencias y desastres de diversos tipos.

Con el propósito de proteger la información y asegurar la continuidad del procesamiento de la información necesaria para el adecuado desempeño de sus funciones institucionales, UNICA presenta el documento **"Plan de Contingencia y Seguridad de la Información".**

A medida que la tecnología ha ido evolucionando y con ella, la importancia de los sistemas de información de las instituciones públicas y privadas, la seguridad del entorno informático (hardware, software, comunicaciones, etc.) se ha convertido en una de las grandes preocupaciones de los profesionales de esta actividad. Esta preocupación debe ser adecuadamente comprendida y compartida por los directivos, los cuales deben considerar a las inversiones en medidas de seguridad informática, como un gasto necesario, que contribuye a mantener la operatividad y rentabilidad de la Institución.

Esto implica que los responsables del Servicio Informático deban explicar con la suficiente claridad y con un lenguaje inteligible, las potenciales consecuencias de una política de seguridad insuficiente o incluso inexistente. El presente documento pretende ayudar a comprender mejor la problemática implícita de los sistemas de información, ya que toda institución debe estar preparada para el caso de ocurrencias imprevistas.

Considerando que no hay dos instituciones ni dos sistemas informáticos iguales, los aspectos de seguridad que se desarrollan en el presente documento, deben tomarse como un intento de establecer un "denominador común", que pueda ser aplicable al mayor número posible de instituciones, y, en cada caso particular, deberán adaptarse al contexto propio de cada entidad.

Objetivo:

Restaurar los servicios que la Unidad de Servicios de Cómputo Académico ofrece a la Facultad de Ingeniería en el menor tiempo, de manera eficiente y con el menor costo y pérdidas posibles.

Análisis de riesgos

- ¿A qué riesgos en la seguridad informática se enfrenta UNICA?

  - Al fuego, que puede destruir los equipos y archivos.
  - Al robo común, llevándose los equipos y archivos.
  - Al vandalismo, que dañen los equipos y archivos.
  - A fallas en los equipos, que dañen los archivos.
  - A equivocaciones, que dañen los archivos.
  - A la acción de virus, que dañen los equipos y archivos.
  - A terremotos, que destruyen el equipo y los archivos.
  - A accesos no autorizados, filtrándose datos no autorizados.
  - Al robo de datos, difundiéndose los datos sin cobrarlos.

- ¿Qué probabilidad hay de que tenga efecto alguno de los riesgos mencionados?

  Al fuego, que puede destruir los equipos y los archivos.

  - ¿UNICA cuenta con protección contra incendios?
  - ¿Se cuenta con sistemas de aspersión automática?
  - ¿Diversos extintores?

- ¿Detectores de humo?
- ¿Los empleados están preparados para enfrentar un posible incendio?

A un **robo común**, llevándose los equipos y archivos.

- ¿Las computadoras se ven desde la calle?
- ¿Hay personal de seguridad en la Institución?
- ¿Cuántos vigilantes hay?
- ¿Los vigilantes, están ubicados en zonas estratégicas?

Al **vandalismo**, que dañen los equipos y archivos.

- ¿Existe la posibilidad que un ladrón desilusionado o frustrado cause daños?
- ¿Hay la probabilidad que causen algún otro tipo de daño intencionado?

A **fallas en los equipos**, que dañen los archivos.

- ¿Los equipos tienen un mantenimiento continuo por parte de personal calificado?
- ¿Cuáles son las condiciones actuales del hardware?
- ¿Es posible predecir las fallas a que están expuestos los equipos?

A **equivocaciones** que dañen los archivos.

- ¿Cuánto saben los empleados de computadoras o redes?
- Los que no conocen del manejo de la computadora, ¿saben a quién pedir ayuda?

A la acción de **virus**, que dañen los archivos.

- ¿Se prueba software sin hacerle un examen previo?
- ¿Todas las máquinas tienen unidades de disquetes?
- ¿Se cuentan con procedimientos contra los virus?

A **terremotos**, que destruyen los equipos y archivos.

- ¿La Institución se encuentra en una zona sísmica?
- ¿El edificio cumple con las normas antisísmicas?
- Un terremoto, ¿cuánto daño podría causar?
- A accesos no autorizados, filtrándose datos importantes

Al **robo de datos**; difundiéndose los datos.

- ¿Cuánto valor tienen actualmente las Bases de Datos?

- ¿Cuánta pérdida podría causar en caso de que se hicieran públicas?
- ¿Se ha elaborado una lista de los posibles sospechosos que pudieran efectuar el robo?
- La lista de sospechosos, ¿es amplia o corta?
- ¿Contamos con Sistemas de Seguridad en el Correo Electrónico o Internet?

Resumen de los riesgos ordenados por el factor de riesgo de cada uno.

Protecciones actuales

- *Generales.*-Se hace una copia cada semana de los archivos de los usuarios.
- *Robo común.*- Se cierran ventanas. Las puertas de entrada se cierran con llave. Poner la chapa de seguridad en los cubículos cuando se sale por alguna razón (aunque sean unos minutos). No s epermite la entrada a personas extrañas en el área de trabajo.
- *Vandalismo.*- Se cierra la puerta de entrada con doble chapa.
- *Falla de los equipos.*- Se tratan con cuidado, se realiza el mantenimiento preventivo de forma periódica, no se permite fumar, beber o comer cualquier tipo de alimento en las salas.
- *Los programas de dominio público y de uso compartido.*- Sólo se usan si proceden de una fuente fiable.
- *Equivocaciones.*- Los becarios tienen buena capacitación.
- *Terremoto.*- Se cuenta con alarma sísmica ubicada en la dirección de la Facultad de Ingeniería.
- *Acceso no autorizado.*- Se cierra la puerta de entrada. Varias computadoras disponen de llave de bloqueo del CPU.
- *Robo de datos.*- Se cierra la puerta principal. Varias computadoras disponen de llave de bloqueo del CPU.
- *Fuego.*- En la actualidad no se cuenta con nada. Sin embargo, podemos solictar extintores al Departamento de Bomberos. Para realizar lo anterior, llamamos al número telefónico 56 16 15 60, donde nos dijeron que debemos realizar lo siguiente:

    - Hacer una pertición a la Directora de Protección Civil la Dra. Ma. Elena y Arena del Rosario. Se encuentra ubicado en la Dirección de Servicios Generales.

    - La petición se debe de mandar con copia para el Jefe del Departamento del Departamento de Prevención y Combate de Siniestros, el cual le informará al Mayor Colchado del Departamento de Bomberos.

    - El Mayor Colchado nos informará que tenemos que hacer.

Listas de notificación.

NOMBRE	TELEFONO
CARRERA FOURNIER MARGARITA	Conocido*
CRUZ HERNÁNDEZ EDGAR RICARDO	Conocido*
CRUZ MARÍN NOÉ	Conocido*
FUENTES SERRANO LUIS FERNANDO	Conocido*
GARCÍA ROSALES GUILLERMO	Conocido*
RAMÍREZ PICHARDO JOSÉ DE JESÚS	Conocido*
SÁNCHEZ QUIJADA VICTOR HUGO	Conocido*
SANDOVAL VAZQUEZ RAFAEL	Conocido*

**Se omiten por privacidad*

Requerimientos de recursos.

- Cintas magnéticas.
- Unidad de cintas.
- Discos duros.
- Computadora con las mismas características que el servidor.

Plan de recuperación de desastres.

Cuando ocurra una contingencia, es esencial que se conozca a detalle el motivo que la originó y el daño producido, lo que permitirá recuperar en el menor tiempo posible el proceso perdido.

- Actividades previas al desastre.

  Ver el punto 8.7.2 del Capítulo 8.

- Pérdidas de información de los usuarios.

  En un error, la recuperación puede suponer pérdida de información. Siempre que sea posible conviene recuperar en un lugar distinto al original y sólo se deben recuperar los archivos necesarios.

  Generalmente, los programas de propósito general permiten la recuperación de todo el contenido o bien sacan una lista de todos los archivos para señalar aquellos que deseamos recuperar.

Restaurar archivos.

En este apartado se trata la restauración de un archivo o un grupo de archivos, en contraposición a la restauración de un sistema de archivos completo.

1. Determinar en qué cinta se encuentran los archivos a restaurar. Los usuarios generalmente buscan la última versión del archivo, pero no siempre es así. La existencia y ubicación del archivo dependen del esquema de respaldo empleado. Se deberán revisar las cintas más probables según la fecha indicada por el usuario, o recorrer todo el conjunto desde el respaldo nivel 0 inmediato anterior.
2. Crear un directorio donde recuperar los archivos. Muchas versiones de *restore* requieren reponer la ruta entera de directorios para recuperar el archivo. No usar */tmp*; su contenido será borrado en un re-arranque imprevisto.
3. Si se han colocado varios archivos de respaldo en una misma cinta, se deberá consultar la documentación de ubicación de cada uno, determinar el lugar en que se encuentra el de interés y usar el comando *mt* para ubicar el comienzo del archivo de respaldo.
4. Restaurar el archivo. Usar el comando complementario del respaldo: si se usó *dump* para respaldar, usar *restore*; si se usó *rdump*, usar *rrestore*.
5. Entregar el archivo al usuario. Se puede copiar el archivo hacia el directorio del usuario, verificando que no exista ya un archivo con ese nombre. *En ningún caso debe sobrescribirse un archivo de otro usuario.* Otra alternativa es dejarlo en el lugar de recuperación para que el usuario lo copie. En este caso, será preciso limpiar regularmente el directorio de recuperación.
6. Notificar al usuario.

Ejemplo completo de recuperación del archivo perdido.arch del usuario juanpe, con la cinta en la máquina paris:

Montar la cinta en la unidad de la máquina *paris*.

```
$ su
# cd /var/tmp
```

La recuperación se hará en el directorio /var/tmp.

```
# rsh paris mt -f /dev/mt0 fsf 3
```

Salta hasta el 4o. archivo de respaldo en la cinta.

```
# rrestore xf paris:/dev/mt0
 > /usr/users/juanpe/docs/perdido.arch
```

Ejecuta el comando e imprime mensajes; observar continuación del comando en la segunda línea.

```
# ls /var/tmp/usr/users/juanpe/docs
perdido.arch
```

Muestra la presencia del archivo recuperado.

```
# ls /usr/users/juanpe/docs
otro1.arch otro2.arch
```

Verifica que el archivo recuperado no existe en el directorio propio del usuario, para no reescribirlo.

```
# cp -p /var/tmp/usr/users/juanpe/docs/perdido.arch
 /usr/users/juanpe/docs
```

Copia el archivo recuperado hacia el directorio propio del usuario.

```
# mail -s "Archivo recuperado" juanpe
Su archivo perdido.arch fue recuperado.
Se encuentra en su directorio, bajo docs.
Saludos,
El Administrador.
.
```

Envía correo al usuario avisando la recuperación.

```
# exit
S
```

Fin de la tarea.

restore admite la opción *i*, para uso interactivo: el comando lee el catálogo de la cinta; se recorren los archivos como si se tratara de un árbol de directorios común, usando ls, cd y pwd; se van seleccionando los archivos a restaurar con add; cuando se han seleccionado todos, indicando extract los recupera de la cinta.

Ejemplo de recuperación interactiva. El indicador de root # cambia a restore> al operar dentro del comando.

```
# rrestore if paris:/dev/mt0
restore> ls
.:
arnoldo/ beiro/ juanpe/ lost+found/ vega/
restore> cd juanpe
restore> ls
carta01.txt core docs/ mbox perdido.arch varios/
restore> add perdido.arch
```

El archivo se agrega a la lista de archivos a recuperar. Agregar un directorio, agrega todo su contenido.

```
restore> ls
carta01.txt core docs/ mbox perdido.arch* varios
```

El asterisco indica que está marcado para recuperar.

```
restore> extract
```

Muestra mensajes; si no se sabe en qué volumen está el archivo, debe comenzarse por el último y proceder hacia el principio; aquí asumimos saber que está en el primer volumen.

```
Specify next volume #: 1
```

Se realiza la extracción; pregunta si el directorio raíz de la cinta debe intepretarse como directorio corriente; se usa sólo al restaurar sistemas de archivos completos.

```
set owner mode for '.'? [yn] n
#
```

Sale de restore, fin de la tarea.

Restaurar sistemas de archivos.

Antes de restaurar un sistema de archivos completo, se debe estar seguro de haber eliminado las causas que provocaron su destrucción.

1. Crear un sistema de archivos en la partición donde se va a restaurar y montarlo.
2. Cambiar al directorio raíz (punto de montaje) del nuevo sistema de archivos. Montar la primera cinta del último respaldo nivel 0. Arrancar la restauración con restore r. El comando pedirá las cintas sucesivas.
3. Al terminar de restaurar el nivel 0, continuar con los diferentes niveles en el mismo orden del esquema de respaldos empleado.

Ejemplo de restauración de un sistema de archivos a partir de un respaldo de 3 niveles.

```
# newfs /dev/dsk/c201d6s0 QUANTUM_PD1050S
# mount /dev/dsk/c201d6s0 /home
# cd /home
```

Crea el sistema de archivos, lo monta y se posiciona en él. Montar ahora la cinta 1 del último respaldo nivel 0 de /home.

```
# restore r
```

Montar las cintas restantes del respaldo nivel 0. Montar luego la primer cinta del respaldo nivel 1 siguiente.

```
# restore r
```

Montar las siguientes cintas del respaldo nivel 1. Montar luego la primer cinta del respaldo nivel 2 siguiente.

```
# restore r
```

Montar las siguientes cintas del respaldo nivel 2. Montar luego la primer cinta del respaldo nivel 3 siguiente.

```
# restore r
```

Esta secuencia repone el sistema de archivos a su estado original más cercano, al momento de pérdida. En el esquema de respaldos empleado, la única diferencia es la recuperación de los archivos que fueron borrados. Hay versiones de restore que llevan registro de los archivos borrados.

En una actualización del sistema operativo, debe hacerse un respaldo nivel 0 antes de la actualización, efectuar luego la actualización cuidando de reponer los archivos de configuración necesarios en los sistemas de archivos afectados por la actualización. Una vez que todo esté funcionando, realizar inmediatamente un nuevo respaldo nivel 0. Esto es imprescindible para asegurar la coherencia de los siguientes niveles, ya que la actualización puede haber modificado fechas de archivos preexistentes.

- Pérdida total o si el servidor está comprometido.

  - Instalar el sistema operativo realizando las particiones exactamente como las tenía el servidor (este dato se irá actualizando de acuerdo con la instalación que se realice del servidor):

Filesystem	Size	Mounted on
/dev/sdc5	1.4G	/

/dev/sda1	23M	/boot
/dev/sda3	8.1G	/home
/dev/sdc2	16G	/users
/dev/sdb1	3.8G	/usr
/dev/sdc1	16G	/usuarios
/dev/sdb3	29G	/var

- Recuperar los archivos importantes de los respaldos que se encuentran en disquetes o cd room y cintas magnéticas, en nuestro caso son /etc/passwd, /etc/shadow, /etc/hosts, /etc/hosts.deny,/etc/hosts.allow.
- Configurar los siguientes servicios:

*** Servicio NIS**

"Matar" los siguientes demonios: *ypserv*, *ypbind* y *portmap*.

```
#/etc/init.d/ypserv  stop
#/etc/init.d/ypbind  stop
#/etc/init.d/portmap  stop
```

Configuración del Servidor

```
#domainname  unixunica
```

En el archivo /etc/yp.conf agregar al final la siguiente línea

```
#vi /etc/yp.conf
```

```
# /etc/yp.conf - ypbind configuration file
# Valid entries are
#
#domain NISDOMAIN server HOSTNAME
#       Use server HOSTNAME for the domain NISDOMAIN.
#
#domain NISDOMAIN broadcast
#       Use  broadcast  on  the local net for domain NISDOMAIN
#
#ypserver HOSTNAME
#       Use server HOSTNAME for the  local  domain.  The
#       IP-address of server must be listed in /etc/hosts.
#
domain unixunica server 132.248.54.10
```

Crear la base de datos del NIS

#/usr/lib/yp/ypinit -m ← (ENTER)

next host to add: vgla.fi-c.unam.mx
:
(Aquí se agregan las máquinas a las que se les va a dar el servicio de NIS)
<Ctrl-d> para salirse.

#

Si se desea agregar más clientes, se necesitará levantar la base otra vez.

Hay que ver que estén "corriendo" los siguientes demonios:

ypserv
ypbind
portmap

para eso teclear:

#/etc/init.d/ypserv status

#/etc/init.d/ypserv status

#/etc/init.d/ypserv status

*** Servicio NFS (Network File Systems)**

Primero, levantar los siguientes demonios:

/etc/init.d/portmap start
/etc/init.d/nfs start

Entrar al archivo /etc/exports y colocar las siguientes líneas:

#vi /etc/exports

/home 132.248.54.13(rw) 132.248.54.3(rw)
/users 132.248.54.13(rw) 132.248.54.3(rw)
/usuarios 132.248.54.13(rw) 132.248.54.3(rw)
/var 132.248.54.85(rw,insecure,no_root_squash)

En seguida actualizamos los cambios

#exportfs –ra

* Servicio de correo

1. Quitar la línea que contenga la siguiente palabra DAEMON_OPTIONS o comentarla, tomando en cuenta que en este archivo los comentarios son con dnl.

2. Activar los cambios.

   # m4 /etc/mail/sendmail.mc > /etc/sendmail.cf

3. Levantar el demonio del sendmail.

   #/etc/init.d/sendmail start

4. Para permitir o denegar el relay, editamos el archivo /etc/mail/access, de tal manera que quede de la siguiente manera:

   # Check the /usr/share/doc/sendmail-8.11.6/README.cf file for a description

   # of the format of this file. (search for access_db in that file)

   # The /usr/share/doc/sendmail-8.11.6/README.cf is part of the sendmail-doc

   # package.

   #

   # by default we allow relaying from localhost...

localhost.localdomain	RELAY
localhost	RELAY
127.0.0.1	RELAY
132.248.54	RELAY
132.248.139	RELAY
132.248.52	RELAY

5. Actualizar los cambios.

   # makemap hash /etc/mail/access </etc/mail/access

8.9 Tendencias en la Seguridad Informática

A través de la historia siempre hubo necesidad de proteger la información. Hace 2000 años, en los tiempos de Julio César, se utilizó el primer sistema de encriptación del que se tiene conocimiento. El sistema, por cierto bastante fácil de descifrar, consistía en intercambiar cada letra del alfabeto por aquélla que distaba un número fijo de posiciones a la izquierda o a la derecha. Por ejemplo, un desplazamiento de dos posiciones a la derecha en la palabra "ataque" producía "cvcswg".

La seguridad es un proceso continuo con el que deberemos aprender a vivir, para intentar mejorarlo día a día. Por ello a continuación mencionaremos lo que se ha hecho, lo que se está desarrollando y hacia dónde va la seguridad informática.

a) Lo que se está haciendo.

- *Para el comercio electrónico.*

  La necesidad de proveer de mecanismos de seguridad a los sistemas de información involucrados sobre todo con el comercio electrónico, se hace indispensable.
  Desde los inicios de la era de la computación, los sistemas de seguridad para acceso a la información se han basado en el rudimentario método de "usuario" y "contraseña". La gran evolución que viene experimentando la informática con el paralelo crecimiento de Internet, ha aumentado los riesgos de la seguridad. La convergencia de un conjunto de tendencias tecnológicas ha extendido la idea de dotar de mecanismos de seguridad a las comunicaciones electrónicas, a la vez que están cambiando la forma de los sistemas de información actuales. Estas tendencias se pueden resumir en:

  - Un uso creciente de infraestructuras públicas de bajo costo para comunicaciones de datos.
  - El cambio de un sistema centralizado a un sistema distribuido.
  - La proliferación de computadoras personales, portátiles y usuarios que acceden a ellos remotamente.
  - El aumento, tanto en el número como en el tamaño de las redes LAN's y WAN's.
  - El creciente interés por realizar operaciones de comercio electrónico a través de Internet.
  - Una mayor aceptación por parte de los usuarios de realizar transacciones electrónicamente.

  Desde el punto de vista de la seguridad, las consecuencias más interesantes que conllevan estas tendencias se resumen en tres:

  - Los usuarios ya no se encuentran conectados localmente a los sistemas de información, sino que ahora se pueden encontrar en su casa, en la habitación de un hotel o en el coche.

- El intercambio de información abre sus fronteras mas allá de la empresa, sobre todo desde la aparición del correo electrónico.
- Existe un conglomerado compuesto por redes de comunicaciones, pudiendo ser estas líneas de teléfono, comunicaciones inalámbricas o vía satélite, que es por donde fluye la información.

En este entorno de evolución permanente, sin las medidas de seguridad apropiadas, la información puede ser tan accesible a extraños como al destinatario de la misma. Por lo tanto, en la era de las telecomunicaciones, *la seguridad ya no es un complemento sino una necesidad.*

En el mundo de las transacciones electrónicas es fundamental que se cumplan una serie de paradigmas que garanticen la seguridad informática: **autentificación** (demostrar que la persona a la que nos dirigimos es la correcta); **confidencialidad** (posibilidad de acceso a la información únicamente por usuarios autorizados); **integridad** (garantía de no manipulación de la información); y **no repudio** (que las partes implicadas no rechacen haber realizado la transacción).

Estos cuatro requisitos que debe cumplir un sistema de seguridad informática son fácilmente comparables con el mundo real, y no nos deben resultar ajenos, ya que se nos presentan cotidianamente.

Las Autoridades de Certificación

En el caso de las redes abiertas, como Internet, no era posible garantizar plenamente la confidencialidad de la información ni la identidad de los participantes, tanto en las transacciones de carácter económico como en otras que incluyeran algún tipo de información sensible o secreta; cosa que no ocurría con los sistemas de redes cerradas donde todos los usuarios son conocidos de antemano.

En Internet faltaba ese grado de confianza que deben tener todas las comunicaciones. Es aquí donde entran en juego las *Agencias de Certificación*, que emiten certificados digitales que permiten establecer relaciones de confianza entre grupos numerosos de usuarios. O lo que es lo mismo, son proveedores de servicios de certificación y, dada la calidad de sus funciones, deben demostrar que son entidades lo suficientemente estables como para que los certificados que emitan puedan considerarse fiables.

El certificado electrónico es emitido por la Agencia de Certificación, permitiendo verificar la identidad del propietario.

El certificado electrónico contiene el nombre del usuario, la clave pública y la fecha de caducidad del certificado, además de otros datos accesorios, que verifican las identidades electrónicas de los usuarios. La autenticidad e integridad de los certificados electrónicos se garantiza a través de la firma digital creada con la clave privada de la *Autoridad de Certificación* (*AC*). Los usuarios verifican esta firma en los certificados utilizando la clave pública de verificación.

La firma digital de la *AC* proporciona tres elementos de seguridad y confianza en el certificado. Primero, una firma digital del certificado válida es garantía de la integridad de éste. Además, puesto que sólo la *AC* tiene acceso a su clave privada, cualquiera que verifique la firma digital del certificado sabe que sólo esa *AC* pudo crear la firma. Por último, puesto que únicamente la *AC* tiene acceso a su clave privada, no puede negar haber firmado ese certificado.

La firma electrónica

La introducción de la firma electrónica y su reconocimiento de validez revoluciona, en cierta medida, nuestra actividad cotidiana, permitiendo la obtención de documentos tales como el pasaporte o cualquier certificado oficial desde casa y la realización de transacciones de comercio electrónico.

Una firma electrónica se fundamenta en la criptografía, es decir, es el resultado de una operación matemática que precisa de unas determinadas garantías para evitar su vulnerabilidad. Se emplea la criptografía como elemento de codificación que implica una seguridad informática.

Existen dos métodos generales de cifrado, el simétrico y el asimétrico. El cifrado simétrico se utiliza cuando se emplea la misma clave en las operaciones de cifrado y descifrado y el asimétrico se aplica cuando hablamos de una pareja de claves, la pública y la privada. En este último método de cifrado, la clave privada se mantiene secreta, mientras que la pública es conocida.

La Infraestructura de Clave Pública –PKI

La *PKI* (*Public Key Infrastructure*) es el conjunto de sistemas que proporcionan los servicios de cifrado y firma digital basados en la *Tecnología de Claves Públicas*. Su propósito es gestionar claves y certificados para que una organización mantenga un entorno de red fiable.

La *PKI* permite que las organizaciones aborden el problema de la seguridad con una infraestructura central que gestione las claves uniformemente en todas las aplicaciones, una *PKI* ofrece un marco de seguridad único, cumpliendo los paradigmas de **autentificación, confidencialidad, integridad y no repudio.** Una *PKI* gestionada debe ser capaz de realizar las tareas que se detallan a continuación.

Uso y verificación de certificados de clave pública. A la hora de crear certificados, la *Autoridad de Certificación* actúa como un agente de confianza dentro de la *PKI* y sólo en la medida en que los usuarios confíen en la *Autoridad de Certificación*, podrán confiar en los certificados emitidos por ella. Esto es lo que se conoce como confianza a tres bandas.

"Backup" y recuperación de claves. La *PKI* debe soportar un sistema de copia de seguridad y recuperación de las claves privadas de descifrado, por si ocurriera alguna incidencia y un usuario perdiera el acceso a su información cifrada

Soporte de "no repudio". El repudio ocurre cuando un usuario niega la realización de una transacción. El no repudio significa que un usuario debe hacerse responsable de la transacción realizada. El requisito básico para el no repudio es que la clave utilizada para crear firmas digitales sea generada y almacenada de forma segura, bajo el control exclusivo del usuario en todo momento. Además, hay que tener la completa certeza de que las claves privadas de firma no abandonarán nunca el sistema ni se realizarán copias de seguridad de las mismas.

Renovación automática y gestión histórica de las claves. Los pares de claves (pública y privada) deben ser actualizados cada cierto tiempo y, durante el proceso, los usuarios no tienen que experimentar una negación de servicio porque sus claves no sean válidas. Una vez actualizadas las claves, la historia de las anteriores debe ser mantenida para que los datos antiguos cifrados puedan ser descifrados.

Repositorio de certificados escalable. Las empresas tienen que distribuir los certificados para que sean utilizados por las aplicaciones. Los repositorios almacenan los certificados con el objetivo de que las aplicaciones los recuperen a petición del usuario y para minimizar el costo de la distribución de los certificados. Todas las aplicaciones integradas con la *PKI* deben usar un mismo repositorio de certificados escalable.

Revocación de certificados. La aplicación debe estar segura de que el certificado es válido en el momento de usarlo, ya que los que no son fiables son revocados por la *Autoridad de Certificación.*

Soporte de certificación cruzada. Una certificación cruzada, permite determinar el grado de confianza de cualquier certificado emitido por una *Autoridad de Certificación* externa.

- *Presupuesto*

La Cámara de Representantes del Congreso de Estados Unidos ha aprobado por unanimidad una medida que triplicará el gasto federal en un programa destinado al aumento de la investigación en e-seguridad.

El proyecto de ley otorgará 903 millones de dólares (la misma cantidad en euros) durante cinco años en donaciones, becas y otros incentivos para aumentar la investigación académica en ciberseguridad.

La iniciativa fue aprobada por el Senado en octubre de 2002. Ahora se espera que el presidente, George W. Bush, la firme para convertirla en ley. El espectacular aumento de los fondos en ciberseguridad refleja el enorme interés que ha tomado Washington en el asunto, después de que varios ataques desestabilizadores estremecieran Internet el año pasado.

➢ *Encriptación*

El gobierno de los Estados Unidos decidió actualizar el estándar de seguridad en el intercambio de información y en las transacciones electrónicas.

La adopción del nuevo Advanced Encryption Standard (AES) por parte de entidades públicas y privadas fortalecería la seguridad en una gran variedad de transacciones electrónicas, desde la extracción de dinero de los cajeros automáticos hasta el comercio electrónico o el envío de e-mails.

Antes de acordar el estándar, los científicos del Instituto Nacional de Estándares y Tecnología (NIST) probaron fórmulas matemáticas durante cuatro años. La fórmula definitiva, llamada Rijndael desordena la información contenida en las comunicaciones generando números aleatorios de 128, 192 o 256 dígitos.

Una clave de 128 bits puede crear un número de combinaciones complicado de escribir (340 seguido de 36 ceros), mientras que la de 256 bits eleva las posibilidades a 11x1076. Estas combinaciones dejan al Data Encryption Standard (DES) en pañales, ya que usaba claves de 56 dígitos, con lo que las combinaciones posibles se reducían a 72 x 1015.

Además, este incremento en la protección de información sensible llevará al gobierno estadounidense a permitir al software dotado con AES salir de sus fronteras, después de limitar durante años la exportación de programas encriptados.

➢ *Dos cabezas para un disco*

La compañía Scarabs, de origen japonés, ha desarrollado un sistema que asegura puede convertirse en la protección definitiva de un servidor de Internet contra ataques de intrusos.

El sistema (no es una idea nueva, aunque hasta ahora nadie la había desarrollado como protección anti- hacker), consiste en un disco duro con dos cabezas independientes una de otra (nos referimos a dos cabezas por comodidad, ya que en realidad un disco duro posee de hecho varios cabezales, pero todos controlados simultáneamente).

Esto permite que mientras un cabezal sigue las órdenes de quienes navegan el sitio o de cualquiera que intentara acceder a él por medios ilícitos a los efectos de modificar o borrar una página, no tuviera oportunidad de grabar los cambios, ya que el cabezal del disco que estaría usando no se lo permitiría, estando sólo preparado para leer los datos del disco, no para grabarlos o modificarlos. Esto también podría impedir la ejecución de un virus.

El disco cuenta con un segundo cabezal (o juego de cabezas), independientes de las anteriores, y que si permitirían la lectura y la grabación de datos, pero a estas cabezas sólo podrían acceder las personas autorizadas para actualizar o mantener el sitio.

De esta forma, los visitantes tendrían acceso únicamente a la lectura de archivos en el servidor, siendo imposible modificarlos. El inventor del sistema, Naoto Takano, actual CEO de Scarabs, había experimentado con esta idea en 1985, cuando aún era un simple investigador, pero el desarrollo se complicó por el hecho de que todos los datos necesariamente debían ser grabados por uno de los cabezales antes de que pudieran ser leídos de nuevo. De todos modos, en esa época, Takano no había imaginado su uso para proteger un servidor de Internet.

La empresa presentó un prototipo de su disco, con un tamaño de solo 1,6 GB, corriendo sobre Windows NT 4.0 y que gestionaba Active Server Pages e IIS, el servidor de Microsoft. Sin embargo, no habría problemas para adaptarlo a otros sistemas operativos. El costo de este prototipo es de unos **863 dólares.**

b) Lo que se sigue desarrollando

En este punto se mencionan aquellos proyectos que se encuentran en constante desarrollo.

- *Redes virtuales*

El espectacular avance de Internet y de la tecnología *IP*, también está provocando en la actualidad la proliferación de las *Redes Privadas Virtuales* (*VPN, Virtual Private Networks*), una solución que permite conectar la Extranet de una organización con los usuarios y las aplicaciones remotas, haciendo uso de Internet como la red principal.

- *Firewall*

Los sistemas firewall han extendido su capacidad para poder realizar comunicaciones cifradas tras organizaciones o bien contra usuarios individuales los que han hecho extender las posibilidades de la interconexión segura de este tipo de comunicaciones. Cada uno de estos aspectos configura los entornos de Redes Privadas Virtuales o VPNs donde el Firewall, a parte de un punto de control y filtrado, se convierte en la pieza clave para el cifrado/descifrado de la información.

- *Internet móvil*

Internet móvil es una tecnología que puede posibilitar nuevos servicios y aplicaciones. Pero también puede amenazar los valores tradicionales de privacidad, seguridad y cortesía.

Para el Internet móvil, la seguridad también es una cuestión esencial, tanto en términos de vulnerabilidad de la red como de la privacidad de los datos. A medida que se facilita la interconexión entre redes inalámbricas y alámbricas, la información que hasta ahora podía controlarse y rastrearse está más expuesta a una utilización maliciosa. Es más, los instrumentos de comercialización, tales como el "spamming" ("inundación") pueden traspasar los límites de lo aceptable y convertirse en una molestia para los usuarios.

c) La seguridad informática hoy

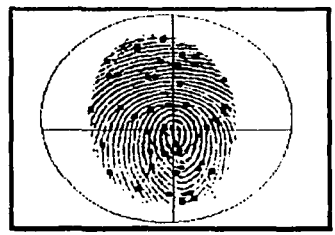
El mercado aparentemente no reacciona a los problemas de seguridad informática, vulnerabilidades básicas siguen apareciendo en los programas, los administradores todavía no realizan actualizaciones y no aplican parches a los sistemas y los usuarios siguen haciendo click sobre los archivos adjuntos enviados por correo electrónico.
Las empresas no pueden solucionar todos los problemas de seguridad porque si lo hacen las aplicaciones críticas que están en producción entran en crisis y los proveedores siguen tratando de explicar que tener permisos habilitados para todo el mundo, utilizar usuarios genéricos y guardar passwords en plano no es tan inseguro.

d) El futuro de la seguridad informática

Parece que la seguridad de datos y las nuevas tecnologías siempre irán unidos, ya que la pérdida de información o el hecho de que ésta caiga en manos ajenas puede suponer un verdadero desastre tanto para los particulares como para las empresas.

- ***Seguridad Biométrica.***

En este campo se ha ido avanzando, casi siempre por el ritmo marcado por los propios ataques, hasta llegar a la incipiente biometría. Esta especialización está centrada en el desarrollo de sistemas de seguridad que, mediante el análisis de un rasgo físico personal del usuario, identifican al usuario. Hay una amplia oferta de métodos biométricos, como los de *scaneado* de huellas digitales, *scaneado* del iris, *scaneado* de retina, análisis de escritura manual, reconocimiento de caracteres impresos manualmente y reconocimiento de la voz. Todo parece apuntar a que, en los próximos años, asistiremos a un incremento del uso de técnicas biométricas como sistema de seguridad.



Aunque en principio nos podría parecer pura ciencia ficción, a finales del año pasado Acer lanzó su computadora portátil TravelMate 740 que integraba el sistema de seguridad de reconocimiento por la huella dactilar para restringir el acceso a la información confidencial. Este modelo en concreto tiene un sensor dentro del propio portátil que puede ser configurado para limitar la entrada a la información que especifique el usuario.

El último fabricante en unirse a este tipo de tecnología es Oki, que acaba de anunciar el desarrollo de una unidad individual de verificación del iris, el IrisPass(R)-h. Esta es una solución compacta que se conecta a cualquier computadora a través de un puerto USB. Dicha unidad permite construir diferentes sistemas de gestión de la seguridad, desde mecanismos independientes de verificación para prevenir accesos no autorizados al PC, hasta sistemas log-on corporativos para acceso, identificando a grandes redes.

En resumen:

- La utilización de los dispositivos biométricos no está tan difundida debido a problemas de interconexión entre los sistemas.
- La tecnología está madura, pero la implementación de la misma resulta compleja.
- La utilización básica se orienta a la autentificación del usuario a nivel sistema operativo.

➢ *Técnicas Criptográficas.*

Las técnicas criptográficas están actualmente consideradas como la herramienta esencial para garantizar tanto seguridad como confianza. Las dos primitivas criptográficas más importantes son la firma digital y el cifrado. El cifrado es la herramienta que ayuda a mantener los datos y la comunicación confidenciales mientras que la firma digital es la herramienta que proporciona tanto la validación como la autentificación de documentos.

➢ *Mejoras para un enfoque de seguridad más completo y en niveles.*

Las empresas resolverán riesgos de seguridad por medio de un enfoque más holístico, incluyendo tanto tecnologías como prácticas. Cada año trae consigo mayor conciencia en cuanto a seguridad y obliga a las empresas a reevaluar sus riesgos, lo cual traerá consigo un mayor enfoque en soluciones que mitiguen la amplia gama de riesgos existentes. Entre los temas principales para muchas organizaciones estará la creciente necesidad de educar a los compradores de Tecnología Informática sobre temas de seguridad, así como la falta de conocimientos internos sobre el tema de seguridad informática. Las organizaciones dependerán cada vez más de terceros (incluyendo fabricantes, revendedores de valor agregado y consultores) para desarrollar políticas completas de seguridad.

Asimismo, las empresas buscarán la forma de combinar tecnologías en implementaciones de múltiples niveles, en vez de depender de una variedad fragmentada de productos en ciertos puntos para proteger la empresa. Mejor descrita como "seguridad en niveles", las empresas buscarán cada vez más la forma de proveer una protección máxima de seguridad en múltiples niveles y puntos de acceso a la red, utilizando tecnologías tales como el estándar 802.1x, firewalls y firewalls perimetrales integrados. "La mayoría de las empresas consideran la seguridad como un abismo negro en el que tienen que arrojar dinero sin conocer los resultados. Pero, a medida que racionalizan sus arquitecturas de seguridad y cuantifican sus riesgos y rendimientos, las empresas reconocerán los ahorros creados al subcontratar los servicios de seguridad a [terceros]", según indica el reporte de Forrester Research " La torpe adolescencia de la seguridad informática" (*IT Security's Awkward Adolescence*).

- ***El aumento en la adopción de tecnología inalámbrica como una necesidad en la empresa.***

  En el 2003, la necesidad de tener LANs inalámbricas (WLANs, por sus siglas en inglés) cambiará dramáticamente. Pasará de ser una moda a ser algo esencial. Este cambio se deberá a la necesidad de tener mayor acceso móvil a la información empresarial crítica y a costos más bajos de cableado o re-cableado de los edificios. La prueba de esta tendencia yace en el continuo crecimiento en compras de WLANs empresariales, a pesar de las problemáticas condiciones económicas que se han suscitado en todas partes. Las WLANs son una de las pocas áreas tecnológicas donde las empresas todavía están haciendo gastos considerables.

8.10 Código de ética de UNICA

INTRODUCCIÓN

La seguridad informática es una de las actividades que requiere de mayor atención, principalmente en aquellas instituciones educativas o empresas preocupadas por proteger la información que se les ha confiado.

Por ello la Unidad de Servicios de Cómputo Académico (UNICA) propone el siguiente código de ética con la finalidad de poder mantener la confianza de los usuarios que hacen uso los servicios que le ofrece la Unidad.

ALCANCE DEL CÓDIGO DE ÉTICA

1. Aplicación del código

El presente código de ética establece algunos puntos que regularán la conducta y el desempeño profesional de las personas encargadas de la seguridad informática de UNICA, a las cuales definiremos como *Administradores de la Seguridad del Sistema*, independientemente del sistema operativo que utilicen; incluyendo a las personas que laboran en UNICA, sin importar el puesto que ocupen.

2. Actitud profesional

La excelencia técnica y ética de los *Administradores de la Seguridad del Sistema* se vuelve indispensable para todos los profesionales de esta área, por lo que es necesario que ellos promuevan la difusión y práctica de los principios expresados en este código.

Los *Administradores de la Seguridad del Sistema* tienen la obligación de regir su conducta de acuerdo a las reglas contenidas en este código, las cuales deben considerarse mínimas pues se reconoce la existencia de otras normas de carácter legal y moral que amplían el de las presentes.

Este código rige la conducta de los *Administradores de la Seguridad del Sistema*, así como el de las personas que pertenecen a UNICA, en sus relaciones con el público en general, con quien presta sus servicios (usuarios) y con sus compañeros de trabajo.

Los *Administradores de la Seguridad del Sistema* y las personas que trabajan en UNICA, deben abstenerse de hacer comentarios sobre sus compañeros de trabajo o usuarios, que perjudiquen su reputación o el prestigio de su profesión, a menos que se soliciten por quién tenga un interés legítimo de ellos.

3. Actitud personal

Los *Administradores de la Seguridad del Sistema* y las personas que trabajan en UNICA deben respeto a toda persona y su comportamiento tanto en lo personal como en lo social, debe atender a la práctica de buenas costumbres y seguir un objetivo útil.

Los *Administradores de la Seguridad del Sistema* y las personas que trabajan en UNICA deben tener la costumbre de cumplir los compromisos adquiridos, no por el hecho de estar escritos, sino por convicción propia.

Los *Administradores de la Seguridad del Sistema* y las personas que trabajan en UNICA deben de respetar y hacer respetar su tiempo y el de los demás, predicar con el ejemplo, poseer espíritu de servicio y habilidad para comunicarse con los demás.

Los *Administradores de la Seguridad del Sistema* y las personas que trabajan en UNICA siempre actuarán cuidando el no afectar la integridad física, emocional ni económica de las personas.

4. Calidad profesional en el trabajo

Se espera de los *Administradores de la Seguridad del Sistema* y de las personas que trabajan en UNICA, un trabajo de calidad en cualquier servicio que ofrezcan a los usuarios.

5. Preparación y calidad profesional

Por ser la información un recurso difícil de manejar, se requiere de *Administradores de la Seguridad del Sistema* que definan estrategias para su generación, administración y difusión; por lo que ninguna persona que no esté relacionada con la informática, computación o sistemas computacionales, que no cuente con experiencia y con la capacidad necesaria para realizar éstas actividades de manera satisfactoria y profesional, por ningún motivo podrá llevar a cabo esta actividad.

Los *Administradores de la Seguridad del Sistema* y las personas que trabajan en UNICA, se preocuparán de que su propia actualización y capacitación profesional sea de crecimiento permanente.

6. Práctica de la profesión

Los *Administradores de la Seguridad del Sistema* y las personas que trabajan en UNICA, deben analizar cuidadosamente las verdaderas necesidades que puedan tenerse de sus servicios, para proponer aquellas que más convengan dependiendo de las circunstancias.

RESPONSABILIDADES HACIA EL USUARIO

1. Importancia del usuario

El principal objetivo de los *Administradores de la Seguridad del Sistema* y las personas que trabajan en UNICA es la atención adecuada al usuario, al cual se le debe brindar todo el respeto .

2. Proteger el interés del usuario

Los *Administradores de la Seguridad del Sistema* deben enseñar al usuario cómo utilizar el sistema operativo de los equipos de cómputo y programas, para obtener un mayor beneficio de este servicio.

Los *Administradores de la Seguridad del Sistema* y las personas que trabajan en UNICA, deben aprovechar las herramientas (software, equipo de cómputo) adquiridas por la Unidad para el beneficio no sólo de ella, sino también de los usuarios.

Los *Administradores de la Seguridad del Sistema* deben asegurarse del buen uso de los recursos informáticos, evitando el mal uso para el que no fueron planeados y autorizados.

3. Responsabilidad profesional

Los *Administradores de la Seguridad del Sistema* y las personas que trabajan en UNICA expresarán su opinión en los asuntos que se les hayan encomendado, teniendo en cuenta los principios expresados en éste código.

Deberán ser objetivos, imparciales en la emisión de sus opiniones o juicios, buscando siempre el beneficio de sus compañeros y usuarios.

4. Acceso a la información

Los *Administradores de la Seguridad del Sistema* podrán tener acceso a la información de carácter privado relativa a las personas, contenida en las bases de datos, con la previa autorización de la persona de que se trate, excepto cuando se requiera una investigación de seguridad o una investigación de carácter legal.

5.- Discreción profesional

Los *Administradores de la Seguridad del Sistema* tienen la obligación de guardar discreción en el manejo de la información que se les ha proporcionado para poder prestar sus servicios. Considerar como confidencial toda la información que le ha sido confiada.

Los *Administradores de la Seguridad del Sistema* no deben permitir el acceso a la información a personal no autorizado, ni utilizar para beneficio propio la información confidencial de los usuarios.

6.- Honestidad profesional

Los *Administradores de la Seguridad del Sistema* no deben cambiar, modificar o alterar la información que se les ha confiado, para beneficio propio o de terceros, ni con fines de encubrir anomalías que afecten directamente los intereses de la Unidad.

Los *Administradores de la Seguridad del Sistema* y las personas que trabajan en UNICA no deben participar en actos que se califiquen de deshonestos.

7. No usar equipo de cómputo ni programas de la Unidad para beneficio personal

Cuando los *Administradores de la Seguridad del Sistema* y las personas que trabajan en UNICA requieran utilizar los equipos de cómputo o programas, propiedad de la Unidad, para uso personal o de beneficio propio, deben consultar al Jefe de la Unidad o a su jefe más inmediato, para obtener su autorización para tal fin.

Los *Administradores de la Seguridad del Sistema* y las personas que trabajan en UNICA no deben usar el equipo de cómputo para fines de esparcimiento que afecten su desempeño profesional, aún cuando tenga la autorización para utilizar el equipo. Ni fomentar que personas ajenas a la Unidad ingresen a las instalaciones y utilicen el equipo y los programas del software.

8. Trato adecuado a los usuarios y compañeros de trabajo

Los *Administradores de la Seguridad del Sistema* y las personas que trabajan en UNICA deben tratar con respeto a todas las personas sin tener en cuenta raza, religión, sexo, orientación sexual, edad o nacionalidad.

9. Finalización del trabajo

Al finalizar un proyecto, independientemente del Departamento de la Unidad que lo solicite, debe cumplir con todos los requisitos de funcionalidad, calidad y documentación pactados inicialmente, a fin de que se pueda obtener el mayor beneficio en la utilización de los mismos.

Al dejar de trabajar en UNICA, los *Administradores de la Seguridad del Sistema* deben cuidar que el equipo de cómputo y los programas propiedad de la Unidad se conserven en buen estado para su uso y aprovechamiento.

Al concluir el trabajo para el cual fue contratado, los *Administradores de la Seguridad del Sistema* y las personas encargadas del desarrollo de sistemas en UNICA deben implementar los mecanismos necesarios, para que tenga la posibilidad de continuar haciendo uso de los programas de aplicación, así como de modificarlos, a pesar de su ausencia.

10. Desarrollo de sistemas

Los *Administradores de la Seguridad del Sistema* y las personas encargadas del desarrollo de sistemas en UNICA deben determinar perfectamente el alcance del sistema y los requerimientos necesarios para su desarrollo.

Los *Administradores de la Seguridad del Sistema* y las personas encargadas del desarrollo de sistemas en UNICA deben determinar de manera clara la entrega de las diferentes etapas de desarrollo y establecer las fechas y compromisos formales de entrega, de cada una de las personas que participen en el desarrollo del sistema.

Los *Administradores de la Seguridad del Sistema* y las personas encargadas del desarrollo de sistemas en UNICA deben llevar a cabo las evaluaciones en las fechas determinadas y entregar los resultados en un tiempo adecuado que permita tomar decisiones.

Los *Administradores de la Seguridad del Sistema* y las personas encargadas del desarrollo de sistemas en UNICA deben dejar siempre documentado el sistema desarrollado, con todos los detalles necesarios, de tal manera que con su consulta se conozca el funcionamiento del sistema.

Los *Administradores de la Seguridad del Sistema* y las personas encargadas del desarrollo de sistemas en UNICA deben tener la capacidad para reconocer sus fallas en las revisiones, hacer correcciones y aclarar las dudas de quien solicitó el sistema, así como proponer posibles alternativas de solución.

Los *Administradores de la Seguridad del Sistema* y las personas encargadas del desarrollo de sistemas en UNICA deben comunicar los problemas que se les vayan presentando.

En el caso del líder de proyecto debe comunicar a su jefe inmediato qué personas que intervienen en el proyecto no han cumplido con las actividades asignadas con la finalidad de evitar problemas a tiempo.

RESPONSABILIDAD HACIA LA PROFESIÓN

1. Respeto a sus compañeros de trabajo y a su profesión

Los *Administradores de la Seguridad del Sistema* y las personas que laboran en UNICA cuidarán las relaciones que sostienen con sus compañeros de trabajo y colegas, buscando mejorar el ambiente de trabajo y fomentar el trabajo en equipo.

Los *Administradores de la Seguridad del Sistema* y las personas que laboran en UNICA deberán basar su reputación en la honestidad, honradez, lealtad, respeto, laboriosidad y capacidad profesional, observando las reglas de ética más elevadas en sus actos y evitando toda publicidad con fines de lucro o auto elogio.

Buscarán la manera de hacer cumplir y respetar este código de ética; además de fomentar la adopción de un código de ética.

2. Difusión y enseñanza de conocimientos

Los *Administradores de la Seguridad del Sistema* y las personas que laboran en UNICA deben mantener altas normas profesionales y de conducta, especialmente al transmitir sus conocimientos, logrando contribuir al desarrollo y difusión de los conocimientos de su profesión.

3. Especialización profesional de los Administradores del Sistema

Los *Administradores de la Seguridad del Sistema* debe tener una orientación hacia cierta rama de la informática, computación o sistemas computacionales, debiéndose mantener a la vanguardia en el área de conocimiento de su interés.

4. Competencia profesional

Es obligatorio para los *Administradores de la Seguridad del Sistema* y las personas que laboran en UNICA mantener actualizados todos los conocimientos inherentes a las áreas de su profesión, así como participar en la difusión de éstos conocimientos a otros miembros de la profesión.

Los *Administradores de la Seguridad del Sistema* deben informarse permanentemente sobre los avances de la informática, la computación y los sistemas computacionales, además de invertir los recursos necesarios para su capacitación y formación profesional y personal.

5. Evaluación de capacidades

Los *Administradores de la Seguridad del Sistema* y las personas que laboran en UNICA deben autoevaluarse periódicamente con la finalidad de determinar si cuentan con los conocimientos suficientes para ofrecer un trabajo de calidad.

En caso de que los *Administradores de la Seguridad del Sistema* y las personas que laboran en UNICA tengan personas a su cargo deberán asegurarse de que sean evaluados sus conocimientos periódicamente.

6. Personal a su servicio

Los *Administradores de la Seguridad del Sistema* y las personas encargadas del desarrollo de sistemas en UNICA deben realizar una supervisión del desempeño de las personas que colabore con ellos en el desarrollo de sistemas.

Los *Administradores de la Seguridad del Sistema* y las personas encargadas del desarrollo de sistemas en UNICA deben hacerse totalmente responsables del personal que colabore con ellos en el desarrollo del sistema.

DE LOS ADMINISTRADORES DE LA SEGURIDAD INFORMÁTICA ASÍ COMO DE LAS PERSONAS QUE PERTECEN A UNICA COMO INSTRUCTORES O PROFESORES

1. Práctica docente

Los *Administradores de la Seguridad del Sistema* y las personas que pertenecen a UNICA que den clases en la Facultad de Ingeniería o que den cursos propuestos por la Unidad, deben considerar al alumno como su principal objetivo para orientarlo a que actúe con apego a las normas de ética profesional.

Es obligación de los *Administradores de la Seguridad del Sistema* y las personas que pertenecen a UNICA que den clases en la Facultad de Ingeniería o que den cursos propuestos por la Unidad, mantenerse actualizados en las áreas de su ejercicio, a fin de transmitir al alumno los conocimientos de la materia o curso en particular.

Los *Administradores de la Seguridad del Sistema* y las personas que pertenecen a UNICA que den clases en la Facultad de Ingeniería o que den cursos propuestos por la Unidad deben fomentar el estudio y la investigación, así como la integración del alumno en equipos de trabajo que le permitan el crecimiento y desarrollo personal, social y profesional.

Los *Administradores de la Seguridad del Sistema* y las personas que pertenecen a UNICA que den clases en la Facultad de Ingeniería o que den cursos propuestos por la Unidad deben dar a conocer el temario que se va a desarrollar durante el tiempo que dure la enseñanza, así como los procedimientos de evaluación.

2. Relación con los alumnos

Los *Administradores de la Seguridad del Sistema* y las personas que pertenecen a UNICA que den clases en la Facultad de Ingeniería o que den cursos propuestos por la Unidad deben dar a sus alumnos un trato digno y respetuoso, instándolos permanentemente a su constante superación personal y profesional.

Los *Administradores de la Seguridad del Sistema* y las personas que pertenecen a UNICA que den clases en la Facultad de Ingeniería o que den cursos propuestos por la Unidad deben abstenerse de hacer comentarios que perjudiquen la reputación o prestigio de alumnos, catedráticos u otros profesionales en general.

Los *Administradores de la Seguridad del Sistema* y las personas que pertenecen a UNICA que den clases en la Facultad de Ingeniería o que den cursos propuestos por la Unidad deben evitar hacer comentarios alabadores a los alumnos sobresalientes con el objetivo agredir o hacer sentir mal al resto de los alumnos.

Es necesario que los *Administradores de la Seguridad del Sistema* y las personas que pertenecen a UNICA que den clases en la Facultad de Ingeniería o que den cursos propuestos por la Unidad manejen una conducta de respeto hacia el alumno y de esta manera puedan exigir respeto también de éste.

Los *Administradores de la Seguridad del Sistema* y las personas que pertenecen a UNICA que den clases en la Facultad de Ingeniería o que den cursos propuestos por la Unidad deben evitar hacer comentarios que deterioren la autoestima del alumno con problemas de aprendizaje. Deben de evitar la intimidación del alumno.

Los *Administradores de la Seguridad del Sistema* y las personas que pertenecen a UNICA que den clases en la Facultad de Ingeniería o que den cursos propuestos por la Unidad deben buscar procedimientos para comunicarse con los alumnos cuando no puedan asistir a clases.

3. Discreción como instructor o profesor

Los *Administradores de la Seguridad del Sistema* y las personas que pertenecen a UNICA que den clases en la Facultad de Ingeniería o que den cursos propuestos por la Unidad, podrán referirse en sus clases a casos reales para ilustrar los conocimientos que impartan, pero se abstendrán de proporcionar información que identifique a personas, empresas o instituciones relacionadas con dichos casos, salvo que los mismos sean del dominio público.

4.-Cumplimiento de obligaciones

Los *Administradores de la Seguridad del Sistema* y las personas que pertenecen a UNICA que den clases en la Facultad de Ingeniería o que den cursos propuestos por la Unidad deben cumplir con su responsabilidad en asistencia y puntualidad en el salón de clases.

Los *Administradores de la Seguridad del Sistema* y las personas que pertenecen a UNICA que den clases en la Facultad de Ingeniería o que den cursos propuestos por la Unidad deben contar, si es permitido por la Facultad de Ingeniería o UNICA, con una persona que tenga la capacidad de sustituirlo cuando sea inevitable la inasistencia.

5. Evaluaciones a los alumnos

Los *Administradores de la Seguridad del Sistema* y las personas que pertenecen a UNICA que den clases en la Facultad de Ingeniería o que den cursos propuestos por la Unidad deben comunicar los procedimientos de evaluación durante el tiempo que dure la enseñanza.

Los *Administradores de la Seguridad del Sistema* y las personas que pertenecen a UNICA que den clases en la Facultad de Ingeniería o que den cursos propuestos por la Unidad deben llevar a cabo las evaluaciones en las fechas determinadas y entregar los resultados en un tiempo adecuado, así como también hacer una revisión total del examen y aclarar todas las dudas que resulten derivadas de su aplicación.

Los *Administradores de la Seguridad del Sistema* y las personas que pertenecen a UNICA que den clases en la Facultad de Ingeniería o que den cursos propuestos por la Unidad deben tener la capacidad suficiente para reconocer sus fallas en las revisiones, hacer correcciones y aclarar las dudas del alumno.

Los *Administradores de la Seguridad del Sistema* y las personas que pertenecen a UNICA que den clases en la Facultad de Ingeniería o que den cursos propuestos por la Unidad deben llevar una

supervisión del desempeño del alumno en forma personal preocupándose por establecer si los bajos resultados son resultado del desempeño del alumno o del profesor o instructor.

USO DE INTERNET

1. Normas generales para su uso

Es obligación de los *Administradores de la Seguridad del Sistema* y las personas que pertenecen a UNICA, y usuarios en general a navegar en Internet con responsabilidad.

Para el buen uso de Internet, los *Administradores de la Seguridad del Sistema* deben observar las reglas de este código de ética cuyas infracciones, se considerarán actos reprobatorios. Es obligación de los *Administradores de la Seguridad del Sistema* fomentar y hacer que los usuarios de la red cumplan estas normas, para evitar el mal uso del Internet.

2. Creación y uso de páginas en Internet

Ver *Normatividad del Web* (Apéndice VIII).

3. Correo electrónico

Ver *Políticas de la Unidad de Servicios de Cómputo Académico.*

8.10 Código de conducta

Es un conjunto de normas concretas de actuación y de convivencia de acuerdo a las situaciones y actividades que desarrolla una institución. Es un compromiso de cada miembro de la institución con los demás para convivir en armonía y mejorar el desempeño de esta. Es un pacto voluntario y su única sanción es la presión social.

Un código de conducta no es un código de ética, no es una ley, no es una reglamentación, no es una norma disciplinaria, no sustituye a ninguna de ellas. No las debe contradecir y las puede complementar.

Un código de conducta sirve para:

- Aclarar y definir las normas de convivencia laboral y social.
- Ayuda a mejorar las relaciones interpersonales y el desempeño laboral de la institución.
- Motiva actitudes y conductas de apego a la legalidad y de lealtad institucional.
- Funciona como guía para resolver conflictos de conducta.
- Contribuye a mejorar la eficacia y eficiencia de la institución.

A continuación se muestra el código de conducta para centros de tecnología de información, el cual es una aportación del Ingeniero Heriberto Olguín Romo, profesor de la Facultad de Ingeniería que imparte la asignatura de Organización y Administración de Centros de Cómputo.

CENTROS DE TECNOLOGÍA DE INFORMACIÓN
CÓDIGO DE CONDUCTA

NUESTRA MISIÓN

ESTABLECER RELACIONES DE LARGO PLAZO, DONDE NUESTRO COMPROMISO ES LA GENERACIÓN DE VALOR PARA NUESTRO CENTRO DE TECNOLOGÍA DE INFORMACIÓN (CTI) A TRAVÉS DE LA TECNOLOGÍA, INTEGRANDO INFORMACIÓN, PROCESOS Y GENTE, INDEPENDIENTEMENTE DE DONDE SE ENCUENTREN, CON EL FIN DE CONTRIBUIR A LA GRANDEZA DE LAS ORGANIZACIONES Y DE LAS PERSONAS.

NUESTROS VALORES

- **COMPROMISO:**
  IMPLICA CUMPLIR CONSISTENTEMENTE Y SIN DESVIACIONES, LAS PROMESAS QUE LIBREMENTE ADQUIRIMOS.

- **CONFIANZA:**
  CADA PERSONA REALIZA SU MEJOR ESFUERZO PARA CUMPLIR SUS COMPROMISOS BASÁNDOSE EN SUS HABILIDADES Y MODELOS MENTALES.

- **APRENDIZAJE:**
  ES LA ENERGÍA QUE SUSTENTA NUESTRA TRANSFORMACIÓN, LA CAPACIDAD DE NUESTROS COLABORADORES PARA INTEGRAR DE MANERA CONTINUA, NUEVOS CONOCIMIENTOS, IDEAS Y EXPERIENCIAS PARA LA MEJORA DE NUESTRO DESEMPEÑO.

- **LIDERAZGO:**
  TODA PERSONA EN NUESTRO CTI ES UN AGENTE DE CAMBIO, ALGUIEN QUE HA RENUNCIADO A LA MEDIOCRIDAD Y ESTÁ COMPROMETIDO CON LA GRANDEZA.

- **CALIDAD:**
  ES UNA FORMA DE VIDA, UN PROCESO METÓDICO Y PERMANENTE QUE NOS PERMITE CUMPLIR LAS EXPECTATIVAS DE NUESTROS USUARIOS, HACIÉNDOLO BIEN A LA PRIMERA.

- **GOZO:**
  EL TRABAJO ES UNA OPORTUNIDAD DE GOZO, POR LO QUE PROPICIAMOS LAS CONDICIONES PARA QUE LA GENTE LO DISFRUTE.

EL CENTRO DE TECNOLOGÍA DE INFORMACIÓN

- El CTI es la razón de ser de nuestro trabajo. El CTI se ve representado no sólo por quien nos contrata, sino por los usuarios o cualquier persona con quien tengamos trato. Debemos esmerarnos en todo momento en que la relación sea además de profesional, con un alto sentido de respeto y de atención a sus necesidades. Procurar la cordialidad y disposición.

- Nuestra lealtad es para con el CTI. Nosotros nos organizamos como equipos de trabajo, donde existen roles diferentes.

- Quien verdaderamente califica nuestro desempeño es el CTI.

ACTITUD DEL ASESOR

- Totalmente profesional, desde la presentación hasta la forma de comportarse. Cada actividad o producto debe reflejar esta actitud. Lo anterior sin caer en poses o acartonamiento, sino más bien con una actitud de sencillez, apertura, buenos modales e interés hacia el usuario y hacia el CTI.

- Respeto hacia el propio tiempo y hacia el de los demás, no malgastarlo innecesariamente en charlas intrascendentes o improductivas.

- Adoptar las prácticas y reglas de conducta de cada usuario, relativas a horarios, fumar, tomar café, quitarse el saco, lugares de plática, y demás. Ser muy sensible a la cultura del usuario, para no violentarla.

- Manejar la información del CTI con todo cuidado; de preferencia no sacarla de sus oficinas. Procurar mantener la información que nos sea proporcionada en lugares cerrados bajo nuestro control.

- No hacer ningún acuerdo o promesa que comprometa al Centro de Tecnología de Información más allá de lo establecido como alcance del proyecto, sin que haya una aceptación tácita por parte de nuestro Titular. Lo anterior sobre todo en el caso de que

IMPLIQUE MODIFICAR LOS PRESUPUESTOS CONTEMPLADOS PARA EL PROYECTO.

DISCRECIÓN

- EVITAR RISAS Y BROMAS RUIDOSAS.
- EVITAR EL USO DE MALAS PALABRAS, ESPECIALMENTE AL DIRIGIRSE AL PERSONAL EN GENERAL Y A LOS MISMOS COMPAÑEROS.
- MANTENER UNA ACTITUD MESURADA Y PRUDENTE.
- EN LAS OFICINAS DE USUARIO Y DE NOSOTROS, NO TRATAR ASUNTOS PERSONALES NI MUCHO MENOS RELACIONADOS CON LA COMPRA-VENTA DE PRODUCTOS O SERVICIOS DE NINGUNA ÍNDOLE.

ACERCA DE LOS COMPAÑEROS

- NO SE DEBE CRITICAR PÚBLICAMENTE A NINGÚN COMPAÑERO DE TRABAJO, ESPECIALMENTE EN LO REFERENTE A SU DESEMPEÑO PROFESIONAL. SI SE DESEA BRINDAR RETROALIMENTACIÓN, DEBERÁ BUSCARSE QUE SEA EN PRIVADO Y FUERA DE LAS OFICINAS DEL USUARIO.
- SI EXISTE DESAVENENCIA O DESACUERDO RESPECTO A ALGÚN TEMA, NO LLEVAR LAS DISCUSIONES AL TERRENO PERSONAL Y NUNCA DESCALIFICAR LA OTRA OPINIÓN. NO CONTRADECIR ABIERTAMENTE, SINO MATIZAR.

ACERCA DEL PERSONAL DEL CENTRO DE TECNOLOGÍA DE INFORMACIÓN

- DURANTE EL DESARROLLO DEL PROYECTO, PROCURAR NO LLEVAR LAS RELACIONES HASTA EL PUNTO DONDE HAYA INVOLUCRAMIENTO PERSONAL. TRATAR DE MANTENERLAS CORDIALES Y SATISFACTORIAS, PERO NO OLVIDAR QUE LA IMAGEN DEBE SER LA DE UNA PERSONA SERIA Y PROFESIONAL. DE PREFERENCIA EVITAR CITAS PERSONALES.
- EVITAR LA CONFIANZA EXCESIVA.
- NUNCA CRITICAR O HACER MOFA DE LA PERSONA DE NINGÚN USUARIO, MUCHO MENOS EN LAS OFICINAS DEL MISMO.
- NO INVOLUCRARSE EN LAS CUESTIONES POLÍTICAS DEL USUARIO, NI TOMAR ABIERTAMENTE PARTIDO POR ALGÚN GRUPO, YA QUE ESTO RESTA OBJETIVIDAD, FACTOR CLAVE DE CUALQUIER INTEGRANTE DEL CTI.

ACERCA DEL CENTRO DE TECNOLOGÍA DE INFORMACIÓN

- Nunca tratar cuestiones internas enfrente del usuario, especialmente en lo tocante a relaciones laborales, percepciones, políticas internas y demás.
- No revelar ninguna cuestión confidencial acera del CTI ni de otros usuarios o proyectos del mismo.
- En general, ser sumamente prudente y hermético en cuanto a la información que se divulgue de nuestro CTI. Si el usuario desea información del mismo referirlo a la fuente oficial correspondiente.

ACERCA DEL TRABAJO REALIZADO

- Nunca manifestar enfrente del usuario, opiniones negativas acerca de proyectos o productos anteriores efectuados por el CTI o sus integrantes. En caso de pretender brindar retroalimentación, escoger un momento y lugar adecuado y hacerlo en privado.

ACERCA DE OTROS USUARIOS

- No revelar información confidencial de ningún usuario o proyecto. En general ser extremadamente prudente en cuanto a los comentarios acerca de otros usuarios, ya que el actual pensará que lo mismo se dirá de él en el futuro.
- Si se desea ejemplificar, de preferencia no revelar el nombre del usuario del cual se está hablando. Tratar de nunca mencionar en particular a otras personas excepto cuando haya algo bueno que decir de ellas.

ACERCA DEL LUGAR DE TRABAJO

- Procurar dejarlo siempre lo más limpio y ordenado posible.
- No comer en las áreas de trabajo. De preferencia no ingerir frituras ni refrescos directamente de la lata.
- Hacer uso racional de las facilidades proporcionadas por el CTI.

SALIDAS O AUSENCIAS

- Siempre hay que tener la atención de avisar cuando no se pueda asistir o haya que salir por alguna necesidad. De preferencia de manera interna, para que siempre haya forma de dar una respuesta oficial y única a la no asistencia.

SALIDAS O AUSENCIAS (CONTINUACIÓN)

- Nunca dar la razón de que se va a ver otro usuario u otro proyecto, ya que puede mandar señales de falta de prioridad al usuario o proyecto en que se participa.
- En el caso de ausencias, siempre avisar a la brevedad posible. Comunicar aquello que pueda causar algún problema o retraso, para que pueda ser atendido por otro integrante.

ASISTENCIA A REUNIONES Y COMIDAS

- Procurar ser selectivo en cuanto a la asistencia a reuniones extra laborales con personal del usuario. No asistir a demasiadas ni a aquellas donde el ambiente tiende a relajarse mucho.
- En caso de tomar bebidas alcohólicas procurar no excederse. Cuidar mucho el tipo de comentarios que se hacen, procurando no caer en las alusiones personales.

PUNTUALIDAD Y USO DEL TIEMPO

- Indispensable ser puntual y cumplir indefectiblemente los compromisos con los usuarios. En caso de que por alguna razón válida no se puedan cumplir compromisos, notificarlo al usuario con anticipación.
- La puntualidad debe cuidarse en extremo, ya que habla por sí sola de la disciplina y formalidad de los integrantes y su incumplimiento es una falta de respeto y cortesía hacia el usuario.
- Procurar ser muy eficiente dentro de los horarios de trabajo establecidos, de manera que excepcionalmente haya necesidad de trabajar fuera de los mismos. En el CTI queremos gente completa, que tenga oportunidad de disfrutar de otras

PUNTUALIDAD Y USO DEL TIEMPO (CONTINUACIÓN)

ACTIVIDADES Y DE CONVIVIR CON SU FAMILIA.

- EN CASO DE NO TENER UNA ASIGNACIÓN O ACTIVIDADES DEFINIDAS, RECURRIR AL COORDINADOR CORRESPONDIENTE DE MANERA QUE SE PUEDAN ASIGNAR LAS REQUERIDAS, O EN SU CASO APROVECHAR PARA ESTUDIAR O PROFUNDIZAR SOBRE ALGÚN TEMA. ANTE EL USUARIO NUNCA MOSTRAR FALTA DE ACTIVIDADES U OCIO.

LLAMADAS TELEFÓNICAS

- TRATAR DE MINIMIZAR LAS PERSONALES. SER SUMAMENTE DISCRETO CUANDO SE HAGAN ÉSTAS.
- MINIMIZAR EL TIEMPO DE CONVERSACIÓN.
- NO TRATAR POR TELÉFONO ASUNTOS DELICADOS DEL CTI O DEL USUARIO.

PRESENTACIÓN PERSONAL

- PERSONAL MASCULINO: USAR TRAJE, DE PREFERENCIA DE UNA PIEZA CON COLORES SERIOS. PROCURAR QUE LA PRESENTACIÓN SEA IMPECABLE, CUIDANDO INCLUSIVE EL LUSTRADO DE LOS ZAPATOS. TRATAR DE NO USAR ROPA QUE SALGA DE UNA PRESENTACIÓN FORMAL (BOTAS, ROPA DE PIEL, MEZCLILLA O PANA).
- PERSONAL MASCULINO: CORTE DE PELO CONSERVADOR, AFEITADA DIARIA INDISPENSABLE. SI ACOSTUMBRA USAR BARBA O BIGOTE DEBE DE ESTAR ARREGLADO.
- PERSONAL FEMENINO: ROPA FORMAL, DE PREFERENCIA VESTIDOS, FALDAS Y EN CASO DE LOS PANTALONES QUE NO SEAN DE CORTE CASUAL. ES PRUDENTE EVITAR LAS MINIFALDAS Y PANTALONES AJUSTADOS.
- PERSONAL FEMENINO: SI SE ACOSTUMBRA MAQUILLAJE, QUE SEA ADECUADO PARA UNA OFICINA. INDISPENSABLE MEDIAS Y ZAPATOS FORMALES.

8.11 Resumen de las propuestas y medidas de seguridad implantadas en UNICA

CON RESPECTO A	PROPUESTAS Y MEDIDAS DE SEGURIDAD
Seguridad Física	✓ Propuesta para una buena administración del equipo. ✓ Propuesta contra incendio.
Seguridad Lógica	✓ Propuesta de Procedimientos Preventivos y Correctivos ✓ Herramientas de seguridad • Anti-espionaje: snort, portsentry y scanlogd. • Contraseñas: John the Ripper v 1.6 • Anti-spam: Antivirus MailScanner con F-prot • Auditoría: Tripwire, Nessus. • Autentificación: ssh. • Firewall interno en el servidor cancun con iptables.
Organización	✓ Propuesta de Políticas de Cómputo de UNICA ✓ Propuesta del Organigrama para el Departamento de Redes y Operación de Servidores. ✓ Creación del Área de Seguridad. ✓ Propuesta de Código de Ética de UNICA. ✓ Aportación del Código de Conducta por parte del Ing. Heriberto Olguín Romo. ✓ Capacitación y actualización. ✓ Manual de Usuario. ✓ Formato de Control de Incidentes de Seguridad.
Plan de Contingencia	✓ Análisis de riesgos. ✓ Protecciones actuales. ✓ Listas de notificación. ✓ Requerimientos de recursos. ✓ Plan de recuperación de desastres. ✓ Restaurar archivos. ✓ Restaurar sistema de archivos.

Tabla 8.2. Resumen de las propuestas y medidas de seguridad implantadas en UNICA.

Conclusiones

CONCLUSIONES

La Unidad de Servicios de Cómputo Académico emplea el sistema operativo Linux Red Hat porque le ha permitido administrar y proporcionar los servicios que requieren los usuarios de la Facultad de Ingeniería.

Se tomaron medidas de seguridad enfocadas a resolver los problemas de seguridad de UNICA, ya que si se implantan medidas innecesarias podrían entorpecer el servicio. Por eso se realizó un análisis de riesgos (punto 8.2 del capítulo 8) que nos permitió detectar los problemas que actualmente enfrenta UNICA como son: el robo de equipo, la falta de políticas para sancionar a aquellos usuarios internos o externos que pongan en riesgo la seguridad del sistema, la ética dentro de cualquier campo laboral es importante y no se cuenta con un código de ética, no existen pasos a seguir ante un incidente de seguridad, no hay una clara diferencia entre las actividades de administración y seguridad, no se cuentan con las herramientas suficientes de seguridad para prevenir vulnerabilidades en el sistema, no se restringe el acceso sólo a los servicios prestados.

Es importante que en cualquier organización, sin importar su tamaño, existan políticas que establezcan claramente lo que se puede y no se debe realizar con los recursos de la misma, dejándolo por escrito. Consideramos que las políticas de seguridad siempre son necesarias, ya que ayudas a poner orden en el caos.

Con la propuesta de políticas de seguridad para UNICA pretendemos que permitan a los responsables de mantener la seguridad respaldarse ante eventualidades que pongan en riesgo la integridad del sistema. Teniendo presente que para la implementación exitosa de las mismas: se deben publicar y divulgar de manera adecuada, es decir, asegurarnos de que todos los usuarios las entiendan; y que las políticas reciban el apoyo de los directivos de la Unidad.

Se recomienda hacer un revisión periódica de las mismas para que estas sean capaces de seguir cubriendo las necesidades de UNICA.

Es necesario tener por escrito los pasos a seguir en caso de que se presente un incidente de seguridad, para que el servicio no se vea interrumpido por mucho tiempo, sin importar el cambio constante de personal. Por esta razón se crearon procedimientos preventivos y correctivos, así como un plan de contingencia, el cual permitirá restablecer el funcionamiento del servidor en el menor tiempo posible, aumentando la confiabilidad del mismo.

Se buscaron herramientas de seguridad para el sistema operativo Linux Red Hat como: tripwire, nessus, snort, John the Ripper, portsentry, scanlogd, antivirus MailScanner con f-prot e iptables, que permitirán disminuir los riesgos a que está expuesto.

Se propone un código de ética con el objetivo de uniformar el comportamiento de las personas que laboran en UNICA, el cual les ayudará a actuar con más libertad al conocer claramente cual es el comportamiento que deben tener, permitiendo llevar a cabo la misión de la Unidad. Debido a que los problemas de seguridad que se presentan en los sistemas de cómputo son más constantes, nos parece adecuado aplicar la ética a la Informática y dotar a esta nueva disciplina de un conjunto de normas claras de comportamiento, con el propósito de contar con

contenidos éticos y de conducta profesional en la enseñanza de la Seguridad Informática, que ayudarán a abordar y resolver cualquier problema que se presente en el ejercicio profesional de esta área.

Debido a la gran cantidad de información que se maneja proponemos la creación de un área de seguridad, para prevenir o solucionar los incidentes de seguridad que se presentan cuando los usuarios, tanto internos como externos, tienen acceso a la red de la Facultad de Ingeniería. Por eso consideramos necesario reestructurar la organización del Departamento de Redes y Operación de Servidores para distribuir el trabajo y responsabilidades, donde el área de seguridad se coordinará con el área de administración para proporcionar un mejor servicio.

Generalmente, se le da demasiada importancia a la seguridad lógica y como pudimos ver también se le debe dar a la seguridad física, ya que no en todos los casos la pérdida de información es a través de una intrusión al sistema. Con las medidas de seguridad física propuestas consideramos que ayudarán a mejorar no sólo la infraestructura de UNICA, sino también situaciones como el robo de equipo.

Para lograr lo anterior se requiere: Primero, hacerles ver tanto a las personas que laboran en UNICA como a los usuarios, la importancia de tomar medidas de seguridad para brindar un mejor servicio. Segundo, destacar que su participación es indispensable, debido a que ellos son uno de los principales factores que afectan a la seguridad del sistema, porque hacen uso de los recursos que les ofrece la Unidad, es decir, existe la posibilidad de que se altere la información por la mala intención o el mal uso de ella. Y que sin su apoyo no podrán llevarse a cabo estas medidas dentro de la Unidad.

Estamos conscientes de que nada ni nadie asegura que un sistema sea seguro al 100%, pero con las medidas de seguridad mencionadas anteriormente, se puede proteger la integridad de la información, así como los servicios y la operación de la Unidad, cumpliendo con el objetivo principal de esta tesis. Además, consideramos que la seguridad en un sistema de cómputo es la combinación del Administrador y del sistema operativo utilizado.

Nuestras perspectivas a futuro serían: convencer tanto al Jefe de UNICA como a los directivos de la Facultad de Ingeniería de lo importante que es su apoyo para el buen funcionamiento de las políticas de seguridad y de que es conveniente considerar una asignación presupuestal para la seguridad informática; educar a toda la comunidad de la Facultad de Ingeniería sobre la importancia de apegarse a las buenas prácticas de la seguridad informática y concienciar de que la seguridad es responsabilidad de todos.

La seguridad puede verse como un producto en constante cambio, que no se realiza una sola vez, sino que debe ser un proceso de supervisión, revisión, actualización y capacitación continuos. La mejor solución para evitar que ocurra un incidente de seguridad, es conocer el valor de nuestros recursos, así como los riesgos que enfrentan; buscando las medidas y acciones con que podemos protegerlos.

Apéndice I

Sistema de archivos ext3

SISTEMA DE ARCHIVOS EXT3

1. Principales características del sistema de archivos ext3.

El sistema de archivos ext3 es una extensión con journaling del sistema de archivos ext2. Con el journaling se obtiene una enorme reducción en el tiempo necesario para recuperar un sistema de archivos después de una caída, y es por tanto muy recomendable en entornos donde la alta disponibilidad es muy importante, no sólo para reducir el tiempo de recuperación de máquinas independientes sino también para permitir que un sistema de archivos de una máquina caída sea recuperado en otra máquina cuando se tiene un cluster con algún disco compartido. Además, se posibilita que el sistema de archivos caído de una máquina (por ejemplo, un servidor) esté disponible cuanto antes para el resto de máquinas a través de la red (nfs, samba, ftp, http, etc.).

El principal objetivo del ext3 es la disponibilidad del sistema cuando se apague incorrectamente la máquina, es decir, tenerlo totalmente disponible al momento, después de volver a arrancar sin necesidad de que se tenga que esperar a pasar un "fsck", el cual tarda mucho tiempo.

Ext3 en realidad es ext2 con un archivo adicional de registro, es decir, es una capa adicional sobre ext2 que mantiene un archivo de registro *log* de transacciones. Debido a que está integrado en el ext2 puede que no explote todas las posibilidades de los sistemas de journaling puros, pero se está trabajando en esta área para mejorarlo.

2. Ventajas de utilizar ext3.

Existen cuatro razones principales para migrar de un sistema de archivos ext2 a ext3: disponibilidad, integridad de los datos, velocidad y fácil migración.

- **Disponibilidad.**

  Después de un apagado incorrecto de la máquina los sistemas de archivos ext2 no pueden ser montados de nuevo hasta que su consistencia haya sido verificada por el programa "fsck". El tiempo que tarda el programa "fsck" está determinado por el tamaño del sistema de archivos, por lo que se tarda mucho tiempo en recuperar el sistema de archivos si son demasiados. Esto limita seriamente la disponibilidad.

  En contraste, el ext3 no requiere un chequeo del disco, incluso después de un apagado incorrecto del sistema. Esto es debido a que los datos son escritos al disco de tal manera que el sistema de archivos siempre está consistente. Sólo se realizará un "fsck" en el caso de fallos de hardware (por ejemplo, fallos físicos del disco duro) y en el caso de que el sistema de archivos esté configurado para que se verifique completamente de forma automática cada cierto periodo de tiempo o cada cierto número de montajes para prevenir posibles fallos. Además, con ext3 se utiliza (si fuese necesario) exactamente el mismo "fsck" que se utiliza con ext2.

El tiempo necesario para recuperar un sistema de archivos ext3 después de un apagado incorrecto no depende del tamaño del sistema de archivos ni del número de archivos que tenga, sólo depende del tamaño del "journal" (espacio usado para almacenar la información transaccional) utilizado para mantener la consistencia. Con el tamaño que se utiliza por defecto para el "journal" (tamaño fijado automáticamente por la utilidad de creación del sistema de archivos "mkfs") se tarda alrededor de un segundo en restaurar un sistema de archivos inconsistente (dependiendo de la velocidad del hardware).

- **Integridad de los datos.**

  Usando ext3 se puede proporcionar integridad a los datos del sistema de archivos en el caso de un apagado incorrecto del sistema, escogiendo el tipo y nivel de protección. Se puede escoger que los datos sean consistentes con el estado del sistema de archivos, esto significa que nunca habrá "datos basura" de un archivo recientemente escrito después de una caída del sistema. Esta ultima opción es la utilizada por defecto.

- **Velocidad.**

  Ext3 es en algunos casos incluso más rápido que el ext2 por que el journaling del ext3 optimiza el movimiento de cabeza del disco duro. Con ext3 se puede escoger entre tres modos de journaling diferentes para optimizar la velocidad, equilibrando esta con una mayor o menor integridad de los datos dependiendo de las necesidades.

  Los diferentes modos son:

  - *data=writeback*: Este es el modo jouraling por defecto en muchos otros sistemas de archivos journaling, esencialmente proporciona las garantías más limitadas de integridad en los datos y simplemente evita el chequeo en el reinicio del sistema.
  - *data=ordered* (modo por defecto): Garantiza que los datos son consistentes con el sistema de archivos. Los archivos escritos recientemente nunca aparecerán con contenidos basura después de una caída.
  - *data=journal*: Requiere un "journal" grande para una velocidad razonable en la mayoría de los casos y por lo tanto tarda más tiempo en recuperar el sistema en el caso de un apagado incorrecto. Algunas veces es más rápido para algunas operaciones, por ejemplo, en los *spools* de correo o servidores NFS sincronizados. No obstante, utilizar el modo "journal" para un uso normal resulta con frecuencia un poco más lento.

  El modo por defecto (*ordered*) es el recomendable, pudiendo cambiar el modo en el montaje del sistema de archivos.

- **Fácil migración**

  Las particiones ext3 no tienen una estructura de archivos diferente a los de ext2, por lo que se puede pasar de ext2 a ext3 y viceversa; esto es útil sobre todo si el registro se

corrompe accidentalmente, por ejemplo, debido a sectores malos del disco. Es decir, existe total compatibilidad entre ext2 y ext3. Además de poder montar un sistema de archivos ext3 como ext25 (ya que la estructura de formateo del disco es la misma).

Es posible pasar de un sistema a otro sin necesidad de tener que realizar un tedioso proceso de backup, formateo y restauración de los datos, con la posibilidad de que se produzca algún error.

Resumiendo, ext3 es totalmente compatible en ambos sentidos con ext2. Se puede migrar un sistema ext2 a ext3 muy fácilmente, se puede montar un sistema ext3 como ext2 sin modificar nada del sistema de archivos journal y también eliminar el journal para volver al sistema ext2 anterior.

Otras ventajas importantes de utilizar ext3 son:

1. El ext3 como el ext2 tiene múltiples desarrolladores y organizaciones involucradas en su desarrollo, por lo que su evolución no depende de una sola persona o empresa.
2. Ext3 proporciona y hace uso de una capa genérica de journaling (Journaling Block Device, JBD) la cual puede ser usada en otros contextos. Otros dispositivos soportados por Linux pueden ser utilizados con ext3 (NVRAM, disk-on-chip, USB flash memory drives, etc.).
3. Ext3 tiene una amplia compatibilidad con todas las plataformas, trabaja tanto en arquitecturas de 32 como de 64 bits; así como, en sistemas little-endian como big-endian. Algunos sistemas operativos (por ejemplo, algunos clones y variantes de UNIX y BeOS) pueden acceder a archivos en un sistema de archivos ext2, estos sistemas también lo pueden hacer en un sistema de archivos ext3.
4. Ext3 no requiere profundos cambios en el *kernel* y no requiere tampoco nuevas llamadas al sistema.
5. Ext3 reserva uno de los i-nodos especiales de ext2 para el registro de journal, pero los datos del mismo pueden estar en cualquier conjunto de bloques, y en cualquier sistema de archivos. Inclusive se puede compartir el registro de journal entre distintos sistemas.
6. El programa de recuperación de sistemas de archivos "e2fsck" tiene mucho éxito en la recuperación de datos cuando el software o el hardware falla y corrompe un sistema de archivos. Ext3 usa el mismo código que el "e2fsck" para salvar el sistema de archivos después de una posible corrupción, y por consiguiente tiene la misma robustez que el ext2 contra posibles pérdidas catastróficas de datos cuando haya fallos de corrupción en los mismos.

Todas estas peculiaridades del ext3 son totalmente transparentes al usuario, el cual trabajará igual que lo hacía con ext2, incluido el montaje y utilización de otros sistemas de archivos (NFS, dispositivos de almacenamiento externos, etc.).

Apéndice II

Formato para el control de equipo de cómputo

FACULTAD DE INGENIERÍA
UNIDAD DE SERVICIOS DE CÓMPUTO ACADÉMICO

FORMATO PARA EL CONTROL DE EQUIPO DE CÓMPUTO

Fecha: _____

Realizó: _____
(Nombre y firma)

DEPARTAMENTO	BIEN	INVENTARIO UNAM	UBICACIÓN	RESPONSABLE	E-MAIL	TELÉFONO	COMPLETO

_____
Jefe del DROS

Apéndice III

Manual de Usuario

MANUAL DE USUARIO

Salas de Cómputo

ENERO 2003

FACULTAD DE INGENIERÍA

UNIDAD DE SERVICIOS DE CÓMPUTO ACADÉMICO

1. Para hacer uso de las computadoras con Sistema Operativo Linux de las Salas 1 y H, debes ingresar los siguientes datos:

   Login (Usuario): alumno
   Password (Contraseña): alumno

2. Para hacer uso de tu cuenta, deberás hacer una conexión remota empleando *ssh* e ingresar el login y password que te fue proporcionado por los administradores del sistema.

   Para las computadoras con sistema operativo Linux:

   [alumno@maquina alumno]$ ssh –l [login] [servidor]

   o

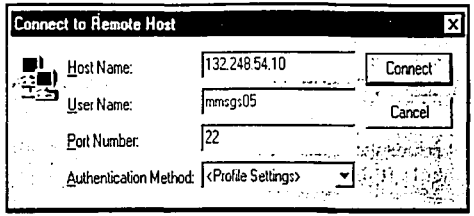
   [alumno@maquina alumno]$ ssh login@servidor

   Por ejemplo:

   [alumno@maquina alumno]$ ssh mmsgs05@cancun.fi-a.unam.mx

   Para computadoras con Windows:

   Utiliza la aplicación *Secure Shell Client* e ingresa el login y password que te fue proporcionado por los administradores del sistema.



3. Si es la primera vez que realizas una conexión remota, el siguiente paso es cambiar tu password, de la siguiente manera:

   a) Teclea el comando *passwd.*
   b) Ingresa el password que te proporcionó el administrador del sistema.
   c) Proporciona tu nuevo password, el cual debe ser mínimo de 6 caracteres, alternando mayúsculas, minúsculas y/o números. Por ejemplo: **JM-.6tA**

   En caso, de que se te olvide tu password, deberás acudir con el administrador del sistema.

4. Para realizar transferencia de archivos desde una computadora con sistema operativo Linux, deberás utilizar el comando *scp.*

   [alumno@maquina alumno]$ scp [archivo] login@servidor:[ruta donde se va a copiar]

   o

   [alumno@maquina alumno]$ scp login@servidor:[archivo] [lugar donde se va a copiar]

   Por ejemplo:

   [alumno@maquina alumno]$ scp trabajo.doc mmsgs05@cancun.fi-a.unam.mx:/users/minas/mmsgs00

   o

   [alumno@maquina alumno]$ scp mmsgs05@cancun.fi-a.unam.mx:/users/minas/mmsgs00/proyecto.zip /home/alumno/

   En ambos casos, te pedirá tu password.

5. Para realizar transferencia de archivos desde una computadora con Windows, utiliza la aplicación *Secure File Transfer Client*

6. Para hacer uso de tu cuenta de correo electrónico en el servidor cancun.fi-a.unam.mx, es de la siguiente manera:

   - Utilizar el comando *pine*

     Este comando lo puedes utilizar cuando ya hayas hecho una conexión remota al servidor.

     [mmsgs05@cancun]$ pine

   - Utilizar un navegador de Internet, ya sea el Internet Explorer o Netscape. La dirección es:

     https://correo.fi-a.unam.mx

NOTA: Este Manual de Usuario estará en constante actualización para un mejor servicio en las Salas de Cómputo de Unidad de Servicios de Cómputo Académico.

Apéndice IV

Formato de control de incidentes de seguridad

FORMATO DE CONTROL DE INCIDENTES DE SEGURIDAD

Reporte N° _____
Fecha _____ Hora: _____
Departamento _____
Quien lo reporta: _____
Quien realiza el reporte del incidente: _____

Antecedentes

1) Descripción del incidente.

   a) Cómo se detectó.
   b) Cómo se analizó el incidente.

2) Describir lo que se encontró (Nombre del software y versión, archivos, herramientas, etc.)

3) Consecuencias o daños del incidente.

4) Primeras medidas en respuesta al incidente.

Respuesta al incidente

5) Recursos comprometidos (Sistema operativo, servicios de red, hardware, etc.)

6) ¿Se detectó al intruso, interno y/o externo?, (describir cómo se detectó).

7) ¿Se implementó algún recurso que bloqueara definitivamente la posibilidad de ocurrencia de dicho incidente? Describa lo que se hizo.

8) Observaciones

Nota:
El reporte debe ser llenado con el mayor detalle, respondiendo a cada inciso.
Anexe las hojas necesarias para contestar el formato incluyendo información que respalde o aclare la forma en que se desarrolló el incidente.

Apéndice V

Formato para el registro de direcciones IP

DISTRIBUCIÓN DE DIRECIONES IP. SUBRED: 132.248.XX.
DIVISIÓN O ÁREA: XXXXXXXXXXXXXXXXXXXX

FECHA: 30-ene-01

	DIRECCION IP			EQUIPO			USO	APLICACIONES Y DUE JUSTIFICAN EL USO DE LA IP - OBSERVACIONES	DIRECCION ETHERNET	USUARIO		DEPARTAMENTO / AREA AL QUE SE LE ASIGNA LA IP	TIEMPO DE USO APROXIMADO DEL SERVICIO E DIA [HRS]
# ITEM	NUMERO	TIPO DE IP	ESTADO	NOMBRE	SISTEMA OPERATIVO	UBICACIÓN FISICA				CARGO AL QUE SE ASIGNA LA IP	RESPONSABLE DEL EQUIPO		
ejemplo 1	132.248.54.10	REAL	OCUPADA	cancun	LINUX (HP-UX) 10.0	Sala W.S de UNICA	ACADEMICO	Servicio de correo, ftp, compilaciones, lenguajes, aplicaciones, servicio para alumnos	0050DA89C222	Jefe de Departamento	Ma de Cruz Marin	DEPTO DE REDES Y OPERACIÓN DE SERVIDORES (UNICA)	24 horas Siempre prendido
ejemplo 2	132.248.54.2	REAL	NO UTILIZADA-ASIGNADA	N/A	N.A	N.A	ADMINISTRATIVO	La direccion ha sido asignada a la area, pero por el momento no es utilizada. Esta destinada para futuros crecimientos	N.A	N.A	N.A	Departamento XXXXX	N.A
ejemplo 3	132.248.54.240	REAL	LIBRE	N.A	N.A	N.A	N.A	No ha sido asignada la direccion a ninguna	N.A	N.A	N.A	N.A	N.A
ejemplo 4	192.168.1.1	FIREWALL/PROXY	OCUPADA	dumnet	LINUX 7.0	Sala W.S de UNICA	ACADEMICO	Sala de servicios a alumnos de la FI	0050DAA4BC13	Jefe de Departamento	Ma Cruz Marin	DEPTO DE REDES Y OPERACIÓN DE SERVIDORES (UNICA)	12 horas
1	132.248.XX.1												
2	132.248.XX.2												
3	132.248.XX.3												
4	132.248.XX.4												
5	132.248.XX.5												
6	132.248.XX.6												
7	132.248.XX.7												
8	132.248.XX.8												
9	132.248.XX.9												
10	132.248.XX.10												
11	132.248.XX.11												
12	132.248.XX.12												
13	132.248.XX.13												
14	132.248.XX.14												
15	132.248.XX.15												
16	132.248.XX.16												
17	132.248.XX.17												
18	132.248.XX.18												
19	132.248.XX.19												
20	132.248.XX.20												
21	132.248.XX.21												
22	132.248.XX.22												
23	132.248.XX.23												
24	132.248.XX.24												
25	132.248.XX.25												
26	132.248.XX.26												
27	132.248.XX.27												
28	132.248.XX.28												
29	132.248.XX.29												
30	132.248.XX.30												
31	132.248.XX.31												
32	132.248.XX.32												
33	132.248.XX.33												
34	132.248.XX.34												
35	132.248.XX.35												
36	132.248.XX.36												
37	132.248.XX.37												
38	132.248.XX.38												

Apéndice VI

Código Penal Federal

CÓDIGO PENAL FEDERAL

CAPÍTULO II Acceso ilícito a sistemas y equipos de informática

Artículo 211 bis 1

Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

Artículo 211 bis 2

Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

Artículo 211 bis 3

Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.

Artículo 211 bis 4

Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún

mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Artículo 211 bis 5

Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

Artículo 211 bis 6

Para los efectos de los artículos 211 Bis 4 y 211 Bis 5 anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 Bis de este Código.

Artículo 211 bis 7

Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.

CAPITULO II Operaciones con recursos de procedencia ilícita

Artículo 400 Bis

Se impondrá de cinco a quince años de prisión y de mil a cinco mil días multa al que por sí o por interpósita persona realice cualquiera de las siguientes conductas: adquiera, enajene, administre, custodie, cambie, deposite, dé en garantía, invierta, transporte o transfiera, dentro del territorio nacional, de éste hacia el extranjero o a la inversa, recursos, derechos o bienes de cualquier naturaleza, con conocimiento de que proceden o representan el producto de una actividad ilícita, con alguno de los siguientes propósitos: ocultar o pretender ocultar, encubrir o impedir conocer el origen, localización, destino o propiedad de dichos recursos, derechos o bienes, o alentar alguna actividad ilícita.

La misma pena se aplicará a los empleados y funcionarios de las instituciones que integran el sistema financiero, que dolosamente presten ayuda o auxilien a otro para la comisión de las conductas previstas en el párrafo anterior, sin perjuicio de los procedimientos y sanciones que correspondan conforme a la legislación financiera vigente.

La pena prevista en el primer párrafo será aumentada en una mitad, cuando la conducta ilícita se cometa por servidores públicos encargados de prevenir, denunciar, investigar o juzgar la

comisión de delitos. En este caso, se impondrá a dichos servidores públicos, además, inhabilitación para desempeñar empleo, cargo o comisión públicos hasta por un tiempo igual al de la pena de prisión impuesta.

En caso de conductas previstas en este artículo, en las que se utilicen servicios de instituciones que integran el sistema financiero, para proceder penalmente se requerirá la denuncia previa de la Secretaría de Hacienda y Crédito Público.

Cuando dicha Secretaría, en ejercicio de sus facultades de fiscalización, encuentre elementos que permitan presumir la comisión de los delitos referidos en el párrafo anterior, deberá ejercer respecto de los mismos las facultades de comprobación que le confieren las leyes y, en su caso, denunciar hechos que probablemente puedan constituir dicho ilícito.

Para efectos de este artículo se entiende que son producto de una actividad ilícita, los recursos, derechos o bienes de cualquier naturaleza, cuando existan indicios fundados o certeza de que provienen directa o indirectamente, o representan las ganancias derivadas de la comisión de algún delito y no pueda acreditarse su legítima procedencia.

Para los mismos efectos, el sistema financiero se encuentra integrado por las instituciones de crédito, de seguros y de fianzas, almacenes generales de depósito, arrendadoras financieras, sociedades de ahorro y préstamo, sociedades financieras de objeto limitado, uniones de crédito, empresas de factoraje financiero, casas de bolsa y otros intermediarios bursátiles, casas de cambio, administradoras de fondos de retiro y cualquier otro intermediario financiero o cambiario.

Apéndice VII

Códigos de Ética

CÓDIGOS DE ÉTICA

CÓDIGO DE ÉTICA DEL INGENIERO MEXICANO (UMAI)

El Código de Ética Profesional del Ingeniero Mexicano se publicó el 1 de julio de 1983, y firmó como testigo el C. licenciado Miguel de la Madrid Hurtado, Presidente Constitucional de los Estados Unidos Mexicanos, el cual se transcribe a continuación.

CONSIDERANDO QUE:

1. El ingeniero mexicano sustenta su conducta en el **respeto y amor a la patria.**
2. El ingeniero en nuestro país ha logrado la práctica de su profesión **gracias a la oportunidad** que le brinda la nación mexicana.
3. Por su preparación tiene un **mayor compromiso** para coadyuvar a satisfacer las necesidades y **elevar la calidad de vida** de los mexicanos, con la convicción y responsabilidad moral de **sostener un desarrollo con justicia social.**
4. Es un deber propiciar el desempeño de la actividad de acuerdo con un Código de Ética que precise las obligaciones sociales, que hacen posible el respeto de cada profesional para con los demás, en **busca de una justa y armoniosa convivencia humana** dentro de cada nación y entre las naciones.
5. Los principios universales y nuestras mejores tradiciones consideran un alto deber la **solidaridad** internacional y el respeto a los **valores morales** de otros pueblos, en particular donde el ingeniero amplíe su preparación o eventualmente ejerza la profesión.
6. Los diversos códigos de ética profesional de colegios y asociaciones de ingenieros confluyen en una misma concepción.
7. La unión de ingenieros mexicanos se ha dado en torno a principios y normas de conducta.

La Asamblea General Ordinaria de la UMAI adopta el siguiente Código de Ética Profesional del Ingeniero Mexicano:

El ingeniero reconoce que ***el mayor mérito es el trabajo,*** por lo que ejercerá su profesión comprometido con el ***servicio a la sociedad*** mexicana, atendiendo al bienestar y progreso de la mayoría.

Al transformar la naturaleza en beneficio de la humanidad, el ingeniero debe acrecentar su conciencia de que ***el mundo es la morada del hombre*** y de que su interés por el universo es una garantía de la superación de su espíritu y del conocimiento de la realidad para hacerla ***más justa y feliz.***

El ingeniero debe ***rechazar*** los trabajos que tengan como fin atentar contra el interés general; de esta manera evitará situaciones que impliquen ***peligros*** o constituyan una ***amenaza contra el medio ambiente, la vida, la salud y demás derechos*** del ser humano.

Es un ***deber ineludible*** del ingeniero sostener el prestigio de la profesión y velar por su cabal ejercicio; asimismo, ***mantener una conducta profesional*** cimentada en ***la capacidad, la honradez, la fortaleza, la templanza, la magnanimidad, la modestia, la franqueza y la justicia***, con la conciencia de subordinar el bienestar individual al bien social.

El ingeniero debe procurar el ***perfeccionamiento*** constante de sus conocimientos, en particular de su profesión, ***divulgar*** su saber, ***compartir*** su experiencia, ***proveer oportunidades*** para la formación y la capacitación de los trabajadores, brindar ***reconocimiento***, apoyo moral y material a la institución educativa en donde realizó sus estudios; de esta manera ***revertirá a la sociedad*** las oportunidades que ha recibido.

Es responsabilidad del ingeniero que su trabajo se realice con ***eficiencia*** y apoyo a las ***disposiciones legales***. En particular, velará por el cumplimiento de las ***normas de protección a los trabajadores*** establecidas en la legislación laboral mexicana.

En el ejercicio de su profesión, el ingeniero debe cumplir con diligencia los compromisos que haya asumido y desempeñará con dedicación y lealtad los trabajos que se le asignen, ***evitando anteponer su interés personal*** en la atención de los asuntos que se le encomienden, o ***coludirse para ejercer competencia desleal*** en perjuicio de quien reciba sus servicios.

Observará una ***conducta decorosa***, tratando con respeto, diligencia, imparcialidad y rectitud a las personas con las que tenga relación, particularmente a sus colaboradores, absteniéndose de incurrir en desviaciones y ***abusos de autoridad*** y de disponer o autorizar a un subordinado ***conductas ilícitas***, así como de favorecer indebidamente a terceros.

Debe ***salvaguardar*** los ***intereses*** de la institución o persona para la que trabaje y hacer ***buen uso de los recursos*** que se le hayan asignado para el desempeño de sus labores.

Cumplirá con eficiencia las disposiciones que en ejercicio de sus atribuciones le dictaminen sus superiores jerárquicos, respetará y hará respetar su posición y trabajo; si discrepara de sus superiores tendrá la obligación de ***manifestar*** ante ellos las razones de su ***discrepancia***.

El ingeniero tendrá como norma ***crear y promover la tecnología nacional***; pondrá especial cuidado en vigilar que la transferencia tecnológica se adapte a nuestras condiciones conforme al marco legal establecido. Se obliga a guardar ***secreto profesional*** de los datos confidenciales que conozca en el ejercicio de su profesión, salvo que le sean requeridos por autoridad competente.

CÓDIGO DE ÉTICA DE LA IEEE

Nosotros, los miembros del IEEE, en reconocimiento de la importancia de nuestras tecnologías afectando la calidad de vida a lo largo del mundo, y recibiendo una obligación personal a nuestra profesión, sus miembros y las comunidades que nosotros servimos, nos comprometemos por la presente a la más alta conducta ética y profesional y acordamos a:

1. Aceptar la responsabilidad tomando las decisiones de la ingeniería consistente con la seguridad, salud y bienestar del público, y descubrir factores que podrían poner en peligro el público o el ambiente rápidamente;
2. Evitar conflictos de interés real o percibido siempre que sea posible, y descubrir a los afectados cuando ellos existen;
3. Ser honrado y realista declarando demandas o estimaciones basadas en los datos disponibles;
4. Rechazar el soborno en todas sus formas;
5. Mejorar la comprensión de tecnología, su aplicación apropiada, y las consecuencias potenciales;
6. Mantener y mejorar nuestra competencia técnica y sólo emprender las tareas tecnológicas para otros si poseemos entrenamiento o experiencia, o después de descubrir nuestras limitaciones pertinentes;
7. Buscar, aceptar y ofrecer la crítica honrada de trabajo técnico, para el conocimiento y para corregir errores, y para acreditar las contribuciones de otros;
8. Tratar a todas las personas justamente sin tener en cuenta la raza, religión, género, invalidez, edad, o el origen nacional;
9. Evitar dañar a otros, su propiedad, reputación, o empleo por la acción falsa o malévola;
10. Ayudar a los colegas y co-obreros en su desarrollo profesional y apoyarlos siguiendo este código de ética.

CÓDIGO DE ÉTICA DE LOS MIEMBROS

DE

AMERICAN SOCIETY FOR INDUSTRIAL SECURITY (ASIS)

La seguridad y protección es una actividad profesional que exige a quienes se dedican a ella, un alto desempeño y la observancia de normas éticas y de conducta cuyos estándares son mucho más altos que en cualquier otra profesión, lo que nos obliga a mantener una imagen profesional que inspire confianza a nuestros asesorados, a las autoridades y a otros profesionales con los que nos relacionamos diariamente; por lo tanto, exhortamos a los presentes a cumplir y hacer cumplir los preceptos fundamentales de nuestra Asociación y que dicen que todo miembro de ASIS:

1. Se desarrollará profesionalmente de acuerdo a los más altos principios éticos y morales y dentro del marco legal vigente.
2. Velará por que se respeten los preceptos de la verdad, honestidad e integridad.
3. Se conducirá con eficiencia y eficacia en el desarrollo de sus responsabilidades profesionales.
4. Se mantendrá actualizado en las tecnologías y sistemas de la seguridad y protección.
5. Protegerá la información confidencial relativa a la seguridad de las personas, bienes y propiedades que proteja, previniendo y controlando cualquier indiscreción que pueda causar un riesgo a otros.
6. Jamás difamará maliciosamente a otro miembro de la Asociación o a cualquier profesional de la seguridad y protección, evitando también que otros lo hagan.

LOS PROFESIONALES DE LA SEGURIDAD UNIDOS POR EL BIEN DE MÉXICO

CÓDIGO DE ÉTICA DE LA AMIPCI

OCTUBRE 25, 2000

TÍTULO I

DISPOSICIONES GENERALES

Artículo 1º. **Definiciones.** Para los efectos de este Código se entenderá por:

I. **AMIPCI.** Asociación Mexicana de la Industria Publicitaria y Comercial en Internet, A. C.

II. **Industria.** La Industria comercial y publicitaria de Internet en México, incluyendo prestadores de servicios de acceso, sitios y portales, proveedores de equipo de cómputo, de software, de servicios profesionales, de servicios de telecomunicaciones, empresas desarrolladoras y comercializadoras de contenidos, así como de publicidad, mercadotecnia en Internet y disciplinas afines.

III. **Asociados.** Todas las personas físicas o morales que pertenezcan a la ASOCIACIÓN MEXICANA DE LA INDUSTRIA PUBLICITARIA Y COMERCIAL EN INTERNET, A.C. (**AMIPCI**)

IV. **Usuarios.** Aquellas personas físicas o morales que celebran cualquier acto, convenio o contrato con un Asociado para que le sea proporcionado un bien o servicio relacionado con la Industria.

V. **Código.** El presente Código de Ética.

VI. **Comité de Ética.** Al órgano de la **AMIPCI** encargado de aplicar las disposiciones del presente Código en relación a la conducta de los Asociados, así como recibir quejas, resolver controversias entre los Asociados y/o usuarios y, en su caso, imponer las sanciones y/o medidas correctivas que procedan.

VII. **Consejo Directivo.** Al órgano de Gobierno de la **AMIPCI** formando por su Presidente, Vicepresidente, Secretario y Tesorero, así como por los Directores de los Comités de la Asociación.

Artículo 2º. **Normatividad.** El presente Código establece las normas que regularán la conducta que deben de seguir los Asociados, las que se consideran como mínimas reconociéndose que existen otras de carácter legal y moral que complementan al presente.

Artículo 3º. **Alcance del Código.** Cualquier persona física o moral, por el sólo hecho de asociarse a la **AMIPCI**, adquiere la obligación de ajustar su conducta y sus actividades comerciales, así como la prestación de sus servicios a las disposiciones contenidas en el presente Código.

Artículo 4°. **Interpretación.** En los casos de duda acerca de la conducta de alguno de los Asociados, o del alcance del presente Código, los integrantes del Comité de Ética serán las personas facultadas para resolver las cuestiones que se susciten.

TÍTULO II

CAPÍTULO I

DERECHOS DE LOS ASOCIADOS

Artículo 5°. **Descripción de los Derechos de los Asociados.** Todos los Asociados tendrán Derecho a:

a) Presentar quejas contra otro Asociado y/o usuario que incumpla con lo dispuesto en el presente Código.

b) Solicitar el testimonio de otro(s) Asociado(s) que ayuden a confirmar o a esclarecer las pruebas en contra de cualquier Asociado y/o usuario.

c) Sugerir cambios o modificaciones al presente Código en beneficio de la generalidad y de la mejora constante para el beneficio de la Industria.

d) Vigilar que se cumplan las normas y procedimientos contenidos en el presente Código y reportar cualquier desviación al Consejo Directivo de la **AMIPCI**, para efectos de que de considerarse conducente, se turne el caso al Comité de Ética de la Asociación y se proceda en los términos que se previenen en las presentes normas.

CAPÍTULO II

OBLIGACIONES GENERALES DE LOS ASOCIADOS

Artículo 6°. **Descripción de las obligaciones generales de los Asociados.**

Todos los Asociados de la **AMIPCI** adquieren la obligación de:

a) Respetar y ajustarse al presente Código de Ética.

b) Ejercer plenamente los derechos descritos en el Artículo 5°.

c) Acatar las sanciones que fijen los miembros del Comité de Ética.

CAPÍTULO III

OBLIGACIONES DE LOS ASOCIADOS CON LA SOCIEDAD

Artículo 7º. **Ejemplo en el ámbito empresarial.** Todos los Asociados deberán distinguirse en el ámbito empresarial por su actuación ejemplar, agregando a sus valores personales, los valores de la Asociación y obligándose a demostrar en el total de sus operaciones comerciales, el más alto nivel de profesionalismo, moralidad, calidad y desempeño.

Artículo 8º. **Independencia de criterio.** El Asociado acepta la obligación de sostener un criterio libre e imparcial al emitir sus opiniones respecto a las consultas que se le hagan acerca de cualquier producto y/o servicio relacionado con la Industria.

Se considera falta de imparcialidad cuando:

a) Se toma ventaja indebida de la clientela de algún producto, persona, empresa, nombre comercial o símbolo, mediante publicidad impresa o en línea a través de Internet o en cualquier otro medio de difusión.

b) No se explica adecuadamente y con objetividad y veracidad, el costo, funciones, ventajas o desventajas de cualquier producto o servicio.

Artículo 9º. **Calidad de los productos y/o servicios y garantías.** Todo Asociado acepta la obligación de proporcionar los productos y/o servicios y garantías, en forma eficaz, honesta, leal, y en cumplimiento de las disposiciones legales, con el fin de dignificar a la Industria y a sus Asociados.

Artículo 10º. **Respecto al personal a su cargo.** Todos los Asociados se obligan a respetar al personal a su cargo y al personal de otros Asociados, como seres humanos, sin distinción de ningún tipo y promoviendo la superación y la mejora continua del personal a su cargo.

Artículo 11º. **Responsabilidad de su personal.** El Asociado siempre asumirá la responsabilidad de cualquier acto, trabajo, consejo o servicio proporcionado por su personal y en los términos de los artículos contenidos en este Código.

Artículo 12º. **Proposición o Aceptación de trabajos.** Todo Asociado queda obligado a no proponer ni aceptar trabajos, prestar servicios o comercializar productos, que vayan en contra de la honestidad o de la leal competencia o que violen la confidencialidad de la información de terceros, que en virtud del presente Código de Ética debe observar o que infrinjan o violen los derechos de propiedad intelectual e industrial que protejan a los productos o servicios a los que tengan acceso en el curso de sus actividades comerciales o de prestación de servicios.

Artículo 13º. **Respeto a los derechos de los consumidores.** Todo Asociado queda obligado a dar cumplimiento a las disposiciones legales en materia de protección a los consumidores en cuanto a la confidencialidad de la información establecida en el Capítulo VI de éste Código y demás disposiciones aplicables de las Leyes Federales de Protección al Consumidor.

CAPÍTULO IV

OBLIGACIONES DE LOS ASOCIADOS CON LA INDUSTRIA

Artículo 14º. Dignificación de la actividad. Todo Asociado, en la comercialización de sus productos o servicios deberá generar una imagen positiva tanto de la Industria como de su actuación.

Se entiende que los Asociados se valdrán de sus conocimientos, experiencia, calidad y proyección, como medios para cumplir con el fin descrito en el párrafo anterior.

Artículo 15º. Respeto a los colegas. Todos los Asociados procurarán tener buenas relaciones con los demás Asociados, así como con la **AMIPCI**, buscando y promoviendo siempre el apoyo mutuo para la dignificación de la actividad.

Los Asociados se abstendrán de hacer comentarios desleales sobre otro Asociado, cuando dichos comentarios perjudiquen su reputación, buen nombre, crédito comercial, calidad moral y prestigios personales o de la Industria en general.

Todos los Asociados deberán basar sus actividades exclusivamente en los méritos de sus productos o servicios.

Resultará violatorio de este Código, referirse a los competidores, sus productos o servicios por medio de declaraciones falsas, insinuaciones o manifestaciones que induzcan al error. Asimismo, el realizar comparaciones que puedan injustificadamente, arrojar dudas sobre la competencia. Toda comparación de productos, precios o servicios, deberá ser realizada en forma justa, correcta, veraz y comprobable y en ninguna forma deberá tender a inducir error o confusión.

Artículo 16º. Confidencialidad. Todo Asociado tiene la obligación de no revelar, divulgar o aprovecharse indebidamente de la información confidencial, los secretos industriales o comerciales, así como los hechos, datos, circunstancias o proyectos de que tenga conocimiento en el ejercicio de su actividad y provengan de sus proveedores, competidores u otras fuentes, cuya divulgación no hubiere sido autorizada, salvo que los propios titulares de dicha información otorguen expresamente su consentimiento o cuando dicha información sea del dominio público. Ningún Asociado debe emplear formas inapropiadas para adquirir o utilizar los secretos comerciales de los competidores, prestadores de servicios u otro tipo de información confidencial.

Se considerarán como violaciones al presente Código, acciones como el espionaje industrial, soborno, acceso ilícito a lugares, robo e intervención de líneas telefónicas, entre otras conductas ilegales.

Asimismo, resultará violatorio del presente Código, contratar empleados de la competencia, con objeto de obtener información confidencial, así como buscar datos confidenciales entre los empleados o los clientes de la competencia.

Artículo 17º. Condiciones. Ningún Asociado estará obligado a otorgar condiciones comerciales especiales a Asociado alguno por el simple hecho de pertenecer a la **AMIPCI**, a menos que exista un convenio especial aprobado por el Consejo Directivo de la misma y que se trate de condiciones de índole general para todos los Asociados.

Artículo 18º. Libre Competencia. Los Asociados que comercialicen productos o servicios relativos a la Industria concurrirán al mercado con plena responsabilidad y respeto hacia los demás Asociados, propiciando una competencia limpia y leal que permita además del éxito individual, el crecimiento sostenido de la industria.

Los Asociados evitarán toda práctica monopólica, o acuerdo tendiente a tener una ventaja indebida que se traduzca en perjuicio de los usuarios, consumidores u otros Asociados.

Los Asociados evitarán el otorgar dádivas, bonos, regalos, comisiones o cualquier otro beneficio tangible a persona o entidad alguna a cambio del beneficio del negocio en contra de cualquier competencia que se presente y en aras de la imagen de moralidad, honestidad, profesionalismo y seriedad de los demás Asociados y de la Industria.

Todos los Asociados quedan obligados a cumplir cabal y lealmente los preceptos de la Ley de Adquisiciones y Obras Públicas, así como a respetar las disposiciones de la Ley de Responsabilidades de Funcionarios Públicos.

Sin perjuicio de lo anterior, durante el proceso de adquisiciones a través de una licitación pública o cualquiera otra adquisición gubernamental, el Asociado que compita por la adjudicación, no debe intentar influir indebidamente en las decisiones u obtener información confidencial de los funcionarios responsables, que actúan en representación de la Entidad o Dependencia Gubernamental.

Artículo 19º. Propiedad Industrial e Intelectual. Todo Asociado estará obligado a respetar escrupulosamente los Derechos de Propiedad Industrial y/o Intelectual de los Titulares de los Derechos correspondientes, asegurándose de la mejor manera que quienes trabajan para él, sean igualmente respetuosos y obligándose a observar escrupulosamente todas y cada una de las estipulaciones contenidas al efecto, tanto en la Ley Federal del Derecho de Autor como en la Ley de la Propiedad Industrial. Asimismo cuando se trate de productos provenientes del extranjero y que explícitamente se prohíba su uso, enajenación, reproducción o cualquier otro tratamiento sin el pago de los derechos correspondientes.

Lo previsto anteriormente, aplica igualmente al respeto que se deberá observar en relación a cualquier producto, equipo, dispositivo, servicio, tecnología, asistencia técnica o know-how, información del mercado, estrategias de renta o listas de precios, campañas publicitarias, etc., cuyo acceso, divulgación y utilización se encuentren restringidos o sean designados como información confidencial o se encuentren protegidos por patentes, marcas, secretos industriales, derechos de autor o cualquier privilegio de acuerdo a la legislación de la materia.

CAPÍTULO V

OBLIGACIONES DE LOS ASOCIADOS CON LA EDUCACIÓN

Artículo 20°. **De la transmisión de conocimientos.** Dentro del espíritu de cooperación en la industria, los Asociados aceptarán compartir información con el resto de la membresía, siempre y cuando dicha información no tenga el carácter de confidencial o restringida y dicha información sea compartida en forma general a todos los Asociados.

Dicha información así divulgada, sólo será para el beneficio exclusivo de la membresía y no podrá revelarse ni difundirse a ningún otro tercero que no sea miembro de la **AMIPCI.**

El Asociado que de cualquier manera, transmita sus conocimientos, tendrá como objetivo fundamental el mantener las más altas normas de profesionalismo y de conducta, y contribuir al desarrollo y difusión de los conocimientos propios de la Industria.

El Asociado que desempeñe cualquier actividad docente se obliga a impartir una enseñanza técnica útil, y orientar al alumno para que en el futuro desempeño de su actividad profesional, actúe en estricto apego a las reglas de Ética, debiendo asimismo, mantenerse actualizado en las áreas de su ejercicio, a fin de transmitir a los alumnos los conocimientos más avanzados sobre la materia tanto en la teoría como en la práctica.

Los Asociados que realicen una actividad docente deberán siempre reforzar los siguientes temas para beneficio del nuevo profesionista y de la Industria:

a) Prácticas comerciales de leal y libre competencia;

b) Negativa a la corrupción como medio para hacer negocio; y en general

c) Respeto a la propiedad intelectual, a los diferentes sectores de la Industria y a sus colegas.

Artículo 21°. **Formación de nuevas generaciones.** Los Asociados se obligan a apoyar a las nuevas generaciones de profesionistas en la Industria, apoyando su formación, desarrollo personal, cultivando sus aptitudes y creando nuevas generaciones de profesionales de la Industria con la más alta calidad técnica y humana.

Los Asociados que puedan participar en la actividad docente o en la formulación de planes de estudio tendrán la obligación de vigilar que las nuevas generaciones reciban un conocimiento completo en las diferentes ramas de la Industria y que cumplan con las necesidades de trabajo que el mercado requiere.

CAPITULO VI

OBLIGACIONES DE LOS ASOCIADOS PARA LA PROTECCIÓN DE LA PRIVACIDAD DE LA INFORMACIÓN

Artículo 22º. **Normas y Políticas.** Los miembros de la **AMIPCI** deberán dar cumplimiento a las normas orientadas hacia la privacidad de los usuarios en línea. Estas políticas serán diseñadas para proteger la información asociada a un individuo (información personal) en un ambiente en línea o de comercio electrónico. Las políticas, para adaptarse a los estándares de la **AMIPCI**, estarán compuestas de las siguientes partes:

a) Adopción y puesta en práctica de una política de privacidad.

b) Avisos y divulgación.

c) Opciones y consentimiento.

d) Calidad de los datos.

e) Limitaciones de uso.

f) Seguridad.

Cada miembro de la **AMIPCI** podrá modificar particularmente las políticas de privacidad para necesidades particulares. Sin embargo, todas las políticas particulares se ajustarán a los estándares mínimos establecidos por la **AMIPCI**, en el presente Capítulo o los que llegue a establecer en el futuro.

Artículo 23º. **Adopción y puesta en práctica de una política de privacidad.** Todos los socios de la **AMIPCI** cuya actividad se encuentre orientada hacia el comercio electrónico o a establecer actividades en línea, tiene la responsabilidad de adoptar y poner en práctica un conjunto de políticas para proteger la privacidad de los Datos Personales (en adelante: DP). Debe también tomar medidas para fomentar la adopción y puesta en práctica de políticas de privacidad para cualquier otra organización relacionada, que incluye compartir esa filosofía con socios comerciales y clientes.

Artículo 24º. **Opciones y consentimiento.** Los usuarios deberán de tener opciones sobre de qué manera se utilizarán sus DP. Los miembros de la **AMIPCI** deberán proporcionar opciones al usuario en los siguientes casos:

a) Cuando los DP vayan a ser utilizados para cualquier otro fin distinto a los fines por los cuales fueron recolectados originalmente.

b) La recopilación de información, tales como comportamientos de navegación asociables a sus DP.

c) El uso de los DP para futuras opciones de comercialización.

d) El hecho de compartir los DP con terceros.

En un esfuerzo de asegurar el uso apropiado del correo electrónico para propósitos de comercialización, la **AMIPCI** establecerá como estándar mínimo el hecho de que el usuario decida si desea recibir o no este tipo de correo electrónico.

Artículo 25º. **Calidad de los datos.** Las organizaciones que crean, mantienen, usan o distribuyen DP deben tomar medidas para asegurar que los datos son exactos, completos, relevantes y oportunos para los fines en que serán utilizados.

Los miembros de la **AMIPCI** deben tomar las medidas necesarias para proveer a los usuarios la capacidad de modificar inexactitudes en sus DP.

Artículo 26º. **Limitaciones de Uso.** Las políticas de privacidad de las organizaciones deberán hacer referencia a por qué se están recopilando DP, y a cómo serán utilizados. El uso de DP se debe limitar al propósito original especificado.

Si los DP van a ser utilizados para un propósito no especificado, o el uso de los DP cambia, los usuarios deben ser notificados claramente de esto. De la misma forma se proporcionará al usuario una manera sencilla de oponerse a dicho cambio.

Las políticas de privacidad deberán de incluir una declaración referente al uso de la información en caso de que sea requerida por la ley. En este caso, el acceso a los DP puede ocurrir sin el consentimiento del usuario.

Artículo 27º. **Seguridad.** Los miembros de la **AMIPCI** que crean, mantienen, usan o diseminan DP, deberán tomar medidas para asegurar su confiabilidad y tomar precauciones para proteger los DP contra pérdida, uso erróneo o alteraciones.

Los Asociados deberán utilizar procedimientos de seguridad de la industria tales como el uso de conexiones seguras para la transmisión de la información. Los detalles de esta información deberán de estar contenidos en sus políticas de privacidad.

Los Asociados deberán tomar las medidas necesarias para asegurar que, en caso de que transfieran DP a terceros, estos estén enterados de las medidas de seguridad y a su vez tomen las medidas necesarias para continuar garantizando su seguridad.

CAPÍTULO VII

OBLIGACIONES DE LOS ASOCIADOS CON LA AMIPCI

Artículo 28º. **Cumplimiento de las disposiciones.** Todo Asociado tiene la obligación de respetar las normas, disposiciones, políticas, procedimientos y directrices que sean emitidas por la Asociación.

Asimismo, es obligación de todos los Asociados el dar cumplimiento en el desempeño de sus actividades a todas las disposiciones legales aplicables de la materia, y muy particularmente, a aquellas que rigen los aspectos de la leal competencia y la protección de los derechos de la propiedad intelectual.

Artículo 29º. **Participación.** Todo Asociado deberá hacer todo lo posible por participar en las actividades, comités de trabajo, eventos promovidos por la Asociación, actos y cualquier otra actividad que sea organizada por la misma, buscando en todo momento el mejoramiento de la Industria y de los demás Asociados.

Artículo 30º. **Captación de socios.** Todo Asociado está obligado a promover a la Asociación entre sus colegas y miembros de la Industria, buscando su afiliación, motivándolos a la participación continua y comunicando los beneficios de la **AMIPCI** en la Industria y en la Sociedad.

Artículo 31º. **Terminación de la membresía.** Todo Asociado que por cualquier motivo deje de pertenecer a la Asociación deberá dejar de ostentarse como miembro de la misma y evitará cualquier acción que por beneficio propio o por cualquier otra causa, afecte a la Asociación, a sus miembros o a la Industria.

TÍTULO III

CAPÍTULO I

SANCIONES

Artículo 32º. **Sanciones.** Todo Asociado que incumpla con las disposiciones enunciadas en este Código de Ética, se hará acreedor a la sanción que le imponga el Comité de Ética de la **AMIPCI.**

Artículo 33º. **Imposición de las sanciones.** Para la imposición de las sanciones se tomará en cuenta la gravedad de la violación cometida, evaluándola de acuerdo con la trascendencia que la falta tenga para el prestigio y estabilidad de la actividad de la Asociación y de sus miembros y la responsabilidad que le corresponda.

Artículo 34º. **Diferentes tipos de sanciones.** Las sanciones pueden consistir en:

1. Amonestación.
2. Suspensión temporal de sus Derechos como Asociado.
3. Suspensión definitiva o expulsión.

CAPÍTULO II

PROCEDIMIENTO PARA LA APLICACIÓN DE LAS SANCIONES

Artículo 35º. **Apertura de la investigación.** Para que se proceda a la apertura de una investigación contra algún Asociado, el denunciante formulará una queja ante el Comité de Ética, sin perjuicio de que el Comité podrá proceder a investigar de oficio cualquier violación, cuando así lo estime conveniente.

Artículo 36º. **Denunciante.** El denunciante podrá ser cualquier Asociado de la **AMIPCI**, así como usuarios que conozcan del caso.

Artículo 37º. **Requisitos para las quejas.** Para la presentación de cualquier queja se deberán reunir los siguientes requisitos:

a) Presentar la queja por escrito, dirigida al Comité de Ética de la **AMIPCI.**

b) Enviarla o entregarla personalmente con acuse de recibo firmada por personal de la **AMIPCI** o por miembros del Comité de Ética de la misma.

c) Contener las declaraciones necesarias para que se funde la queja, acompañada de las pruebas correspondientes.

Artículo 38º. **Procedimiento.** Después de ser presentada la queja, los integrantes del Comité de Ética en reunión plenaria darán lectura a la queja, la cual le será asignada a alguno(s) de sus miembro(s) para que estudie y recabe los datos suficientes para emitir, en breve término un informe detallado al Comité respecto de la queja presentada, expresando en su caso los motivos que consideró para aceptar la queja y señalando las pruebas que fueran aportadas así como los argumentos a considerar para dictar la resolución correspondiente.

El Comité deberá informar por escrito al denunciante inmediatamente después de su primer lectura con el fin de que el denunciante conozca que su caso está siendo atendido y se le está dando trámite, a efectos del Artículo 41.

Los integrantes del Comité de Ética estarán obligados a guardar la más absoluta confidencialidad respecto de la queja de la cual tengan conocimiento, en el ejercicio de su encargo, debiendo abstenerse de divulgar los aspectos relacionados con la queja, así como las partes involucradas en la misma.

Artículo 39º. **Audiencia.** El Asociado acusado tiene el derecho de asistir a una reunión plenaria del Comité de Ética, previa notificación del motivo de la acusación para que, en un término de diez días hábiles, produzca su defensa y exhiba las pruebas necesarias para demostrar su inocencia, en el entendido que de no presentar los documentos o pruebas en el término antes referido, se le tendrá por perdido tal derecho, y por lo tanto, por aceptados los hechos y/o conductas que se le imputan.

Artículo 40°. **Resolución.** Cumplidos los pasos anteriores, incluyendo el de la garantía de audiencia y defensa del acusado, el Comité de Ética en reunión plenaria y de acuerdo con el informe al que se refiere el Artículo 40°, acordará la procedencia de la queja, y según el caso, dictará la resolución correspondiente.

TÍTULO IV

DEL COMITÉ DE ÉTICA

Artículo 41°. **Funciones.** El Comité de Ética será el organismo encargado de:

a) Aplicar las disposiciones del presente Código en relación a la conducta de los Asociados y/o de los usuarios de la industria.

b) Recibir quejas por violaciones al presente Código.

c) Imponer las sanciones con fundamento en el presente Código.

d) Interpretar el presente Código.

e) Defender a los Asociados en caso de queja injustificada.

f) Resolver las controversias que se susciten en el ejercicio de la actividad entre Asociados.

Artículo 42°. **Reuniones.** El Comité de Ética se reunirá cada vez que sea convocado por su Presidente, por el Presidente de la **AMIPCI** o a solicitud de cualquier Asociado para conocer de las quejas presentadas, según las normas establecidas en el Título III del presente Código.

Artículo 43°. **Publicación.** Sin perjuicio de lo dispuesto por el Artículo 33°, el Comité podrá ordenar se difunda y publique por cualquier medio, el fallo que se hubiere dictado, cuando así se determine en la resolución respectiva.

En caso de que durante la votación para la resolución de un caso existiera empate, el Presidente tendrá voto de calidad para decidir la resolución del caso.

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

CÓDIGO DE ÉTICA UNIVERSITARIO

A LA COMUNIDAD UNIVERSITARIA

Considerando que la Universidad Nacional Autónoma de México, como organismo descentralizado del estado, está comprometida con una responsabilidad moral y ética en el sentido de actuar de acuerdo a normas y principios que rijan la conducta del buen vivir de su comunidad.

Que esa responsabilidad ética obliga a una continua evaluación del comportamiento social y público de sus funcionarios y empleados, a fin de garantizar en todo momento el respeto al derecho y la observancia de su Normatividad evitando con ello faltas a las normas éticas que pongan en riesgo la estabilidad de la institución.

Que para fortalecer la confianza de la comunidad universitaria, así como la del pueblo de México, es preciso adoptar medidas tendientes a reforzar la grandeza de la institución, haciéndolos sentir parte importante de la misma, además de propiciar que sus labores no vulneren los principios de una ética institucional.

Se emite el presente Código de Ética para los funcionarios y empleados universitarios cuya implementación, es de trascendental importancia para esta Universidad.

ALCANCE Y OBJETIVO DEL CÓDIGO

Reglamentar la conducta de los funcionarios y empleados universitarios y, en general, a toda persona que desempeñe un empleo, cargo o comisión de cualquier naturaleza en la administración universitaria.

PRINCIPIOS FUNDAMENTALES

I. Todo funcionario y empleado universitario considerará un deber, desempeñar su trabajo en apego a este Código de Ética.

II. Todo funcionario y empleado universitario, para apoyar y promover el honor y la dignidad de la institución con las normas más elevadas de la ética deberá:

   a) Interesarse en el bienestar común y aplicar sus conocimientos profesionales para beneficio de la institución así como de sus integrantes.
   b) Desarrollar sus deberes con honestidad e imparcialidad y servir con dedicación a sus superiores, sus empleados y a la comunidad universitaria general.
   c) Reconocer que la trayectoria universitaria es el origen de una disponibilidad económica que debe permitir vivir con decoro, procurando asegurar para los suyos los recursos materiales y los elementos morales que le sean indispensables para su progreso y bienestar.

d) Esforzarse por aumentar la competencia y prestigio de los trabajadores y empleados universitarios en todas sus actividades.

POSTULADOS

I. Responsabilidad hacia la sociedad en general

Bien común: Asumo un compromiso irrenunciable con el bien común, entendiendo que la Universidad es patrimonio de la Nación, que sólo se justifica y legitima cuando se procura ese bien común, por encima de los intereses particulares.

Imparcialidad: Actuaré siempre en forma imparcial, sin conceder preferencias o privilegios indebidos a persona alguna.

Vocación de Servicio: Entiendo y acepto que trabajar para esta Universidad constituye al mismo tiempo el privilegio y el compromiso de servir a la sociedad, porque es ella quien contribuye a pagar mi salario.

Liderazgo: Promoveré y apoyaré estos compromisos con mi ejemplo personal, abonando a los principios morales que son base y sustento de una sociedad exitosa en institución ordenada y generosa.

Dignidad con la sociedad: Respetaré en el debate y en la toma de decisiones, la dignidad de las personas, siendo justo, veraz y preciso en mis apreciaciones, reconociendo la legítima diversidad de opiniones.

II. Responsabilidad hacia la comunidad universitaria

Honradez: Nunca usaré mi cargo para ganancia personal, ni aceptaré prestación o compensación alguna a mis remuneraciones a las que tengo derecho, de ninguna persona u organización que me pueda llevar a actuar con falta de ética mis responsabilidades y obligaciones.

Justicia: Ceñiré mis actos a la estricta observancia de la Normatividad Universitaria, impulsando una cultura de procuración efectiva de justicia y de respeto a la Institución.

Transparencia: Acepto demostrar en todo tiempo y con claridad suficiente, que mis acciones como funcionario y empleado universitario se realizan con estricto y permanente apego a las normas y principios de la Institución, fomentando su manejo responsable y eliminando su indebida discrecionalidad.

Rendición de cuentas: Proveeré la eficacia y la calidad en la gestión de la administración universitaria, contribuyendo a su mejora continua y a su modernización, teniendo como principios fundamentales la optimización de sus recursos y la rendición de cuentas.

Respeto: Respetaré sin excepción alguna la dignidad de la persona humana y los derechos y libertades que le son inherentes, siempre con trato amable y tolerancia para toda la comunidad universitaria.

Lealtad: Afirmo que todos mis actos se guían e inspiran por exaltar a la institución y a sus símbolos; así como el respeto a su Ley Orgánica y demás Normatividad que de ella emana y por la más firme creencia en la dignidad de la persona humana.

Responsabilidad: Acepto estar preparado para responder de todos mis actos de manera que la comunidad universitaria y la gente con que trato en particular, aumenten permanentemente su confianza en mí y en nuestra capacidad de servirles.

Competencia: Reconozco mi deber de ser competente, es decir, tener y demostrar los conocimientos y actitudes requeridos para el ejercicio eficiente de las funciones que desempeño, y actualizarlos permanentemente para aplicarlos al máximo de mi inteligencia y de mi esfuerzo.

Efectividad y Eficiencia: Comprometo la aplicación de mis conocimientos y experiencias de la mejor manera posible, para lograr que los fines y propósitos de la Universidad se cumplan con óptima calidad y en forma oportuna.

Manejo de recursos: Todos los recursos propiedad de la Universidad sin importar su origen, los aplicaré únicamente para la consecución de los objetivos institucionales.

Calidad del personal: Contrataré para los cargos de mi dependencia, sólo a quienes reúnan el perfil para desempeñarse con rectitud, aptitud y la actitud necesarios.

III. Responsabilidad hacia los compañeros de trabajo

Valor civil: Reconozco mi compromiso de ser solidario con mis compañeros y conciudadanos; pero admito mi deber de denunciar y no hacerme cómplice de todo aquel que contravenga los principios éticos y morales contenidos en este instrumento.

Igualdad: Haré regla invariable de mis actos y decisiones el procurar igualdad de oportunidades para todos los universitarios, sin distingo de sexo, edad, raza, credo, religión o preferencia política.

Probidad: Declaro que todos los recursos y fondos, documentos, bienes y cualquier otro material confiado a mi manejo o custodia debo tratarlos con absoluta probidad para conseguir el beneficio colectivo.

Diálogo: Privilegiaré el diálogo y la concertación en la resolución de conflictos.

Apéndice VIII

Normatividad del Web

NORMATIVIDAD Y LINEAMIENTOS GENERALES PARA USO DE PÁGINAS WEB EN LA FACULTAD DE INGENIERÍA

NOVIEMBRE DEL 2001

CONTENIDO

1.- GENERALES

El *World Wide Web*, o simplemente *Web*, como generalmente se denomina, es un servicio que se obtiene a través de Internet. Está formado por una colección de documentos (conocidos como páginas) interconectados que se encuentran almacenados en computadoras ubicadas por todas partes del mundo. Dichos documentos pueden contener texto, gráficos y sonidos, y son conocidos como páginas.

La Facultad de Ingeniería cuenta con una página principal de *Web* para publicar información sobre sus actividades académicas y culturales. A partir de esta, se tienen ligas a otras páginas relacionadas con la Facultad (Divisiones, Secretarías y de profesores, entre otras). Debido a la necesidad de mantener una presencia adecuada y una organización de la información en estas páginas, es preciso regular su diseño, contenido, y edición. Por tal motivo, todos los nodos que tengan funciones de servidores de *Web* de la Facultad de Ingeniería, deberán seguir los lineamientos contenidos en el presente documento.

El área responsable de la página Web de la Facultad de Ingeniería, es la **Secretaría General.** Como parte integrante de Secretaría General, la Unidad de Servicios de Cómputo Académico (UNICA), será la responsable técnica de la operación, seguridad y respaldos; el Departamento de Información y Estadística será la responsable de los contenidos y la Coordinación de Comunicación de la imagen gráfica institucional (ver detalles en el ANEXO 1).

La página de la Facultad de Ingeniería será el punto de partida para acceder a las demás páginas de Secretarías y Divisiones. Quedando estrictamente prohibido que las páginas de otras Divisiones o Secretarías que no sea la de la Secretaría General den la impresión de representar a la Facultad de Ingeniería en forma oficial. El formato acordado es:

PÁGINA PRINCIPAL

http://www.fi-a.unam.mx

PÁGINA SECUNDARIA

Los diseños de logos, fondos, imágenes etc., deben ser originales.

Cualquier caso no previsto en el presente documento, será resuelto por el Comité Asesor de Cómputo de la Facultad de Ingeniería. ***Y en caso específico del punto 2.2.3 por el Consejo Técnico y/o en su caso por la Comisión de Vigilancia de la elección correspondiente.***

2.- REGLAMENTO PARA LA PUBLICACIÓN DE PÁGINAS DE *WEB* EN LA FACULTAD DE INGENIERÍA

2.1 USUARIOS

Para que una persona pueda crear y/o mantener una página en la *Web* en la Facultad de Ingeniería, deberá ser miembro de la comunidad (alumno, personal académico o personal administrativo debidamente autorizado), y cumplir con:

* **PARA ALUMNOS:** Ser usuario de las salas de la red de cómputo de la Facultad de Ingeniería y su trabajo deberá estar avalado por un integrante del personal académico de la Facultad de Ingeniería.
* **PARA EL PERSONAL:** Identificarse como personal laboral activo de la Facultad de Ingeniería.

El solicitante debe llenar un formato en el área correspondiente en el que indique las razones por las cuales desea que su página se publique en algún servidor de *Web* de la Facultad de Ingeniería. Este formato deberá dirigirse al webmaster de la División o Secretaría, en la cual, quiera que aparezca su página. La página debe estar terminada por completo.

Será responsabilidad del webmaster que reciba esta solicitud, revisar el contenido de la página. No se publicará la página hasta que sea aprobada por el webmaster correspondiente. No se darán de alta páginas que estén bajo construcción.

En el caso de páginas dependientes de la página principal ver el procedimiento descrito en el ANEXO 2.

Los puntos que se tendrán en cuenta para su aprobación son los siguientes:

- La publicación de las páginas de los usuarios estará en función de la capacidad que se tenga en cuanto a espacio en los servidores de *Web*. Si el webmaster o el administrador de red consideran que los recursos del servidor no son suficientes, no se podrá publicar la página aunque esta cumpla con los demás requisitos. Por lo tanto, se debe recomendar a las personas interesadas en elaborar una página, que pregunte al webmaster correspondiente sobre los recursos de que puede disponer, incluyendo la cantidad máxima en disco duro que puede utilizar.
- El contenido de las páginas deberá ser **académico o de aplicación administrativa** de interés para la Facultad.
- El tema sobre el que trate la página será libre, con la restricción de no lucrar con el servicio que la Facultad le brinda.

  Nota: Salvo en aquellos proyectos especiales en que la Facultad de Ingeniería participe en convenios con la iniciativa privada.
- El objetivo, (y si es aplicable visión y misión) debe expresarse claramente.
- En el caso de páginas de contenido Institucional, siempre debe tenerse presente la imagen institucional, no personal de la información a publicar.
- Mantener el respeto que nos reconoce como universitarios.
- No se publicarán páginas que contengan errores ortográficos. En caso de encontrarlos, el webmaster le indicará al usuario que debe corregirlos.

- Toda página deberá estar escrita con un mínimo del 90% de idioma español. En caso de que se requiera publicar la información en otro idioma, se deberá contar con una referencia de cambio de idioma (icono, imagen, etc.)
- Las páginas no podrán dar a entender que representan en forma oficial a la Facultad de Ingeniería ni alguna de sus Divisiones o Secretarías. Por ello, queda prohibido el uso de escudos y logotipos de la Facultad, que en su apariencia sean similares a los de alguna Secretaría o División.
- Todas las páginas principales deben contar con una liga a la página principal y en todos los casos debe tener opción de retorno a la página principal si se hubiese accedido desde la página principal.
- Todas las páginas deben tener una firma de responsable.

Una vez aprobada la página, se aplicará lo siguiente:

- La permanencia de la página será de un semestre escolar.
- La renovación de la publicación de la página estará sujeta a los recursos disponibles en el servidor *Web* (ejemplo, espacio en disco duro).
- El usuario podrá promocionar su página en uno o varios exploradores de Internet. Cada usuario deberá realizar el procedimiento necesario para dar de alta su página en cada explorador, posteriormente deberá enviar un correo al administrador de *Web* correspondiente, notificando estas altas.
- El webmaster de la División o Secretaría en la cual se encuentre la página del usuario revisará periódicamente el contenido de las páginas. Si observa que el usuario realizó modificaciones que no cumplan con lo estipulado, tiene la facultad de desligar la página del usuario. En caso de reincidencia, se dará de baja su página permanentemente.

2.2 PUBLICACIÓN DE TRABAJOS EN LA *WEB*

2.2.1 PUBLICACIÓN DE INFORMACIÓN SOBRE ACTIVIDADES ACADÉMICAS Y CULTURALES EN LA *WEB*

Estas páginas contendrán información relacionada con las actividades de una Secretaría o División y aprobada por el representante del Comité Asesor de Cómputo del área en cuestión. El contenido del tema deberá estar avalado por un integrante del personal académico de la Facultad de Ingeniería.

2.2.2 TESIS

Este apartado se refiere a aquellas personas que hayan realizado su trabajo de tesis para publicarse en la *Web* y esté en alguna de las siguientes modalidades:

a) El contenido de la tesis esté diseñado para colocarse en la *Web*. No importando el tema.
b) Que la tesis en sí sea una aplicación en la *Web*.

b1) Aplicación o sistema externo que no tenga que ver con la Facultad de Ingeniería.

b2) Aplicación orientada para la *Web* de la Facultad de Ingeniería y se quiera incorporar de forma oficial.

Para dar de alta las páginas, los tesistas, deberán presentar una carta firmada por su director de tesis que avale su contenido. La carta deberá ser entregada al webmaster de la División o Secretaría donde se desee publicar la página.

En el caso de páginas dependientes de la página principal ver el procedimiento descrito en el ANEXO 2.

La duración de la publicación de la tesis en la *Web* será de al menos un semestre, condicionada a la normatividad vigente y quedando a consideración del webmaster la permanencia de la página en función de los recursos disponibles.

Para el caso en que la tesis se encuentre en el inciso b2, aplicará lo siguiente:

- Los tesistas tendrán que proporcionar una copia de los archivos de su aplicación.
- El trabajo de tesis será evaluado técnicamente en su funcionamiento por el webmaster y/o el administrador de red, para decidir si es conveniente incorporar su publicación en forma oficial en la página de la Facultad. En caso de que existan dos tesis con temas similares, se seleccionará la más apta funcionalmente, brindando el debido reconocimiento a su(s) autor(es).
- Los tesistas deben estar conscientes de que están cediendo su aplicación a la Facultad, por lo que esta puede ser actualizada, conservando sus correspondientes créditos.
- Las páginas de tesis incorporadas podrán ser referenciadas desde cualquier hoja de la Facultad.

2.2.3 PROSELITISMO ACADÉMICO Y ESTUDIANTIL PARA ELECCIONES

Para la publicación de páginas en WEB en los servidores de la Facultad y que tenga como fin realizar proselitismo electoral a favor de alguna fórmula que participe en los diferentes procesos electorales que se llevan a cabo en la dependencia, se deberán tomar en cuenta las siguientes observaciones:

a) No utilizar logotipos de la Facultad o de la Universidad.
b) El periodo de permanencia y el contenido estará sujeta a lo establecido en el capítulo referente a propaganda electoral de la convocatoria respectiva.
c) La página deberá sujetarse a lo establecido en el presente reglamento.

Las páginas de la WEB residentes fuera de la Universidad también deberán apegarse a los incisos a) y b).

3.- SUGERENCIAS TÉCNICAS PARA LA PUBLICACIÓN DE LAS PÁGINAS *WEB* EN LA FACULTAD DE INGENIERÍA

Esta sección presenta sugerencias técnicas para el desarrollo de páginas *Web,* empleando el lenguaje de programación HTML, con el fin de dar un mejor soporte en la organización, diseño e integridad de la información que se habrá de presentar al concluir la construcción de una página. Se hace la aclaración de que estas sugerencias se realizan vigentes a la fecha del presente documento, lo cual se debe de tener en consideración, debido a la dinámica que existe en el área de cómputo.

El lenguaje de programación HTML proporciona diversas herramientas para la creación de una página de *Web* y el objetivo principal es sugerir el uso óptimo de éstas.

IDEAS DE ORGANIZACIÓN

Elementos para una mejor presentación en línea

- Ortografía y redacción.
- Escribir con claridad y ser breve. Organización óptima para evitar la pérdida de los objetivos.
- Estructura de autosoporte.
- Resaltar sólo lo importante.
- Tomar en cuenta las plataformas en las que se pueda estar visualizando su página.
- Diseño y formato.
    - * Imágenes.
    - * Encabezados.
    - * Agrupación de la información congruente.
    - * Formato constante.
    - * Vínculos correctos.
        - ° División en las mismas páginas.
        - ° Generación de documentos vinculados.
        - ° Estructuras.

ORTOGRAFÍA Y REDACCIÓN

Cuando se consulta una página *Web*, generalmente la primera impresión que se recibe es básica para continuar revisándola, pero por muy buena presentación que ésta tenga, si contiene errores ortográficos el usuario podría optar por cancelar la exploración. La buena ortografía habla bien del diseñador de la página. Por lo que es recomendable dar a leer el texto a otra persona para que ésta detecte posibles errores de redacción y ortografía.

CLARIDAD Y BREVEDAD EN EL TEXTO

Una página *Web* debe ser prometedora para aquellos que la consulten, por lo que se recomienda ser concisos y directos, debido a que un mensaje efectivo expresa una idea con las palabras adecuadas y con brevedad. Por otra parte, entre más "cargada" sea una página, mayor será su tiempo de despliegue, lo que puede provocar la desesperación del usuario.

Si una página requiere definiciones densas o largas explicaciones, se puede introducir dicha información dentro de archivos externos, los cuales se pueden llamar con un FTP (empleando el URL apropiado), indicando el tamaño de los archivos, esto ayuda al usuario a calcular el tiempo que requiere la transferencia. El usuario puede entonces decidir si realmente desea el archivo, cuándo programar la carga y cuánto espacio mínimo disponible necesita en su disco duro.

Es recomendable que dentro de la página los encabezados y los títulos den una idea concisa del objetivo de la página, ésta debe seguir la regla de brevedad y claridad. En esta parte se puede hacer uso de las herramientas que nos proporciona HTML para resaltar ideas: tipo y tamaño de letra, imágenes (se aplica la frase de que una imagen dice más que mil palabras), listas de elementos las cuales pueden servir para tener un contexto general del contenido, etc.

También se puede hacer uso de listas para realizar menús de las anclas que se hacen dentro de la página.

Se recomienda colocar la información más importante al inicio de los párrafos y organizar la información, para hacer más ligera la exploración de la página.

ESTRUCTURA DE AUTOSOPORTE

La búsqueda de tópicos en Internet puede dar lugar a acceder a un hipertexto en cualquier punto de su estructura, y no precisamente al inicio de ésta. Por lo tanto, no necesariamente alguien que explore la página lo hará en orden progresivo. Entonces, si una página no se sostiene por si misma y depende de las anteriores, el objetivo inicial del lector al abrirla estará perdido y decidirá buscar otra que satisfaga su necesidad de conocimiento. Lo anterior se puede evitar otorgando independencia a cada parte del hipertexto:

⇒ Utilizar títulos descriptivos y encabezados con la relación que guarda con las otras páginas.
⇒ Si existe una dependencia inevitable, se deben proporcionar los vínculos básicos:
  ◊ Con la página que depende inmediatamente en forma vertical.
  ◊ Con la página principal de la presentación.
⇒ Evitar frases de dependencia a párrafos o páginas anteriores o posteriores, es decir, que si con frases se hace alusión a información de otras páginas sin explicarlo, el usuario se confundirá.

Tomar en cuenta que no todos emplearán el mismo visualizador. Cada visualizador posee características que lo hacen diferente de los demás. Si dentro de una presentación se hace mención de éstas, como formas de navegación, se estará individualizando la exploración del hipertexto. Por ejemplo, se puede sustituir el "haga click..." por "seleccione". No hacer mención de los colores ya que no todos los monitores son multicromáticos. Tomar en cuenta que los visualizadores tienen distintas formas de acceder los vínculos, es decir, no se debe hacer mención de las especificaciones gráficas de algún vínculo. También se debe evitar hacer mención de los comandos que posee un visualizador para ejecutar acciones.

Para el acceso de páginas con imágenes se debe tener en cuenta que no todos los monitores tienen la misma resolución y dimensiones.

DISEÑO Y FORMATO DE LA PÁGINA:

La regla básica para un diseño exitoso en una presentación es hacer el diseño tan sencillo como sea posible, reducir la cantidad de elementos (imágenes, encabezados, plecas) y asegurarse de que sólo las cosas más importantes se enfaticen en el formato.

Imágenes

Igual que la carga de texto, el exceso de imágenes dentro de una página toma mucho tiempo en terminar de acceder; tiempo valioso para el usuario, por lo tanto, se debe reducir el uso de imágenes a la necesidad real de ellas dentro de la página. Evite desviar la atención del usuario con imágenes innecesarias.

Considere el tamaño de las imágenes en dimensiones y en variedad de colores, la transferencia de archivos gráficos pequeños es más rápida. Si se considera que un archivo de 20KB tarda varios segundos en desplegarse con un enlace SLIP de 14.4K baudios, al multiplicar este tiempo por cada una de las imágenes que despliega una página se puede tener una idea del tiempo que tomaría el explorarla. Es por ello que se recomiendan 20KB de tamaño máximo para las imágenes. La cantidad de imágenes en una presentación sigue la regla del cuestionario: preguntarse si realmente son necesarias, si pueden ser sustituidas por texto y qué tanto mejoran el diseño de la página.

Encabezados

Los encabezados ayudan al usuario a llevar un registro de dónde se encuentra dentro del hipertexto, describen cómo se relaciona dicho archivo con todo el documento y proporcionan un ambiente de trabajo más agradable cuando las páginas son fáciles de usar. Los encabezados claros ayudan al usuario a saber qué es lo que está viendo y si están redactados apropiadamente, describen en forma concisa el contenido o la función del archivo.

Agrupación de la información congruente

Cuando se introduce información en una página *Web*, se necesita alcanzar ciertos niveles mínimos de calidad si desea llamar la atención de la gente.

Agrupar la información que guarda cierta relación es una tarea que se realiza tanto en la redacción del documento como en el diseño del mismo. Al agrupar la información congruente bajo un mismo encabezado hace que la misma sea más fácil de rastrear. Si una página de la *Web* contiene varias secciones con información distinta, se debe buscar la manera de separar visualmente esas secciones por medio de un encabezado o una línea horizontal.

Formato constante

El principal objetivo de hacer esto es que el usuario sepa que aún se encuentra en su documento y no se ha perdido en algún vínculo que encontró en su página.

a) Logotipo o imágenes que identifiquen su documento. Intente agregarlas en cada una de sus páginas, de preferencia en el mismo lugar.
b) El mismo fondo para todas las páginas de su documento es un buen tip para dar un formato constante.
c) Si existen vínculos de relación entre las páginas de su hipertexto, procure ponerlos siempre en el mismo sitio.
d)Los títulos de las páginas se sugieren antecedidos de una frase consistente.

Vínculos correctos

Verificar si los vínculos son necesarios o únicamente es información redundante o de más, pues cada vínculo debe cumplir un propósito bien definido. Genere vínculos por razones de importancia. Además, si un vínculo no tiene importancia para el contenido que se está tratando sólo servirá para confundir al lector.

- Vínculos de navegación explícitos: Son los que le muestran al lector hacia dónde se debe mover desde cualquier página a otra del mismo documento (Atrás, Adelante, etc) .
- Vínculos de navegación implícitos: Indican que al ser seleccionado se obtendrá mayor información sobre el tema que se está tratando, pero no es necesario que las palabras que conforman el texto del mismo lo digan literalmente.
- Vínculos para definiciones de palabra o concepto: Sirven para incluir glosarios, al vincular la primera aparición de una palabra dada dentro del documento a su definición en algún otro lugar de la red.
- Vínculos tangentes o de información relacionada: son útiles cuando cierta parte del texto se aparta del propósito fundamental del documento, sólo es información adicional que el lector decidirá si se consulta o no.

Características de los vínculos

- Texto breve. Ser descriptivo.
- Usar menús de vínculos, es decir, organizarlos según el tema del que se trate en forma de lista o algún otro formato breve.
- No usar vínculos ambiguos, se necesita ser conciso en los nombres o texto de los vínculos.
- Evitar la tendencia a crear vínculos con una sola palabra "aquí" resaltada, para describirlo después en algún lugar incierto.
- Se debe estar consciente de que no todos los usuarios tendrán la posibilidad de oprimir o hacer click con el mouse, ya que algunos usuarios estarán empleando un visualizador en modo texto.
- Son de gran importancia los vínculos de navegación: Atrás (back), Home, Adelante (forward). Éstos nos guiarán dentro de la página *Web*, el uso correcto de estos vínculos producirá un mejor entendimiento, mayor atracción al usuario y sobre todo el cumplimiento del objetivo individual de la página. Así no se ocasiona la pérdida de algunos objetivos o la del interés por parte del usuario al ocuparse en buscar la página que le antecede a la actual, o por ejemplo si no existe un vínculo que lleve a la página HOME después de haber consultado la información tendrá que recorrer las demás páginas verticalmente hasta llegar a la página principal y poder iniciar una búsqueda horizontal.
- Adicionar un vínculo "mailto" para correo electrónico que permita cumplir con uno de los objetivos de la *Web*: ser interactivo con el creador de la página.

División en las mismas páginas

Esta parte se refiere a la gran ventaja que trae consigo el reducir el número de páginas dentro de su documento, de tal forma que puedan existir ligas a una misma página para representar información distinta. Así es más fácil manejar un único documento y los vínculos que contengan no se romperán si mueve los elementos o renombra los archivos. Una página presentada de esta forma se asemeja más a la estructura de un documento impreso común; si se debe distribuir documentos tanto de forma impresa como en línea.

También existen desventajas por seguir esta metodología, ya que vuelve a aparecer el tiempo de carga que lógicamente se exagerará, además de que se forma una estructura bastante rígida empleando una estructura lineal.

Tipo de Estructuras recomendadas

Estructura lineal de documentos de varias páginas. El usuario avanza o retrocede por los archivos como si estuviera dando vuelta a las páginas de un libro. Un archivo HTML sigue a otro. Cada archivo HTML, contiene un vínculo a los archivos anterior y siguiente. Usted determina el orden en el que se presenta la información.

Estructura no lineal de documentos de varias páginas. En esta estructura el usuario pasa de una página a otra, también determinará el orden en el que desea que se le presente la información, según las posibilidades que el documento le ofrezca.

Las ventajas de crear una estructura no lineal son que los documentos pequeños se cargan con mayor rapidez, mejor rastreo de información para el usuario.

Pero también existen desventajas y éstas pueden ser por ejemplo que es más complicado manejar vínculos externos que internos, y sobre todo si son una gran cantidad, además que demasiados saltos pueden distraer al usuario de su objetivo inicial, como ya se había mencionado.

Rigidez en la presentación:

El tiempo que tarde en desplegarse la información completa de la página es importante tanto para el creador como para el usuario, debido a la diversidad de páginas que se pueden encontrar en la red.

Existen diseños de páginas que se presentan empleando la herramienta FRAMES, lo que toma mayor tiempo de carga. Para esto se sugiere añadir la posibilidad de que el usuario elija la forma en que quiere que se despliegue la página que visita, es decir, dar la posibilidad de que la misma página se presente en una forma menos rígida NOFRAMES, quizás menos atractiva, pero si con mayor facilidad y rapidez en el manejo.

ANEXO 1

CONSIDERACIONES SOBRE LA PÁGINA PRINCIPAL WEB DE LA FACULTAD DE INGENIERÍA

El Departamento de Información y Estadística tendrá las siguientes funciones en la Web principal de la Facultad de Ingeniería:

Planear el contenido de la página principal de la Facultad de Ingeniería, así como establecer la estructura de las páginas.

Dar de alta las ligas de las páginas que tengan los Vo.Bo. de la Secretaría General correspondientes en las que se incluyen las de las divisiones, profesores, asociaciones, tesistas, alumnos etc.; y cualquier página que se desee depender de la página principal.

Dar la ubicación de las nuevas páginas dentro de la estructura de la página principal.

Actualizar y mantener el contenido de las páginas de la Web principal de la Facultad de Ingeniería.

Administrar las cuentas de correo y la Web de fainge y webmaster (fainge@cancun.fi-a.unam.mx y webmaster@cancun.fi-a.unam.mx)

Deshabilitar las páginas que rompan con la normatividad de la Web.

La Unidad de Servicios de Cómputo Académico tendrá las siguientes funciones en la Web principal de la Facultad de Ingeniería:

Mantener la operación Física del servidor de la Web.

Instalar, mantener y actualizar el sistema operativo del servidor

Instalar, mantener y actualizar el software de administración de la Web.

Implementar la Seguridad del Sitio Web y el Sistema Operativo, así como la revisión de bitácoras.

Instalar las aplicaciones requeridas para la operación del sitio Web.

Realizar los respaldos del servidor Web.

Asesorar técnicamente a las áreas de la Facultad en tópicos relacionados con la Web.

Proponer nuevas innovaciones de tecnología para crear servicios de la Web para el beneficio de la Facultad (como el caso de la Biblioteca Digital, Búsqueda, Bolsa de trabajo etc.)

Actualizar y mantener el área de la Web correspondiente a UNICA.

La Coordinación de Comunicación tendrá las siguientes funciones en la Web principal de la Facultad de Ingeniería:

Diseñar la imagen gráfica institucional.

Crear, diseñar, recabar las imágenes como fotos, backgrounds, íconos, etc. que se usarán en el sitio de la Web.

ANEXO 2

PROCEDIMIENTO PARA DAR DE ALTA PÁGINAS EN SITIO WEB PRINCIPAL DE LA FACULTAD DE INGENIERÍA

El contenido de las páginas deberá ser académico o de aplicación administrativa y con objetivos afines a los de la Facultad (docencia, investigación y difusión de la cultura).

En todos los casos, la creación, mantenimiento y diseño de la página serán responsabilidad del solicitante. No se darán de alta páginas que estén bajo construcción.

Para dar de alta páginas dependientes de la página principal deberá seguirse el siguiente procedimiento:

El solicitante deberá enviar un oficio dirigido a la Secretaría General donde indicará:

Objetivos de la página.
Breve descripción de la página
Responsable de la página (nombre, teléfono y correo electrónico)

La página debe estar terminada por completo en caso de que ya cuente con un sitio de Web.

En el caso del personal académico:

Si la página de la Web es personal, deberá tener la siguiente leyenda al Inicio:

" El contenido de esta página es responsabilidad del Autor"

Autor:
Cargo- División o área:

Las páginas podrán contener tareas, apuntes personales, ejercicios, ligas de apoyo a la materia o cualquier otra actividad que apoye su actividad de académico.

Las páginas deberán ser alojadas primeramente en los servidores de la división al cual pertenece el académico.

En caso de que la División o Secretaría no contase con la infraestructura necesaria, el solicitante podrá manifestar el requerimiento de una cuenta para el alojamiento de su página. Las cuentas estarán sujetas de acuerdo a los recursos e infraestructura con que cuente la Facultad y a sus condiciones de operación. La cuenta será intransferible y deberá apegarse a la normatividad de la Web vigente.

El archivo principal de la cuenta deberá llamarse index.html y deberá estar ubicado en el subdirectorio WWW en su directorio casa (home directory).

La página deberá renovarse al inicio de cada año escolar.

ANEXO 3

LOS ADMINISTRADORES DE LA *WEB*

Este apartado se refiere a aquellas personas que coordinan la publicación de páginas en la *Web*, conocidas como administradores de la *Web* o webmasters.

Para una mejor administración de la *Web* en la Facultad de Ingeniería, se creó el subcomité de webmasters, el cual es un grupo de administradores de la *Web*, cada elemento integrante representando a una Secretaría o División. Este subcomité del Comité Asesor de Cómputo es el encargado de apoyar en los temas relacionados con la estructuración, presentación y contenido de las páginas de la Facultad, y tiene como objetivos, los siguientes:

- Llevar a cabo la normalización de la administración de la *Web* en la Facultad de Ingeniería.
- Participar en la normatividad de la *Web*.
- Administrar de manera óptima los recursos que tiene la Facultad destinados a la *Web*.
- Control de la información que se publicará en la *Web*.

El subcomité de webmasters estará presidido por el webmaster de la Secretaría General, quien fungirá como moderador de las juntas y tomará nota de los acuerdos a los que se llegue. Estos acuerdos se tomarán como base para la creación de todas las páginas que dependan de la Facultad de Ingeniería.

Entre algunas de las funciones que tienen los webmaster, se encuentran:

* Creación, mantenimiento y control de las páginas del área a la cual pertenecen.

* Asistir a las juntas de webmasters, las cuales serán al menos una vez por mes.

* Estar pendiente de la información e instrucciones de las áreas correspondientes a efecto de incluir, modificar y borrar oportunamente la página correspondiente.

* Responder los correos que les sean enviados, relacionados con el área a la cual pertenezcan. En caso de que no tuviesen la información que se les solicita, indicarán el nombre de alguna persona que pueda resolver la duda.

* Calificar técnicamente y en su caso dar de alta las páginas de los usuarios.

* Hacer del conocimiento de los usuarios el reglamento que deben cumplir para poder tener derecho a la publicación de sus páginas.

* Revisar periódicamente las páginas de los usuarios en su área, con la facultad de desactivar aquellas que no cumplan con los lineamientos del presente documento.

* El webmaster de la Secretaría General podrá reconvenir sobre la estructura y contenidos de las páginas, siempre que éstas no se apeguen a los lineamientos que se indiquen en el presente documento. Tiene además la facultad de deshabilitar páginas que no cumplan con los lineamientos establecidos.

En la reunión del Comité Asesor de Cómputo, efectuada el 8 de noviembre del 2001, los Integrantes de las áreas del comité dan su visto bueno (VoBo.) del documento **"NORMATIVIDAD Y LINEAMIENTOS GENERALES PARA USO DE PÁGINAS *WEB* EN LA FACULTAD DE INGENIERÍA.**

NOMBRE	ÁREA	FIRMA

Apéndice IX

Hackers y Crackers famosos

HACKERS Y CRACKERS FAMOSOS

CRACKERS

DRAPER JOHN, "CAPTAIN CRUNCH"

En septiembre de 1970 John Draper, conocido como Captain Crunch, descubre que el obsequio ofrecido en las cajas de cereal Captain Crunch (un silbato) duplica perfectamente la frecuencia de tono de 2600 Hz, permitiéndole hacer llamadas telefónicas gratis y la víctima era AT&T. Este descubrimiento llevó a John a crear la primera "Blue Box" una caja electrónica mágica para los teléfonos.

HOLLAND WAU Y WENERY STEFFEN

"Lo logramos, por fin ... Sólo hay algo seguro, la infinita inseguridad de la seguridad". Fue lo que escribió Wau Holland, en su cuaderno de notas, el 2 de mayo de 1987. Los dos hackers alemanes, de 23 y 20 años respectivamente, habían ingresado sin autorización al sistema de la central de investigación aeroespacial más grande del mundo (NASA).

¿Por qué lo hicieron?, "Porque es fascinante, la única aventura posible está en la pantalla de una computadora", respondieron.

Cuando Wau y Steffen advirtieron que los técnicos los habían detectado, le enviaron un telex, avisando de su intrusión.

ING-HOU CHEN

Taipei, Taiwan, Abril 30 de 1999. El autor del virus "Chernobyl", dijo a los investigadores que el creó el bug con la esperanza de humillar y vengarse de los que llamó "proveedores incompetentes de antivirus para software". Pero él admitió que no esperaba que CIH (iniciales de su autor) causara daño alrededor del mundo. Este virus devastó cientos de miles de computadoras alrededor del mundo.

Chen creó el virus en Abril, cuando todavía era estudiante de ingeniería computacional en el Instituto Tecnológico.

Este inusual virus destructivo, programado para funcionar el 26 de Abril, (13° aniversario del desastre nuclear de Chernobyl), trata de borrar el disco rígido y escribir "basura" en algunos otros componentes, evitando de este modo el futuro encendido de la computadora.

KEVIN Y RONALD

Ronald y Kevin, con los nombres de guerra Makeveli y TooShort en el ciberespacio, asaltaron las computadoras del Pentágono en marzo del año 1998, a la tierna edad de 17 años. Estos dos forajidos virtuales, con sus conocimientos y con un equipo básico informático, se introdujeron en cuatro sistemas de la Marina y siete de las fuerzas aéreas, relacionados con centros digitales en Estados Unidos y Okinawa.

LA MACCHIA DAVID

En 1994 David La Macchia, estudiante de 20 años del prestigioso y serio MIT, reconoce que ha distribuido en Internet multitud de programas informáticos obtenidos sin licencia y por valor de un millón de dólares. Para ofrecerlos a los cibernautas montó su propia BBS.

LEVIN VLADIMIR

Un matemático ruso de 24 años, penetró vía Internet desde San Petersburgo en los sistemas informáticos centrales del banco Citybank en Wall Street. Este pirata logró transferir a diferentes cuentas de EE.UU., Rusia, Finlandia, Alemania, Israel, Holanda y Suiza fondos por valor de 10 millones de dólares, según el FBI. Detenido en el Reino Unido a principios de 1995.

MITNICK KEVIN, "EL CÓNDOR", "EL CHACAL DE LA RED"

Como hacker, la carrera de Mitnick tiene sus inicios en 1980 cuando apenas contaba con 16 años y, obsesionado por las redes de computadoras, rompió la seguridad del sistema administrativo de su colegio, pero no para alterar sus notas, lo hizo "sólo para mirar".

La primera vez que lo detuvieron fue en 1981 por robar manuales de la Pacific Telephone. La información robada tenía un valor equivalente a los 200 mil dólares y tuvo que cumplir una condena de tres meses de cárcel y un año bajo libertad condicional.

En 1983 intentó ingresar en las computadoras de la Universidad de California del Sur y poco después penetró el sistema de la agencia de créditos TRW.

En 1987 lo condenaron a treinta y seis meses de libertad condicional por robo de software, tras hackear los sistemas del Departamento de Defensa de EE.UU. y la NASA.

Un año más tarde fue arrestado de nuevo cuando era estudiante de la Universidad del Sur de California. En esta ocasión entró ilegalmente a ARPAnet (la predecesora de Internet) y trató de acceder a la computadora del Pentágono. Lo sentenciaron a seis meses de cárcel en una prisión juvenil en California.

Durante ese tiempo le negaron el acceso a los teléfonos y a lo largo de los doce meses de rehabilitación no pudo acercarse a una computadora.

Más tarde, ya en libertad, se apoderó de 16 códigos de seguridad de MCI y junto a un amigo, Jenny Dicicco, entraron a la red del laboratorio de investigaciones de Digital Corporation, conocida como Easynet.

Ambos hackers querían obtener una copia del prototipo del nuevo sistema operativo de seguridad de Digital llamado VMS. El personal de seguridad de Digital se dio cuenta inmediatamente del ataque y dieron aviso al FBI, y comenzaron a rastrear a los hackers.

Mitnick fue arrestado en 1998 por invadir el sistema de Digital Equipment. La empresa acusó a Mitnick y a DiCicco ante un juez federal de causarles daños por 4 millones de dólares en el robo de su sistema operativo. Fue declarado, culpable de un cargo de fraude en computadoras y de uno por posesión ilegal de códigos de acceso de larga distancia.

Adicional a la sentencia el fiscal obtuvo una orden de la corte que prohibía a Mitnick el uso del teléfono en la prisión alegando que el prisionero podría obtener acceso a las computadoras a través de cualquier teléfono. A petición de Mitnick el juez lo autorizó a llamar únicamente a su abogado, a su esposa, a su madre y a su abuela y sólo bajo supervisiones de un oficial de la prisión.

Este caso produjo revuelo en los Estados Unidos, no sólo por el hecho delictivo sino por la táctica que utilizó la defensa. Su abogado convenció al juez que Mitnick sufría de una adicción por las computadoras equivalente a la de un drogadicto, un alcohólico o un apostador. Gracias a esta maniobra de la defensa, Mitnick fue sentenciado a sólo un año de prisión y al salir de allí debía seguir un programa de seis meses para tratar su "adicción a las computadoras". Durante su tratamiento le fue prohibido tocar una computadora o un módem y llegó a perder más de 45 kilos.

Para 1991 ya era el hacker que había ocupado la primera plana del New York Times y uno de sus reporteros, Jonh Markoff, decidió escribir un libro de estilo Cyberpunk narrando las aventuras de Mitnick. Al parecer a Mitnick no le gustó el libro ya que luego de salir a la venta, la cuenta en Internet de Markoff fue invadida, cambiando su nivel de acceso, de manera que cualquier persona en el mundo conectada a Internet podía ver su correo electrónico.

En 1992, y luego de concluir su programa, Mitnick comenzó a trabajar en una agencia de detectives. Pronto se descubrió un manejo ilegal en el uso de la base de datos y fue objeto de una investigación por parte del FBI quien determinó que había violado los términos de su libertad condicional. Se ofreció una recompensa de 1 millón de dólares a quien arrestara a Mitnick.

Luego de convertirse en prófugo de la justicia cambió de táctica y concluyó que la mejor manera de no ser rastreado era utilizando teléfonos celulares.

Luego de varios intentos infructuosos, en cuanto a calidad de información, se encontró con la computadora de Tsutomu Shimomura la cual invadió en la Navidad de 1994. Shimomura, físico computista y experto en sistemas de seguridad del San Diego Supercomputer Center, era además un muy buen hacker, pero era de los "chicos buenos", ya que cuando hallaba una falla de seguridad en algún sistema lo reportaba a las autoridades, no a otros hackers.

Shimomura notó que alguien había invadido su computadora en su ausencia, utilizando un método de intrusión muy sofisticado y que él nunca antes había visto. El intruso le había robado su correo electrónico, software para el control de teléfonos celulares y varias herramientas de seguridad en Internet. Allí comenzó la cuenta regresiva para Mitnick. Shimomura se propuso como orgullo personal atrapar al hacker que había invadido su privacidad.

Más tarde, el 16 de febrero de 1995, Mitnick fue capturado, juzgado y condenado a 25 años de prisión, lejos de computadoras y teléfonos.

Pero, el 22 de marzo de 1999, se consigue un acuerdo con jueces y fiscales. Los términos concretos se desconocen, pero se sabe que en marzo de 2000 Mitnick quedaría en libertad con la condición irrevocable de no poder acercarse a una computadora.

Kevin Mitnick, este sencillo nombre, oculta la verdadera identidad de uno de los mayores crackers de la historia. Fue una de las mayores pesadillas del Departamento de Justicia de los Estados Unidos. Entró virtualmente en una base de misiles, llegó a falsificar 20,000 números de tarjetas de crédito y a causar pérdidas millonarias a varias empresas.

MORRIS ROBERT

En noviembre de 1988, Morris lanzó un programa "gusano", diseñado por él mismo, buscando debilidades en sistemas de seguridad, y que pudiera ejecutarse y multiplicarse por sí solo. La expansión exponencial de este programa causó el consumo de los recursos de más de 6000 sistemas, los cuales resultaron dañados o fueron seriamente perjudicados. Eliminar al gusano de sus computadoras causó a las víctimas muchos días de productividad perdidos, millones de dólares.

Como consecuencia, se creó el CERT (Equipo de Respuesta de Emergencias Computacionales) para combatir problemas similares en el futuro. Morris fue condenado y sentenciado a tres años de libertad condicional, 400 horas de servicio comunitario y US $10000 de fianza, bajo el cargo de fraude computacional y abuso. La sentencia fue fuertemente criticada debido a que fue muy ligera, pero reflejaba lo inocuo de las intenciones de Morris más que el daño causado.

MURPHY IAN, "CAPTAIN ZAP"

En julio de 1981 Ian Murphy, un muchacho de 23 años que se autodenominaba "Captain Zap", gana notoriedad cuando entra a los sistemas en la Casa Blanca, el Pentágono, BellSouth Corp. TRW y deliberadamente deja su currículum.

En 1981, no había leyes muy claras para prevenir el acceso no autorizado a las computadoras militares o gubernamentales. "Captain Zap" mostró la necesidad de hacer más clara la legislación. Con cargos de robo de propiedad, finalmente, Murphy fue multado por US$ 1000 y sentenciado a 2½ años de prueba.

"PAINT" Y "HAGIS"

Estos son los seudónimos de los dos hackers que el 10 de Diciembre de 1997 accedieron a uno de los buscadores mas utilizados en Internet. Los terroristas informáticos autodenominados "Paints & Hagis", accedieron al servidor del popular navegador Yahoo! Y dejaron un mensaje amenazante a los casuales visitantes.

Este ataque no resultó ser más que una modificación de una página Web, y un ejemplo temprano de las muchas que se modifican hoy día a día.

PETERSON JUSTIN TANNER, "AGENT STEAL"

Peterson crackeaba las agencias de crédito. Esta falta de personalidad le llevó a su caída y a la de otros. Tiempo después, se dice, obtuvo un trato con el FBI. Esto le facilitó su salida de la cárcel y "no" pudo ser demostrado un fraude mediante una transferencia de dinero.

POULSEN KEVIN, "DARK DANTE"

En diciembre de 1992 Kevin Poulsen fue acusado de robar órdenes de tarea relacionadas con un ejercicio de la fuerza aérea militar americana. Se acusó Poulsen del robo de información nacional bajo una sección del estatuto de espionaje federal y fue condenado a 10 años en la cárcel (salió bajo palabra a los 5 años).

Como cracker, siguió el mismo camino que Kevin Mitnick, pero fue más conocido por su habilidad para controlar el sistema telefónico de Pacific Bell. Incluso llegó a "ganar" un Porsche en un concurso radiofónico, si su llamada era la 102, y así fue. Poulsen también crackeó todo tipo de sitios, pero él se interesaba por los que contenían material de defensa nacional. Esto fue lo que lo llevó a su estancia en la cárcel, 5 años. Fue liberado en 1996, supuestamente "reformado".

SMITH DAVID

Programador de 30 años, detenido por el FBI y acusado de crear y distribuir el virus que ha bloqueado a miles de cuentas de correo, "Melissa". Entre los cargos presentados contra él, figuran el de "bloquear las comunicaciones públicas" y de "dañar los sistemas informáticos". Acusaciones que en caso de demostrarse en el tribunal podrían acarrearle una pena de hasta 10 años de cárcel.

Por el momento y a la espera de la decisión que hubiese tomado el juez, David Smith está en libertad bajo fianza de US$ 10,000. Melissa en su "corta vida" había conseguido contaminar a más 100,000 computadoras de todo el mundo, incluyendo a empresas como Microsoft, Intel, Compaq, administraciones públicas estadounidenses como la del gobierno del estado de Dakota del Norte y el Departamento del Tesoro.

Sin embargo, la detención de Smith no significa que el virus haya dejado de actuar. Compañías informáticas siguen alertando que aún pueden quedar miles de usuarios expuestos a sus efectos, por desconocimiento o por no haber instalado en sus equipos sistemas antivíricos que frenen la actividad de Melissa u otros virus, que han venido apareciendo últimamente como Happy99 o Papa.

THE MENTOR Y GRUPO H4G13

El autodenominado grupo H4G13, con Mentor a su cabeza quería demostrar hasta donde eran capaces de llegar, y lo dejaron plasmado de una manera efectiva, colocando en la página principal de la NASA, durante media hora, el "manifiesto" hacker más conocido hasta el momento.

ZINN HERBERT, "SHADOWHACK"

Herbert Zinn, (expulsado de la educación media superior), y que operaba bajo el seudónimo de "Shadowhack", fue el primer sentenciado bajo el cargo de fraude computacional y abuso. Zinn tenía 16 años cuando violó el acceso a AT&T y los sistemas del Departamento de Defensa. Fue sentenciado el 23 de enero de 1989, por la destrucción del equivalente a US$ 174,000 en archivos, copias de programas, los cuales estaban valuados en millones de dólares. Además, publicó contraseñas e instrucciones de cómo violar la seguridad de los sistemas computacionales. Zinn fue sentenciado a 9 meses de cárcel y a una fianza de US$ 10,000.

HACKERS

ABENE MARK, "PHIBER OPTIK"

Mark Abene, conocido como **Phiber Optik**, a la edad de 17 años se convirtió en un genio de la computación y de la tecnología telefónica. Lideró en New York, al grupo de hackers denominado "Master of Deception", MOD (Maestros de la Decepción).

El grupo ocupó las primeras planas cuando en Noviembre de 1989, hizo colapsar las computadoras de WNET, uno de los principales canales de televisión de la ciudad de New York, dejando un mensaje "**Happy Thanksgiving you turkeys, from all of us at MOD**" (Feliz Día de Acción de Gracias a Uds. pavos, de parte de todos nosotros en MOD).

Como miembro fundador del grupo Masters of Deception, Phiber Optik inspiró a miles de adolescentes alrededor de los Estados Unidos, a "estudiar" los mecanismos internos de los sistemas telefónicos de todo el país.

Un juez federal intentó "enviar un mensaje" a otros hackers al sentenciarlo a un año de prisión, pero el mensaje fue desatendido: cientos de adherentes organizaron una fiesta de bienvenida en honor a Abene, en un club de primera clase en la ciudad de Manhattan.

Muy poco después, una revista de New York lo catalogó, como "una de las 100 personas más inteligentes de la nación".

En Julio de 1992, Abene y cuatro miembros de MOD fueron arrestados por una serie de cargos criminales. Abene se declaró culpable de los cargos federales de acceso desautorizado a computadoras de la compañía de teléfonos, incursión a computadoras y conspiración. Mark Abene pasó 10 meses en la prisión del condado Schuylkill de Pennsylvania, donde recibió tantas visitas y concedió entrevistas a periodistas y reporteros de canales de televisión, que sus compañeros de celda los apodaron CNN.

En una tienda del condado de Queens en New York, donde trabajaba su madre, se encontraron las primeras computadoras usadas por Abene: una Apple II, la Timex Sinclair y una Commodore 64. Aunque el primer equipo de Mark fue una Radio Shack TSR 80.

También había un receptor telefónico tantas veces usado, que tenía una cinta plástica enrollada para sostener sus partes internas, desgastadas por el excesivo uso. Mark Abene era un experto en patrones de discado en receptores telefónicos.

"Los crímenes de Hacking", manifestó el juez Stanton, "constituyen una real amenaza a la **creciente súper carretera de la información**".

Al negársele el uso de una computadora mientras estuvo en prisión, Mark Abene se convirtió en un héroe muy popular. Al salir en libertad fue empleado por su amigo Stacy Horn, del BBS denominado ECHO. Las hazañas de Abene le dieron tanta fama, que inspiraron a Michelle Slatalla y Joshua Quittne a escribir un libro titulado "**The Gang That Ruled Cyberspace**" (La Banda que dominó el Ciberespacio).

ARDITA JULIO CÉSAR, "EL GRITÓN"

Es considerado el hacker más famoso de Argentina. Nació en Río Gallegos, el 28 de marzo de 1974. Utilizó su primera computadora mientras estudiaba la secundaria. En quinto año, junto con dos compañeros ayudaron a informatizar el sistema de notas y facturación del colegio en el cual estudiaba.

Este muchacho, saltó a la fama el 28 de diciembre de 1995, día de los Santos Inocentes, cuando su domicilio fue allanado por la justicia argentina, luego de que Estados Unidos alertará sobre reiteradas intrusiones a varias de sus redes informáticas de Defensa, entre ellas la del Pentágono.

Las intrusiones provenían de una computadora conectada a la línea telefónica desde un departamento de Barrio Norte, en la capital federal. "El Gritón" ingresaba en la red de computadoras de la empresa Telecom a través de líneas gratuitas 0800, para luego realizar intromisiones en sistemas informáticos ajenos.

En la causa argentina número 45048/95, con carátula "Ardita Julio C., sobre defraudación", el juzgado de Instrucción número 38 a cargo de la jueza Wilma López, dispuso que Ardita compareciera ante un tribunal oral pero por fraude telefónico (estimado por la empresa Telecom en $50), ya que las intrusiones informáticas están contempladas en el Código Penal.

Sin embargo, por el mismo episodio, Ardita ya tuvo una demanda penal en los Estados Unidos, donde las intrusiones informáticas, las violaciones de códigos secretos y la posesión de claves ajenas sí son delitos graves. El proceso terminó el 19 de mayo de 1999, cuando un tribunal de la ciudad de Boston, lo condenó a 3 años de libertad condicional y a pagar una multa de US$ 5,000 por haber vulnerado, entre otros, el sistema informático de la Marina.

BARAM PAUL

Posiblemente el mayor hacker de la historia. Ya hackeaba Internet antes de que existiera. Él fue quien introdujo el concepto de hacker.

ELGRANOSCARÍN

ElGranOscarín es un hacker español de 27 años, autor del troyano *Cabronator*, cuyas iniciales son **O.L.H** y que en los primeros días de abril del 2003 fuese detenido por la Guardia Civil de España, en un operativo denominado **CLON** que se inició en agosto del 2002. Su impresionante ego está casi a la par con sus prolíficas creaciones de todas sus herramientas de hacking y cracking, virus, juegos obscenos, etc.

Sin embargo, como reza el viejo dicho "la Justicia tarda pero llega", finalmente fue detenido, aunque actualmente se encuentra en libertad bajo fianza, a la espera de una acción legal de las cortes de Justicia de España.

FARMER DAN

Trabajó Con Spafford en la creación de COPS(1991) y al mismo tiempo con el famoso Computer Emergency Response Team (CERT). Tiempo más tarde Farmer ganó gran notoriedad al crear el System Administrator Tool for Analyzing Networks (SATAN). Una gran herramienta para analizar vulnerabilidades en redes.

GATES BILL Y ALLEN PAUL

En sus tiempos de aprendices, estos dos hombres de Washington se dedicaban a hackear software. Empezaron en los 80 y han creado los mayores imperios de software de todo el mundo.

HELSINGIUS JOHAN

Johan Helsingius operó el más grande y popular re-enviador de correo anónimo (*anonymous remailer*), denominado penet.fi, hasta que fuera clausurado en septiembre de 1996.

Los problemas de Helsingius empezaron cuando fue detenido por la policía filandesa después que la denominada *Church of Scientology* (Iglesia de Cienciología), denunciara que un cliente usuario de penet.fi estaba publicando secretos de esta "iglesia" en Internet. La Corte obligó a Helsingius a revelar los verdaderos nombres de sus clientes registrados, los mismos que bajo un seudónimo (nickname) figuraban en su boletín electrónico mensual.

Algo paradójico constituye el hecho que, el más grande remailer anónimo de Europa era controlado desde una computadora con arquitectura 486 y un disco duro de apenas 200 MB. Lo insólito de este caso fue que Helsingius nunca enviaba mensajes anónimos.

El objetivo de un remailer anónimo es proteger la identidad del usuario. El servidor Remailer, no almacena los mensajes sino que sirve como un canal de re-transmisión de los mismos. El Remailer re-envía estos mensajes, sin dar a conocer la identidad del remitente original.

LAMO ADRIÁN

En el 2000, Lamo se hizo conocido en los círculos de hackers al haber ingresado en las redes de America on Line, Yahoo y Worldcom, informando a sus administradores la forma cómo lo hizo.

En enero del 2002 encontró un fuga en la red hermética de la corporación Excite@Home. Lamo encontró una vulnerabilidad en la red del periódico The New York Times en menos de dos minutos. Recientemente creó un grupo de noticias (USENET).

RITCHIE DENNIS, THOMSON KEN Y KERNIGHAN BRIAN

Programadores de los Laboratorios Bell. Son los desarrolladores de UNIX y C. Se les considera los padres de la informática masiva al desarrollar el sistema operativo y el lenguaje más poderoso de la actualidad.

SPAFFORD EUGENE

Profesor de informática de la Universidad de Purdue. Colaboró para crear el Computer Oracle Password Security System (COPS), un sistema de seguridad para redes. Es un hombre muy respetado en el campo de la seguridad.

STALLMAN RICHARD

Se unió al Laboratorio de Inteligencia Artificial de la MIT en 1971, lo que le valió crear sus propias aplicaciones en esa área. Fue ganador del premio McArthur Genius por sus desarrollos de software. Fue fundador de Free Software Foundation, creando aplicaciones y programas gratis para entornos UNIX.

THE DECEPTIVE DUO

The Deceptive Duo ("El dúo engañoso") ingresaron ilegalmente al sistema de la **Federal Aviation Administration** de los Estados Unidos en abril de 2002 y descargaron información confidencial relacionada a las filmaciones de las actividades de los pasajeros de los aeropuertos.

También en la **Marina de Guerra de los Estados Unidos**, colocando información obtenida del servidor del sistema de reservaciones de pasajes de la aerolínea **Midwest Express**.

Cada sitio web incursionado por estos hackers, mostraba una supuesta "patriótica misión" en la cual preconizaban ser ciudadanos de los Estados Unidos de América, determinados a salvar al país de una "amenaza extranjera" al exponer los huecos de inseguridad en Internet. Incluso incluyeron el logo del grupo, el cual consiste de dos armas de fuego delante de una bandera norteamericana.

TORVALDS LINUS

Torvalds empezó a conocer el UNIX y a tomar clases de programación en C en los 90. Un años después empezó a escribir un sistema operativo parecido al UNIX. Después de otro año, lo subió a Internet pidiendo colaboración, hoy es llamado LINUX.

VEHEMA WIETSE

Vehema viene de la Universidad de Tecnología de Eindhoven, en los Países Bajos. Un gran programador, con un don para ello, además de tener un amplio historial en programas sobre seguridad. Es el coautor del SATAN con Farmer. Vehema escribió el TCP Wrappers, uno de los programas de seguridad más usado en el mundo.

Glosario

GLOSARIO

ACL's (*Access Control Lists*).- Proveen de un nivel adicional de seguridad a los archivos extendiendo el clásico esquema de permisos en Unix. Las Listas de Control de Acceso van a permitir asignar permisos a usuarios o grupos concretos.

Administrador.- Persona que se encarga de la instalación, configuración y mantener en buen estado un equipo de cómputo.

ADP (*Automatic Data Processing*).- Procesamiento automático de datos.

Amenaza.- Persona, circunstancia, evento, fenómeno o una idea maliciosa que plantea algún daño a un recurso.

Análisis de Riesgos.- Es el proceso de examinar los posibles riesgos y clasificarlos por nivel de severidad, esto involucra hacer decisiones costo-beneficio. No se debe de llegar a una situación donde se gasta más para proteger aquello que es menos valioso.

Antivirus.- Es un programa que se ejecuta en la computadora para buscar indicios de virus. Si encuentra alguno, guía al usuario en los pasos a seguir para la remoción del mismo. Estos pasos pueden restaurar el archivo infectado a su estado original o de ser necesario borrarlo. El programa antivirus debe ser actualizado periódicamente con nuevas definiciones de virus.

Aplicaciones sensitivas.- Son todos aquellos programas y sistemas desarrollados para la administración de sistemas, como pueden ser herramientas de administración, configuración o seguridad.

Archivo.- Conjunto de datos con un nombre asociado.

Archivos de configuración.- Son archivos que contienen información importante relativa al sistema o al usuario.

ARPA (*Advanced Research Projects Agency*, Agencia de Proyectos de Investigación Avanzada).- Nombre actual del organismo militar norteamericano anteriormente llamado DARPA, dedicado a desarrollar proyectos de investigación con propósitos militares que a veces también tienen utilización civil. Agencia del Departamento de Defensa de los Estados Unidos que creó ARPANET, la red que dio origen a Internet.

ARPANET(*Advanced Research Projects Agency Network*, Red de la Agencia de Proyectos de Investigación Avanzada).- Red pionera de larga distancia financiada por ARPA (antigua DARPA) a fines de la década de los 60. Fue la base inicial de la investigación sobre redes y constituyó el eje central de éstas durante el desarrollo de Internet. ARPANET estaba constituida por computadoras de conmutación individual de paquetes, interconectados mediante líneas telefónicas. Se le considera el origen del actual Internet.

ASCII (*American Standard Code of Information Interchange*).- Código normalizado estadounidense para el intercambio de la información. Código que permite definir caracteres alfanuméricos; se usa para lograr compatibilidad entre diversos procesadores de texto.

Ataque.- Es la realización de una amenaza.

Ataque pasivo.- Es aquel que no causa modificación o cambio en la información o recurso; es decir, únicamente la observa, escucha, obtiene o monitorea mientras está siendo transmitida.

Ataque activo.- Es aquel que implica algún tipo de modificación del flujo de datos transmitido (modificación de la corriente de datos) o la creación de un falso flujo de datos (creación de una corriente falsa).

Auditoría.- Es el registro, análisis y revisión de las actividades relacionadas con la seguridad de un sistema confiable. Consiste en revisar los eventos que pueden ser importantes para detectar un posible ataque al sistema.

Autentificación.- Proceso de verificar la identidad de una persona.

BBC.- British Broadcasting Corporation

Bit.- Número de base dos de un solo dígito (es decir, cero o uno). Se trata de la unidad mínima de información que se maneja en una computadora. Se deriva de la contracción de la expresión *binary digit* (dígito binario).

Bitácoras.- Son archivos en donde se almacena todo lo que va sucediendo en el sistema, pensados para poder llevar un control.

Bombas.- Pueden ser tanto programas completos como fragmentos de código insertados en otros programas. La principal diferencia entre los caballos de Troya y las bombas es que estas últimas se activan cuando ocurre un determinado evento, caso de las bombas lógicas, o cuando se llega a una determinada fecha, caso de las bombas de tiempo.

Bridge.- Se utiliza para conectar dos redes a nivel de capa de enlace. El dispositivo conecta dos o más segmentos de la misma LAN. Las dos LAN's a ser conectadas pueden ser similares o no, por ejemplo, el bridge puede conectar dos Ethernets entre sí o una ethernet y una Token Ring. A diferencia de los routers, los bridges son independientes del protocolo y transparentes para la capa de red (capa 3). Los bridges realizan funciones de *forwarding* y filtrado de paquetes sin rerutear mensajes, en consecuencia pueden ser mas rápidos que los routers, pero son mucho menos versátiles.

Bucaneros.- Es simplemente un comerciante, el cual no tiene escrúpulos a la hora de explotar un producto de *cracking* a nivel masivo.

Bug.- En inglés significa bicho. Término aplicado a los errores de programación al ejecutar un programa informático o de implementación de un programa que causan cualquier tipo de situaciones anómalas. Fue usado por primera vez en el año 1945 por Grace Murray Hooper,

una de las pioneras de la programación moderna, al descubrir cómo un insecto *(bug)* había dañado un circuito de la computadora Mark.

Business impact.- Forma de desarrollar un análisis y diseño de un plan de contingencia que se basa en el estudio del impacto (pérdida económica o de imagen que ocasiona la falta de algún recurso) de los que soporta la actividad del negocio.

Byte.- Conjunto de ocho bits que se utiliza, por ejemplo, para representar un carácter ASCII.

Caballos de Troya.- Toman su nombre del famoso mito del caballo de Troya, son programas que imitan la ejecución de otros programas pero realizan otras funciones completamente distintas a las esperadas. Normalmente causan daños irreversibles.

CCITSE (*Common Criteria for Information Technology Security*, Criterios Comunes para Evaluación de Seguridad de Tecnología de la Información).- Nuevo esquema de evaluación de seguridad que reemplaza al TCSEC y al ITSEC, a finales de 1998, mejor conocido como **CC.**

CERT (*Computer Emergency Response Team*, Equipo de Respuesta para Emergencias Informáticas).- Fue creado por DARPA en Noviembre de 1988 como respuesta a las carencias mostradas durante el incidente del gusano *(worm)* de Internet. Los objetivos del CERT son trabajar junto a la comunidad Internet para facilitar su respuesta a problemas de seguridad informática que afecten a los sistemas centrales de Internet, dar pasos proactivos para elevar la conciencia colectiva sobre temas de seguridad informática y llevar a cabo tareas de investigación que tengan como finalidad mejorar la seguridad de los sistemas existentes. Los productos y servicios del CERT incluyen asistencia técnica 24 horas al día para responder a incidentes sobre seguridad informática, asistencia sobre vulnerabilidad de productos, documentos técnicos y cursos de formación. Adicionalmente, el CERT mantiene numerosas listas de correo (incluyendo una sobre Avisos CERT) y ofrece un sitio web (http://www.cert.org) y un servidor de FTP anónimo, en ftp://cert.org, donde se archivan documentos y herramientas sobre temas de seguridad informática.

Certificado.- Consiste en una pareja, clave privada-clave pública. Físicamente son dos archivos que unidos, permiten definir un conjunto de claves de encriptación y una identidad certificada. La clave privada nunca abandona el servidor, por lo que NADIE obtiene esta información, por lo que NADIE podrá suplantar la identidad del servidor certificado.

CGI (*Common Gateway Interface*).- Estándar que describe la manera en que el navegador Web trasmite la información a un servidor Web. Los programas CGI pueden leer información, procesarla y devolver los resultados al navegador.

Chip.- Abreviatura de "microchip". Circuito muy pequeño, compuesto por miles a millones de transistores impresos sobre una oblea de silicio.

Cliente.- Es una computadora o un proceso que hace uso de los servicios que brindan otras computadoras en la red.

Código de ética.- Es un conjunto de normas o principios que tratan el comportamiento según principios éticos, su normatividad es nada más mostrar una declaración de intenciones sobre la "misión" de una institución y la coerción real con que se imponen es pequeña, aunque en algunos casos se incluyen expulsiones de la asociación en cuestión.

Conejos o Bacterias.- Son programas que no hacen nada útil, sino que simplemente se dedican a reproducirse hasta que el número de copias acaba con los recursos del sistema. Normalmente, los recursos que tienden a obtener son el procesador, la memoria, el espacio en disco, etc.

Confidencialidad.- Conocida como privacidad de la información, es la necesidad de que la misma sólo sea conocida por personas autorizadas.

Contraseña (*password*).- Conjunto de caracteres alfanuméricos que permite al usuario de un sistema o una red tener acceso a un determinado recurso o la utilización de un servicio dado en un sistema determinado. Es totalmente confidencial.

Control.- Permite asegurar que sólo los usuarios autorizados pueden decidir cuándo y cómo permitir el acceso a la información.

Cookie.- Procedimiento ejecutado por el servidor que consiste en guardar información acerca del cliente para su posterior recuperación. En la práctica, la información es proporcionada desde el navegador al servidor del Word Wide Web, vía una forma o un método interactivo que puede ser recuperado nuevamente cuando se accede al servidor en el futuro. Es utilizado, por ejemplo, para el registro a un servicio.

Copyhackers.- Poseen conocimientos de tecnología y son denominados por la obsesión de ser superiores, pero no terminan de aceptar su posición. Por ello "extraen" información del verdadero hacker para terminar su trabajo.

Crack.- Programa utilizado para eliminar las protecciones de los programas. Da acceso libre a las funciones del mismo.

Cracker.- Son hackers cuyas intenciones van más allá de la investigación. Es una persona que tiene fines maliciosos o de venganza, quiere demostrar sus habilidades pero de manera equivocada o simplemente personas que hacen daño sólo por diversión. La diferencia básica es que los hackers construyen cosas y los crackers las rompen.

Criptografía.- Este término se forma del vocablo griego krupíos, "oculto", que en otras palabras se traduce como: "Arte de escribir de manera peculiar o de modo esotérico". En computación se refiere a los mensajes que son enviados por un emisor que oculta el contenido del mensaje a manera de que sólo ciertas personas previamente seleccionadas tendrán acceso a la información por medio de una clave después de haberla descifrado.

Criptografía simétrica.- Método criptográfico tradicional que opera a partir de una palabra que sirve para codificar y decodificar información, conocido como contraseña (*password*).

Criptografía asimétrica.- Consiste en poner en cada extremo de la comunicación un par de llaves, una pública y otra privada.

Criptograma.- Mensaje encriptado.

Criptología.- Se conforma de dos amplias áreas: la **"criptografía"** que se dedica a la construcción y operación de sistemas de seguridad informática; el **"criptoanálisis"** cuyo fin es desencriptar los criptogramas y acceder de manera ilegítima a la información contenida en los mensajes mediante ciertas técnicas con las que no es preciso conocer la clave de cifrado.

Cuenta.- Dentro de sistemas de información se conoce como cuenta, al registro de un usuario dentro de un sistema, lo cual implica que este usuario podrá acceder a los servicios que este proporcione.

DAC (Control de Acceso Discrecional).- Es un método para restringir el acceso a los archivos (y a otros objetos del sistema) basándose en la identidad de los usuarios y/o los grupos a los que pertenecen.

DARPA (*Defense Advanced Research Projects Agency*, Agencia de Proyectos de Investigación Avanzada para la Defensa).- Organismo creado en 1954 por el Departamento de Defensa norteamericano (DoD) encargado de la investigación y desarrollo en el campo militar y que jugó un papel muy importante en el nacimiento de Internet a través de la red ARPANET.

Dato.- Es la unidad mínima con la se compone cierta información.

Debug.- Encontrar y corregir errores o bugs.

Decisión.- Elección de un curso de acción determinado entre varios posibles.

Decodificador.- Aparato que hace el proceso inverso de la codificación, es decir, obtener en un formato entendible o establecido a partir de una entrada.

Delito informático.- Es toda conducta que utiliza la computadora como medio para cometer un ilícito que tenga como fin el perjuicio de un tercero.

Deontología.- Ciencia o tratado de los deberes y normas éticas, en especial si conciernen al profesional de una rama determinada.

Demonio (*daemon*).- Programa que está ejecutándose constantemente en el sistema en espera de que algún servicio haga una petición de él para realizar determinadas tareas.

DES (*Data Encryption Standard*, Estándar de Cifrado de Datos).- Algoritmo de cifrado de datos desarrollado a fines de los años 70, aprobado como estándar por la administración de EE.UU. Se basa en el sistema de llave única.

Desastre.- Surgen de las fuerzas naturales tales como las inundaciones, los terremotos, el fuego, el viento.

DHCP (*Dynamic Host Configuration Protocol*).- Es una extensión del protocolo BOOTP (BOOTP habilita a clientes *diskless* a inicializar y automáticamente configurar TCP/IP). DHCP centraliza y administra la información de la configuración de TCP/IP, automáticamente asigna direcciones IP a las computadoras configuradas para utilizar DHCP.

Digest.- Es la representación de un texto en una cadena sencilla de dígitos, creada usando una función *hash* de una sola vía (sin regreso). Encriptando el mensaje con una llave privada para crear una firma digital, lo cual se utiliza como medio electrónico de autentificación.

Dirección IP (*IP address*).- Número compuesto por 32 dígitos binarios que identifica a todo emisor o receptor de información en Internet. Número de identificación de cada computadora en Internet con el formato xxx.xxx.xxx.xxx, donde xxx es un número de 0 a 255.

Directorio.- Son archivos cuyo contenido son otros archivos de cualquier tipo (planos, o más directorios, o archivos especiales.

Directriz.- Conjunto de instrucciones o normas para realizar algo.

Disponibilidad.- Es la capacidad de la información de estar siempre disponible para ser procesada por las personas autorizadas.

DNS (*Domain Name System*, Sistema de Nombres de Dominio).- Es un servicio de búsqueda de datos de uso general, distribuido y multiplicado. Su utilidad principal es la búsqueda de direcciones IP de sistemas anfitriones *(hosts)* de Internet basándose en los nombres de éstos. El estilo de los nombres de *host* utilizado actualmente en Internet es llamado nombre de dominio. Los dominios originarios, a los que se añadieron algunos más en el año 2000, son: .com (comercial, empresas), .edu (educación, centros docentes), .org (organización sin ánimo de lucro), .net (operación de la red), gov (gobierno o administración pública) y .mil (ejercito de los EE.UU.). La mayoría de los países tienen un dominio propio. Por ejemplo: .mx (México), .es (España), .au (Australia).

DOD (*Departament of Defense*).- Departamento de Defensa de los Estados Unidos.

Dominio (*domain*).- Conjunto de caracteres que identifica un sitio de la red accesible por un usuario. Así, por ejemplo, el nombre de dominio .mx identifica a los usuarios dados de alta en el registro mexicano de nombres de dominio. Conjunto de computadoras que comparten una característica en común, como el estar en el mismo país, en la misma organización o en el mismo departamento. Cada dominio es administrado por un servidor de dominios.

DVB (*Digital Video Broadcasting*).- Difusión de Vídeo Digital.

EAL (*Evaluation Assurance Level*, Niveles de Garantía de Evaluación).- Definen la escala de CC predefinidos para garantizar la valoración para los TOEs.

Elemento activo.- Son todos aquellos usuarios o procesos que poseen la capacidad de crear, modificar, leer, escribir o borrar información.

Encriptación.- Es el método por el cual la información puede ser protegida a través de programas encargados de cifrarla, firmarla para identificar eficientemente al remitente, y cerrarla para que sólo pueda ser abierta nuevamente por quien tenga la clave apropiada., agregándose además métodos para corroborar la integridad de la información recibida, o sea, para validar que la información no haya sido modificada en el camino.

Enmascaramiento.- Es la suplantación de identidad. Un intruso se hace pasar por una entidad diferente para tener acceso al sistema. O se le llama también al método de emplear alguna herramienta que permita que una máquina pueda realizar conexiones remotas asignándole una IP virtual.

Espionaje.- Actividad encaminada a obtener información reservada o secreta.

Esteganografía.- Técnica que consiste en ocultar un mensaje secreto dentro de otro más largo, de tal forma que terceras personas no puedan descubrirlo.

Estrategia.- El conjunto de reglas que aseguran una decisión óptima en cada momento.

Ética.- Principios directivos que orientan a las personas en cuanto a la concepción de la vida, el hombre, los juicios, los hechos y la moral.

Ética informática.- Es una nueva disciplina que pretende abrirse campo dentro de las éticas aplicadas. La existencia de la ética informática tiene como punto de partida el hecho de que las computadoras suponen problemas éticos particulares y por tanto distintos a otras tecnologías.

Etiqueta.- Son identificadores que se les asignan a los usuarios o a los objetos dentro del sistema, se utilizan estos identificadores para verificar los permisos que tiene el usuario o el objeto para permitir o denegar las acciones.

Etiqueta sensitiva de usuario.- Especifica el grado, o nivel de confianza, asociado con ese usuario, la etiqueta de usuario sensitiva es usualmente llamada como certificado de paso.

Etiqueta sensitiva de archivo.- Especifica el nivel de confianza que un usuario puede ser capaz de tener al acceder a ese archivo.

Evento.- Son todas las acciones generadas por un usuario o un proceso que van a exigir una respuesta por parte de un objeto.

Finger.- Programa que muestra información acerca de un usuario(s) específico(s) conectado(s) a un sistema local o remoto. Habitualmente se muestra el nombre y apellidos, hora de la ultima conexión, tiempo de conexión sin actividad, línea del terminal y situación

de éste. Puede también mostrar archivos de planificación y de proyecto del usuario. *Finger* es una palabra inglesa que significa "dedo" o, en su forma verbal, "apuntar con el dedo".

Firewall.- Mecanismo de seguridad y protección. Se utiliza para impedir el acceso a una red.

Firma digital.- Grupo de datos, añadidos a un conjunto de datos o transformaciones de estos, que permiten al receptor probar el origen e integridad del conjunto de datos recibidos, así como protegerlos contra falsificaciones.

Firmware.- Conjunto de instrucciones integrado en el hardware que controla y dirige actividades de la memoria del microprocesador. Se define como hardware en software, es decir memorias ROM que contienen instrucciones o datos necesarios para el sistema, un ejemplo son los BIOS de la mayoría de las computadoras.

FTLS (Especificación Formal de Alto Nivel).- Es una especificación del sistema que incluye las definiciones abstractas de las funciones que el TCB (*Trusted Computer Base*) realiza y de los mecanismos de la dotación física y/o del firmware que se utilizan para usar dominios separados de ejecución

FTP (*File Transfer Protocol*, Protocolo de Transferencia de Archivos).- Protocolo (parte de la arquitectura TCP/IP) utilizado para la transferencia de archivos.

Gusanos.- Son programas que se reproducen copiándose de una computadora a otra a través de la red. A diferencia de los virus, los gusanos son programas independientes y no necesitan otro programa en el cual alojarse. Normalmente, los gusanos no producen ningún tipo de daño en el sistema, excepto malgastar los recursos, llegando incluso a sobrecargar la red.

Hackeable.- Término que se utiliza para decir que la seguridad de un sistema puede llegar a ser burlada, viene de hacker.

Hacker.- Es una persona que está en una continua búsqueda de información, vive para aprender y todo para él es un reto; no existen barreras, y lucha por la difusión libre de información (*Free Information*), distribución de software sin costo y la globalización de la comunicación.

Hacking.- Técnicas de entrada de forma no autorizada en un sistema informático con el ánimo de obtener información, siempre y cuando esto se use con fines educativos o de diversión, no para adueñarse de conocimientos que no son suyos o con ánimo de lucro. Estos actos no presuponen la destrucción de la información, ni la instalación de virus. No obstante no es extraño la instalación de troyanos para disponer de códigos de acceso actualizados.

Hardware.- Conjunto formado por todos los elementos físicos de una computadora.

Herramienta de seguridad.- Programas que permiten incrementar la fiabilidad de un sistema de cómputo. Existe una gran variedad de ellas, casi todas de libre distribución.

Host.- Computadora que, mediante la utilización de los protocolos TCP/IP, permite a los usuarios comunicarse con otros sistemas centrales de una red. Los usuarios se comunican utilizando programas de aplicación, tales como el correo electrónico, telnet, WWW y FTP. Computadora central en un sistema informático complejo.

HTTP (*HyperText Transfer Protocol*).- Protocolo utilizado por los servidores de Web para la visualización de páginas.

Hub.- Punto común de conexión de dispositivos en una red. Los hubs son usados comúnmente para conectar segmentos de una LAN. Un hub contiene múltiples puertos. Cuando un paquete llega al puerto, es copiado a los otros puertos, de esta manera los otros segmentos de la LAN pueden ver todos los paquetes. Un hub pasivo simplemente sirve de conductor de datos entre los diferentes puertos. Los llamados hubs inteligentes incluyen servicios adicionales como permitir a un administrador monitorear el tráfico y configurar cada puerto del hub. Estos hubs se conocen generalmente como hubs administrables (*manageable hubs*). Un tercer tipo de hub, llamado *switching hub*, lee la dirección de destino en cada paquete y lo envía al puerto correcto.

Identificación.- Momento en que el usuario se da a conocer en el sistema.

IDS (*Intrusion Detection System*, Sistema de Detección de Intrusos).- Es el arte de detectar actividad inapropiada, incorrecta o anónima. Los sistemas de detección de intrusos que operan en un *host* para detectar actividad maliciosa se les conoce como Sistemas de Detección de Intrusos para *host* y los sistemas de detección de intrusos que operan en el flujo de datos de una red se les conoce como Sistemas de Detección de Intrusos para red.

Incidente.- Suceso que se interpone inesperadamente en el transcurso normal de una acción.

IEEE (*Institute of Electrical and Electronic Engineers*).- Una sociedad de profesionales internacional que publica sus propios estándares y es miembro de la ANSI y de la ISO.

IMAP (*Internet Message Access Protocol*, Protocolo de Acceso a Mensajes de Internet).- Protocolo diseñado para permitir la manipulación de mailboxes remotos como si fueran locales. IMAP requiere de un servidor que haga las funciones de oficina de correos pero en lugar de leer todo el mailbox y borrarlo, solicita sólo los encabezados de cada mensaje. Se pueden marcar mensajes como borrados sin suprimirlos completamente, pues estos permanecen en el mailbox hasta que el usuario confirma su eliminación.

Información.- La información es el conjunto de datos que tiene un significado específico más allá de cada uno de éstos, y tendrá un sentido particular según cómo y quién la procese y la interprete. La información es cualquier mensaje (conjunto de datos) que le interese al receptor, entienda o lo ignore antes de recibirlo.

Información sensitiva.- Es toda aquella información que no está disponible a todos los usuarios por poseer un cierto grado de confidencialidad.

Informática.- Descrita como una ciencia multidisciplinaria que estudia tanto la tecnología de la información (TI) en su relación con las actividades humanas administrativas y productivas y sus aplicaciones, así como las relaciones entre la información natural y la representativa, abstracta o artificial.

Insiders.- Pueden ser empleados disconformes o personas externas con acceso a sistemas dentro de la empresa u organización, los cuales utilizan sus permisos para alterar archivos o registros.

Integridad.- Implica que el contenido de la información permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada para posteriores controles o auditorías.

Interfaz.- Conexión entre dos componentes de hardware, entre dos aplicaciones o entre un usuario y una aplicación. También apariencia externa de una aplicación informática.

Internauta.- Usuario que navega virtualmente por Internet.

Internet.- Red informática de comunicación internacional que permite el intercambio de todo tipo de información entre sus usuarios. El nombre proviene del acrónimo de las palabras inglesas *International Network* (Red Internacional).

Intranet.- Es como la red Internet pero a nivel de una organización o empresa. Usando el popular software para Internet, la intranet le permite a los usuarios intercambiar datos dentro de la organización como si lo hicieran con el resto del mundo a través de Internet.
Intruso.- Persona que accede (o intenta acceder) sin autorización a un sistema ajeno, ya sea en forma intencional o no.

IT (*Information Technology*).- Tecnología de Información.

ITSEC (*Information Technology Security Evaluation Criteria*, Criterio para Evaluación de Seguridad de Tegnología de Información).- Creado por los gobiernos de Francia, Alemania, los Países Bajos y el Reino Unido. A principios de los 90's, proveía niveles de seguridad donde la funcionalidad del producto desarrollado se definía.

Kernel (Núcleo).- Es la parte central y más importante del sistema operativo. En los sistemas tipo UNIX se puede modificar.

Lamer.- Son individuos con ganas de hacer *Hacking*, pero que carecen de cualquier conocimiento.

Ley.- Normas o preceptos de carácter obligatorio cuyo cumplimiento supervisa una autoridad. Esta autoridad puede regular, obligar o prohibir una cosa, generalmente en consonancia con la justicia y la ética.

Licencia GPL (GNU *General Public License*, Licencia Pública GNU).- Esta licencia indica que el código fuente de un software debe ser distribuido libremente y que cualquier

persona está permitida a hacer las copias para su propio uso, vender o darlas a la gente (con algunas restricciones).

Linux.- Versión de libre distribución del sistema operativo UNIX; desarrollado por Linus Torvalds basándose en el Minix. Ha tenido una amplia difusión por su desarrollo independiente de cualquier empresa.

Lista de correo.- Son una aplicación que envía automáticamente correo a un grupo determinado de usuarios. Son muy utilizadas para mantener informado a los miembros sobre las noticias de algún área de interés para ellos.

Lista de correo moderada.- Lista de correo en la cual los mensajes, antes de ser distribuidos, son filtrados manualmente por uno o más moderadores.

Lista de correo no moderada.- Lista de correo en la cual los mensajes no son revisados, se envían automáticamente.

Mainframe.- Un sistema de computadora a gran escala que pueden alojar software comprensivo y varios periféricos.

Medidas proactivas.- Son medidas o decisiones que se toman para prevenir un problema.

Medidas reactivas.- Son medidas o decisiones que se toman cuando el daño se produce.

MIME (*Multipurpose Internet Mail Extensions*).- Técnica para codificar archivos y anexarlos a un mensaje de correo electrónico. Permite principalmente enviar archivos binarios como parte de un mensaje.

Moderador.- Persona, o pequeño grupo de personas, que se dedica a moderar listas de correo y grupos de noticias *(newsgroups)* y son responsables de decidir qué mensajes de correo electrónico pueden incluirse en dichos grupos y listas.

Monitoreo del sistema.- Se le llama monitoreo del sistema cuando una persona revisa e inspecciona lo que está sucediendo en el sistema, incluye verificar a los usuarios y lo que se encuentran haciendo para asegurar que no pongan en riesgo la seguridad del sistema.

Moral.- Procede del latín "*mos*", que significa costumbre, hábito, en el sentido de conjunto de normas o reglas adquiridas por medio de hábito, se utiliza para referirse a la conducta del hombre que obedece a unos criterios valorativos acerca del bien y el mal.

NCSC (*National Computer Security Center*).- Este es un centro de seguridad para computación a nivel nacional en los Estado Unidos de América. Este centro se formó en 1981 con el propósito de proporcionar sistemas de información informáticos fiables para uso en misiones críticas y sensibles.

Newbie.- Es un novato, o más particularmente es aquel que navega por Internet, tropieza con una página de *hacking* y descubre que existe un área de descarga de buenos programas de hackeo.

Nivel de sensitividad.- Es cuando toda la información almacenada o todos los usuarios que tienen acceso a esa información poseen exactamente los mismos permisos.

Norma.- Regla que se debe seguir o que se debe de ajustar a las conductas, actividades o tareas.

Objeto.- Son todos los elementos identificables dentro del sistema, como son directorios, archivos, dispositivos, puertos, etc.

OSD.- Control Digital OSD.

Outsiders.- Son personas que atacan desde fuera de la ubicación física de la organización, estas personas ingresan a la red simplemente averiguando una contraseña válida.

Parche.- Es el archivo que realiza correcciones en un archivo ejecutable o en sus datos para eliminar errores.

Perseguir.- Dentro de la estrategia a seguir cuando se detecta a un intruso, es darle seguimiento a un acto que pone en riesgo la seguridad del sistema.

PGP (*Pretty Good Privacy*).- Desarrollado por el criptólogo estadounidense Phil Zimmermann, es mundialmente conocido como sistema de firma digital para correo electrónico. Aparte de esta función, PGP permite también el cifrado de archivos de forma convencional mediante criptografía simétrica.

Phreacker.- Posee conocimientos profundos de los sistemas de telefonía, tanto terrestres como móviles. En la actualidad también poseen conocimientos de tarjetas prepago, ya que la telefonía celular las emplea habitualmente.

Phreacking.- Es una extensión del hacking y cracking.

PID (*Process Identifier*).- Cada proceso tiene uno distinto a los demás y sirve al sistema para poder distinguirlos.

Ping (*Packet Internet Groper*).- Aplicación usada en Internet para determinar si está o no activa la conexión a una máquina específica, o para averiguar la factibilidad de alcanzar a otra máquina.

Plan de contingencia.- Conjunto de procedimientos que permiten recuperar y reestablecer el correcto funcionamiento del sistema en un tiempo mínimo después de que se haya producido el problema; considerando las acciones que se llevarán a cabo antes, durante y después del desastre, para tener el mínimo de pérdidas posibles.

Portabilidad.- Representa la facilidad de poder visualizar o transportar la información.

Política.- Definiciones establecidas por la dirección que determina criterios generales a adoptar en distintas funciones y actividades donde se conocen las alternativas ante circunstancias repetidas.

Política de Seguridad.- Es un conjunto de leyes, reglas y prácticas que regulan la manera de dirigir, proteger y distribuir recursos en una organización para poder llevar a cabo los objetivos de seguridad informática dentro de la misma.

POP o POP3 (*Post Office Protocol*).- Un cliente de correo POP establece una conexión con el servidor sólo el tiempo necesario para enviar o recibir correo, y luego cierra la conexión. Da un uso más eficiente del ancho de banda que SMTP, ya que no es inútilmente mantenida una conexión mientras el usuario está leyendo o redactando correo.

PP(*Protection Profile*, Perfil de Protección).- Es un requerimiento que define un problema de seguridad general de un consumidor o grupo de consumidores. Básicamente un Perfil de Protección establece: esto es lo que se necesita.

Privacidad.- Es la necesidad de que la información sólo sea conocida por personas autorizadas.

Procedimiento.- Conjunto de pasos o reglas que describen la forma de realizar algo.

Procesar.- Someter a algo a cualquier proceso de transformación o elaboración. Legalmente se refiere a seguir cuando alguien a cometido un delito.

Proceso.- Conjunto de fases sucesivas de un fenómeno natural o de una operación artificial. es un programa en ejecución. Cada proceso es identificado de forma unívoca por el sistema mediante su PID (*Process IDentifier*) y además cada uno tiene sus privilegios y sus propiedades.

Prompt.- Cabecera que aparece en cada línea a la espera de la introducción de un comando dentro del sistema.

Proteger.- Cuidar o mantener intacto una persona o cosa.

Protocolo.- Reglas que gobiernan como las computadoras se comunican entre ellas. Un conjunto formal de convenciones que gobiernan el formateado y el tiempo relativo del intercambio de mensajes entre dos sistemas de comunicaciones.

Proxy.- Computadora encargada de guardar copias de los archivos más solicitados para reducir el tráfico de la red e impedir su colapso, se trata de caches de red.

Puertas traseras (backdoors).- Son mecanismos implementados en los programas por sus creadores, que les permiten a éstos realizar acciones determinadas sin tener que pasar por determinadas secciones del programa, como procesos de autentificación, mecanismos de seguridad, etc.

Puerto.- Número que identifica un socket de forma que todos los paquetes además de tener una dirección IP de destino tienen también un puerto de destino, el número de puerto es fijo en el servidor y depende del servicio que preste (por ejemplo, un servidor web está en el puerto 80 siempre) y en el usuario depende de la conexión, pues utiliza un número de puerto distinto para cada computadora con la que se conecta.

Red de computadoras.- Consiste de dos computadoras (desde un nivel básico) o más, conectadas por un canal de comunicación de manera tal que puedan compartir datos y recursos (espacio en discos duros, impresoras, programas, etc.). A cada una de las computadoras conectadas a la red se le denomina "nodo".

Redundancia.- Es hacer múltiples copias de la información importante y dichas copias son frecuentemente almacenadas en diferentes lugares, para asegurarse de que esa información no se perderá.

Respaldo.- Se conoce como respaldo a realizar copias de seguridad de la información, en caso de que esta sufra algún daño.

RFC (*Request For Comments*).- Serie de documentos iniciada en 1967 que describe el conjunto de protocolos de Internet y experimentos similares. No todos los RFC's (en realidad muy pocos de ellos) describen estándares de Internet pero todos los estándares Internet están escritos en forma de RFC's. La serie de documentos RFC es inusual en cuanto los protocolos que describen son elaborados por la comunidad Internet que desarrolla e investiga, en contraste con los protocolos revisados y estandarizados formalmente que son promovidos por organizaciones como CCITT y ANSI.

Riesgo.- Es una medida del costo de una realización de una vulnerabilidad que incorpora la probabilidad de éxito de un ataque.

Risk analysis.- Forma de desarrollar un análisis y diseño de un plan de contingencia que se basan en el estudio de los posibles riesgos desde el punto de vista de probabilidad de que los mismos sucedan.

Root.- Es el usuario que tiene todos los privilegios en un sistema Unix o Linux. Como poseedor de todos los usuarios, podrá acceder a cualquier recurso o mirar el contenido de cualquier directorio. Es el único que podrá cambiar la configuración del sistema, añadir o eliminar nuevos usuarios, instalar nuevas aplicaciones, etc. Así que es conveniente no olvidarse de su password. Se debe tener cuidado porque trabajando con este usuario se podría modificar alguna parte crítica del sistema sin saberlo y luego éste podría no funcionar correctamente.

Router.- Dispositivo que distribuye tráfico entre redes. La decisión sobre a dónde enviar se realiza en base a información de nivel de red y tablas de direccionamiento. El router se necesita cuando las dos redes utilizan la misma capa de transporte y tienen diferentes capas de red. Por ejemplo, para una conexión entre una red local ethernet y una red pública X.25, se necesitaría un router para convertir las tramas ethernet a la forma que exige la red X.25.

RPM.- El Red Hat Package Manager (RPM). Es un sistema de gestión de paquetes que puede ser utilizado por cualquiera y funciona sobre la plataforma Red Hat Unix como otras distribuciones de sistemas Linux y Unix, Red Hat, etc.

Sabotaje.- Es la destrucción de equipo y/o información relevante por una persona que normalmente pertenece a la institución y se encuentra resentida o por otros intereses.

Sanción.- Acto solemne mediante el cual se confirma una ley.

Scanner.- Programa que permite rastrear la red en busca de puertos abiertos por los cuales tener acceso y manipular un sistema o introducir un virus o troyano.

Script Kiddie.- Denominados Skid Kiddie o Script Kiddie, son el último eslabón de la red. Se trata de simples usuarios de Internet, sin conocimientos sobre Hack o el Crack. Simplemente, son internautas que se limitan a recopilar información de la red.

Script.- Serie secuencial de instrucciones que permite realizar tareas sencillas y repetitivas, generalmente son interpretadas en tiempo de ejecución, aunque hay sistemas que permiten compilar los scripts. Algunos de los sistemas de scripts son verdaderos lenguajes de programación.

Seguridad.- Se refiere a todo tipo de precauciones y protecciones que se llevan a cabo para evitar cualquier tipo de daño y riesgo.

Seguridad de la Información.- Se refiere a la prevención y a la protección, a través de ciertos mecanismos, para evitar que ocurra de manera accidental o intencional, la transferencia, modificación, fusión o destrucción no autorizada de la información.

Seguridad física.- Como seguridad física debemos entender todo aquello que nos lleva proteger el hardware de nuestro sistema o acceso a él.

Seguridad Informática.- Es una colección de herramientas y procedimientos diseñados para proteger datos y detener a los intrusos, es decir, es la protección de los sistemas de cómputo para evitar amenazas de confidencialidad, integridad o disponibilidad.

Seguridad lógica.- Consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo.

Seguridad de la red.- Consiste en la protección de los recursos de la red, la información y servicios contra las amenazas de seguridad.

Servidor.- Computadora o software que proporciona algún servicio a otras computadoras conocidas como clientes.

SFUG .- Guía del Usuario de Características de Seguridad.

Shell.- Intérprete de comando de un sistema operativo. Se encarga de tomar las órdenes del usuario y hacer que el sistema operativo las ejecute. Se sitúa entre el *kernel* y el usuario.

Sistema.- Conjunto de partes que interactúan en busca de un fin común.

Sistema biométrico.- Es un sistema que normalmente se utiliza para la autentificación de personas el cual se basa en características biológicas de las personas.

Sistema de archivos.- Es aquella parte del sistema responsable de la administración de los datos en dispositivos de almacenamiento secundario.

Sistema de decisión informatizado.- Es un sistema que permite tomar decisiones por medio de la información que presenta, y esta implementado por medio de equipo de cómputo.

Sistema operativo.- Conjunto de programas que administran los recursos de hardware y software de una computadora. Es la interfaz entre el usuario y la computadora.

SMTP (*Simple Mail Transport Protocol*).- Un cliente de correo SMTP establecerá y sostendrá conexión con el servidor durante el tiempo en que esté corriendo, ya sea que el correo esté siendo transferido o no. En tal sentido no tiene un aprovechamiento tan eficiente del ancho de banda como el POP.

Sniffer.- Es un programa que monitorea y analiza el tráfico dentro de una red y gracias a su uso se puede detectar problemas y embotellamiento. También se denomina sniffer al uso legal o ilegal de captura de paquetes de información transmitida a través de una red. Esa es la razón por la que este segundo significado está más popularizado en la red.

Socket.- Se trata del dispositivo lógico de la recepción y envío de datos en una red, todos los dispositivos físicos de una computadora tienen una dirección lógica a donde enviar los datos y de dónde se esperan las respuestas; de la misma manera se utiliza un conjunto de dispositivos lógicos para controlar las conexiones con otras computadoras como si fueran otros periféricos.

Software.- Códigos fuente y objeto, utilidades, programas de diagnóstico, sistemas operativos, programas de comunicación.

Spam.- Correo electrónico no solicitado, normalmente publicitario.

SSH (*Secure Shell*).- Es una aplicación de seguridad que permite la conexión entre computadoras de forma segura, a través de un demonio sshd.

Superzapping.- Es el uso no autorizado de un programa editor de archivos para alterar, borrar, copiar, insertar o utilizar en cualquier forma no permitida los datos almacenados en los soportes de una computadora.

ST (*Security Target*, Meta de Seguridad).- Es una especificación que define una solución general de un desarrollador para un problema de seguridad. Básicamente una Meta de Seguridad establece: Esto es lo que se ha construido o se construirá en el futuro.

Tarjeta inteligente.- Nombre que reciben unas tarjetas que contienen un pequeño chip en el cual se puede almacenar cierta información.

TCB (*Trusted Computer Base*).- Base de Computadoras Confiable.

TCFS (*Transparent Cryptographic File System*).- Es un *software* desarrollado en la Universidad de Salerno y disponible para sistemas Linux que proporciona una solución al problema de la privacidad en sistemas de archivos distribuidos como NFS.

TCP/IP (*Transmission Control Protocol / Internet Protocol*).- El término describe dos mecanismos de software empleados para posibilitar la múltiple comunicación entre computadoras de manera libre de error. TCP/IP es el lenguaje común de la Internet, el que permite que diferentes tipos de computadoras utilicen la red y comuniquen unas con otras, indiferentemente de la plataforma o sistema operativo que usen.

TCSEC (*Trusted Computer Systems Evaluation Criteria*).- Son criterios de evaluación de sistemas informáticos fiables, los cuales indican niveles de seguridad. La publicación de estos criterios se le conoce también como el Libro Naranja (*Orange Book*).

Tecnología.- Conjunto de los conocimientos, instrumentos y métodos técnicos empleados en un sector profesional.

Telnet .- Programa para Internet basado en texto, usado para enlazarse a una máquina remota. Una vez conectada, la máquina propia se comporta como si el usuario estuviera realmente sentado frente a la otra, aun cuando se hallen en diferentes partes del mundo.

Time frame.- Tiempo que una organización puede asumir con paralización de la actividad operativa antes de incurrir en pérdidas significativas.

TOE(*Target of Evaluation*).- Objetivo de la Evaluación.

Underground.- La traducción literal de este término es "debajo de la tierra", implica que algo no es muy conocido.

UNIX.- Sistema operativo cómodo, rápido y con características de MULTICS desarrollado por un grupo de investigadores de AT&T entre los que se encontraban Ken Thompson, Rudd Canaday, Doug Mellroy, Joe Hosanna y Dennis Ritchie.

URL (*Uniform Resource Locator*).- Es la dirección de un sitio en Internet con el nombre del servidor , el directorio donde esta el material y el nombre del archivo que lo contiene.

Userid.- Número que identifica a un usuario dentro del sistema.

Violación.- Acto de infringir o quebrantar una ley o precepto.

Virus.- Es un fragmento de código que se inserta en un programa ejecutable, de modo que cuando el programa es ejecutado, se ejecuta también el virus. La función que un virus

pretende realizar es propagarse a sí mismo por todo el sistema. Para ello va infectando a otros programas en los que inserta el fragmento de código vírico.

Vulnerabilidad.- Es el debilitamiento o ausencia de una protección en un recurso.

WWW (*World Wide Web*).- Proporciona una manera de enlazar las computadoras en Internet a través del código html y usando hipervínculos que le permiten avanzar de un sitio a otro en la Web.

Bibliografía y Referencias

BIBLIOGRAFÍA

MEDIAVILLA, Manuel. Seguridad en UNIX. Colombia, Editorial Alfaomega, 1998. 224 p.

ANÓNIMO. Linux máxima seguridad. Edición especial. España, Editorial Prentice-Hall, 2000. 780 p.

KRICK, Edward. Introducción a la Ingeniería y al Diseño en la Ingeniería. 2da. Edición. México, Editorial Limusa, 1982. 240 p.

PIZARRO, Gil Julio. Diccionario General de Informática. Editorial ABETO. España.1999. p. 276.

RINCÓN, Antonio. Diccionario conceptual de Informática y Comunicaciones. España, Editorial Paraninfo, 1998. p. 329.

QUEZADA, Reyes Cinthia y GUTIÉRREZ, Rodríguez Sergio. Fundamentos de Seguridad de la Información. Tesis (Licenciatura en Ingeniería en Computación). México, D.F., Universidad Nacional Autónoma de México, Facultad de Ingeniería, 2001. pp. 29-43.

Diccionario de la Lengua Española. Real Academia Española. 1992. p. 1317.

O'REILLY. Seguridad Práctica en Unix e Internet. México, Editorial Mc Graw Hill, 1999. p. 13.

ALVAREZ, Ricardo y AMEZCUA Luis. UNIX. México, Editorial Facultad de Ingeniería, 1994. pp. 1-4.

ARDITA, Julio César. Director de Cybsec S.A. Security y exHacker. Entrevista realizada el día 15 de enero de 2001 por Cristian F. Borghelio en instalaciones de Cybsec S.A.

MONTT, Manuel. General del Ejército de Chile. La guerra, su conducción político-estratégica. 1970. p. 29.

RFC 1244: Site Security Handbook. J. Reynolds – P. Holbrook. Julio 1991.

Susan Peppard et al. *Unix Unleashed.* Sams Publishing, 1st edition, 1994.

Dave Curry et al. *RFC1244: Site Security Handbook.* Internet Activities Board, Julio 1991.

Karanjit Siyan and Chris Hare. *Internet y seguridad en redes.* Prentice Hall, 1995.

ESCOBAR Valenzuela, Gustavo. Ética. Cuarta edición. México, Editorial McGraw-Hill, 1999. 223 p.

GARZA de Flores, Rosa María. Ética. México, Editorial Alambra, 1998. 296 p.

RODRÍGUEZ, Lozano V. Ética. México, Pearson Educación, 1998. 243 p.

ESCOBAR, Valenzuela Gustavo. Ética. Cuarta Edición. México, Editorial McGraw-Hill, 1999. 223 p.

MOOR, James H. "What is Computer Ethics?", *Metaphilosophy*. Vol. 16, No. 4, October 1985.

LEGA, Carlos. *Deontología de la profesión de Abogado*. Madrid, Editorial Civitas, 1976.

HOLVAST, Jan. "Codes of Ethics: Discussion Paper" en INTERNATIONAL FEDERATION FOR INFORMATION PROCESSING (IFIP), *Ethics of Computing: Information Technology and Responsibility*. Madrid, 1992.

PARKER, Donn B., SWOPE, Susan y BAKER, Bruce N. *Ethical conflicts in information and computer science, technology, and business*, QED Information Sciences. MA (USA), Wellesley, 1990.

BERLEUR, Jacques. "Final Remarks: Ethics, Self-Regulation and Democracy" en BERLEUR, Jacques y BRUNNSTEIN, Klaus (eds.): *Ethics of Computing. Codes, spaces for discussion and law*. London, Chapman & Hall, 1996.

JOHNSON, Deborah G. y MULVEY, John M. "Accountability and Computer Decision Systems". *Communications of the ACM*, Diciembre 1995. Vol. 38, No. 12.

REFERENCIAS

Nota: Por el continuo movimiento de las direcciones de Internet es posible que algunas de las enumeradas a continuación no se encuentren disponibles para consultas.

- DGSCA.
  http://sistemas.dgsca.unam.mx
- INEGI.
  http://www.inegi.gob.mx
- Grupo ASISA de México S.A. de C.V.
  http://gamsagdl.galeon.com/index.html
- Jorge Machado. Hackers famosos.
  http://www.perantivirus.com/sosvirus/hackers/index.htm
- Páginas personales de profesores. M.I. Ma. Jaquelina López Barrientos.
  http://www.fi-b.unam.mx/index2.html
- Sekureit. Consultores de Seguridad. 2001-2003.
  http://www.sekureit.com/
- JIPS, BankHackers. Instalación del Scanner de Mail en Linux: MailScanner y Sendmail . 2002.
  http://webmaster.bankhacker.com/mailscanner/
- Víctor A. González Barbone. Respaldo.
  http://iie.fing.edu.uy/ense/asign/admunix/respaldo.htm#RstSistemas
- DDiego. Crackeando Pass en Unix con Nuestro Amigo John.
  http://www6.gratisweb.com/disidents/ascii/ezine/john.html
- Criptoanálisis.
  http://www.igf.es/manuales/Manuales%20Programacion%20Vol.%201/Criptografia/PGP/INTRODUC/CRIPTO.HTM.
  http://www.umsanet.edu.bo/sociedad/CRIPTO/DEFINICION.HTM
- Anónimo.
  http://www.elcarmenvigo.com/lista.htm
- ArCERT. Coordinación de Emergencia en Redes Teleinformáticas de la Administración Pública en Argentina. Manual de Seguridad en Redes.
  http://www.arcert.gov.ar/webs/manual/manual_de_seguridad.pdf
- Seminario GASU.
  http://www.seguridad.unam.mx/Eventos/Gasu/prox.html
- Microasist.Servicios/Contingencia.
  http://microasist.com..mx/servicios/definicion.shtm
- NIST. Advanced Encryption Standard.
  http://csrc.nist.gov/encryption/aes/
- Seguridad. Entrebits.
  http://www.entrebits.com/php/seguridad/articulosVer.php?idSec=186&date=2002-07-24&extSec=jpg
- El Congreso de EEUU triplica el gasto en ciberseguridad. 2002.
  http://www.elmundo.es/navegante/2002/11/13/seguridad/1037146155.html

- Unidad de la Comunicación de la Computación Tendencias de Políticas y Estrategias.2002.
  http://www.itu.int/itunews/issue/2002/08/policy-es.html
- IDG. El futuro de la seguridad de la información.
  http://www.aliaconsultores.com/futuro_de_la_seguridad_de_la_inf.htm
- Fernández, Calvo Rafael. Glosario básico inglés-español para usuarios de Internet. julio de 2001.
  http://www.ati.es/novatica/glosario/buscador/buscador_gloint.html
- Molina, Diego. Seguridad[en línea]. Universidad del Salvador.
  http://www.salvador.edu.ar/molina.htm#Seguridad
- Guardia Civil. (2001). Seguridad informática. *En profundidad* [en línea].
  http://www.guardiacivil.org/00revista/profundidad/index.asp?numrevista=687
- Montoya, Edwin y ALONSO, Cañón Jorge (1997). Riesgos, Políticas y Herramientas de Seguridad en Redes. *Revista Universidad EAFIT* [en línea].
  http://www.eafit.edu.co/revista/107/montoya.pdf
- The Linux Counter. The Linux Webring [en línea].
  http://counter.li.org
- Howard, John D. An Analysis of security on the Internet 1989-1995. Tesis(Doctor en Filosofía)[en línea]. EE. UU., Carbegie Institute of Technology, Carnegie Mellon University, 1995. Capítulo 6, p. 59.
  http://www.cert.org/research/JHThesis/Word6
- Huerta, Villalón Antonio. *Seguridad en Unix y Redes*[en línea]. Versión 2.1. Julio 2002. Capítulo 22. Gestión de la Seguridad.
  http://www.rediris.es/cert/doc/unixsec/unixsec.pdf
- SPAFFORD, Gene.(2000). "Manual de seguridad en redes" [en línea]. Argentina, ArCERT.
  http://www.arcert.gov.ar/webs/manual/manual_de_seguridad.pdf
- Políticas de seguridad informática[en línea]. Madrid, 9 Noviembre 2001.
  http://www.delitosinformaticos.com/articulos/100530260583540.shtml
- Instituto Nacional de Estadística e Informática. Seguridad en Redes de Datos [en línea].
  http://www.inei.gob.pe/web/BiblioInei/ListaItemByTemaPalabra.asp?c=15&tt=Seguridad%20de%20la%20Informaci%C3%B3n
- Listas de Correo.
  http://www.elcarmenvigo.com/lista.htm
  http://www.rediris.es/cert/links/listas.es.html
  http://xforce.iss.net/xforce/maillists/otherlists.php
- Departamento de Auditoría Informática. (sin fecha). *Plan de Contingencias*[en línea]. DGSCA.
  http://sistemas.dgsca.unam.mx/publica/pdf/Contingencias1.PDF
- Microasist.
  http://microasist.com.mx/servicios/definicion.shtml
- Curso Administración UNIX.
  http://iic.fing.edu.uy/ense/asign/admunix/respaldo.htm#RstSistemas
- BORGHELLO, Cristian F. (2001). Capítulo 9. Políticas de Seguridad en Seguridad Informática [en línea].
  http://www.htmlweb.net/seguridad/seguridad.html
- Godoy, Emma. ¿Qué son y para qué sirven los valores? [en línea].

http://www.mty.itesm.mx/dhcs/centros/cvep/lecturas

- Tcp-Wrappers.
  ftp://ftp.asc.unam.mx/Herramientas/Unix/TCP_Wrappers
- Netlog.
  ftp://ftp.asc.unam.mx/Herramientas/Unix/Monitor_Red/Netlog
- argus.
  ftp://ftp.andrew.cmu.edu/pub/argus/
- tcdump.
  ftp://ftp.asc.unam.mx/Herramientas/Unix/Monitor_Red/Tcpdump
- Traceroute.
  ftp://ftp.asc.unam.mx/Herramientas/Unix/Monitor_Red/Traceroute
- Netcat.
  http://www.atstake.com/research/tools/index.html
- Ident-Scan.
  http://208.176.57.92/~daveg/projects/i-scan.html
- Strobe.
  ftp://suburbia.net/pub/
- Nmap.
  http://www.insecure.org.nmap
- Ethereal.
  http://www.ethereal.com
- Dsniff.
  http://monkey.org/~dugsong/dsniff/
- Hping2.
  http://www.hping.org
- Sniffit.
  http://sniffit.rug.ac.be/~coder/sniffit/sniffit.html
- Cheops-ng.
  http://cheops-ng.sourceforge.net
- Libnet.
  http://www.packetfactory.net/libnet
- IPTraf.
  http://cebu.mozcom.com/riker/iptraf/about.html
- ISS.
  ftp://coast.cs.purdue.edu/pub/tools/unix/iss
  http://www.cert.org/advisories/CA-93.14.Internet.Security.Scanner.html
- Swatch.
  ftp://ftp.stanford.edu/general/security-tools/swatch /
- TARA.
  http://www-arc.com/tara/
- Tripwire.
  http://www.tripwire.com
- Nessus.
  http://www.nessus.org
- SATAN.
  http://www.fish.com/satan
- Saint.

http://www.wwdsi.com/saint

- SARA.
  http://www-arc.com/sara
- Logcheck.
  http://www.psionic.com/products/logsentry.html
- Merlin.
  ftp://ciac.llnl.gov/pub/ciac/sectools/unix/merlin/
- anlpasswd.
  ftp://info.mcs.anl.gov/pub/systems/
  ftp://ftp.seguridad.unam.mx/Herramientas/Unix/Autenticacion/Anlpasswd/
  ftp://ftp.cerias.purdue.edu/pub/tools/unix/pwdutils/anlpasswd/
- Crack.
  http://www.users.dircon.co.uk/~crypto/
  ftp://ftp.cerias.purdue.edu/pub/tools/unix/pwdutils/crack/
- Cracklib.
  http://www.users.dircon.co.uk/~crypto/
  ftp://ftp.cerias.purdue.edu/pub/tools/unix/libs/cracklib/
- passwd+.
  ftp://ftp.dartmouth.edu/pub/security/
- S/Key.
  ftp://thumper.bellcore.com/pub/nmh/docs/skey.txt
  ftp://thumper.bellcore.com/pub/nmh/
- John the Ripper.
  http://www.openwall.com/john/
  http://www6.gratisweb.com/disidents/ascii/ezine/john.html
- Kerberos.
  http://consult.stanford.edu/afsinfo/kerberos.shtml
  ftp://athena-dist.mit.edu/pub/kerberos/
- pidentd.
  ftp://ftp.cerias.purdue.edu/pub/tools/unix/daemons/pidentd/servers/
- ssh.
  http://ftp.ssh.com/pub/ssh
- OpenSSH.
  http://www.openssh.com/
- swatch.
  http://www.oit.ucsb.edu/~eta/swatch/
- Spar Show Process Accounting Records.
  ftp://net.tamu.edu/pub/security/TAMU/
- Watcher.
  ftp://ftp.unm.edu/pub/unix/
- Snort.
  http://www.snort.org/
- Hunt.
  http://lin.fsid.cvut.cz/~kra/index.html#HUNT
- scanlogd.
  http://www.openwall.com/scanlogd/
- NFR.

http://www.nfr.com/about/

- Lids.
  http://www.be.lids.org/about.html
- HostSentry.
  http://www.psionic.com/products/hostsentry.html
- MailScanner.
  http://webmaster.bankhacker.com/mailscanner/
- Seguridad de Cómputo de la UNAM.
  http://www.asc.unam.mx/
- Políticas de Seguridad.
  http://www.htmlweb.net/seguridad/tesis/Cap9.pdf
- Código Penal Federal
  http://www.cddhcu.gob.mx/leyinfo/
- Quispe Otazú Rodolfo. Ética Informática. Bilbao, julio de 1997.
  http://www25.brinkster.com/educarodo/manuales/manual0010.asp
- José M. Guibert Ucín, SJ. ¿Qué es la ética informática?
  http://paginaspersonales.deusto.es/guibert/1etic-info.html
- Gerardo Silvestre Reyna Caamaño. Informática: Ética vs Competitividad. 2000.
  http://www.geocities.com/Paris/Chateau/9164/papers/infoetica.htm
- Lecturas complementarias.
  http://www.mty.itesm.mx/dhcs/centros/cvep/lecturas/
- Rainbow Series Library.
  http://www.radium.ncsc.mil/tpep/library/rainbow/
- Itrain online.
  http://www.itrainonline.org/itrainonline/spanish/glossary.shtml
- Sala de Informática.
  http://www.atheneum.doyma.es/Socios/sala_inf/glosario.html#request
- Manuel Gómez Salazar. Underground & seguridad.
  http://www.duiops.net/hacking/
- Grupo Clarín.
  http://www.clarin.com.ar/suplementos/informatica/htm/glosario.htm
- My Web.
  http://members.tripod.com/webprototype/linux02.html
- Rafael Fernández Calvo. Glosario básico inglés-español para usuarios de Internet.
  http://www.ati.es/novatica/glointv2.html