UIVERSIDAD NACIONAL AUTONOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN

TUTORIAL DE SEGURIDAD INFORMÁTICA

T E S I S

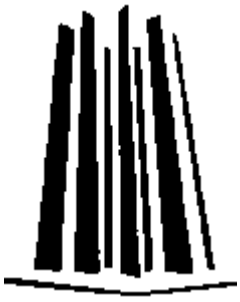
QUE PARA OBTENER EL TITULO DE:

INGENIERO EN COMPUTACIÓN

P R E S E N T A:

JACOB BENJAMÍN HERNADEZ RODRÍGUEZ

ASESOR: M.EN C. MARÍA JAQUELINA LÓPEZ BARRIENTOS



SAN JUAN DE ARAGON, ESTADO DE MÉXICO 2010

Agradecimientos

A Dios por darme la vida y la capacidad para afrontar cualquier reto.

A la UNAM por darme la oportunidad de presentar éste proyecto.

A mi familia por apoyarme en mis decisiones.

A mi asesora de tesis por tenerme paciencia y enseñarme tantas cosas.

Muchas gracias a todos.

Tutorial de Seguridad Informática

Introducción.

Desde su creación las computadoras han evolucionado enormemente, la mejora constante de estas tecnologías les permiten realizar operaciones más complejas en menor tiempo, reducir la posibilidad de que ocurran errores y mejorar la interacción con los usuarios mediante interfaces mas sencillas.

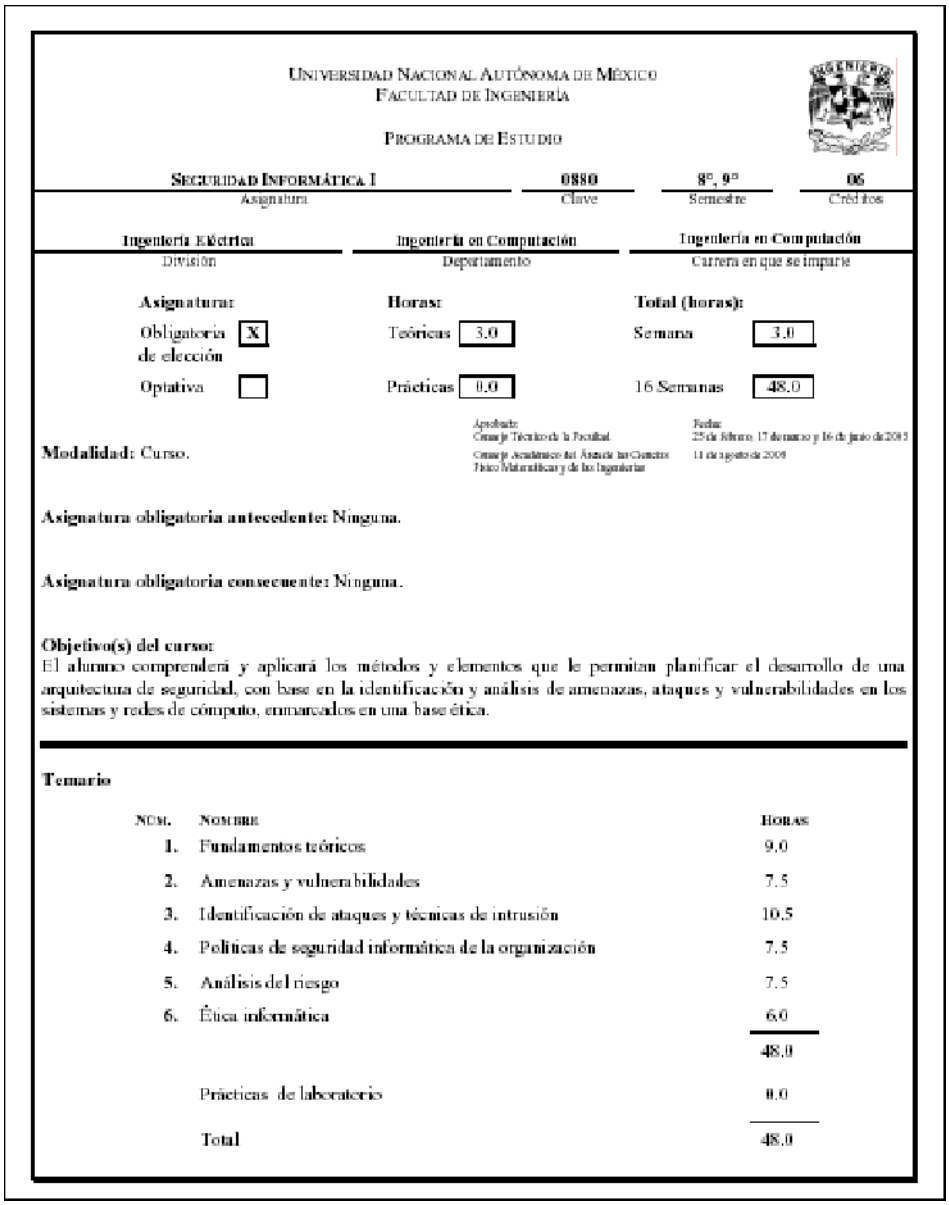
A la par con su evolución, las computadoras cada vez más forman parte de las actividades humanas, tales como los procesos industriales, el préstamo de servicios, actividades artísticas (herramientas de diseño gráfico o edición de música en formato digital por ejemplo), recopilación, almacenamiento y difusión de la información, entre otras aplicaciones. Tal es la presencia de estas tecnologías que muchas actividades se volverían difíciles de realizar sin su utilización, incluso aquellas que en otros tiempos no tenían relación alguna con tecnologías computacionales.

Poco a poco las personas se han familiarizado con el uso de las computadoras, así como los términos mas usuales relacionados a ellas, conceptos como correo electrónico, sistema operativo, base de datos o Internet que antes resultaban oscuros y difíciles ahora forman parte del lenguaje cotidiano de personas de diferentes niveles laborales.

Ahora más que antes, es importante fomentar una cultura de seguridad, enseñar a los usuarios lo significativo que es proteger sus recursos computacionales, asegurar la disponibilidad e integridad de sus equipos y sistemas, así como la certeza de que la información que manejan esté protegida contra entidades no deseadas.

Este conjunto de ideas forman parte importante de lo que es la Seguridad Informática.

Con el propósito de que los alumnos obtengan los conocimientos relacionados al tema de Seguridad Informática, la Universidad Nacional Autónoma de México por medio del Consejo Académico del Área de las Ciencias Físico Matemáticas y de las Ingenierías aprobó las asignaturas de la Seguridad Informática I y II como parte del plan de estudios 2006 de la carrera de Ingeniería en Computación en la Facultad de Ingeniería de la UNAM (véanse figuras 1 y 2).



UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
FACULTAD DE INGENIERÍA

PROGRAMA DE ESTUDIO

SEGURIDAD INFORMÁTICA I	0880	8°, 9°	06
Asignatura	Clave	Semestre	Créditos

Ingeniería Eléctrica	Ingeniería en Computación	Ingeniería en Computación
División	Departamento	Carrera en que se imparte

Asignatura:		Horas:		Total (horas):	
Obligatoria de elección	X	Teóricas	3.0	Semana	3.0
Optativa		Prácticas	0.0	16 Semanas	48.0

Aprobado: Consejo Técnico de la Facultad — Fecha: 25 de febrero, 17 de marzo y 16 de junio de 2008
Consejo Académico del Área de las Ciencias Físico Matemáticas y de las Ingenierías — 18 de agosto de 2008

Modalidad: Curso.

Asignatura obligatoria antecedente: Ninguna.

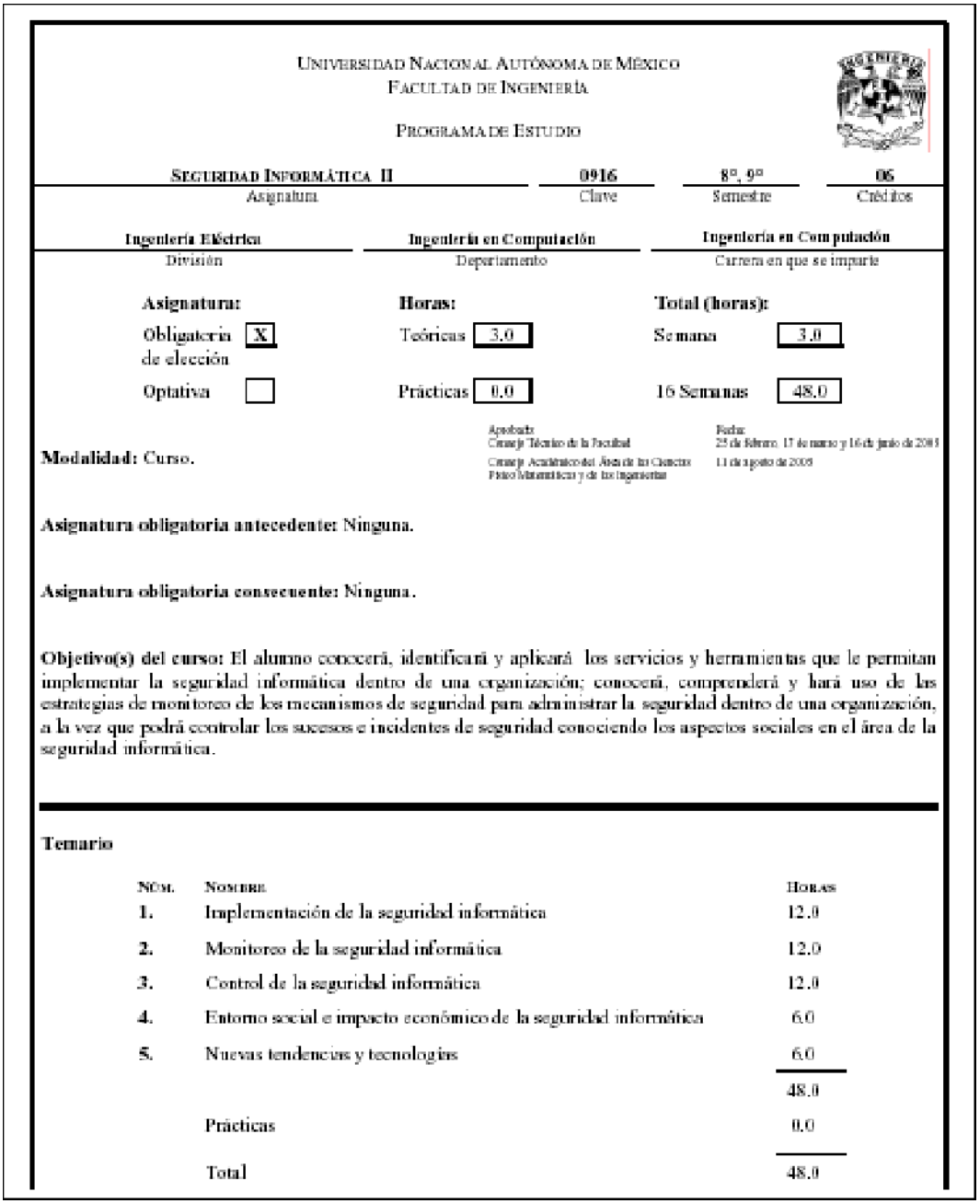
Asignatura obligatoria consecuente: Ninguna.

Objetivo(s) del curso:
El alumno comprenderá y aplicará los métodos y elementos que le permitan planificar el desarrollo de una arquitectura de seguridad, con base en la identificación y análisis de amenazas, ataques y vulnerabilidades en los sistemas y redes de cómputo, enmarcados en una base ética.

Temario

NÚM.	NOMBRE	HORAS
1.	Fundamentos teóricos	9.0
2.	Amenazas y vulnerabilidades	7.5
3.	Identificación de ataques y técnicas de intrusión	10.5
4.	Políticas de seguridad informática de la organización	7.5
5.	Análisis del riesgo	7.5
6.	Ética informática	6.0
		48.0
	Prácticas de laboratorio	0.0
	Total	48.0

Figura 1. Portada del temario de Seguridad Informática I



UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
FACULTAD DE INGENIERÍA

PROGRAMA DE ESTUDIO

SEGURIDAD INFORMÁTICA II	0916	8°, 9°	06
Asignatura	Clave	Semestre	Créditos

Ingeniería Eléctrica	Ingeniería en Computación	Ingeniería en Computación
División	Departamento	Carrera en que se imparte

Asignatura:		Horas:		Total (horas):	
Obligatoria de elección	X	Teóricas	3.0	Semana	3.0
Optativa		Prácticas	0.0	16 Semanas	48.0

Aprobado: Consejo Técnico de la Facultad; Consejo Académico del Área de las Ciencias Físico Matemáticas y de las Ingenierías
Fecha: 25 de febrero, 17 de marzo y 16 de junio de 2005; 11 de agosto de 2005

Modalidad: Curso.

Asignatura obligatoria antecedente: Ninguna.

Asignatura obligatoria consecuente: Ninguna.

Objetivo(s) del curso: El alumno conocerá, identificará y aplicará los servicios y herramientas que le permitan implementar la seguridad informática dentro de una organización; conocerá, comprenderá y hará uso de las estrategias de monitoreo de los mecanismos de seguridad para administrar la seguridad dentro de una organización, a la vez que podrá controlar los sucesos e incidentes de seguridad conociendo los aspectos sociales en el área de la seguridad informática.

Temario

NÚM.	NOMBRE	HORAS
1.	Implementación de la seguridad informática	12.0
2.	Monitoreo de la seguridad informática	12.0
3.	Control de la seguridad informática	12.0
4.	Entorno social e impacto económico de la seguridad informática	6.0
5.	Nuevas tendencias y tecnologías	6.0
		48.0
	Prácticas	0.0
	Total	48.0

Figura 2. Portada del temario de Seguridad Informática II

De igual manera, en la Facultad de Estudios Superiores Aragón ha sido incluida a partir del 2007 la materia de Seguridad Informática (véase figura 3) como parte del plan de estudios de la misma carrera, aunque el temario para ambas facultades difiere en el orden y contenido de los temas, ambos temarios comparten gran parte de los conocimientos indispensables para proporcionar una formación completa en el tema de seguridad informática.

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN

INGENIERIA EN COMPUTACIÓN

SEPTIMO SEMESTRE

ASIGNATURA: Seguridad Informática				AREA DE CONOCIMIENTO: Redes	
		HORAS / SEMANA/SEMESTRE			
CARACTER: Obligatoria	**CLAVE:**	**TEORIA:** 4	**PRACTICA:** 0.0	**HORAS:** 64.0	**CREDITOS:** 08
TIPO	Teórica				
MODALIDAD:	Curso				
ASIGNATURA(S) INDICATIVA(S) PRECEDENTE(S):	Sistemas operativos Sistemas de Información				
ASIGNATURA(S) INDICATIVA(S) SUBSECUENTE(S):	Redes de computadoras II				
OBJETIVO(S): Proporcionar al alumno los conocimientos básicos de la seguridad informática, así como su importancia y las herramientas más utilizadas en el área. Proporcionar al alumno nociones de criptografía.					

UNIDADES TEMATICAS

NUMERO DE HORAS POR UNIDAD	**UNIDAD 1.** SEGURIDAD INFORMATICA	**NUMERO DE HORAS POR UNIDAD**	**UNIDAD 2.** CONTROL DE ACCESO
8.0	1.1 Conceptos básicos. 1.2 Historia. 1.3 Vulnerabilidades, Amenazas y Ataques. 1.4 Seguridad física. 1.5 Seguridad lógica. 1.6 El costo de la seguridad. 1.7 los elementos de la seguridad.	8.0	2.1 Identificación y autenticación. 2.2 Tipos de control de acceso: 2.2.1 Control de acceso voluntario (CAV). 2.2.2 Control de acceso obligatorio (CAO). 2.3 Tipos de autenticación: 2.3.1 Basada en algo que se sabe. 2.3.2 Basada en algo que se es (autenticación biométrica). 2.3.3Basada en algo que se tiene. 2.3.4 Basada en donde se está.
	3.2 Aseguramiento de sistemas tipo UNIX. 3.2.1 Acceso. 3.2.2 Administración de políticas. 3.2.3 Administración de servicios. 3.2.4 Uso de herramientas de seguridad.		
	3.3 Aseguramiento de sistemas comerciales NO UNIX. 3.3.1 Acceso. 3.3.2 Administración de políticas. 3.3.3 Administración de servicios. 3.3.4 Uso de herramientas de seguridad.		—
NUMERO DE HORAS POR UNIDAD	**UNIDAD 5.** SEGURIDAD EN REDES Y BASES DE DATOS	**NUMERO DE HORAS POR UNIDAD**	**UNIDAD 6.** CRIPTOGRAFÍA
18	5.1 Seguridad en redes. 5.1.1 Protocolo UUCP. 5.1.2 Protocolo TCP/IP. 5.1.3 Seguridad en Internet. 5.2. Seguridad en Bases de Datos. 5.2.1 Amenazas a la seguridad en Bases de Datos. 5.2.2 Requerimientos de protección de Bases de Datos. 5.2.3 Control de Acceso. 5.2.4 Prácticas recomendadas.	12	6.1 Criptografía (Clasificaciones) 6.1.1 Por el número de llaves. 6.1.2 Por el modo de proceso. 6.1.3 Por el tipo de operaciones. 6.2 Algoritmos simétricos clásicos y Criptoanálisis. 6.3 DES. 6.4 RSA. 6.6 MD5.
		TOTAL DE HORAS: 64	

Figura 3. Portada del temario de Seguridad Informática de la FES Aragón.

Como parte las actividades de mi servicio social, realicé un proyecto de investigación documental concerniente al tema de Seguridad Informática para el departamento de Ingeniería en Computación de la Facultad de Ingeniería de la UNAM. Tal proyecto me ha servido de base para retomar el tema como objeto de estudio para la realización de mi tesis, la cual a grandes rasgos consistirá en actualizar y expandir esta investigación.

Considerando la importancia de los conocimientos revisados en esta asignatura y que estos deben ser adquiridos por los alumnos universitarios de la mejor manera posible, considero conveniente el desarrollo de una herramienta de apoyo que ayude a los estudiantes a una mejor comprensión del tema.

La herramienta que he optado por desarrollar es un sistema tutorial el cual no pretende sustituir las clases teóricas. El tema de Seguridad Informática es muy amplio, donde cada punto puede ser tratado como el objeto de estudio de una investigación, por ello, el tutorial sólo se limitará a sintetizar de forma concisa los temas indicados en el temario de la asignatura llamada "Seguridad Informática I" la cual es impartida en la Facultad de Ingeniería, así como una selección de temas del programa de "Seguridad Informática" impartida en la FES Aragón.

La decisión de partir de un temario y complementarlo con algunos temas la he tomado con base en tres puntos que considero importantes para este proyecto de tesis:

a) Enfocarme a comunicar los conceptos generales de la seguridad informática, los cuales al ser comprendidos plenamente pueden aplicarse a casos particulares.

Para este propósito el temario correspondiente a "Seguridad Informática I" me parece más apropiado ya que se enfoca a las bases y conocimientos que son fundamento de la seguridad informática sin abundar en los casos específicos.

b) Evitar la redundancia de temas, ya que sólo se incrementaría innecesariamente la longitud de este proyecto. Varios temas son tratados en ambos temarios por lo que no considero pertinente duplicar la misma información.

c) Considero que al complementar ambos temarios, se puede expandir el alcance de esta herramienta, de tal forma que sea útil para los alumnos de ambas entidades.

Así mismo, contar con un temario establecido me permite partir de una base sólida para enfocar este proyecto a una meta definida.

El capitulado de este proyecto de tesis está dividido en los siguientes tema principales:

1. Fundamentos teóricos
2. Amenaza y vulnerabilidades
3. Identificación de ataques y técnicas de intrusión
4. Políticas de seguridad informática de la organización
5. Análisis de riesgo
6. Ética Informática

Y como puede observarse todos son de gran importancia en el campo de la seguridad informática.

La plataforma que se ha elegido para la creación del tutorial es el lenguaje de programación web HTML, lo que facilita su posterior colocación en línea como una página web. Esto se determinó considerando la necesidad de que los alumnos que requieran usar esta herramienta, puedan hacerlo a través de una consulta en línea por Internet.

Los objetivos que se buscan alcanzar en este proyecto son los siguientes:

- Recopilar y exponer de manera ordenada la información relacionada con todos los temas del programa.

- Crear un tutorial confiable y de uso libre que sirva de apoyo a los estudiantes de la Facultad de Ingeniería de la UNAM

- Crear el tutorial en formato HTML incluyendo un menú de navegación que permita una exploración rápida y sencilla de los temas.

Con el desarrollo de este sistema se pretende que tanto los estudiantes como los profesores de la asignatura mencionada cuenten con una herramienta más de apoyo la cual permita acceder a conocimientos de manera expedita.

Para ello el presente trabajo abre en el capitulo 1 Fundamentos teóricos, exponiendo un breve seguimiento histórico de la importancia de proteger la información y posteriormente explicando una serie de conceptos que suponen las bases de la Seguridad Informática.

A continuación en el capitulo 2 Amenaza y vulnerabilidades se expone mas detalladamente el origen y tipos de peligros a los que un sistema informático está expuesto.

El capitulo 3 Identificación de ataques y técnicas de intrusión, parte de los peligros definidos en el capitulo 2 y expone mas a detalle las técnicas usadas por los atacantes para alcanzar sus objetivos de vulnerar un sistema.

En el capitulo 4 Políticas de seguridad informática de la organización, se explica las estrategias que una organización debe tener para prevenir, y enfrentar situaciones desfavorables que pongan en riesgo sus activos.

El capitulo 5 Análisis de riesgo, expone la importancia de identificar las amenazas que se enfrenta, que efectos producen y conocer la probabilidad que ocurran, todo con el propósito de adoptar las estrategias adecuadas para enfrentarlas.

El trabajo concluye en el capitulo 6 Ética Informática tratando uno de los temas mas importantes para la seguridad informática, y eso es la el comportamiento de las personas en un ambiente de tecnologías computacionales.

.

Finalmente, presento las conclusiones a las que llegué al finalizar el desarrollo de la presente tesis.

Metodología

Con la finalidad de facilitar el diseño de la página web que contendrá al tutorial, es conveniente seguir una metodología que facilite su diseño, desarrollo y análisis.

Actualmente no existen metodologías definidas para crear un sitio web, aun así hay una serie de criterios generales que se deben tomar en cuenta para la realización de un proyecto web, procedimientos básicos que incluyen la definición de los objetivos y límites del proyecto, planificación y diseño previo, recolección de los activos necesarios, redacción del contenido, creación de la página y finalmente la implantación.

La metodología de este proyecto parte de estas bases para crear una serie de procedimientos que permitan desarrollar la página web.

I-Planificación

-Planteamiento del objetivo del sitio web.

–Definición de los límites del sitio.

–Determinación del público objetivo.

–Definición del contenido.

II-Diseño de la página

–Diseño gráfico.

–Elaboración de prototipos.

–Elección de un prototipo definitivo.

–Asignación del espacio para los contenidos.

–Vinculación de los enlaces de navegación.

III-Creación de la página web.

–Investigación y recolección de los activos.

–Redacción de los contenidos.

–Revisión ortográfica y de estilo.

–Codificación

–Pruebas y correcciones previas a la publicación.

IV-Publicación.

– Poner a disposición del público o los usuarios la aplicación desarrollada.

A continuación se explican brevemente los puntos de esta metodología.

I-Planificación

En este punto es donde se deciden las generalidades del proyecto web.

-Planteamiento del objetivo del sitio web.

El objetivo es todo aquello que se pretende alcanzar con el desarrollo del proyecto web.

El objetivo de este proyecto es el de desarrollar una herramienta de apoyo que sirva a los estudiantes para adquirir los conocimientos relacionados con el tema de seguridad informática.

-Definición y secuencia congruente con la información a publicar.

Este proyecto se limita a exponer de manera concisa la información referente a la asignatura de Seguridad Informática, evitando la información redundante, los casos específicos definidos sólo para un sistema determinado y cualquier materia que desvíe el tema central del proyecto de los límites del sitio.

Los límites del sitio definen el alcance en los contenidos de la página con el fin de alcanzar los objetivos, manteniendo un orden

-Determinación del público objetivo.

El público al cual está destinado este tutorial, son los estudiantes de las carreras universitarias afines a las tecnologías computacionales, lo que implica que el receptor deberá tener conocimientos básicos sobre diversos temas relacionados a la computación, pues el tutorial no contempla explicar terminología básica sobre temas que no estén directamente relacionados con la seguridad informática.

–Definición del contenido.

El contenido de la página abarca los puntos del temario de la asignatura de Seguridad Informática I de la carrera de Ingeniería en Computación de la Facultad de Ingeniería de la UNAM, así como algunos temas seleccionados del temario de la misma asignatura para la Facultad de Estudios Superiores Aragón.

II-Diseño de la página

Antes de escribir los códigos necesarios para crear la página web, es necesario primero tener un diseño base que sirva como modelo para tener una idea clara de cómo se verá el producto final, y el enfoque de la programación para alcanzar tal modelo.

–Diseño gráfico.

Es el diseño de cómo queremos que se vea la página web ya terminada, en este punto se deciden los elementos gráficos que se desean mostrar.

El esbozo visual de la página puede realizarse con ayuda de herramientas especializadas en el diseño y manipulación de imágenes, o bien, manualmente en hojas de papel.

-Elaboración de prototipos.

De manera opcional podemos crear varias versiones diferentes de cómo se desea mostrar la misma página, esto con el fin de realizar mejoras continuas y ahorrar tiempo antes de realizar una codificación formal.

–Elección de un prototipo definitivo.

Eventualmente se debe elegir la versión que se considere más apropiada para mostrar la página web, esta elección debe considerar un balance entre la facilidad de navegación y el aspecto visual que sea agradable al usuario.

–Asignación del espacio para los contenidos.

Una vez que se ha elegido un diseño visual, se procederá a diseñar el orden del contenido de la página basado en el diseño gráfico.

–Vinculación de los enlaces de navegación.

Una parte importante del diseño es la navegación del sitio web, para facilitar la búsqueda de los temas en el tutorial, es conveniente tener organizados los enlaces de cada tema, esto es, que de un punto clave de la página sea posible ir directamente a otra parte del tutorial sin perder la secuencia de la información ni perder tiempo buscando en un complicado menú. Para tal propósito se necesita diseñar un mapa de enlaces de vínculos que facilite la navegación.

Para este proyecto, el diseño de la página web fue proporcionada por el Ing. Antonio Montalvo, quien anteriormente ya había diseñado el modelo para el tutorial de Redes de Datos **(http://132.248.183.220/tutorial)** el cual ahora se utiliza con el propósito de mantener un estándar en los proyectos en línea

correspondientes al área de Redes y Seguridad en el departamento de Ingeniería en Computación de la Facultad de Ingeniería.

III-Creación de la página web.

–Investigación y recolección de los activos.

Los activos son todos los recursos relacionados con el área de conocimiento y el tema a desarrollar en el sitio web, y abarca desde fuentes bibliográficas hasta imágenes, enlaces y aplicaciones web.

–Redacción de los contenidos.

Una vez recolectada la información, se procede a redactar el contenido de la página tal como se desea aparezca publicada.

–Revisión Ortográfica y de Estilo.

Un trabajo formal requiere una presentación formal, por lo que la ortografía y estilo deben ser impecables, pues el sitio web también representa la imagen de nuestra institución.

–Codificación.

Una vez que el diseño y el contenido están completos, ya es posible crear la página web escribiendo los códigos necesarios.

–Pruebas y correcciones previas a la publicacion.

Después de crear la página web, una serie de pruebas y revisiones son necesarias para asegurar su correcto funcionamiento antes de publicarlo. Las pruebas se llevaron a cabo en la Facultad de Ingeniería y las revisiones correspondientes fueron realizadas por mi asesora de tesis, la Profesora M. en C. María Jaquelina López Barrientos

IV-Publicación.

La aplicación desarrollada se entregó al laboratorio de Redes y Seguridad en la Facultad de Ingeniería para la publicación correspondiente (http ://132.248.52.4/proyectos/tsi/index00.html) a través de su servidor.

Capitulo I Fundamentos teóricos

1.1 Introducción.

Cada vez más los equipos de cómputo forman parte integral en las diversas actividades del ser humano, y la información contenida en los equipos de cómputo es tan importante y vital como el equipo de cómputo en sí. Tal es la importancia de la información que ahora se le considera como un bien y al mismo tiempo un recurso, y por tanto es sumamente importante su administración y protección.

1.1.1 Concepto de la Seguridad Informática

Seguridad informática se puede definir como un conjunto de medidas que impidan la ejecución de operaciones no autorizadas sobre un sistema o red informática, estás medidas pueden ser un conjunto de reglas, planes, actividades y herramientas.
Los efectos que puede tener una operación no autorizada en un sistema informático, pueden conllevar daños sobre la información, comprometer su confidencialidad, autenticidad, integridad, también pueden disminuir el rendimiento de los equipos, desactivar los servicios o bloquear el acceso a los usuarios autorizados del sistema.
Asi mismo es necesario considerar otro tipo de aspectos cuando se habla de Seguridad Informática:

–Cumplimiento de las regulaciones legales aplicables a cada sector o tipo de organización, dependiendo del marco legal de cada país.

–Control en el acceso a los servicios ofrecidos a la información guardada por un sistema informático

–Control en el acceso y utilización de los ficheros con contenido digital protegido por la ley de derechos de autor.

–Identificación de los autores de la información o de los mensajes.
- Registro del uso de los servicios de un sistema informático.

También se debe tener en cuenta que la seguridad de un sistema informático dependerá de diversos factores, entre los que podemos destacar los siguientes:

- La sensibilización de los directivos y responsables de la organización, que deben ser concientes de la necesidad de destinar recursos a está función.

- Los conocimientos, capacidades e implicación de los responsables del sistema informático.

- La mentalización, formación y asunción de responsabilidades de todos los usuarios del sistema.

- La correcta instalación, configuración y mantenimiento de los equipos.

- La limitación en la asignación de los permisos y privilegios de usuarios.

- El soporte de los fabricantes de software y de hardware, con la publicación de parches y actualizaciones de sus productos que permitan corregir los fallos y problemas relacionados con la seguridad.

- La adaptación de los objetivos de seguridad y de las actividades a realizar a las necesidades reales de la organización.

1.1.2 Evolución histórica de la Seguridad Informática

La información puede definirse como la interpretación de un conjunto de datos referentes a un tema, también es considerada un bien valioso, y su importancia varía dependiendo de su uso, propósito y contexto.

Por tanto la protección, y el control de la información ha sido una actividad muy importante para las civilizaciones humanas, pues no ha sido conveniente que todas las personas que lo deseen tengan acceso a ella.
La criptografía es una de las prácticas más antiguas y tiene el propósito de cifrar y descifrar información utilizando técnicas que hagan posible el

intercambio de mensajes de manera que sólo puedan ser leídos por las personas a quienes van dirigidos.

La finalidad de la criptografía es, en primer lugar, garantizar el secreto en la comunicación entre dos entidades (personas, organizaciones, etc.) y, en segundo lugar, asegurar que la información que se envía es auténtica en un doble sentido: que el remitente sea realmente quien dice ser y que el contenido del mensaje enviado, habitualmente denominado criptograma, no haya sido modificado en su tránsito.

El uso más antiguo conocido de la criptografía se halla en jeroglíficos no estándares tallados en monumentos del Antiguo Egipto (hace más de 4500 años).

Hasta el siglo XIX no se desarrolló nada más que soluciones para el cifrado y el criptoanálisis (ciencia que busca debilidades en los sistemas de encriptación).

En la Segunda Guerra Mundial, las máquinas de cifrado mecánicas y electromecánicas se utilizaban extensamente, aunque los sistemas manuales continuaron en uso. Se hicieron grandes avances en la rotura de cifrados, todos en secreto. La información acerca de está época ha empezado a desclasificarse al llegar a su fin el periodo de secreto británico de 50 años, al abrirse lentamente los archivos estadounidenses y al irse publicando diversas memorias y artículos.

Los alemanes hicieron gran uso de diversas variantes de una máquina de rotores electromecánica llamada Enigma. El matemático Marian Rejewski, de la Oficina de Cifrado polaca, reconstruyó en diciembre de 1932 la máquina Enigma del ejército alemán, utilizando la matemática y la limitada documentación proporcionada por el capitán Gustave Bertrand, de la Inteligencia militar francesa. Esté fue el mayor avance del criptoanálisis en más de mil años.

Las computadoras existen desde los años 40 del siglo XX y desde entonces han pasado por una evolución en su diseño, funcionamiento, aplicaciones, etc. hasta llegar a los dispositivos que conocemos ahora.

Aunque desde antes ya se protegía la información procesada por las computadoras, fue hasta en los años 80 cuando se plantearon las bases modernas de la seguridad informática.

Uno de los pioneros en el tema fue James P. Anderson, quien allá por 1980 y a pedido de un ente gubernamental produjo uno de los primeros escritos relacionados con el tema, y es allí donde se sientan también las bases de palabras que hoy suenan como naturales, pero que por aquella época parecían ciencia ficción.

El documento se llamó: Computer Security Threat Monitoring and Surveillance, describe ahí la importancia del comportamiento enfocado hacia la seguridad en materia de informática.

En Esté documento se definen por primera vez en el contexto de seguridad informática, lo que es una amenaza, vulnerabilidad, riesgo, ataque, penetración (ataque exitoso), sentando así bases importantes que siguen siendo importantes hoy en día.

1.1.3 Objetivos y misión de la Seguridad Informática

Entre los principales objetivos de la seguridad informática podemos destacar los siguientes:

- Proteger los recursos de los sistemas informáticos, siendo prioritario la protección a la información, pero abarcando también los equipos, la infraestructura, el uso de las aplicaciones, entre otros.

- Garantizar la adecuada utilización de los recursos y aplicaciones del sistema.

-

- Limitar las pérdidas y conseguir la adecuada recuperación del sistema en caso de un incidente de seguridad.

- Cumplir con el marco legal y con los requisitos impuestos en los contratos.

La misión de la seguridad informática se puede plantear como una serie de actividades especificas para una organización que le permitan alcanzar los objetivos de seguridad.

Entre las más importantes tenemos las siguientes:

–Desarrollo e implantación de políticas de seguridad que estén relacionadas directamente con las actividades reales de una organización.

–Mejora constante de los sistemas de seguridad por medio de su monitoreo y análisis, así como la adquisición y actualización de tecnologías.

–Minimizar gestionar los riesgos y detectar los posibles problemas y amenazas a la seguridad.
–Capacitar al personal encargado de la seguridad del sistema para que tengan conocimientos actualizados que les permitan desempeñar su labor de manera más eficiente.

–Concienciar a los usuarios del sistema informático sobre la importancia de las políticas de seguridad impuestas.

1.1.4 Amenazas a las redes y sistemas computacionales

Una amenaza es la probabilidad de que ocurra un incidente que provoque la pérdida o daños a los recursos informáticos de una organización

Por su origen pueden clasificarse en:

Amenazas de origen humano.

Son todas las amenazas causadas por la intervención directa de los humanos, abarca actos malintencionados, incumplimiento de las medidas de seguridad, actos negligentes, entre otros.

Estos pueden ser el sabotaje, infiltración de usuarios no autorizados, descuido del personal, etc.

–Amenazas de fuerza mayor.

En esta clasificación se encuentran los desastres naturales como inundaciones, terremotos, incendios, etc.

Estos desastres no solo afectan a la información contenida en los sistemas, sino también representan una amenaza a la integridad del sistema completo (infraestructura, instalación, componentes, equipos, etc.) pudiendo dejar al sistema incluso en un estado de inoperabilidad permanente.

–Errores de Hardware.

Se da la amenaza por fallas físicas que presente cualquiera de los dispositivos de hardware que conforman a la computadora. Estos sucesos se pueden presentar por fallas en el suministro de energía (ruido electromagnético, caídas de voltaje, variación de frecuencia, etc.) los cuales dañan a los equipos, desperfectos de fábrica, falta de mantenimiento o maltrato, diseño inapropiado de los componentes, entre otros.

B) Errores de la red.

Son todos los errores que provoquen la no disponibilidad de servicios de una red de cómputo. Esta situación puede ser provocada por el efecto directo de un acto humano o por fallas físicas y lógicas del mismo sistema.

Por ejemplo la saturación del ancho de banda, instalación y configuración incorrecta de los dispositivos de la red, destrucción física de las líneas de transmisión de datos, etc.

C) Problemas de tipo lógico.

Es una falla que se da a nivel software, puede ser causado por un error interno del sistema, pero también abarca el daño causado por códigos maliciosos o un ataque de un intruso humano.

Un gusano informático ilustra está categoría, pues desvía los recursos del sistema para reproducirse, reenviarse y posteriormente causa daños al sistema infectado.

1.2 Normatividad de la seguridad informática

Los activos de información y los equipos informáticos son recursos importantes y vitales, sin ellos las organizaciones quedarían paralizadas en sus actividades y por tal razón es necesario preservarlos. Esto significa que se deben tomar las acciones apropiadas para asegurar que la información y los sistemas informáticos estén apropiadamente protegidos de muchas clases de amenazas y riesgos.

Para tal acción deben emplearse medidas y políticas de seguridad las cuales tienen como finalidad proporcionar instrucciones específicas sobre qué y cómo mantener seguras las tecnologías de información.

1.2.1 Normas de Seguridad a través de la Historia

Common Criteria (criterios comunes) son el resultado final de importantes esfuerzos en el desarrollo de criterios de evaluación unificados para la seguridad de los productos IT (Tecnologías de Información) y ampliamente aceptado por la comunidad internacional.

A principios de los años 80, se desarrollaron en Estados Unidos los criterios de seguridad recogidos bajo el nombre de TCSEC (Trusted Computer System Evaluation Criteria) y editados en el famoso "libro naranja". En las décadas posteriores, varios países tomaron como base el TCSEC americano y evolucionaron las especificaciones para hacerlas más flexibles y adaptables a la constante evolución de los sistemas de IT.

De ahí la comisión europea, en el año 1991 publicó el ITSEC (Information Technology SecurityEvaluation Criteria), desarrollado conjuntamente por Francia, Alemania, Holanda y el Reino Unido.

En Canadá, igualmente sedesarrollaron en 1993 los criterios CTCPEC (Canadian Trusted Computer Product Evaluation) uniendo los criterios americanos y europeos.

En ese mismo año el Gobierno americano publicó los Federal Criteria como una aproximación aunificar los criterios europeos y americanos. Tal escenario comienza a aclararse con la decisión de estandarizar internacionalmente estos criterios para uso general, y en esa labor ISO comienza a trabajar a principios de los años 90 dando como resultado el Common Criteria (ISO-IEC 15408).

1.2.1.1 Normas de seguridad en sistemas operativos.

El sistema operativo es un software encargado de controlar y administrar los recursos de una computadora, es la principal interfaz por la cual el usuario maneja el equipo de cómputo.
Esto es, administrando el manejo de archivos, sincronizando las funciones de los programas de aplicación que funcionan simultáneamente para evitar conflictos entre ellos, verificar el funcionamiento de los dispositivos de hardware y su transmisión de datos. El sistema operativo también está a cargo de gestionar la seguridad, restringiendo el uso del equipo a solo usuarios autorizados, y analizando actividades sospechosas de los usuarios de una red en caso de funcionar como servidor, por citar algunos ejemplos.

Con el fin de que un sistema operativo pueda considerarse seguro, se han enumerado diversos estándares que establecen guías necesarias para tal propósito, estos documentos se describen a continuación.

1.2.1.1.1 TCSEC (Trusted Computer System Evaluation Criteria)

Comúnmente conocido como el libro naranja.
El TCSEC tiene 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.

TCSEC definen siete conjuntos de criterios de evaluación denominados clases (D, C1, C2, B1, B2, B3 y A1). Cada clase de criterios cubre cuatro aspectos de la evaluación: política de seguridad, imputabilidad, aseguramiento y documentación.
Los criterios correspondientes a estas cuatro áreas van ganando en detalle de una clase a otra, constituyendo una jerarquía en la que D es el nivel más bajo y A1 el más elevado. Todas las clases incluyen requisitos tanto de funcionalidad como de confianza.

A continuación se enumeran las siete clases:

Clase D: Protección Mínima.

Son todos los sistemas que han sido evaluados pero no atienen los requerimientos necesarios para alcanzar un mayor nivel.
No distingue usuarios ni establece un control sobre la información.

Clase C1:Nivel de Protección discrecional.

Todos los usuarios en este nivel deben identificarse por medio de un nombre de usuario y un password.

Clase C2: Protección de acceso controlado.

Refuerza las restricciones a las acciones de los usuarios, incluyendo ejecución de comandos y acceso a los archivos. Tales restricciones están basadas en permisos y niveles de autorización.
Este nivel requiere de auditorias de sistema, la cual sirve para llevar los registros de todas las actividades practicadas en el sistema por parte de cualquier usuario.

Clase B1: Protección por seguridad etiquetada.

Protección de seguridad etiquetada. Define que cada objeto del sistema sea etiquetado para establecer un control de acceso entre un nombre de usuario y un nombre de objeto, esto a fin de mantener un control sobre los ficheros. Los permisos de acceso a un objeto solo puede ser otorgada por un usuario autorizado.

Clase B2: Protección estructurada.

Demanda que los accesos de control de la clase B1, se extienda a los objetos del sistema de procesamiento de datos.

Clase B3: Dominios de seguridad.

Establece que las porciones del sistema relacionadas a la seguridad, deben ser diseñados a fin de minimizar su complejidad a fin de facilitar su análisis y pruebas, pero sin descuidar su principal propósito de proteger. En este nivel de seguridad, los accesos se refuerzan por medio de la instalación de terminales de hardware que permiten a los usuarios una ruta de acceso segura.

Clase A: Nivel de protección verificada.

Los sistemas de este nivel funcionan de manera equivalente a los de la clase B3, la diferencia radica en que una serie de pruebas y análisis acreditan que el sistema cumple con todos los requerimientos de seguridad.

1.2.1.1.2 ITSEC (Information Technology Security Evaluation Criteria)

Ha surgido de la armonización de varios sistemas europeos de criterios de seguridad en TI. Tiene un enfoque más amplio que TCSEC.

Los criterios establecidos en ITSEC permiten seleccionar funciones de seguridad arbitrarias (objetivos de seguridad que el sistema bajo estudio debe cumplir teniendo presentes las leyes y reglamentaciones).

Se definen siete niveles de evaluación, denominados E0 a E6, que representan una confianza para alcanzar la meta u objetivo de seguridad. E0 representa una confianza inadecuada. E1, el punto de entrada por debajo del cual no cabe la confianza útil, y E6 el nivel de confianza más elevado. Por ello, los presentes criterios pueden aplicarse a una gama de posibles sistemas y productos más amplia que los del TCSEC.

El objetivo del proceso de evaluación es permitir al evaluador la preparación de un informe imparcial en el que se indique si el sistema bajo estudio satisface o no su meta de seguridad al nivel de confianza precisado por el nivel de evaluación indicado.

En general, la funcionalidad idéntica y a nivel de confianza equivalente, un sistema goza de más libertad arquitectónica para satisfacer los criterios de ITSEC que los de TCSEC.`

1.2.1.1.3 CTCPEC (Canadian Trusted Computer Product Evaluation Criteria)

Es un estándar de seguridad de computadoras publicado en 1993 para proveer un criterio de evaluación para los productos de IT.
Es una combinación de los criterios TCSEC americano (libro naranja) y el ITSEC europeo.
Proporciona un escala para la evaluación de productos comerciales y proporciona bases para desarrollar un método de especificación para productos de cómputo confiables.

1.2.1.1.4 FC-ITS The FC-ITS of the United States NIST and NSA (Federal Criteria for Information Technology Security)

Siguiendo la discusión internacional para satisfacer las necesidades no militares, especialmente aplicaciones comerciales de IT, los Estados Unidos iniciaron un proyecto para producir el sucesor del TCSEC.
El resultado es el documento de "Requerimientos mínimos de seguridad para sistemas operativos de multiusuarios", el cual presenta los requerimientos funcionales de seguridad para sistemas operativos que procesen información no clasificada dentro de un ámbito gubernamental y comercial.
En diciembre de 1992, el bosquejo de la versión 1.0 del FC-ITS (Federal Criteria for Information Technology Security) fue publicado por el Instituto nacional de estándares y tecnología (NIST National Institute of Standards and Technology) creado originalmente para su uso por el Gobierno Federal de los Estados Unidos y por otros grupos designados como apropiados.

El FC-ITS contiene capítulos separados en requerimientos de "Funcionalidad" y "Seguridad", pero introduce una nueva estructura basada en el aspecto de dependencia entre funcionalidad y seguridad.

1.2.2 Criterios Comunes / ISO 15408 (Common Criteria for Information Technology Security Evaluation)

Los criterios comunes (Common Criteria) son estándares usados como base para la evaluación de las propiedades de seguridad de los productos IT y sistemas. Al establecer un como base un criterio consistente, el resultado de una evaluación de seguridad de un producto IT tiene mayor significado a una audiencia más amplia. ISO 15408 es un estándar internacional utilizado para evaluar el nivel de seguridad de los productos provistos y permitiendo la comparación entre diferentes productos IT.

La norma ISO-15408 define estándares de medidas de seguridad TI que se implementan en el hardware, firmware o software. La norma ISO-15408

ignora toda medida de seguridad, que esté fuera de sistema de información, para el cual se ha aplicado, aunque reconoce que se puede aplicar seguridad significativa a través del uso de medidas administrativas, como los controles a las organizaciones, al personal, controles de tipo físico y de procedimiento.

1.2.3 ISO 17799

ISO/IEC 17799 es un estándar para la seguridad de la información publicado por primera vez como ISO/IEC 17799:2000 por International Organization for Standardization y por la comisión International Electrotechnical Commission en el año 2000 y con el título de Information technology - Security techniques - Code of practice for information security management

La norma ISO/IEC 17799 es una guía de buenas prácticas y no especifica los requisitos necesarios que puedan permitir el establecimiento de un sistema de certificación adecuado para esté documento.

La ISO/IEC 17799:2000 considera la organización como una totalidad y tiene en consideración todos los posibles aspectos que se pueden ver afectados ante los posibles incidentes que puedan producirse. Está norma se estructura en 10 secciones o controles en los que cada uno de ellos hace referencia a un aspecto de la seguridad de la organización:

- Política de seguridad
- Aspectos organizativos para la seguridad
- Clasificación y control de activos
- Seguridad del personal
- Seguridad física y del entorno
- Gestión de comunicaciones y operaciones
- Control de accesos
- Desarrollo y mantenimiento de sistemas
- Gestión de continuidad del negocio
- Conformidad legal

En resumen esta norma pretende aportar las bases para tener en consideración todos y cada uno de los aspectos que puede suponer un incidente en las actividades de negocio de la organización.

1.2.4 Nuevas Tendencias

La seguridad y auditoría Informática se están afianzando como una necesidad imprescindible para el desarrollo de la Sociedad de la Información.

Como se recoge en el informe PricewaterhouseCoopers 2006 State of the Internal Audit Profession Study durante los últimos años la sección 404 de la Ley SOX con los requerimientos específicos que obligan a las compañias a "documentar, evaluar, verificar y monitorizar sus controles internos sobre los informes financieros" ha supuesto en EE.UU. un gran paso cualitativo para el afianzamiento de la auditoría informática. Otras disposiciones legales como Basilea II, "HIPAA" (Acta, "Health Insurance Portability and Accountability") y GLBA ("Graham-Leach Bliley Act") también están contribuyendo a este afianzamiento.

La entrada en vigor, durante 2006, de la norma ISO/IEC 27001 como estándar mundial para los Sistemas de Gestión de Seguridad de la Información SGSI y sus requerimientos de auditoría para la obtención de las certificaciones, también han de suponer un gran incremento de la demanda de Auditores Informáticos.

Aunque en la actualidad la legislación existente relacionada con la Informática sigue siendo escasa, en los últimos años los Gobiernos comienzan a tomar conciencia de la necesidad de exigir responsabilidades en los riesgos derivados de los sistemas informáticos y de la necesidad de establecer controles adecuados. Podemos observar como en estas nuevas leyes la Auditoría Informática siempre está presente.

Sobre Seguridad Informática se publican anualmente múltiples informes, entre los más difundidos a nivel mundial podemos destacar:

-CSI/FBI 2006 Computer Crime and Security Survey: Es un informe que anualmente publican Computer Secuity Institute y Federal Bureau of Investigation's Computer Intrusion Squad. Es un informe detallado sobre Seguridad Informática que incluye: principales incidentes que se están produciendo, la situación en empresas y organizaciones de la Seguridad Informática, tecnologías utilizadas, consecuencias económicas, la evolución en los últimos años, etc. Posiblemente este informe es uno de los mas importantes publicados anualmente en el mundo sobre Seguridad Informática y aunque está muy centrado en EE.UU. sus conclusiones son extrapolables a otros países.

–2006 Australian Computer Crime and Security Survey: Es un informe similar al anterior, pero restringido a Australia. En Europa tanto a nivel de Comunidad Europea, como de sus países miembros.

–Ernst & Young's 2006 Global Information Security Survey: En este informe participan más de 1.200 organizaciones. Presenta una fotografía sobre el estado de la seguridad y de sus repercusiones en la industria y los negocios. El informes se realiza analizando las respuestas a un cuestionario con preguntas sobre "como esta dirigida y situada la Seguridad Informática en las organizaciones de quienes responden al cuestionario" . Los cuestionarios son completados mayoritariamente por Directores de Informática y Directores de Seguridad, el informe también incluye conclusiones y recomendaciones.

1.2.4.1 Magerit (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas)

Magerit es una herramienta creada por el Consejo Superior de Administración Electrónica, basada en la premisa de que así como las tecnologías de información traen grandes beneficios para todas las

actividades en que se apliquen , al mismo tiempo generan riesgos que deben reducirse mediante medidas de seguridad que generen confianza en su utilización. Estás medidas de seguridad están basadas en el análisis previo de los riesgos.

Magerit, es un método formal para investigar los riesgos que soportan los sistemas de información, y para recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos.

Magerit persigue los siguientes objetivos:

–Concienciar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de atajarlos a tiempo.

–Ofrecer un método sistemático para analizar tales riesgos.

–Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.

–Apoyar la preparación a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

1.2.4.2 ISO 27000

El ISO 27000 es una serie de estándares que han sido específicamente reservados para asuntos de seguridad de la información. Este estándar también trata con otros temas, incluyendo la calidad de la administración y la calidad del entorno.

La serie que conforma al ISO27000 es la siguiente:

ISO27001. Establece los requisitos del sistema de gestión de seguridad de la información. Es la norma principal de requisitos de un Sistema de Gestión de Seguridad de la Información. Los SGSIs (Sistemas de Gestión de la Seguridad de la Información) deberán ser certificados por auditores externos a las organizaciones. En su Anexo A, contempla una lista con los

objetivos de control y controles que desarrolla la ISO 27002 (anteriormente denominada ISO17799).

ISO27001. Guía de buenas prácticas. Describe los controles y objetivos recomendables en cuanto a la seguridad de la información. Contiene 39 objetivos de control y 133 controles, agrupados en 11 cláusulas. Como se ha mencionado en su apartado correspondiente, la norma ISO27001 contiene un anexo que resume los controles de ISO17799:2005.

ISO27003. En fase de desarrollo; probable publicación en Octubre de 2008. Contendrá una guía de implementación de SGSI e información acerca del uso del modelo PDCA (Plan-Do-Check-Act, es una estrategia de mejora continua de la calidad) y de los requerimientos de sus diferentes fases. Tiene su origen en el anexo B de la norma BS7799-2 y en la serie de documentos publicados por BSI (British Standards Institution) a lo largo de los años con recomendaciones y guías de implantación.

ISO27004. En fase de desarrollo; probable publicación en 2008. Especificará las métricas y las técnicas de medida aplicables para determinar la eficiencia y eficacia de la implantación de un SGSI y de los controles relacionados.

ISO27005. Probable publicación en 2008. Consistirá en una guía para la gestión del riesgo de la seguridad de la información y servirá, por tanto, de apoyo a la ISO 27001 y a la implantación de un SGSI. Incluirá partes de la ISO 13335.

ISO27006. Especifica los requisitos para la acreditación de entidades de auditoria y certificación para los sistemas de información

1.2.4.3 OCTAVE (Operational, Critical, Threat, Asset and Vulnerability Evaluation)

Una evaluación efectiva de riesgos en la seguridad de la información considera tanto los temas organizacionales como los técnicos, examina cómo la gente emplea la infraestructura en forma diaria. La evaluación es de vital importancia para cualquier iniciativa de mejora en seguridad, porque genera una visión a lo ancho de la organización de los riesgos de seguridad de la información, proveyéndonos de una base para mejorar a partir de allí.

Para que una empresa comprenda cuáles son las necesidades de seguridad de la información, OCTAVE es una técnica de planificación y consultoría estratégica en seguridad basada en el riesgo.

En contra de la típica consultoría focalizada en tecnología, que tiene como objetivo los riesgos tecnológicos y el foco en los temas tácticos, el objetivo de OCTAVE es el riesgo organizacional y el foco son los temas relativos a la estrategia y a la práctica.
Cuando se aplica OCTAVE, un pequeño equipo de gente desde los sectores operativos o de negocios hasta los departamentos de tecnología de la información (IT) trabajan juntos dirigidos a las necesidades de seguridad, balanceando tres aspectos: Riesgos Operativos, Prácticas de seguridad Y Tecnología.
OCTAVE apunta a dos aspectos diferentes: riesgos operativos y prácticas de seguridad. La tecnología es examinada en relación a las prácticas de seguridad, permitiendo a las compañías tomar decisiones de protección de información basados en los riesgos de confidencialidad, integridad y disponibilidad de los bienes relacionados a la información crítica.

El método Octave permite la comprensión del manejo de los recursos, identificación y evaluación de riesgos que afectan la seguridad dentro de una organización.

Exige llevar la evaluación de la organización y del personal de la tecnología de la información por parte del equipo de análisis mediante el apoyo de un patrocinador interesado en la seguridad.

El método Octave se enfoca en tres fases para examinar los problemas organizacionales y tecnológicos:

1- Identificación de la información a nivel gerencial
2- Identificación de la información a nivel operacional
3- Identificación de la información a nivel de usuario final

Estos tres pasos dan lugar a otros 5 procesos para completar los 8 puntos de los que consta Octave:

4- Consolidación de la información y creación de perfiles de amenazas
5- Identificación de componentes claves
6- Evaluación de componentes seleccionados
7.-Análisis de riesgos de los recursos críticos
8- Desarrollo de estrategias de protección

1.3 Esquema de Seguridad basado en Criterios Comunes: Perfiles de Protección

Los criterios comunes no necesariamente deben quedarse como una referencia para la evaluación de la seguridad, también es posible crear sistemas o productos IT basados en las propiedades de seguridad estandarizados por los criterios comunes para ello es primero necesario desarrollar un perfil de protección.

1.3.1 Definición y propósito

Un perfil de protección (Protection Profile) es un documento usado como parte del proceso de evaluación de los criterios comunes, el cual define un conjunto de objetivos y requisitos de seguridad, independiente de la implantación, para una categoría de productos que cubre las necesidades de seguridad comunes a varios usuarios. Los perfiles de protección son reutilizables.

El perfil de protección permite la elaboración de estándares funcionales y constituye una ayuda para la formulación del pliego de condiciones de un producto.

EL propósito de un perfil de protección es el de plantear un problema de seguridad a un conjunto de sistemas o productos (conocidos como objetos de evaluación) y especificar los requerimientos de seguridad necesarios para afrontar el problema, sin dictar como estos requerimientos serán implementados.

1.3.2 Estructura

Un perfil de protección es un documento formal con contenido específico, formato y sintaxis requeridos.
Esta formalidad es impuesta para asegurar que los perfiles de protección sean exactos y uniformemente interpretados por todos los diferentes evaluadores.

Un perfil de protección no esta escrito por si mismo, en vez de eso captura los resultados de una serie de análisis conducidos a los clientes para poner en claro, definir y validar sus requerimientos de seguridad.

Toda la información contenida en un perfil de protección debe ser colocada en la sección apropiada donde pueda ser encontrada, leída y evaluada.

1.3.2.1 Introducción

Aquí se identifica la naturaleza, alcance y estado del perfil de protección.
Está sección se divide en dos subsecciones, identificación y descripción.

La subsección de identificación provee los datos generales del perfil de protección, tales como nombre del perfil de protección, versión y fecha (esto permite distintas versiones de un perfila para un mismo sistema) , así como una serie de palabras clave que permiten asociar el perfil de protección con el tipo de tecnología, categoría de producto, fabricante, usuarios, marcas, etc.

La subsección de descripción provee una breve descripción general del perfil de protección y plantea el contexto del resto del documento.

1.3.2.2 Descripción del objeto de evaluación

Está dividido en dos subsecciones: Funcionamiento general y límites del objeto de evaluación.

Funcionamiento general: Provee una descripción general del funcionamiento del producto o sistema, el uso que se le da y el entorno de operación en que normalmente trabaja.

Limites del objeto de evaluación: Uno de los primeros pasos para definir los requerimientos de seguridad es definir los límites del sistema.
Los límites son el alcance de un sistema, todo lo que esté dentro de los límites del sistema debe ser correctamente administrado, ordenado, identificado y controlado. Todo lo que esté fuera de los límites no es considerado parte del sistema pero eso no significa que no vaya a afectar al sistema.
Los limites de un sistema varían dependiendo del enfoque y el punto de vista del que considera el sistema, aun así es necesario definir claramente cuales serán los limites y alcances del sistema, pues dentro de los mismos limites se encuentran sus requerimientos de seguridad, y al mismo tiempo se debe prever una situación que se encuentre fuera de los limites del sistema y por tanto de nuestro control.

1.3.2.3 Entorno de seguridad

El tercer requerimiento de un perfil de protección, el entorno de seguridad, define la naturaleza y alcance de la seguridad del objeto de evaluación. Está se divide en tres subsecciones, hipótesis, amenazas y políticas de la organización.

1.3.2.4 Hipótesis

Proporciona información importante a los administradores para ayudarlos a entender en que panorama de trabajo debe desarrollarse el objeto de evaluación, en otras palabras, es un informe de hipótesis que el objeto de evaluación debe cumplir para que pueda considerarse seguro.

1.3.2.5 Amenazas

Esta subsección caracteriza amenazas potenciales contra el objeto de evaluación para las cuales se requiere protección.
La valoración de amenazas abarca eventos accidentales y maliciosos que intenten esquivar, deshabilitar y comprometer aspectos de seguridad, funciones y procedimientos del objeto de evaluación.
El objeto de evaluación, el entorno IT, la seguridad física, la seguridad de personal y la seguridad operacional, todos están dentro del alcance de la valoración de amenazas, por lo que su importancia no debe ser subestimada, ya que si una valoración de amenazas no es realizada correctamente, el sistema puede proveer una inadecuada protección y como resultado estará expuesto a un inaceptable nivel de riesgo

1.3.2.6 Políticas de la organización

Las políticas de seguridad incluyen reglas, procedimientos y prácticas que la organización impone en un sistema IT para protegerlo.
Las políticas de seguridad proveen una guía a los administradores, programadores y asistentes en la formulación de objetivos de seguridad en la sección 4 del perfil de protección.
Las políticas de seguridad son únicas para cada organización, además las leyes y regulaciones locales, nacionales o internacionales pueden imponer políticas de seguridad adicionales.

1.3.2.7 Nivel de Garantía general requerido

Está parte está destinada a los desarrolladores IT ya que define el criterio de confiabilidad que los evaluadores usan para verificar el desempeño de los desarrolladores y sus productos.

Introduce siete niveles de evaluación de garantía (Evaluation Assurance Level EAL) que define la escala de los Criterios Comunes para clasificar la evaluación obtenida por los productos.
Incluye los niveles de evaluación de garantía que definen una escala para garantizar la medición, los componentes de garantía individual de los cuales los niveles de garantía están compuestos, y los criterios para la evaluación de perfiles de protección.

1.3.2.8 Objetivos de Seguridad

Provee un informe conciso en respuesta al entorno a todos los requerimientos de seguridad identificados.
El objetivo de está sección es dividir responsabilidades entre el objeto de evaluación y su entorno.
Los objetivos de seguridad están clasificados en preventivos, detectivos y correctivos.

Objetivos preventivos: Objetivos que previenen de una amenaza a ser ejecutada, o limitar la manera en que puede ser ejecutada .

Objetivos detectivos: Objetivos que detectan y monitorean la ocurrencia de eventos relevantes a la segura operación del sistema .

Objetivos correctivos: objetivos que requieren que el objeto de evaluación tome acción en respuesta a cualquier posible anomalía , violación de seguridad o cualquier otro evento indeseable , con el objeto de preservar o regresar a un estado de seguridad o limitar cualquier posible daño.

1.3.2.9 Requerimientos Funcionales y de Garantía

Requerimientos funcionales de seguridad, implementan los objetivos de seguridad establecidos en la sección 4 de un perfil de protección. Cada requerimiento funcional de protección cubre uno o más objetivos de seguridad.

La selección de un requerimiento funcional, o el tipo de protección requerida es influenciada por tres factores clave:

1- Sensibilidad y valor de las características que se van a proteger.

2- Importancia del trabajo que el sistema realiza.

3- Consecuencias de lo que pasaría si el sistema se perdiera, corrompiera, fuera destruido, inoperable o no disponible por un extenso periodo de tiempo.
El objetivo es seleccionar un requerimiento funcional que cubra los objetivos de seguridad, y al mismo tiempo que proteja al sistema sin reducir su operabilidad.

Los requerimientos de garantía se encargan de definir los criterios de evaluación para los perfiles de protección y el objeto de evaluación, así como las responsabilidades y actividades de los administradores y evaluadores, con el fin de garantizar que estos cumplan los requerimientos de seguridad .

La selección de los requerimientos de garantía se basa en varios factores:

- Valor de los activos a ser protegidos versus el riesgo percibido de compromiso.
- Viabilidad técnica.
- Costos de producción y evaluación.
- Tiempos, requerimientos y límites de producción y evaluación
- Opciones disponibles de productos IT en el mercado versus productos personalizados.
- Relación y dependencia entre requerimientos de garantía y requerimientos funcionales.

El objetivo es asegurar que el objeto de evaluación alcance los objetivos de seguridad procurando un continuo balance entre funcionalidad y viabilidad técnica, costos y limitaciones de tiempo.

1.4 Servicios de Seguridad

Para hacer frente a las amenazas a la seguridad del sistema, se define una serie de servicios de seguridad, los cuales están encargados de proteger los sistemas de información, sus procesos, el tráfico de datos y el contenido de la información que se maneja dentro de una organización. Estos servicios hacen uso de uno o varios mecanismos de seguridad.
Los servicios de seguridad se clasifican en:

-Confidencialidad
-Autenticación
-Integridad
-No repudio
-Control de Acceso
-Disponibilidad

1.4.1 Confidencialidad

Es cuando se requiere que la información solamente sea accesible a las entidades autorizadas, esto es porque la información es un recurso valioso de una organización y debe mantenerse en secreto para toda entidad no autorizada que en potencia le puede dar mal uso.
La confidencialidad de datos se aplica a todos los datos intercambiados por las entidades autorizadas.

El servicio de confidencialidad se divide en dos aspectos que son:

Confidencialidad de contenido: Se encarga de que la información no pueda ser descubierta, leída o modificada sin autorización.

Confidencialidad de flujo de mensaje: Encargado de que la información no sea interceptada durante la comunicación de entidades.

1.4.2 Autenticación

Se encarga de la identificación correcta del origen del mensaje, asegurando que la entidad no es falsa.
Se distinguen dos tipos autenticación:

Autenticación de entidad. Se asegura que la identidad de las entidades participantes en la comunicación sean correctas.

Autenticación de origen de información. Se asegura que las unidades de información provengan de la entidad que dicen ser.

1.4.2.1 Tipos de autenticación

Las entidades con las que un sistema informático se comunica, por lo general son usuarios, y para asegurar que se trata de un usuario autorizado, el sistema necesita realizar un proceso que verifique su autenticidad como tal.
Existen diferentes tipos de autenticación, cada uno basado en diferentes criterios.

1.4.2.1.1Basada en algo que el usuario sabe.

Es el modelo más básico de autenticación, consiste en que el usuario proporcione un conocimiento que previamente solo él puede conocer, esto puede ser un password, un NIP, u otro tipo de contraseña.
Este esquema es barato y fácil de implantar, pero también el mas vulnerable, pues cualquiera puede pasar la seguridad con tan solo conocer una clave válida.

1.4.2.1.2 Basada en algo que el usuario tiene.

Es un modelo basado en autenticar la identidad por medio de un objeto que acredite la identidad del poseedor y que él mismo posea. El ejemplo más común es una tarjeta de identificación que por lo general tiene un tipo de chip o banda magnética con información almacenada del usuario.

Los sistemas de seguridad basados en este tipo de autenticación generalmente se les combina con un sistema de contraseñas para crear un sistema más fiable.

1.4.2.1.3 Basada en algo que el usuario es (autenticación biométrica).

Este modelo se basa en autenticar la identidad de un usuario basado en sus características físicas, puede ser su huella dactilar, firma, voz, retina, u otra característica que pueda ser analizada por medio de un sensor electrónico.
Los sistemas basados en este modelo son fiables debido a la dificultad de falsificar las características requeridas, y al mismo tiempo es fácil para los usuarios pues no tienen que recordar claves ni transportar algún tipo de llave.
No obstante, las tecnologías que se requieren regularmente tienen costos elevados.

1.4.2.1.5 Basada en donde se está.

En este modelo se toma en cuenta el lugar donde se conectan los usuarios para autentificar su identidad. Además de una contraseña o una llave, solo se puede acceder al sistema desde una terminal autorizada ubicada en una región geográfica especifica , de la misma manera también se puede negar el acceso a usuarios de determinadas regiones.
Para identificar el lugar desde el cual un usuario se conecta, estos sistemas pueden valerse de tecnologías GPS (Global Positioning System) o métodos de administración de direcciones IP

1.4.3 Integridad

La integridad de datos asegura que los datos recibidos no han sido modificados por entidades no autorizadas y que la secuencia de datos se mantenga durante la transmisión.
La modificación incluye escritura, cambio, borrado, creación, inserción y supresión de los mensajes transmitidos.

La integridad de secuencia de datos asegura que la secuencia de los bloques o unidades de datos recibidas no ha sido alterada y que no hay unidades repetidas o pérdidas

1.4.4 No repudio

El no repudio ofrece protección para que las entidades de un procesos de comunicación no puedan negar su participación. De está manera la entidad emisora prueba que envió cierta información, y la entidad receptora puede probar que recibió cierta información.

Los servicios de no repudio presentan pruebas a una tercera entidad de que se realizo un comunicación entre entidades, esté servicio se efectúa por medio de una colección de evidencias irrefutables que permitirán la resolución de cualquier disputa.

Los siguientes servicios son los que pueden ser proporcionados.

–No repudio de origen: Provee pruebas del origen de los datos, protegiendo al receptor de que el emisor niegue haber enviado el paquete de datos.

–No repudio de envió: Provee pruebas del envió de los datos, previene al receptor de cualquier denegación falsa al recibir los datos.
No repudio de presentación: Provee pruebas de presentación de los datos, con ello protege contra cualquier intento falso de negar que los datos fueron presentados para el envió.

–No repudio de transporte: Provee pruebas del transporte de los datos, protege contra cualquier intento de negar que los datos fueron transportados.

–No repudio de recepción: Provee pruebas de la recepción de los datos, protege al emisor de que el receptor niegue haber recibido el mensaje.

1.4.5 Control de Acceso

Esté servicio se presenta cuando se tiene la necesidad de restringir y limitar el acceso a recursos y sistemas internos a usuarios no autorizados. Los componentes básicos de un mecanismo de control de acceso son las entidades de red, los recursos de la red y los derechos de acceso. Los usuarios, los recursos y la información pueden ser clasificados al asignarse diferentes niveles de seguridad, por lo que los usuarios autorizados para cierto nivel pueden acceder a todos los recursos disponibles de ese nivel pero no a otros niveles a los que no esté autorizado.

1.4.5.1Tipos de control de acceso

Se pueden distinguir dos tipos de control de acceso:

1.4.5.1.1 Control de acceso voluntario (CAV).

También conocido como Control de Acceso Discrecional (DAC). Este tipo de acceso está basado en la idea de que cada objeto o elemento del sistema tiene un propietario, el cual configura y otorga los permisos a cualquier otro usuario siempre y cuando no atente contra las normas de seguridad impuestas.

1.4.5.1.2Control de acceso obligatorio (CAO).

Conocido también como Control de Acceso Mandatario (MAC). En este tipo de acceso, el sistema informático tiene definida una serie de criterios de seguridad con base en los cuales asigna a cada uno de los usuarios registrados los permisos de acceso correspondientes. Tanto los usuarios como los objetos tienen una serie de atributos de seguridad.

1.4.6 Disponibilidad

El servicio de disponibilidad se encarga de que los recursos del sistema informático estén disponibles a las entidades autorizadas cuando lo soliciten y las veces que sea necesario.

La disponibilidad se refiere al tiempo para obtener la información sin asegurar que la información transmitida es correcta o no.

La falta de disponibilidad se manifiesta principalmente de dos formas:

–La denegación, o repudio, del servicio debido a la falta de garantías de la prestación del mismo, tanto por parte del prestador del servicio como del solicitante o tomador (controles de identificación fehaciente, falta de prestaciones de los equipos, congestión de líneas, etc.).

–La pérdida de servicios de los recursos de información por causa de catástrofes naturales o por fallos de equipos, averías, acción de virus, etc.

Capitulo II Amenazas y Vulnerabilidades.

Para aplicar controles adecuados de seguridad, es preciso comprender primero quién o qué es lo que amenaza dicho entorno, así como conocer los riesgos asociados a dichas situaciones si llegan a materializarse. Los problemas de seguridad se dividen principalmente en amenazas y vulnerabilidades.

2.1 Amenazas

2.1.1 Definición

Las amenazas son eventos que pueden causar alteraciones a la información de la organización ocasionándole pérdidas materiales, económicas, de información, y de prestigio.
Las amenazas se consideran como exteriores a cualquier sistema, es posible establecer medidas para protegerse de las amenazas, pero prácticamente imposible controlarlas y menos aún eliminarlas.

2.1.2 Fuentes de amenaza

Aunque todas las amenazas tienen la característica de ser las posibles causantes de destrucción a los sistemas, las amenazas pueden tener diferentes orígenes. Existen varias categorías de amenazas, para esta investigación se clasificaran por su origen, de esta forma se dividirán en cinco tipos los cuales son: amenazas humanas, de hardware, de software, de red y desastres naturales.

2.1.2.1 Factor humano

Las personas son la principal fuente de amenaza que existe en los sistemas de información y son el tipo de amenaza en el que se invierten más recursos para controlarlos y contrarrestar sus efectos.

Abarca actos malintencionados, incumplimiento de las medidas de seguridad como consecuencia de actos negligentes o falta de controles adecuados.

2.1.2.1.1 Tipos de amenazas humanas.

Los actos humanos que pueden afectar la seguridad de un sistema son variados, entre los más comunes e importantes están:

Curiosos: se trata de personas que entran a sistemas (en algunos casos de manera accidental) a los que no están autorizados, motivados por la curiosidad, por el desafió personal, o por el deseo de aprender o averiguar. Generalmente este tipo de intrusos no tienen los conocimientos apropiados para lograr causar daños, pero no por eso se les debe ignorar sin tomar las precauciones necesarias.

Aunque se afirma que no tienen intenciones maliciosas, su sola intrusión al sistema representa una peligrosa amenaza ya que pueden causar daños no intencionales o dejar expuesta la estructura y seguridad del sistema.

Intrusos remunerados: este tipo de atacante se encarga de penetrar a los sistemas a cambio de un pago. Aunque son menos comunes, en realidad son muy peligrosos ya que se trata de personas que poseen los conocimientos, experiencia y herramientas necesarias para penetrar en los sistemas, incuso en aquellos que tienen un nivel alto de seguridad.

Personal enterado: se trata de personas que tienen acceso autorizado o conocen la estructura del sistema de cierta organización. Por lo general es el mismo personal interno de una empresa o un exempleado, sus motivaciones van desde revanchas personales hasta ofertas y remuneraciones de organizaciones rivales.

Terroristas: tienen como objetivo causar daños con diferentes fines por ejemplo proselitistas o religiosos.

Robo: se refiere a la extracción física de la información por medio de unidades de almacenamiento secundario (diskettes, CD, cintas, etc.), robo físico de los componentes de hardware del sistema e incluso también se considera como robo el uso de los equipos para actividades diferentes a los que se les asigna en la organización.

Sabotaje: consiste en reducir la funcionalidad del sistema por medio de acciones deliberadas dirigidas a dañar los equipos, logrando la interrupción de los servicios e incluso la destrucción completa del sistema. Puede ser perpetuada por el personal interno o por opositores externos.

Fraude: estas actividades no tienen como principal fin la destrucción del sistema, si no aprovechar los recursos que se manejan para obtener beneficios ajenos a los objetivos de la organización.
Aun cuando los responsables del fraude sean identificados y detenidos, este tipo de actividad comúnmente se trata con suma discreción sin hacerle publicidad debido a que le da mala imagen a la organización implicada.

Ingeniería social: en el campo de la seguridad informática ingeniería social es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos llevándolos a revelar información sensible, o bien a violar las políticas de seguridad típicas.
Con este método, los ingenieros sociales aprovechan la tendencia natural de la gente a confiar en su palabra, antes que aprovechar agujeros de seguridad en los sistemas informáticos.

2.1.2.2 Hardware

Se da la amenaza por fallas físicas que presente cualquiera de los elementos de hardware que conforman al sistema de cómputo. Estas fallas físicas pueden ser defectos de fabricación o mal diseño del hardware, pero también pueden ser el resultado de un mal uso y descuido en el mantenimiento.

2.1.2.2.1 Tipos de amenazas de hardware

Mal diseño: es cuando los componentes de hardware del sistema no son apropiados y no cumplen los requerimientos necesarios, en otras palabras, dicha pieza del módulo no fue diseñada correctamente para trabajar en el sistema.

Errores de fabricación: es cuando las piezas de hardware son adquiridas con desperfectos de fabricación y posteriormente fallan al momento de intentar usarse. Aunque la calidad de los componentes de hardware es responsabilidad del fabricante, la organización que los adquiere es la más afectada por este tipo de amenaza.

Suministro de energía: las variaciones de voltaje dañan los dispositivos, por ello es necesario verificar que las instalaciones de suministro de energía funcionen dentro de los parámetros requeridos. También debe procurarse que dichas instalaciones proporcionen los voltajes requeridos para hacer funcionar un dispositivo, pues existen componentes de hardware que necesitan ser energizados a ciertos niveles de voltaje especificados por los fabricantes, de lo contrario se acortara su vida útil.

Desgaste: el uso constante del hardware produce un desgaste considerado como normal, con el tiempo este desgaste reduce el funcionamiento optimo del dispositivo hasta dejarlo inutilizable.

Descuido y mal uso: todos los componente deben ser usados dentro de los parámetros establecidos por los fabricantes, esto incluye tiempos de uso, periodos y procedimientos adecuados de mantenimiento, así como un apropiado almacenamiento. No seguir estas prácticas provoca un desgaste mayor que trae como consecuencia descomposturas prematuras y reducción del tiempo de vida útil de los recursos.

2.1.2.3 Red de datos

Esta amenaza se presenta cuando la red de comunicación no está disponible para su uso, esto puede ser provocado por un ataque deliberado por parte de un intruso o un error físico o lógico del sistema mismo. Las dos principales amenazas que se presentan en una red de datos son, la no disponibilidad de la red, y la extracción lógica de información a través de ésta.

2.1.2.3.1 Tipos

Topología seleccionada: la topología es la disposición física en la que se conectan los nodos de una red de ordenadores o servidores, cada una presenta una serie de ventajas y desventajas. Dependiendo el alcance y recursos compartidos en una red, puede ser mas conveniente seleccionar una topología sobre otra, pero debe tomarse en cuenta que las desventajas de cada arquitectura no solo limitan la comunicación, incluso pueden dejar la red fuera de servicio.
Por ejemplo en una red de anillo la comunicación se da por el paso de un token o testigo, que se puede conceptuar como un cartero que pasa recogiendo y entregando paquetes de información, de esta manera se evitan eventuales pérdidas de información debido a colisiones, pero si la comunicación en algún nodo se pierde, entonces la comunicación en todo el anillo se pierde.

Sistema operativo: aunque el modelo OSI permite la comunicación entre equipos con diferentes sistemas operativos, se dan casos en los que ciertas opciones de operación difieren entre sistemas operativos, haciendo difícil el compartir ciertos recursos.
También cada sistema operativo tiene un nivel de protección diferente que los hace mas susceptibles a ataques que otros, y a partir de ahí el atacante puede tomar acciones contra otros sistemas operativos con mayor nivel de seguridad. Este último punto es considerado más una vulnerabilidad que una amenaza.

Incumplimiento de las normas de instalación de la red: la instalación del cableado físico de las redes de datos, deben seguir ciertas normas y estándares de diseño conocidos también como cableado estructurado. El cableado estructurado corresponde a un conjunto de normas internacionales que consiste en el tendido de cables en el interior de un edificio con el propósito de implantar una red de área local, es el sistema colectivo de cables, canalizaciones, conectores, etiquetas, espacios y demás dispositivos que deben ser instalados para establecer una infraestructura de telecomunicaciones genérica en un edificio, para ello hay que tener en

cuenta las limitaciones de diseño que impone la tecnología de red de área local que se desea implantar:

- La segmentación del tráfico de red.
- La longitud máxima de cada segmento de red.
- La presencia de interferencias electromagnéticas.
- La necesidad de redes locales virtuales.

No tomar en cuenta estos puntos puede resultar en fallas de diseño que causen problemas de transmisión de datos, operabilidad o indisponibilidad de los recursos de red.

2.1.2.4 Software

Las amenazas de software incluyen posibles fallas dentro del software de un sistema operativo, software mal desarrollado, mal diseñado o mal implantado, además de que existe software de uso malicioso que representa una amenaza directa contra un sistema.

2.1.2.4.1 Tipos

Software de desarrollo: es un tipo de software personalizado, puede ser creado con el fin de atacar un sistema completo o aprovechar alguna de sus características para violar su seguridad.

Software de aplicación: este software no fue creado específicamente para realizar ataques, pero tiene características que pueden ser usadas de manera maliciosa para atacar un sistema.

Código malicioso: es cualquier software que entra en un sistema de cómputo sin ser invitado e intenta romper las reglas, esto incluye caballos de Troya, virus, gusanos informáticos, bombas lógicas y otras amenazas programadas.

Virus: este tipo de código malicioso tiene como principal característica la capacidad de duplicarse a si mismo usando recursos del sistema infectado, propagando su infección rápidamente.

Troyanos: este tipo de código se presenta escondido en otros programas de aplicación aparentemente inofensivos, para posteriormente activarse de manera discreta cumpliendo su propósito nocivo.

Gusanos: es muy similar a los virus, con la diferencia de que éstos aprovechan mas los recursos de los sistemas infectados, atacando diferentes programas y posteriormente duplicándose para redistribuirse.

Errores de programación y diseño: el software creado para cumplir alguna función dentro de la organización (Por ejemplo un sistema de transacciones financieras, sistema de nomina, sistemas operativos, etc.) también pueden causar perdida o modificación de la información. Esto ocurre cuando el software en cuestión no cumple con los estándares de seguridad requeridos pues nunca fue diseñado para dar soporte a una organización. Los errores de programación y fallas generales que puede tener un software de aplicación también representan una amenaza.

2.1.2.5 Desastres naturales

Son eventos que tienen su origen en las fuerzas de la naturaleza. Estos desastres no solo afectan a la información contenida en los sistemas, sino también representan una amenaza a la integridad del sistema completo (infraestructura, instalación, componentes, equipos, etc.) pudiendo dejar al

sistema incluso en un estado de inoperabilidad permanente. Este tipo de amenazas también es más peligrosa si no se toman medidas para afrontar tales catástrofes.

2.1.2.5.1 Tipos

Entre los tipos de desastres naturales que amenazan a un sistema de información, tenemos las inundaciones, los terremotos, incendios, huracanes, tormentas eléctricas, etc. Los cuales provocan cortos circuitos, destrucción total o parcial de los equipos de cómputo, o alteraciones físicas de las localidades, causando que ya no sean apropiadas para albergar un equipo de cómputo.

Es necesario considerar el punto geográfico en el que se llevara a cabo la instalación del equipo de cómputo, centro de servicios de información, centro de cómputo etc. y hacer un estudio que permita determinar las amenazas a las que serian susceptibles a fin de evitar ser victimas de estos.

Adicionalmente considerar la importancia de un cableado no solo en la res de datos sino de las redes de energía eléctrica y suministro de aguas que de manera indirecta podrían causar algún desastre de este tipo y dañar la información de la organización.

El cableado eléctrico de un edificio no solo debe proporcionar continuidad del servicio sino también seguridad

2.2 Vulnerabilidades

Dependiendo del enfoque que se le de a la seguridad informática, un sistema informático está expuesto al peligro por medio de dos factores: Las amenazas y las vulnerabilidades.

Las vulnerabilidades constituyen el otro factor que pone en peligro la seguridad de un sistema, generalmente se cree que una vulnerabilidad es un punto débil de un sistema y aunque no es una definición incorrecta, tampoco expresa en su totalidad lo que es una vulnerabilidad.

2.2.1 Definición

Una vulnerabilidad informática es un elemento de un sistema informático que puede ser aprovechado por un atacante para violar la seguridad, así mismo pueden causar daños por sí mismos sin tratarse de un ataque intencionado.
A las vulnerabilidades se les consideran un elemento interno del sistema, por lo que es tarea de los administradores y usuarios el detectarlos, valorarlos y reducirlos.

2.2.2 Tipos de Vulnerabilidades

Las vulnerabilidades son el resultado de errores de programación (bugs), fallos en el diseño del sistema, incluso las limitaciones tecnológicas pueden ser aprovechadas por los atacantes.
Para esta investigación, se clasifican las vulnerabilidades en seis tipos: Físicas, naturales, de hardware, de software, de red y de factor humano.

2.2.2.1 Física

Está relacionada con el acceso físico al sistema. Es todo lo referente al acceso y de las instalaciones donde se tienen los equipos de cómputo que contienen la información o forman partes de los procesos esenciales del sistema.
Las vulnerabilidades de este tipo se pueden presentar en forma de malas prácticas de las políticas de acceso de personal a los sistemas y uso de medios físicos de almacenamiento de información que permitan extraer datos del sistema de manera no autorizada.

2.2.2.2 Natural

Recordemos que las amenazas naturales son todo tipo de desastres causados por fuerzas naturales que causan daño a un sistema, por el lado de

las amenazas naturales, estas se refieren al grado en que el sistema se puede ver afectado por este tipo de eventos.
Las vulnerabilidades de tipo natural se presentan principalmente en deficiencias de las medidas tomadas para afrontar los desastres, por ejemplo no disponer de reguladores, no-breaks, mal sistema de ventilación o calefacción, etc.

2.2.2.3 Hardware

Las vulnerabilidades de hardware representan la probabilidad de que las piezas físicas del sistema fallen (ya sea por mal uso, descuido, mal diseño etc.) dejando al sistema desprotegido o inoperable. También trata sobre las formas en que el hardware puede ser usado por personas para atacar la seguridad del sistema, por ejemplo el sabotaje de un sistema al sobrecargarlo deliberadamente con componentes de hardware que no han sido diseñados correctamente para funcionar en el sistema.

2.2.2.4 Software

Cada programa (ya sea de paquetería o de sistema operativo) puede ser usado como medio para atacar a un sistema más grande, esto se da debido a errores de programación, o porque en el diseño no fueron considerados ciertos aspectos (por ejemplo controles de acceso, seguridad, implantación, etc.).
Ambos factores hacen susceptible al sistema a las amenazas de software.

2.2.2.5 Red

Las redes pueden llegar a ser sistemas muy vulnerables, al tratarse de una serie de equipos conectados entre si compartiendo recursos, es posible atacar a toda la red penetrando primero en uno de los equipos y posteriormente expandirse al resto.
En una red la prioridad es la transmisión de la información, así que todas las vulnerabilidades están relacionadas directamente con la posible intercepción

de la información por personas no autorizadas y con fallas en la disponibilidad del servicio.
Estos dos puntos hacen que las vulnerabilidades de las redes lleguen a ser una combinación de vulnerabilidades de hardware, software, físicas e incluso naturales.

2.2.2.6 Factor humano

Los elementos humanos de un sistema son los mas difíciles de controlar lo que los convierte en constantes amenazas y al mismo tiempo una de las partes mas vulnerables del sistema.
Las vulnerabilidades de origen humano mas comunes son la falta de capacitación y concienciación, lo que puede dar lugar a la negligencia en el seguimiento de las políticas de seguridad, y mal uso del equipo de cómputo. Los actos contra la seguridad realizados a conciencia por un elemento humano (Como el robo de información o la destrucción de los sistemas) pueden ser el resultado de una vulnerabilidad humana, ya sea por un usuario que accidentalmente revela las contraseñas de acceso o no revisa periódicamente las bitácoras de actividades de los equipo de cómputo a fin de buscar actividades sospechosas por citar algunos ejemplo.

Un usuario resentido o con poca lealtad a la organización es una amenaza y una vulnerabilidad humana al mismo tiempo, pues él puede convertirse en el autor directo de ataques al sistema o revelar intencionalmente información del sistema a personas no convenientes.

Finalmente es importante hacer una reflexionen el sentido de que las vulnerabilidades se pueden reducir, eliminar o controlar lo que ayuda entonces a contrarrestar la posibilidad de que una amenaza se materialice y llegue a convertirse en un ataque.
De manera que el riesgo es el daño potencial que puede surgir por un proceso presente o suceso futuro, es decir, es la posibilidad de que un peligro pueda materializarse.
"El riesgo es el producto de la ocurrencia de la amenaza y su consecuencia"

Capitulo III
Identificación de ataques y técnicas de intrusión

La definición de un ataque es simple; Partiendo de que una amenaza se define como una condición del entorno del sistema de información (persona, máquina, suceso o idea) que, dada una oportunidad, podría dar lugar a que se produjese una violación de la seguridad (confidencialidad, integridad, disponibilidad o uso legítimo), un ataque no es más que la realización de una amenaza.

Para este capitulo nos enfocaremos a los ataques que son provocados deliberadamente.

Una técnica de intrusión es un conjunto de actividades que tienen por objetivo violar la seguridad de un sistema informático. Estas técnicas no solo deben ser conocidas por los atacantes, es imprescindible que sean conocidas por todos aquellos profesionales de las tecnologías de información a fin de proteger y resguardar los sistemas y medios de información de manera veraz y oportuna.

3.1 Reconocimiento y Obtención de Información.

Ya se ha remarcado la importancia de la información para una organización, pero también es valiosa para los atacantes, tal que muchos ataques no tienen como propósito destruir el sistema, sino acceder a la información contenida en éste, extraerla, descifrarla, y posteriormente salir del sistema sin dejar rastro ni daños, con el fin de que tal sistema siga siendo útil para seguir extrayendo información.

La forma de obtener la información, así como protegerla varía dependiendo del medio y del método usado.

3.1.1 Bases de Datos Públicas.

Una de las razones por las cuales las vulnerabilidades en las bases de datos están tan extendidas es el hecho de que la mayoría de las bases que existen en Internet han sido programadas por usuarios para dar dinamismo a sus páginas pero sin preocuparse de las implicaciones de seguridad.

El usuario que programa una base de datos y la sube a su Web, a menudo no es consciente de que un fallo de seguridad puede comprometer todo el servidor que hospeda su página. Y los administradores de servidores Web que ofrecen servicios a sus clientes, no pueden hacer mucho para evitarlo ya que es una labor muy extensa la de supervisar todas las acciones de los usuarios uno por uno.

3.1.2 WEB

El World Wide Web es un sistema de documentos de hipertexto e hipermedios (Documentos que pueden bifurcarse o ejecutarse cuando sean solicitados) enlazados y accesibles a través de la red de computadoras Internet.

Este tipo de ejecución puede prestarse para ocultar códigos maliciosos en las páginas Web, los cuales son ejecutados por los usuarios sin que la mayoría de las veces lo noten, dejando expuesta la seguridad del sistema. Por otra parte, el Internet es una red tan grande que su control y regulación es casi imposible, por lo que su uso supone una constante exposición a diversos tipos de amenazas y su seguridad recae en todos y cada uno de sus usuarios.

3.1.3 DNS

El DNS (*Domain Name Service)* es un sistema de nombres que permite traducir de nombre de dominio a dirección IP y vice-versa. Aunque Internet sólo funciona con base en direcciones IP, el DNS permite que los humanos usemos nombres de dominio que son bastante más simples de recordar. Los ataques al DNS están basados principalmente en la suplantación de identidades, tomando la identidad de otro elemento para realizar ciertas acciones dañinas, por ejemplo interceptando a los usuarios que quieren acceder a ciertos recursos en línea redirigiendo su petición a cualquier otro sitio.

3.1.4 Keyloggers

Los keyloggers son un tipo de software encargado de registrar todas las actividades del teclado de un equipo de cómputo sin que el usuario se de cuenta; generalmente son usados para obtener paswords de acceso autorizado a sistemas.

Los keyloggers también pueden ser usados en favor de la seguridad informática pues permiten llevar un registro de lo que hacen los usuarios cuando usan los equipos.

Por ejemplo pueden usarse para determinar qué acciones realizó un usuario durante una sesión de trabajo al interpretar las secuencias introducidas por medio del teclado. Tales acciones pueden delatar si el usuario ingresó a una cuenta que no le corresponde o si modificó información importante del sistema.

Aunque menos comunes, los keyloggers también pueden ser dispositivos de hardware conectados al puerto del teclado

3.1.5 Ingeniería Social

La ingeniería social es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Un ingeniero social usará comúnmente el teléfono o Internet para engañar a la gente y llevarla a revelar información sensible, o bien a violar las políticas de seguridad típicas. Generalmente se está de acuerdo en que "los usuarios son el eslabón débil" en seguridad; éste es el principio por el que se rige la ingeniería social.

3.1.6 Otros

Jamming o Flooding: este tipo de ataques desactivan o saturan los recursos del sistema. Por ejemplo, un atacante puede consumir toda la memoria o espacio en disco disponible, así como enviar tanto tráfico a la red que nadie más puede utilizarla.

Packet Sniffing: muchas redes son vulnerables al eavesdropping (literalmente traducido como "escuchar secretamente"), que consiste en la pasiva intercepción (sin modificación) del tráfico de red. En Internet esto es realizado por paquetes sniffers o husmeadores, los cuales son programas que monitorean los paquetes de red que están dirigidos a la computadora donde están instalados. El sniffer puede ser colocado tanto en una estación de trabajo conectada a red, como a un equipo router o a un gateway de Internet, y esto puede ser realizado por un usuario con legítimo acceso, o por un intruso que ha ingresado por otras vías.

Snooping Y Downloading: los ataques de esta categoría tienen el mismo objetivo que el sniffing, obtener la información sin modificarla. Sin embargo los métodos son diferentes. Además de interceptar el tráfico de red, el atacante ingresa a los documentos, mensajes de e-mail y otra información guardada, realizando en la mayoría de los casos un downloading, esto es, un proceso de descarga de la información a su propia computadora.

Tamppering O data Diddling: esta categoría se refiere a la modificación desautorizada de los datos, o del software instalado en un sistema, incluyendo borrado de archivos. Este tipo de ataques son particularmente serios cuando el que lo realiza ha obtenido derechos de administrador o supervisor, con la capacidad de ejecutar cualquier comando y por ende alterar o borrar cualquier información que puede incluso terminar en la baja total del sistema en forma deliberada.

3.2 Identificación de Vulnerabilidades

Las vulnerabilidades son los aspectos del sistema que son aprovechados por los atacantes para violar la seguridad. Es difícil detectar un ataque por medio de una vulnerabilidad, pues el atacante aprovecha una característica del funcionamiento del sistema (Puede ser de hardware, software o de la misma organización del sistema) en vez de perpetrar un ataque por la fuerza usando medios externos.

Identificar las vulnerabilidades del sistema es una actividad importante para ambos bandos, el atacante y el defensor; no se puede suprimir a una vulnerabilidad si de entrada se desconoce sus existencia.

3.2.1 Ataques a Redes Telefónicas

El hecho de que las nuevas redes telefónicas corporativas estén unidas a las redes de datos corporativas las convierte en un objetivo muy atractivo para los atacantes, que pueden emplearlas como una vía de entrada a los sistemas informáticos. Desde ahí, podrán robar información corporativa, escuchar conversaciones y crear confusión en el sistema debido al desconocimiento de la procedencia del ataque.

La principal amenaza y forma de ataque a las redes telefónicas, es la intercepción de la información, aunque también la instalación de terminales no autorizadas supone un problema importante en este medio de comunicación.

También se llegan a presentar casos donde el servicio queda no disponible, ya sea a causa de una sobresaturación del medio de transmisión o incluso daños a la infraestructura.

3.2.2 Ataques a la Telefonía Inalámbrica

En el mercado existen dos tipos de teléfonos inalámbricos: los digitales y los analógicos.

En ambos casos, son blancos de ataques de intercepción de información, aunque los sistemas digitales se les considera mas seguros debido a las técnicas de encriptación y transmisión de datos que usan, aun así estas técnicas no son infalibles, y cada vez se descubren nuevas formas para infringir la seguridad de estos sistemas.

La intercepción de la información no está limitada a escuchar las llamadas telefónicas, también se pueden interceptar los números telefónicos que se marquen y otro tipo de datos (como información de transacciones financieras) que puedan manejarse durante una operación telefónica.

Estos ataques se valen de recursos diferentes, como algoritmos y programas de descriptación, equipos de hardware especializados, programas maliciosos e ingeniería social.

Cada vez son mas diversos los servicios que se prestan por telefonía inalámbrica y también los equipos telefónicos presentan mas características similares a los de una PC, esto hace que los teléfonos sean mas prácticos y versátiles, pero al mismo tiempo los hace susceptibles a otro tipos de ataques, en la actualidad ya existen virus, troyanos, spyware y otros tipos de códigos maliciosos que afectan a un equipo de telefonía inalámbrica y se transmiten a través de tecnologías y servicios como Bluetooth, mensajes de texto, mensajería instantánea, correo electrónico, redes WiFi, puertos USB, audio y vídeo, y el acceso a Internet

Una tercera amenaza que existe en un sistema de telefonía inalámbrica es la no disponibilidad del sistema, generalmente esto se da cuando el ancho de banda del sistema se satura, esto puede ser causado de manera intencional o no. Se han reportado casos de ataques intencionales que consisten en saturar el ancho de banda por el envío excesivo de mensajes de texto.

3.2.3 Barrido de Puertos

El barrido o escaneo de puertos consiste en verificar cuáles puertos están disponibles para ser explorados dentro de una o más computadoras en una red. Por sí solo, el barrido de puertos es una actividad normal que frecuentemente es usado para mejorar los servicios de seguridad y rendimiento de una red, pero también puede convertirse en una actividad nociva ya que puede ser usada para buscar puntos de acceso vulnerables para forzar la entrada al sistema.

Existen casos en que el sistema tiene varios puertos abiertos y son desconocidos para el encargado de seguridad, y en consecuencia estos puertos no son vigilados y los datos pueden fluir a través de ellos sin ningún tipo de control de seguridad, convirtiéndole en una vulnerabilidad del sistema.

Esto puede ser consecuencia de una mala configuración de los sistemas de seguridad (por ejemplo los Firewalls) los cuales pueden dejar por default varios puertos abiertos, y los administradores del Firewall olvidan revisar minuciosamente la configuración para verificar todos los puertos disponibles.

3.2.4 Identificación de Firewalls

Un Firewall es un dispositivo de seguridad encargado de filtrar los paquetes de datos a partir de una serie de reglas y criterios definidos por el administrador de una red. Este dispositivo puede ser una maquina específicamente diseñada y construida para esta función, aunque también puede ser un software que se instala en una computadora conectada a la red a través de la cual se filtran los datos antes de distribuirse a los otro equipos de la red. Cada computadora puede tener un software de Firewall instalado para un filtrado individual.

Los atacantes pueden saltar la seguridad de un Firewall aprovechando los puertos abiertos del sistema. Un método común para descubrir los puertos vulnerables es enviando una serie de paquetes de datos defectuosos (por ejemplo dirigidos a una IP que no existe en la red), los cuales al ser filtrados, el Firewall los interceptará y no permitirá su enrutamiento, pero si el puerto no está siendo filtrado, entonces permitirá pasar el paquete y al no poder enrutarlo correctamente, el Firewall mandará un mensaje de error ICMP (Internet Control Message Protocol)indicando que el paquete no fue filtrado. Se puede crear un esquema para indicar qué puertos no están siendo filtrados con base en los mensajes de error que se generen con este proceso.

3.2.4.1 Interpretación de reglas y filtros

Las reglas de filtrado son una serie de condiciones que un usuario, equipo de la red o paquete de datos debe cumplir con base en las políticas de seguridad de la información de la organización para tener acceso a un equipo a través de los puertos protegidos por un sistema de seguridad (Firewall).

Desde el punto de vista del atacante, la interpretación de filtros se refiere a los procedimientos que se lleva a cabo para descifrar las condiciones necesarias que se necesitan para pasar información a través de los firewalls sin ser un usuario autorizado. Estos procedimientos incluyen ataques por la fuerza e incluso ingeniería social.

3.2.5 Identificación de Sistemas Operativos / OS Fingerprinting

OS Fingerpriting es el proceso para identificar el sistema operativo de un usuario remoto de una red, esta identificación se basa en las características que diferencian a cada uno de los sistemas de los demás: distintas implementaciones de la pila TCP/IP, diferentes comportamientos ante el envío de paquetes que presentan una conformación especial, distintas respuestas en función del protocolo utilizado (TCP, ICMP, ARP), etc.
El objetivo de esta técnica no sólo se limita a identificar el sistema operativo remoto, también se puede obtener información de cómo funciona en caso de ser un sistema personalizado que no se puede encontrar en un listado comercial.
El Fingerpriting tiene aplicaciones benéficas para la seguridad informática, pero como la mayoría de este tipo de recursos, también puede usarse para un ataque, siendo la identificación de un sistema operativo remoto, uno de los primeros pasos a realizar para un ataque.

3.2.5.1 Métodos de Identificación

Existen dos métodos de Fingerprinting clasificados como activo y pasivo.

Fingerprinting activo: este tipo de identificación del Sistema Operativo se basa en analizar la respuesta del servidor que se quiere revisar cuando se le envían determinados paquetes TCP y UDP.
El Fingerpriting activo tiene la ventaja de que se puede experimentar enviando diversos tipos de paquetes para forzar diferentes respuestas por parte del sistema, esto da una mayor variedad de resultados a la hora de ser analizados, los cuales son muy útiles para determinar las características del sistema.

Su mayor desventaja es que es fácil de detectar e interceptar por parte de los dispositivos de seguridad (por ejemplo firewalls) implementados en la red donde esté el sistema analizado.
Como se ha mencionado, el tipo de pruebas que se hacen al sistema analizado por este método, consiste en enviar paquetes y analizar las respuestas.

Fingerpriting pasivo: el Fingerpriting pasivo se basa en capturar paquetes de datos provenientes del sistema remoto, contrario al Fingerpriting activo en que se envían paquetes.
Esta captura de paquetes se logra por medio de programas llamados sniffers, los cuales son programas que registran las actividades y tramas de datos que entran y salen de una computadora conectada en una red.
Basándose en los paquetes capturados de un sniffer de dichos paquetes, se puede determinar el sistema de operación del sistema remoto. Igual que en el caso de la identificación activa, la pasiva se basa en el principio de que todas las direcciones IP aportan información sobre las características del sistema operativo. Analizando los paquetes capturados e identificando dichas diferencias se puede determinar el sistema operativo de la máquina remota.

3.2.6 Escaneo a Redes Inalámbricas

Una red inalámbrica es un conjunto de dispositivos informáticos, comunicados entre sí por medios no tangibles (Por ejemplo, ondas de radio). Mientras que en las redes cableadas es más complicado conectarse de forma ilegítima -habría que conectarse físicamente mediante un cable-, en las redes inalámbricas esta tarea es más sencilla. Debido a esto hay que poner especial cuidado en proteger una red inalámbrica.
El primer paso para conectarse a una red inalámbrica es detectar primero su presencia, así como recabar información sobre su configuración. El método mas simple para detectar una red es utilizar la propia herramienta de redes inalámbricas que incorpora el sistema operativo o que incluye el fabricante de la tarjeta inalámbrica. Esta herramienta permite realizar una exploración de las redes disponibles, mostrando una lista con indicación del nombre SSID la red y tipo de red (Si esta cifrada o no) de cada uno de los puntos de acceso detectados. Si una red no esta cifrada, se dice que es una red

abierta, pero no significa que está desprotegida, ya que puede estar usando un sistema de protección distinto al cifrado WEP/WPA (Sistema de cifrado diseñado para redes Wi-Fi).
Estos datos son suficientes para conectarse a una red propia, pero para entrar a una red a la que no se está autorizado se necesita recopilar más datos.

Las herramientas de los intrusos utilizan dos métodos para recopilar información:

Pasivo. Estos sistemas se limitan a escuchar e interpretar la información que reciben. Por ejemplo, las redes suelen emitir su identificación SSID, por tanto, basta recibir esos paquetes para identificar este nombre. Los ataques pasivos afectan la confidencialidad pero no influyen necesariamente a la integridad de la información.

Activo. En este caso los sistemas no se limitan a escuchar, sino que interactúan de una u otra forma, con la red. Por ejemplo, si no reciben el nombre SSID, interactúan con el punto de acceso o los equipos de los usuarios para conseguir dicha información. Los ataques activos pueden llegar a modificar, eliminar o inyectar tráfico a la red.

La información que se puede conseguir utilizando estos métodos es del siguiente tipo:

–Nombre SSID, aunque el punto de acceso lo tenga oculto

–Esquema de direccionamiento IP de la red.

–Marca y modelo del hardware.

–Versión del software.

–Tipo de cifrado utilizado.

–-Clave de cifrado WEP.

–Puertos IP abiertos.

–Información intercambiada.

Toda esta información no puede conseguirse en un solo ataque o con una sola herramienta, por lo que el atacante deberá recopilar la información en diversos pasos sin ser descubierto y usar todo tipo de herramientas y métodos incluyendo, de ser necesaria la ingeniería social.

3.2.7 Instalaciones Físicas

La Seguridad Física consiste en la "Aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial". Se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo así como los medios de acceso remoto hacia y desde el mismo, implementados para proteger el hardware y los medios de almacenamiento de datos.
Las principales amenazas que se prevén en la seguridad física son:

1.- La probabilidad de que desastres naturales, incendios accidentales tormentas e inundaciones afecten a los sistemas de información, así como también la falta de instalaciones apropiadas para afrontarlas.

2.- Amenazas ocasionadas por el hombre, robos, disturbios, sabotajes internos y externos deliberados.

A veces basta recurrir al sentido común para darse cuenta que cerrar una puerta con llave o cortar la electricidad en ciertas áreas siguen siendo técnicas válidas en cualquier entorno.
Ya se ha tratado un tema referente a las amenazas a las instalaciones físicas en el capítulo 2.

Control de Accesos

Este punto del tutorial se refiere a la seguridad fisica de las instalaciones. El control de acceso no sólo requiere la capacidad de identificación, sino también asociarla a la apertura o cierre de puertas, permitir o negar acceso

basado en restricciones de tiempo, área o sector dentro de una empresa o institución. Los controles de acceso incluyen la utilización de personal de seguridad, dispositivos electrónicos de acceso y verificación, cerraduras manuales y electrónicas, e implantación de políticas y normas de seguridad entre el mismo personal.

Una intrusión a las instalaciones físicas generalmente se da por los mismos empleados que conocen y tienen acceso directo a las instalaciones, en casos muy raros puede perpetuarse por personas totalmente ajenas como por ejemplo ladrones, espías y terroristas.

3.2.8 Configuración de Servicios y Servidores

Existen muchos casos en que los riesgos pueden reducirse simplemente por verificar la configuración de todos los servicios que forman parte de un sistema.

Todos los servicios vienen con una configuración estándar que pueden permitir una instalación rápida y un uso fácil, pero no es la mas apropiada para cubrir las necesidades de seguridad. Muchas veces un servicio mal configurado se convierte en una grave vulnerabilidad que será aprovechada por los atacantes. Por ello cuando se implanta un servicio o dispositivo dentro de una red, es necesario realizar una configuración personalizada que cumpla con las políticas de seguridad, manteniendo un balance entre la funcionalidad del sistema y la seguridad.

3.2.9 Software

Los atacantes pueden aprovechar diferentes vulnerabilidades de un software (errores de programación, mal diseño, mala configuración, etc) para penetrar en una red o sistema, pero también existe software que sin ser necesariamente maliciosos, pueden ser usados para romper la seguridad. En el mercado existen numerosas aplicaciones que fueron creadas para ayudar en la mejora continua de la seguridad, la administración de sistemas o facilitar la conectividad de una red, pero que también son herramientas usadas en el acceso desautorizado a los sistemas.

Ejemplos más concretos son Nmap, un software que permite hacer un rastreo de puertos TCP y UDP, o Netslumber, una aplicación que explota de forma continua el espectro radioeléctrico en busca de redes inalámbricas disponibles.

También existe software personalizado, creado por los mismos atacantes con el propósito de ayudar a penetrar la seguridad de los sistemas.

3.3 Explotación y obtención de acceso a Sistemas y Redes

Ya se ha mencionado que cada sistema o red tiene puntos vulnerables que pueden ser aprovechados por los atacantes para acceder al sistema, a esta actividad se le conoce como explotación del sistema, y puede ser llevada a cabo por personas externas o los mismos usuarios internos.

La explotación de sistemas no se limita al aprovechamiento de errores de programación o puertos abiertos, con ingenio también se puede sacar provecho de las características bien ejecutadas del sistema mismo. Esta práctica puede ser ejecutada por distintos medios, así que para combatirla es necesario desarrollar sistemas de cómputo con técnicas de programación segura, así como también hacer uso de distintas tecnologías, estrategias y políticas de seguridad.

A continuación se dará un resumen de las formas más comunes de explotación de sistemas.

3.3.1 Promiscuidad en Redes

El propósito de una red es la comunicación entre distintos equipos de cómputo, por lo que es obvia la idea de que distintos usuarios transmitan información a través de una red.

La promiscuidad en redes, se refiere a una red donde diversos usuarios transmiten y reciben información con niveles de seguridad muy bajos. Esto representa una amenaza para los usuarios y para la red, ya que un usuario puede propagar fácilmente algún tipo de virus, infectando a los otros usuarios e inclusive a los servidores, a través de los cuales pueden seguir infectando a otros usuarios que se conecten posteriormente.

Este tipo de situaciones se da principalmente en redes de uso público que existen en el Internet, aunque las redes privadas tampoco están exentas inclusive si su seguridad es más estricta.

3.3.2 Robo de Identidad

Este tipo de ataque se efectúa cuando el atacante se hace pasar por otro usuario, con el propósito de ganar acceso a la red, obtener privilegios de usuario superior o realizar transacciones financieras fraudulentas. El atacante pude robar la identidad usando directamente el equipo de cómputo de la víctima, obteniendo la clave de usuario y contraseña de acceso, o falsificando las identificaciones electrónicas y digitales. Una variante del robo de identidad es el robo de sesión, como el nombre indica, consiste en apropiarse de la sesión iniciada por otro usuario, teniendo acceso a todos los recursos a los que la víctima tiene acceso. También suplantar una dirección IP es un robo de identidad, pues hacen pasar un equipo de cómputo por otro. Este tipo de suplantación es posible al modificar manualmente la configuración de red del equipo.

3.3.3 Engaño a Firewalls y Detectores de Intrusos

Los Firewalls y otros programas de seguridad tienen por propósito cuidar la información de usuarios no autorizados y otras amenazas, pero estos sistemas tampoco son infalibles, y es posible entrar a ellos por medio de una serie de procedimientos que por lo general no pueden ser ejecutados por una sola aplicación automática, si no por un atacante humano, de ahí la importancia de tener políticas claras de seguridad a fin de que la configuración de los dispositivos sea la adecuada para brindar la protección que se desea.

En la sección de fingerpriting y puertos, ya se mencionaron algunos ejemplos de cómo penetrar estos sistemas de seguridad, el robo de identidad también es una forma de pasar por estos medios, pues el atacante accede al sistema usando una sesión autorizada, y los detectores

de intrusos no pueden verificar que el usuario sea realmente quien dice ser. Uno de los más graves problemas que genera el que uno de estos sistemas

sean burlados, es que toma tiempo antes de que los encargados de seguridad se den cuenta que hay un intruso, y en ese lapso de tiempo pudo causar daños graves.

3.3.4 Vulnerabilidades en el Software

Las vulnerabilidades en el software pueden ser errores de programación, configuración, análisis, diseño o implantación y pueden presentarse en los programas de seguridad, navegadores de Internet, administradores de bases de datos, aplicaciones varias, y el mismo sistema operativo.
La forma en que un atacante aprovecha estas vulnerabilidades para entrar a un sistema varía dependiendo del sistema, software y herramientas con las que cuenta, por lo que cada caso es diferente, pero un paso común a seguir, es primero reunir toda la información posible sobre el sistema objetivo.
A partir de este punto se tratarán varias vulnerabilidades de software que generalmente son usadas para atacar la seguridad de un sistema.

3.3.4.1 Buffer Overflows

Se trata de un error de programación, en el que un proceso intenta guardar datos mas allá de los límites de memoria asignados, dando por resultado la escritura de datos en direcciones cercanas de memoria correspondientes a otro procesos, dando resultados incorrectos, bloqueo o interrupción.
Este error también puede ser causado por la ejecución de código malicioso y es la causa de muchas vulnerabilidades de software pues puede ser aprovechado para corromper la ejecución de un programa produciendo una sobreescritura de la dirección de retorno de una función y haciendo que apunte directamente hacia un código concreto (generalmente un shell) logrando que se ejecute.

3.3.4.2 Heap Overflows

Es otro tipo de buffer overflow que causa una modificación en los datos contenidos de una pila o heap (área de memoria dinámicamente reservada por la aplicación) en vez de modificar la dirección de retorno, logrando modificar la lógica de funcionamiento de un programa.

3.3.4.3 Errores en el Formato de Cadena (Format Strings Bugs)

Descubierto por primera vez en 1999. Comúnmente aparece cuando el programador desea imprimir una cadena conteniendo los datos ingresados por el usuario. El programador puede confundir por error printf (bufer) con printf("%s", buffer). La primera función interpreta buffer como una cadena de formato y ejecuta cualquier instrucción que pueda contener. La segunda función imprime la cadena en pantalla que es lo que el programador intentaba. Con esta técnica podemos leer todo el contenido de la pila y situar ESP en la posición que queramos. Al igual que en el caso de los buffer overflows, el objetivo no es otro que sobrescribir la dirección de retorno.

3.3.4.4 Condición de Carrera (Race Conditions)

Una condición de carrera describe el error que se produce en programas o circuitos lógicos cuando no han sido diseñados adecuadamente para su ejecución simultánea con otros. Se produce cuando una serie de instrucciones se va ejecutando e inesperadamente una instrucción se sustituye inmediatamente por otra diferente, pero se le otorgan los mismos permisos y prioridades que el anterior, pudiendo acceder a archivos a los que normalmente no tiene permiso.

3.3.4.5 SQL Injection

Este bug surgió con el boom de las aplicaciones web que utilizan bases de datos. Se da cuando se introducen datos suministrados por el usuario como parte de una consulta SQL. Una inyección SQL sucede cuando se inserta o "inyecta" un código SQL "invasor" dentro de otro código SQL para alterar su funcionamiento normal.

Al ejecutarse esa consulta por la base de datos, el código SQL inyectado también se ejecutará y podría hacer un sinnúmero de cosas, como insertar registros, modificar o eliminar datos, autorizar accesos e, incluso, ejecutar código malicioso en el computador.

3.3.4.6 Cross-Site & Cross-Domain Scripting
Cross-Site-Scripting

El Cross-Site-Scripting es una vulnerabilidad que puede causar un impacto tanto a una aplicación web como a usuarios que de manera inconsciente activen dicha secuencia de comandos.

Dicho código malicioso se compone de cadenas de datos cuyo contenido son scripts completos contenidos en enlaces o ejecutados desde formularios. En caso de que sea ejecutado el mismo se ejecutara en el equipo del usuario con todos los privilegios permitidos por las políticas de seguridad configuradas en el navegador del usuario o del sitio visitado.

La mayor problemática es que estas cadenas de código se encuentran ocultas a la sombra de vínculos en donde el usuario normalmente no hace una vista del código de dicho enlace y lo ejecuta con una política de confianza total, dicha ejecución se realiza de una manera indirecta, ya sea por una activación vía hipervínculo o por la ejecución al momento de la carga de un sitio afectado por este tipo de ataque, el atacante no realiza su acción pensando en un usuario en especifico si no que actúa de manera de que afectan a cualquier usuario que inocentemente caiga en dicha trampa, las formas mas comunes de realizar dicha agresión es por medio de correos electrónicos, vínculos falsos o ataques directos a sitios no preparados para este tipo de ataque.

Cross Domain

Esta vulnerabilidad se basa en el elemento OBJECT, permitido en HTML 4, y que es usado para incluir objetos externos dentro de una página Web. Estos objetos pueden ser cualquier control ActiveX como WebBrowser, además de imágenes, applets y otros.

Los controles WebBrowser (controlan diversas acciones en el navegador), incluidos en esta etiqueta pueden eludir las restricciones de seguridad ordinarias aplicadas para otros elementos del código HTML. Esto hace posible evitar las restricciones de seguridad en los servidores, y en las computadoras de los usuarios eludir las zonas de seguridad.
Esto literalmente significa que se puede ejecutar código malicioso al visitar una página Web o al recibir un mensaje electrónico con formato HTML, tal como si fuera ejecutado en forma local, sin advertencia alguna del Internet Explorer.

3.3.4.7 Virus y Gusanos

Un virus es un código escrito con la intención expresa de replicarse. Un virus se adjunta a sí mismo a un programa host y, a continuación, intenta propagarse de un equipo a otro. Un verdadero virus no se difunde sin la intervención humana, alguien debe compartir un archivo o enviar un mensaje de correo electrónico para propagarlo.
Un gusano, al igual que un virus, está diseñado para copiarse de un equipo a otro, pero lo hace automáticamente. En primer lugar, toma el control de las características del equipo que permiten transferir archivos o información. Una vez que un gusano esté en su sistema, puede viajar solo. El gran peligro de los gusanos es su habilidad para replicarse en grandes números. Por ejemplo, un gusano podría enviar copias de sí mismo a todos los usuarios de su libreta de direcciones de correo electrónico
Un gusano puede consumir memoria o ancho de banda de red, lo que puede provocar que un equipo se bloquee.

3.3.5 Ataques a Contraseñas

Un ataque a contraseña es toda acción dirigida a obtener, modificar o borrar las contraseñas de acceso de un sistema informático. Estos ataques pueden ser perpetuados más fácilmente si los usuarios autorizados usan contraseñas débiles, es decir, contraseñas limitadas por un número y tipo de caracteres, también se considera débil a una contraseña cuando se usan palabras completas (o deformaciones simples) contenidos en un idioma. Se suele recomendar usar combinaciones aleatorias de caracteres para formar una contraseña robusta, con la desventaja de que la mayoría de los

usuarios no pueden recordar este tipo de contraseñas y generalmente anotan las contraseñas en otros medios (como un archivo de texto o una nota de papel) donde pueden extraviarla o puede ser revisado por otros usuarios.

Acceso a los ficheros de contraseñas.

Este ataque es bastante sencillo, y se basa en las vulnerabilidades de un sistema al guardar las contraseñas existentes en ficheros visibles donde pueden ser fácilmente encontrados y la información interpretada. Una forma de enfrentar este problema es usando sistemas de encriptación para cifrar los contenidos de estos ficheros y guardarlos en locaciones donde solo puedan ser leídos por los administradores.

Ataque de diccionario.

Consiste en probar todas las palabras existentes en un diccionario como una posible contraseña.
En este método también se pueden combinar las palabras para formar frases, alterar las combinaciones de cadenas, y usar diccionarios de idiomas extranjeros.
Es un método muy efectivo cuando los usuarios tienen contraseñas débiles.

Ataque por la fuerza.

Se trata de combinar todos los posibles caracteres para formar combinaciones hasta obtener la contraseña correcta.
Es el método mas tardado y difícil, y solo puede ser logrado por maquinas potentes que puedan realizar cientos o miles de combinaciones por segundo.

3.3.6 Debilidad de los Protocolos de Red

Los protocolos de red son un conjunto de reglas formales que permiten el intercambio de datos entre entidades que forman parte de una red.

Los elementos de una red pueden ir desde hardware periférico hasta equipos remotos.

Este intercambio de datos no se limita a la información contenida en las bases de datos u otros archivos de aplicación, también incluye instrucciones y procesos.

Por eso una debilidad en los protocolos de intercambio tiene consecuencias diversas que pueden ir desde negación del servicio de red, pérdida y alteracionde información, robo de los recursos de la red e incluso control remoto de los equipos

3.3.7 Ataques a Servicios

Hay varios tipos de ataques a los servicios, entre ellos tenemos los siguientes:

- Ejecutar actividades que consuman una gran cantidad de recursos de las maquinas afectadas, provocando una reducción en su rendimiento y posteriormente la caída del sistema completo.

- Provocar el colapso de redes mediante la generación de grandes cantidades de trafico, generalmente de múltiples equipos.

- Sabotaje de la red mediante routers que se encarguen de proporcionar información falsa sobre las tablas de enrutamiento que impidan el acceso a ciertas maquinas de la red.

- Transmisión de paquetes de datos malformados o que no cumplan las reglas de protocolo, para provocar la caída de los equipos que no están para recibir este tipo de trafico malintencionado.

- Incumplimiento de las reglas de un protocolo.

3.3.8 Negación de Servicio

Los ataques a los servicios tienen por objetivo colapsar un sistema o red para evitar que los servicios y recursos puedan ser utilizados por los usuarios.

3.3.9 Ataques a Redes Inalámbricas

Los ataques a las redes pueden dividirse en pasivos y activos.

Ataques pasivos.

En estos ataques no se modifica la información, el atacante se limita a escuchar, obtener y monitorear la información. Este tipo de ataque es difícil de detectar.

Ataques activos.

Los ataques activos consisten en modificar y/o denegar el acceso a la información, es decir, un usuario no autorizado dentro de la red no solo accede a la información sino que también la modifica y/o impide el acceso a esta.

Sniffing

El sniffing es un ataque pasivo que consiste en que un usuario no autorizado se dedica a hacer un monitoreo de todos lo paquetes de información que circulan por la red mediante un sniffer. El trafico de las redes inalámbricas puede espiarse mas fácilmente que una red convencional pues solo se necesita una tarjeta de red y un equipo para empezar a interceptar los datos, independientemente de si están cifrados o no.
Análisis de tráfico
En este tipo de ataque pasivo el atacante se ocupa de obtener la información que desea por medio de una examinación profunda del tráfico y sus patrones: a qué hora se encienden ciertos equipos, cuánto tráfico envían, durante cuánto tiempo, etc.

Suplantación o enmascaramiento

Este tipo de ataque activo consiste en conseguir varias direcciones válidas mediante un sniffer y analizar el tráfico para saber a que hora poder conectarse para suplantar a un usuario de la red atacada, así cuando llega el momento el atacante se apodera de la dirección del verdadero usuario, y la entrada a la red la identifica como verdadera, pudiendo acceder a la información dentro de la red.
Otra forma de suplantación consiste en instalar puntos de acceso ilegítimos u/o hostiles (Rogue Access Points) para engañar a usuarios autorizados de la red para que se conecten a este AP en lugar de la red a la que pertenecen.

Modificación

Tal como el nombre lo dice, el atacante borra, manipula, añade o reordena mensajes transmitidos.

3.3.9.1 Denegación de Servicio

Éste método de ataque consiste en que el atacante de la red se ocupa de generar interferencias de variados tipos hasta que se produzcan tantos errores en la transmisión que la velocidad caiga abruptamente o que la red cese sus operaciones. Al ser ataques de corta duración es muy difícil defenderse de ellos ya que solo es posible detectarlos en el momento en que actúan.

3.3.9.2 Ataque de Hombre en Medio o Reactuación (Man-in-the-middle)

Es un ataque en el que el enemigo adquiere la capacidad de leer, insertar y modificar a voluntad, los mensajes entre dos partes sin que ninguna de ellas conozca que el enlace entre ellos ha sido violado. El atacante debe ser capaz de observar e interceptar mensajes entre las dos víctimas. Esto provoca una manipulación externa de la información así como un ataque adicional a nivel de intercepción de la comunicación y denegación de servicio.

3.3.9.3 ARP Poisoning

Suplantación de identidad por falsificación de tabla ARP (Protocolo de resolución de direcciones). El ataque consiste en mandar un paquete del tipo "REPLY ARP" en el que otorgamos a una IP una MAC (Media Acces Control o Control de Acceso al Medio) distinta de la real. La mayoría de los sistemas operativos no implementan estados en el protocolo ARP y por tanto aceptan el REPLY aún sin haber realizado ninguna petición.

3.3.9.4 WEP key-cracking

WEP (Wired Equivalent Privacy) es el sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes Wireless que permite cifrar la información que se transmite. Está basado en el algoritmo de cifrado RC4, y utiliza claves de 64 bits (40 bits más 24 bits del vector de iniciación *IV)* o de 128 bits (104 bits más 24 bits del IV).
Para atacar una red inalámbrica se utilizan los denominados packet sniffers y los WEP crackers. Para llevar a cabo este ataque, se captura una cantidad de paquetes suficiente, lo cual será determinado por el número de bits de cifrado, mediante la utilización de un packet snifer y luego mediante un WEP cracker o key cracker se trata de vulnerar el cifrado de la red. Un key cracker es un programa basado generalmente en ingeniería inversa que procesa los paquetes capturados para descifrar la clave WEP. Vulnerar una red para obtener una llave más larga requiere la interceptación de más paquetes, pero hay ataques activos que estimulan el tráfico necesario.

3.4 Mantener el Acceso a Sistemas Comprometidos

Una vez que el intruso ha logrado penetrar a un sistema, no repetir el mismo proceso infiltración cada vez que quiera entrar a ese mismo sistema. Por ello mantener le es conveniente crear una entrada que le facilite la reincidencia en un sistema y al mismo tiempo oculte su presencia.

3.4.1 Puertas Traseras

Las puertas traseras constituyen una vía de acceso no autorizado a un sistema informático, saltándose las medidas de protección previas e implantadas por los administradores.
En algunos casos estas puertas pueden tener su origen en una serie de servicios que se utilizan durante las fases de desarrollo de un sistema informático y que por error o descuido, se mantienen en la versión final distribuida a los clientes.

3.4.2 Caballos de Troya

Son programas aparentemente inofensivos, con una determinada función o utilidad, pero que contienen un código oculto para ejecutar acciones no esperadas por el usuario.
Se tratan de programas nocivos que pueden sustraer la información confidencial de un equipo infectado, mientras se hacen pasar por programas o servicios inofensivos.

3.4.3 Rootkits

Los rootkits son un tipo de troyano que ocultan las puertas traseras que faciliten el acceso y control del sistema infectado con los máximos privilegios posibles (root)
El término viene de Unix, donde la cuenta del administrador se denomina "root", mientras que los conjuntos de herramienta de software reciben el nombre de "kits".
Se distinguen tres tipos de rootkits:

Rootkits binarios: reemplazan a una herramienta del administrador del sistema, sustituyendo el fichero binario original por otro modificado que incluye nuevas utilidades.

Rootkits de kernel: modifican el núcleo (kernel) del sistema operativo en el equipo infectado. De este modo consiguen manipular las respuestas del kernel para poder ocultar nuevos archivos, puertos abiertos, procesos, etc.

Rootkits de librerias: reemplazan las librerías del sistema, incluyendo distintas funciones que son utilizadas por otros programas cuando se ejecutan en el sistema infectado. De esta manera las funciones del troyano pueden afectar a distintos programas que se estén ejecutando en el sistema.

3.5 Eliminación de Evidencias

El trabajo de un intruso no solamente concluyen con haber saltado la seguridad , entrar al sistema y causar daños, ocultar su presencia y rastro también es una actividad en la que el atacante pondrá especial cuidado, pues entre mas tiempo permanezca sin ser detectado por los medios de seguridad, mayor será el daño que pueda causar.

Para ello el atacante intentara eliminar toda evidencia de sus actividades, definiéndose como evidencia, cualquier información que puede ser capturada y analizada para interpretar de la manera mas exacta posible en que ha consistido un incidente de seguridad, que daños ha provocado, cuales son sus consecuencias y quien pudo ser el responsable. Algunos métodos para ocultar o eliminar las evidencias son los siguientes.

3.5.1 Edición de bitácoras

Una bitácora o log de sistema, es un registro de las actividades que ocurren en un sistema de cómputo, la cual queda almacenada en un fichero. La información registrada incluye incidentes, funcionamientos anómalos, existencia de fallos en la configuración de las aplicaciones, desconexión de los dispositivos del sistema, cambios realizados en la configuración de los equipos, la utilización de recursos sensibles por parte de los usuarios del sistema, etc.

Más aún, estos registros digitales pueden mostrar actividades poco habituales en ciertos usuarios, como: intentos de acceder a la cuenta del super usuario, violar mecanismos de seguridad o indagar en lugares del sistema a los que no están autorizados para ingresar.

Los logs son una herramienta útil para mantener la seguridad del sistema pero también presentan una serie de características que entorpecen su uso:

- Redundancia de información.
Al registrar cada acción ocurrida, muchas veces se repite la misma información una y otra vez, aumentando el tamaño del log sin aportar información relevante.

-No hay correlación en los eventos reportados
No todos los analizadores de logs cuentan con una función que permita relacionar los una serie de eventos registrados con algún tipo de patrón u información que permita identificar claramente cuando el sistema esta siendo blanco de un ataque a su seguridad.
Este proceso de relación, se convierte en un trabajo tedioso que se complica mas cuando los usuarios no saben interpretar la información registrada en el log.

-Poca seguridad en el control de registros
El sistema guarda la información de la bitácora en ficheros que pueden ser leídos y modificados por otras aplicaciones. Muchas veces, el acceso a estos ficheros no esta restringido ni vigilado, por lo que son blanco fácil de ataques, siendo copiados, borrados o modificados.
Este ultimo punto es muy sensible, incluso cuando la bitácora puede registrar cuando alguien modifica el contenido, no puede indicar que fue información fue modificada, provocando que la información contenida en el log, ya no sea confiable.

3.5.2 Ocultar Información

En el contexto de la seguridad informática, ocultar la información puede ser un acto que tiene por propósito reforzar la seguridad de un sistema informáticos o bien una táctica usada por el atacante para pasar a través de los medios de seguridad sin ser detectado.

Existen métodos para ocultar la información en un medio digital, tales como las firmas digitales (fingerprinting), y las marcas de agua digitales (watermarking), las cuales a su vez están basadas en la estenografía.

3.5.3 Esteganografía

La esteganografía es una disciplina que trata sobre técnicas que permiten la ocultación de mensajes u objetos, dentro de otros, llamados portadores, de modo que no se perciba su existencia.
Es un error común confundir la esteganografía con la criptografía, o bien pensar que la primera es una rama de la segunda. Ellas tienen objetivos distintos, aunque se complementan perfectamente para incrementar el nivel de seguridad en la mensajería encubierta. Con la criptografía (rama más común y conocida) se intenta cifrar o codificar un mensaje de modo tal que se haga ininteligible si no se posee el decodificador adecuado, pero la existencia del mensaje es conocida; en tanto que la esteganografía intenta ocultar el hecho mismo del envío, escondiendo el mensaje dentro de un portador de apariencia normal e inocua, y no necesariamente el mensaje oculto estará cifrado.

En la esteganografía digital tanto el mensaje como el portador es, en términos generales, un objeto software cualquiera. Aunque los medios portadores preferidos (por sus características) son archivos multimedia (imágenes, audio y vídeo).

Los mensajes ocultos muchas veces son cifrados (criptografía) previamente de alguna manera, lo cual le otorga un nivel de seguridad extra a la esteganografía: el sujeto receptor no sólo deberá conocer la existencia del mensaje, conocer el portador y la técnica (o clave) utilizada para esconderlo; sino que también deberá contar con el descifrador adecuado.

3.5.4 Nuevos métodos

El watermarking o marca de agua digital es una técnica de ocultación de información que forma parte de las conocidas como esteganográficas. Su objetivo principal es poner de manifiesto el uso ilícito de un cierto servicio digital por parte de un usuario no autorizado.

Concretamente, esta técnica consiste en insertar un mensaje (oculto o no) en el interior de un objeto digital, como podrían ser imágenes, audio, vídeo, texto, software, etc. Dicho mensaje es un grupo de bits que contiene información sobre el autor o propietario intelectual del objeto digital tratado (copyright).

A una técnica de watermarking se le suele exigir que sea:

Imperceptible: Que sea invisible al observador

Que no degrade el objeto: Esto es que no altere el contenido del objeto ni la forma en que es percibido.

Robusta: La eliminación o reducción de la marca debe ser difícil o idealmente imposible sin degradar la calidad del objeto digital. Así mismo debe soportar procesos habituales de transformación (compresión, filtrado, conversión de formato, distorsión geométrica,...)

No debe ser ambigua: La marca debe identificar inequívocamente al propietario intelectual de tal forma que pueda reclamar su pertenencia.
Pese a estas premisas también existen marcas de agua que son perceptibles y que degradan el objeto, como por ejemplo, las marcas de agua superpuestas a imágenes indicando la propiedad de las mismas.

Existen tres tipos de ataques que pueden realizarse contra el watermarking:

Sustracción: es cuando se logra detectar y extraer el watermarking dejando la propiedad vulnerable.

Deformación: si el watermarking no puede ser localizado o separado, el atacante esta dispuesto a aceptar una degradación en la calidad del objeto digital, por lo que puede aplicar transformaciones que distorsionen el objeto y por extensión el watermarking que pueda contener.

Adición: es cuando se agrega al objeto un watermark propio, de modo que no se puede demostrar que el anterior watermark preceda a la nueva marca impuesta.

Capitulo IV

Políticas de seguridad informática de la organización

4.1 Políticas de Seguridad Informática

Las políticas son una serie de instrucciones documentadas que indican la forma en que se llevan a cabo determinados procesos dentro de una organización, también describen cómo se debe tratar un determinado problema o situación.

Este documento está dirigido principalmente al personal interno de la organización, aunque hay casos en que también personas externas quedan sujetas al alcance de las políticas.

Las políticas pueden considerarse como un conjunto de leyes obligatorias propias de una organización, y son dirigidas a un público mayor que las normas pues las políticas proporcionan las instrucciones generales, mientras que las normas indican requisitos técnicos específicos. Las normas, por ejemplo, definirían la cantidad de bits de la llave secreta que se requieren en un algoritmo de cifrado. Por otro lado, las políticas simplemente definirían la necesidad de utilizar un proceso de cifrado autorizado cuando se envíe información confidencial a través de redes públicas, tales como Internet.

Entrando al tema de seguridad informática, una política de seguridad es un conjunto de reglas y prácticas que regulan la manera en que se deben dirigir, proteger y distribuir los recursos en una organización para llevar a cabo los objetivos de seguridad informática de la misma.

4.1.1 Objetivo de una política de seguridad

El objetivo de una política de seguridad informática es la de implantar una serie de leyes, normas, estándares y prácticas que garanticen la seguridad, confidencialidad y disponibilidad de la información, y a su vez puedan ser entendidas y ejecutadas por todos aquellos miembros de la organización a las que van dirigidos.

4.1.2 Misión, visión y objetivos de la organización

La misión, visión y objetivos varían mucho de una organización a otra, esto es normal si se considera que una organización es diferente de otra en sus actividades y en el conjunto de elementos que la conforman (Elementos humanos, recursos materiales, infraestructura).
De manera rápida se definirán los conceptos de misión, visión y organización.

Misión.
Una misma organización puede tener varias misiones, que son las actividades objetivas y concretas que realiza. Las misiones también Pretenden cubrir las necesidades de la organización.
La misión es influenciada en momentos concretos por algunos elementos como: la historia de la organización, las preferencias de la gerencia y/o de los propietarios, los factores externos o del entorno, los recursos disponibles, y sus capacidades distintivas

Visión.
Es la imagen idealizada de lo que se quiere crear. Tal idea debe estar bien definida, pues todas las actividades de la organización estarán enfocadas a alcanzar esta visión.

Objetivos.
Son actividades específicas enfocadas a cumplir metas reales, alcanzables y accesibles. Se puede decir que un objetivo es el resultado que se espera logrra al final de cada operación.
Así, se vuelve importante considerar la misión, la visión y el objetivo de ser de la empresa, a fin de realizar un estudio que con base en éstas permita identificar el conjunto de políticas de seguridad informática que garantice la seguridad, confidencialidad y disponibilidad de la información.

4.1.3 Principios fundamentales de las políticas de seguridad

Son las ideas principales a partir de las cuales son diseñadas las políticas de seguridad.
Los principios fundamentales son: responsabilidad individual, autorización, mínimo privilegio, separación de obligaciones, auditoría y redundancia.

4.1.3.1 Responsabilidad individual

Este principio dice que cada elemento humano dentro de la organización es responsable de cada uno de sus actos, aun si tiene o no conciencia de las consecuencias.

4.1.3.2 Autorización

Son las reglas explícitas acerca de quién y de qué manera puede utilizar los recursos.

4.1.3.3 Mínimo privilegio

Este principio indica que cada miembro debe estar autorizado a utilizar únicamente los recursos necesarios para llevar a cabo su trabajo. Además de ser una medida de seguridad, también facilita el soporte y mantenimiento de los sistemas.

4.1.3.4 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. Este principio junto con el de mínimo privilegio reducen la posibilidad de ataques a la seguridad, pues los usuarios sólo pueden hacer uso de los recursos relacionados con sus actividades, además de que facilita el monitoreo y vigilancia de usuarios, permitiendo registrar y examinar sus acciones.

4.1.3.5 Auditoría

Todas las actividades, sus resultados, gente involucrada en ellos y los recursos requeridos, deben ser monitoreados desde el inicio y hasta después de ser terminado el proceso.
Además es importante considerar que una auditoría informática busca verificar que las actividades que se realizan así como las herramientas instaladas y su configuración son acordes al esquema de seguridad informática realizado y si éste es conveniente a la seguridad requerida por la empresa.

4.1.3.6 Redundancia

Trata entre otos aspectos sobre las copias de seguridad de la información, las cuales deben ser creadas múltiples veces en lapsos de tiempos frecuentes y almacenados en lugares distintos.
Sin embargo, la redundancia como su nombre lo indica, busca "duplicar" y en este sentido se puede decir que a través de los respaldos se duplica información, y lo mismo se puede realizar en diferentes aspectos, como por ejemplo: en cuanto a energía eléctrica, una planta de luz para garantizar que opere en casos de emergencia, servidores de datos que entren en operación cuando el primario sufra una avería, etcétera, de manera tal que la redundancia se considera en aquellos casos o servicios que se vuelven imprescindibles para la empresa y que no pueden suprimirse pase lo que pase.

4.1.4 Políticas para la confidencialidad

Desde el primer capítulo de esta investigación, se ha mencionado la necesidad de mantener el control sobre quién puede tener acceso a la información (ya sea a los documentos escritos o a los medios electrónicos) pues no siempre queremos que la información esté disponible para todo aquel que quiera obtenerla.

Por ello existen las políticas de confidencialidad, encargadas de establecer la relación entre la clasificación del documento y el cargo (nivel jerárquico dentro de la organización) que una persona requiere para poder acceder a tal información.

4.1.5 Políticas para la integridad

La política de integridad está orientada principalmente a preservar la integridad antes que la confidencialidad, esto se ha dado principalmente porque en muchas de las aplicaciones comerciales del mundo real es más importante mantener la integridad de los datos pues se usan para la aplicación de actividades automatizadas aún cuando en otros ambientes no es así, como en los ámbitos gubernamental o militar.

4.1.6 Modelos de Seguridad: abstracto, concreto, de control de acceso y de flujo de información

Un modelo de seguridad es la presentación formal de una política de seguridad ejecutada por el sistema. El modelo debe identificar el conjunto de reglas y prácticas que regulan cómo un sistema maneja, protege y distribuye la información.
Los modelos de seguridad pueden ser de dos tipo, abstracto y concreto.

Modelo Abstracto
Se ocupa de las entidades abstractas como sujetos y objetos.

Modelo Concreto

Traduce las entidades abstractas a entidades de un sistema real como procesos y archivos.
También pueden clasificarse como modelos de control de acceso y modelos de flujo de información.

Modelos de control de acceso

Identifican las reglas necesarias para que un sistema lleve a cabo el proceso que asegura que todo acceso a los recursos, sea un acceso autorizado, en otras palabras, se enfoca a la protección, administración y monitoreo de los procedimientos de acceso a la información. Estos modelos refuerzan el principio fundamental de seguridad de autorización, ya que éste protege tanto a la confidencialidad como a la integridad.

Modelos de flujo de información

Una meta de las políticas de seguridad es proteger la información. Los modelos de control de acceso se aproximan a dicha meta indirectamente, sin relacionarse con la información pero sí con objetos (tales como archivos) que contienen información. Estos modelos se enfocan a proteger los objetos con los que se trabajan en el sistema una vez que se han superado los procesos de control de acceso.

4.1.7 Desarrollo de políticas orientadas a servicios de seguridad

Las políticas de seguridad son un conjunto de normas y procedimientos que tienen por objetivo garantizar la seguridad en cada proceso en los que estén involucrados. Esto es aplicable a todos los procesos llevados a cabo en una organización, incluso los servicios de seguridad (Confidencialidad, autenticación, integridad, no repudio, control de acceso, disponibilidad) son diseñados con base en estos documentos.

4.1.8 Publicación y Difusión de las Políticas de Seguridad

Como todos los documentos creados por una organización, se debe decidir correctamente hacia qué grupos van dirigidas las políticas de seguridad, por qué medios se van a dar a conocer, si se desea que otros grupos puedan conocer su contenido.
El objetivo principal de la publicación y difusión es que el grupo objetivo entienda en qué consisten las políticas y se cree conciencia sobre su importancia a través de pláticas y talleres para tal fin.

4.2 Procedimientos y Planes de Contingencia

Solo cuando una organización toma conciencia de lo importante que es la seguridad de sus recursos incluyendo sus tecnologías de la información, es cuando empieza a diseñar y establecer medidas de seguridad que tienen por objetivo protegerla de diversas situaciones perjudiciales. Aunque prevenir éstos desastres es de vital importancia, tampoco se puede descuidar la casi inevitable eventualidad de que sucedan, para ello también se necesita formular y establecer una serie de procedimientos que permitan enfrentar los problemas y posteriormente restaurar las condiciones normales de operación del área afectada.

4.2.1 Procedimientos Preventivos

Contempla todos los procedimientos antes de que se materialice una amenaza, su finalidad es evitar dicha materialización.
Los procedimientos preventivos pueden variar dependiendo del tipo de actividades que realiza la organización, los recursos que tiene disponibles, que es lo que quiere proteger, las instalaciones en que labore y la tecnología que use.

Las actividades que se realizan en este punto son las siguientes:

–Copias de seguridad de las bases de datos y otros tipos de documentos con información indispensable para la organización

–Instalación de dispositivos de seguridad tales como cerraduras, alarmas, puertas electrónicas, cámaras de seguridad, software de protección para los equipos de cómputo, entre otros.

–Inspeccionar y llevar un registro constante del funcionamiento y estado de los recursos informáticos, la infraestructura y las condiciones del edificio.
–Instauración de servicios de seguridad, como líneas telefónicas de emergencia, extintores, construcción de rutas de emergencia (Entrada y salida), plantas eléctricas de emergencia, etc.

–Establecer un centro de servicio alternativo que cuente con los recursos necesarios para continuar las operaciones de la organización hasta el momento en que el centro de trabajo normal pueda ser usado en condiciones normales.

–Capacitación del personal en el uso adecuado de las tecnologías informáticas, en le ejecución correcta de sus labores y en la ejecución de los procedimientos de emergencia.

4.2.2 Procedimientos Correctivos

Los procedimientos correctivos son acciones enfocadas a contrarrestar en lo posible los daños producidos por un desastre, ataque u otra situación desfavorable y restaurar el funcionamiento normal del centro de operación afectado.
Al igual que los procedimientos preventivos, pueden variar según los recursos disponibles, pero también varía dependiendo el daño que se quiere contrarrestar pues no todas las emergencias requieren el uso de todos los procedimientos correctivos definidos por la organización.

4.2.3 Planes de Contingencia

El Plan de Contingencias es el instrumento de gestión para el manejo de las Tecnologías de la Información y las Comunicaciones.
Dicho plan contiene las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad de las operaciones de una institución en caso de desastres y situaciones catastróficas como incendios, terremotos, inundaciones, etc. pero también contiene las medidas para enfrentar los daños producidos por robo, sabotaje e incluso ataques terroristas .
El plan de contingencia es un requisito indispensable para que una respuesta de emergencia sea rápida y efectiva. Sin una previa planificación de contingencia se perderá mucho tiempo en los primeros días de una emergencia.

4.2.3.1 Objetivos y Características de un Plan de Contingencias

Los principales puntos que debe cumplir un plan de contingencia son:

–Reducir la probabilidad de que ocurra un desastre.
–Establecer los procedimientos necesarios para enfrentar y solucionar los eventos negativos que se presenten.
–Aminorar los efectos negativos de un desastre una vez ocurrido.
–Asegurar la continuidad de las operaciones de la organización.
–Reestablecer el funcionamiento normal de las áreas afectadas por el desastre.
–Dar a conocer el plan de contingencia al personal involucrado.

Para lograr tales objetivos, se debe diseñar e implantar una serie de procedimientos acorde a las necesidades y recursos disponibles que permitan responder de manera oportuna y precisa a todos los eventos negativos a los que se enfrente la organización.
Estos procedimientos deben estar basados en los resultados obtenidos de un análisis previo de riesgos y un establecimiento de prioridades.

4.2.3.2 Fases del Plan de Contingencia

Un plan de contingencias está dividido en fases, esto facilita el monitoreo del desempeño de dicho plan así como también ayuda a la detección de fallos e implementación de mejoras, pues cada fase está enfocado a una serie de aspectos específicos y cualquier posible cambio se aplicará a partir de la fase apropiada sin necesidad de modificar todo el plan completo.
Las fases se pueden dividir en análisis y diseño, desarrollo, pruebas y mantenimiento.

4.2.3.2.1 Análisis y Diseño

En esta fase se identifican las funciones de la organización que pueden considerarse como críticas y se les da un orden jerárquico de prioridad. Se define y se documentan las amenazas a las que están expuestas las funciones críticas y se analiza el impacto que tendrá un desastre en las funciones en caso de materializarse.

También se definen los niveles mínimos de servicio aceptable para cada problema planteado.

Se identifican las posibles alternativas de solución así como evaluar una relación de costo/beneficio para cada alternativa propuesta

4.2.3.2.2 Desarrollo de un plan de contingencias

En esta fase se creará la documentación del plan, cuyo contenido mínimo será:
–Objetivo del plan.
–Modo de ejecución.
–Tiempo de duración.
–Costes estimados.
–Recursos necesarios.

–Evento a partir del cual se pondrá en marcha el plan.
–Personas encargadas de llevar a cabo el plan y sus respectivas responsabilidades.

Es necesario que el plan sea validado por los responsables de las áreas involucradas. De igual manera hay que tener en cuenta las posibles consecuencias jurídicas que pudiesen derivarse de las actuaciones contempladas en él.

4.2.3.2.3 Pruebas y Mantenimiento

Consiste en realizar las pruebas pertinentes para intentar valorar el impacto real de un posible problema dentro de los escenarios establecidos en la etapa de diseño. Las pruebas no deben buscar comprobar si un plan funciona, mas bien debe enfocarse a buscar problemas y fallos en el plan para así poder corregirlos.

En la fase de mantenimiento se corrigen los errores encontrados durante las pruebas, pero también se revisa que los elementos preparados para poner en acción el plan de contingencia estén en condiciones óptimas para ser usados de un momento a otro para contrarrestar un desastre. En caso contrario, se les debe reparar o sustituir.

Es necesario documentar las pruebas para su aprobación por parte de las áreas implicadas

Algunas de las actividades realizadas en esta fase son:

–Verificar la disponibilidad de los colaboradores incluidos en la lista del plan de contingencia.

–Verificar los procedimientos que se emplearan para almacenar y recuperar los datos (backup).

–Comprobar el correcto funcionamiento del disco extraíble, y del software encargado de realizar dicho backup.

- Realizar simulacros, capacitando al personal en el uso de los procedimientos indicados en el plan de contingencia para la medición de su efectividad.

Capitulo V Análisis del riesgo

Conocer las vulnerabilidades e implementar procedimientos para combatirlos es importante, sin embargo hasta ahora no existe ninguna medida de seguridad que garantice completamente la protección contra las vulnerabilidades.
Incluso cuando se desea evitar la materialización de un desastre, también es necesario conocer los efectos que provocan en los activos de una Organización a corto y largo plazo.

El análisis de riesgo es el proceso encargado de identificar las amenazas y vulnerabilidades, conocer sus efectos e impacto que producen y conocer la probabilidad de que ocurran.
La información obtenida por este procedimiento permite identificar los controles de seguridad existentes, calcular vulnerabilidades y evaluar el efecto de las amenazas en cada área vulnerable.

5.1 Terminología básica

5.1.1 Activos

Es todo aquello con valor para una organización y que necesita protección, en el ámbito informático pueden ser datos, infraestructura, hardware, software, personal, información, servicios.

5.1.2 Riesgo

Un riesgo es la posibilidad de que se presente algún daño o pérdida, esto es, la posibilidad de que se materialice una amenaza.

5.1.3 Aceptación del riesgo

Es la decisión de recibir, reconocer, tolerar o admitir un riesgo. Esta decisión se toma una vez que se han estudiado los diferentes escenarios posibles para una misma amenaza y se han aplicado todos los

procedimientos posibles para contrarrestar sus efectos y probabilidad de que ocurra.

5.1.4 Análisis del riesgo

Uso sistemático de la información disponible para identificar las fuentes y para estimar la frecuencia de que determinados eventos no deseados pueden ocurrir y la magnitud de sus consecuencias.

5.1.5 Manejo del riesgo

Proceso de identificación, control y minimización o eliminación de riesgos de seguridad que pueden afectar a los sistemas de información, por un costo aceptable.

5.1.6 Evaluación del riesgo

Comparación de los resultados de un análisis del riesgo con los criterios estándares del riesgo u otros criterios de decisión.

5.1.7 Impacto

Son las pérdidas resultantes de la actividad de una amenaza, las pérdidas son normalmente expresadas en una o más áreas de impacto – destrucción, denegación de servicio, revelación o modificación-.

5.1.8 Pérdida esperada

El impacto anticipado y negativo a los activos debido a una manifestación de la amenaza.

5.1.9 Vulnerabilidad

Una vulnerabilidad informática es un elemento de un sistema informático que puede ser aprovechado por un atacante para violar la seguridad, así mismo pueden causar daños por sí mismos sin tratarse de un ataque intencionado.

5.1.10 Amenaza

Una acción o situación potencial que tiene la posibilidad de causar daño.

5.1.11 Riesgo residual

Es el nivel de riesgo que queda después de la consideración de todas las medidas necesarias, los niveles de vulnerabilidad y las amenazas relacionadas. Éste debe ser aceptado como es o reducirse a un punto donde pueda ser aceptado.

5.1.12 Controles

Protocolos y mecanismos de protección que permiten el cumplimiento de las políticas de seguridad de la organización. Un mismo control puede ser implementado para una o varias políticas de seguridad, lo que indica que la relación no es forzosamente de uno a uno.

5.2 Análisis cuantitativo

El análisis cuantitativo es una técnica de análisis que busca entender el comportamiento de las cosas por medio de modelos estadísticos y técnicas matemáticas para ello se encarga de asignar un valor numérico a las variables, e intenta replicar la realidad matemáticamente.
Un modelo cuantitativo habitual es aquel en el que las consecuencias de la materialización de amenazas se asocian a un determinado nivel de impacto en función de la estimación del coste económico que suponen para la organización
En resumen, el análisis de riesgo cuantitativo se ocupa específicamente de la revisión cuantitativa de los riesgos que pueden presentarse en los distintos tipos de industrias, determinando numéricamente la frecuencia de ocurrencia de una amenaza, el valor monetario del activo, el impacto económico y el daño producido.

5.3 Análisis cualitativo

Las métricas asociadas con el impacto causado por la materialización de las amenazas se valoran en términos subjetivos(Impacto Muy Alto, Alto, Medio, Bajo o Muy Bajo). Las consecuencias de la materialización de amenazas se asocian a un determinado nivel de impacto en función de multitud de factores
(Pérdidas económicas efectivas, pérdida de conocimiento, pérdida de competitividad, interrupción de negocio, pérdida de imagen, etc)

5.4 Pasos del análisis de riesgo

El proceso de análisis de riesgo consiste en ocho pasos interrelacionados:
1-Identificación y evaluación de activo
2-Identificar las amenazas correspondientes
3-Identificar las vulnerabilidades
4-Determinar el impacto de la ocurrencia de una amenaza
5-Determinar los controles en el lugar
6-Determinar los riesgos residuales (Conclusiones)
7-Identificar los controles adicionales (Recomendaciones)
8-Preparar el informe del análisis de riesgo

5.4.1 Identificación y evaluación de los activos

El primer paso en la evaluación de riesgo es identificar y asignar un valor a los activos que necesitan protección.
El valor de los activos es un factor significante en la decisión para realizar cambios operacionales o para incrementar la protección de los activos. El valor del activo se basa en su costo, sensibilidad, misión crítica, o la combinación de estas propiedades.
El valor del activo se usará para determinar la magnitud de la pérdida cuando la amenaza ocurra.

5.4.2 Identificación de amenazas

Después de identificar los activos que requieren protección, las amenazas a éstos deben identificarse y examinarse para determinar cuál sería la pérdida si dichas amenazas se presentan. Este paso envuelve la identificación y la descripción de las amenazas correspondientes al sistema que está siendo utilizado y se estima qué tan seguido se puede presentar.

5.4.3 Identificación de vulnerabilidades

El nivel de riesgo se determina analizando la relación entre las amenazas y las vulnerabilidades. Un riesgo existe cuando una amenaza tiene una vulnerabilidad correspondiente, aunque hay áreas de alta vulnerabilidad que no tienen consecuencias si no presentan amenazas.

5.4.4 Impacto de la ocurrencia de una amenaza

Cuando la explotación de una amenaza ocurre, los activos sufren cierto impacto. Las pérdidas son catalogadas en áreas de impacto llamadas:

Revelación: Cuando la información es procesada y se pierde la confidencialidad

Modificación: El efecto de la manifestación de una amenaza cambia el estado original del activo.

Destrucción: El activo se pierde completamente.

Denegación de servicio: Pérdida temporal de los servicios.

5.4.5 Controles en el lugar

La identificación de los controles es parte de la recolección de datos en cualquier proceso de análisis de riesgo. Existen dos tipos principales de controles:

1.- Controles requeridos: Todos los controles de esta categoría pueden ser definidos con base en una o mas reglas escritas. La clasificación de los datos almacenados y procesados en un sistema o red y su modo de operación determinan las reglas a aplicar, y éstas indican cuáles son los controles requeridos.

2.-Controles discrecionales: Este tipo de controles es elegido por los administradores. En muchos casos los controles requeridos no reducen el nivel de vulnerabilidad a un nivel aceptable, por lo que se deben elegir e implementar este tipo de controles para ajustar el nivel de vulnerabilidad a un nivel aceptable.

5.4.6 Riesgos residuales

Siempre existirá un riesgo residual por lo tanto, debe determinarse cuando el riesgo residual, es aceptable o no. El riesgo residual toma la forma de las conclusiones alcanzadas en el proceso de evaluación. Las conclusiones deben identificar:

–Las áreas que tienen alta vulnerabilidad junto con la probabilidad de ocurrencia de la amenaza.

–

–Todos los controles que no están dentro del lugar.

El resultado de estos pasos permite comenzar la selección necesaria de controles adicionales.

5.4.7 Identificación de los controles adicionales

Una vez que el riesgo residual haya sido determinado, el siguiente paso es identificar la forma mas efectiva y menos costosa para reducir el riesgo a un nivel aceptable. Un intercambio operacional –el cual puede tomar la forma

de costo, conveniencia, tiempo, o una mezcla de los anteriores- debe realizarse al mismo tiempo que los controles adicionales son implementados. Las recomendaciones son:

–Controles requeridos: Controles requeridos u obligatorios que no se encuentran en el lugar son la primera recomendación.

–Controles discrecionales: La segunda recomendación generalmente identifica los controles discrecionales necesarios para reducir el nivel de riesgo.

5.4.8 Preparación de un informe del análisis del riesgo.

El proceso de análisis de riesgo ayuda a identificar los activos de información en riesgo y añade un valor a los riesgos, adicionalmente identifica las medidas protectoras y minimiza los efectos del riesgo y asigna un costo a cada control. El proceso de análisis del riesgo también determina si los controles son efectivos. Cuando el análisis está completo, debe prepararse un informe de la evaluación de riesgo.

.

Los detalles técnicos del reporte deben incluir como mínimo:

–Amenazas correspondientes y su frecuencia.

–El ambiente usado.

–Conexión del sistema.

–Nivel o niveles de sensibilidad e los datos

–Riesgo residual, expresado en una base individual de vulnerabilidad.

–Cálculos detallados de la expectativa de pérdida anual.

El análisis del riesgo de seguridad es fundamental en la seguridad de cualquier organización ya que es un método formal para investigar los riesgos de un sistema informático y recomendar las medidas apropiadas que deben adoptase para controlar estos riesgos. Es esencial asegurarse que los controles y el gasto que implican sean completamente proporcionales a los riesgos a los cuales se expone la organización.

5.5 Análisis costo-beneficio

El análisis costo/beneficio es una importante técnica que nos ayuda en la toma de decisiones, pues brinda información necesaria para determinar si una actividad es rentable, o por el contrario representa un impractico desperdicio de recursos.

Este tipo de análisis consiste básicamente en la comparación de los costos invertidos en un proyecto con los beneficios que se planean obtener de su realización.

Primero debe entenderse que los costos son tangibles, es decir, se pueden medir en alguna unidad económica, mientras que los beneficios pueden ser intangibles, es decir, pueden darse en forma objetiva o subjetiva.

Dependiendo del enfoque que use una organización, el análisis costo beneficio puede ser un proceso independiente del análisis de riesgo, pero es necesario que todos los controles instaurados sean evaluados en términos de funcionalidad y viabilidad.

En el campo de seguridad informática, tanto para el análisis de riesgo como para el análisis costo beneficio deben tomarse en cuenta tres costos o valores fundamentales:

- Costo del sistema informático (Ca): valor de los recursos y la información a proteger.

−Costos de los medios necesarios (Cr): los medios y el costo respectivo que un criptoanalista requiere para romper las medidas de seguridad establecidas en el sistema.

−Costo de las medidas de seguridad necesarias (Cs): medidas y su costo para salvaguardar los bienes informáticos.

Para que la política de seguridad del sistema sea lógica debe cumplirse la siguiente relación:
Cr> Ca >Cs

El que Cr sea mayor que Ca significa que el ataque al sistema debe ser mas costoso que el valor del sistema. Por lo que los beneficios obtenidos al romper las medidas de seguridad no compensan el costo de desarrollar el ataque.
El que Ca sea mayor que Cs significa que no deben costar mas las medidas de seguridad que la información protegida. Si esto ocurre, resultaría conveniente no proteger el sistema y volver a obtener la información en caso de pérdida.

Capitulo VI Ética informática

6.1 Concepto de Ética Informática

La ética es la teoría o ciencia del comportamiento moral de los hombres en sociedad, es decir, es la ciencia de una forma específica de conducta humana que permite calificar los actos humanos como buenos o malos
La tecnología informática plantea nuevas situaciones y nuevos problemas y gran parte de estas nuevas situaciones y problemas son de una naturaleza ética; obviamente existen intentos de resolver estos problemas aplicando las actuales reglas y soluciones éticas de carácter general. 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 ética informática tiene como punto de partida el hecho de que las computadoras suponen problemas éticos particulares y por tanto distintos a otras tecnologías. En las actividades profesionales relacionadas con las tecnologías informáticas 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 esa dirección.

La ética informática puede perseguir varios objetivos:

- Descubrir y articular dilemas éticos claves en informática.
- Determinar en qué medida son agravados, transformados o creados por la tecnología 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.

- Utilizar la teoría ética para clarificar los dilemas éticos y detectar errores en el razonamiento ético.
- Proponer un marco conceptual adecuado para entender los dilemas éticos que origina la informática y además establecer una guía cuando no existe reglamentación de dar uso a Internet.

Toda actividad humana debe ser regida por un código de ética y la informática no es la excepción

6.2 Códigos Deontológicos en Informática

El código deontológico es un documento que recoge un conjunto de criterios, normas y valores que formulan y asumen quienes llevan a cabo una actividad profesional. Los códigos deontológicos se ocupan de los aspectos más sustanciales y fundamentales del ejercicio de la profesión que regulan.

Las normas dictadas en el código deontológico son previamente pactadas y aprobadas de manera común y unánime por todos los miembros de la profesión para las que se elaboran. Son, por tanto, pautas de conducta a seguir que tienen como objetivo cumplir con un adecuado trabajo y ayudar a que el conjunto de la sociedad que solicita los servicios de la profesión obtenga plena satisfacción ante la buena ejecución de la labor.

Las asociaciones de profesionales de informática y algunas empresas relacionadas con la informática han desarrollado códigos de conducta profesional. Estos códigos tienen distintas funciones:

- El que existan normas éticas para una profesión quiere decir que un profesional, en este caso un técnico, no es solo responsable de los aspectos técnicos del producto, sino también de las consecuencias económicas, sociológicas y culturales del mismo.
- Sirven también 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 suplemento a la ley y sirven de ayuda a los cuerpos legislativos, administrativos y judiciales.

-Sirven como concienciación 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 sus 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.

6.3 Contenidos de la Ética Informática

La ética informática es una disciplina relativamente nueva, por lo que aun no hay unanimidad en los contenidos referentes a esta área. Aun así es posible recopilar los temas y problemas que frecuentemente son tratados en la ética informática.

–Ética profesional general

Un primer capítulo de problemas de EI (Ética Informática) lo podemos englobar en el epígrafe "ética profesional general" porque hace referencia a problemas que son comunes a otras actividades ocupacionales. Por un lado están los criterios de moralidad personal, entendiendo como tales los

criterios, obligaciones y responsabilidades personales de los profesionales. Por otro lado están los problemas interiores a la empresa: relaciones empleador-empleado, lealtad organizacional, interés público, el comercializar productos similares a los de tu empleador, etc.

En este bloque 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 los equipos computacionales 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 fallos (*bugs),* etc..

-La utilización de la información

Un capítulo de problemas que aparece en esta área es el relativo 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 ojear 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 entre otros). 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**

Otro capítulo de problemas a los que la Ética informática quiere atender hace referencia al software como un bien que tiene características específicas. Los programas de computadora suponen 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 plantearnos la protección de software es qué 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 uno en la universidad o en la empresa, etc.

- Lo informático como instrumento de actos potencialmente dañinos

Uno de los temas con los que más se relaciona a las tecnologías informáticas con la Ética, y es referente a la idea de que las tecnologías informáticas pueden ser usadas como medio para causar 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 introducciones de virus y gusanos. En el fondo se trata no solo 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

En algunos casos se incluyen en la Ética Informática unas consideraciones sobre las visiones antropomórficas de las computadoras como máquinas pensantes o como productores 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 caso concreto es el planteado por los sistemas de decisión informatizados (SDI), que son ya 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.

- 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 no por un afán tecnofóbico o de buscar solo lo negativo en la técnica, sino por 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, el ser humano sirve a la técnica y no ésta a las necesidades humanas.

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 ultracompetitividad, 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.

También se puede mencionar aquí que los informáticos han sido unos trabajadores clave en la investigación, desarrollo y producción de la tecnología militar. Desde la Ética Informática se podría concienciar a los informáticos sobre la eticidad de desarrollar modos "superinteligentes" para idear sufrimiento y destrucción humanos y de alimentar mercados militares en países en desarrollo por parte de los que poseen tecnología. 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.

6.4 Actualidad de la Ética Informática

La proliferación de estudios existentes sobre la Ética Informática está teniendo repercusiones en la formación de los informáticos. Cada vez se van incorporando cursos de Ética a los programas de estudios Informáticos impartidos por las universidades. De acuerdo al Centro en línea de Ética para Ingeniería y Ciencias (Online Ethics Center for Engineering and Sciences) se debe de inducir a los estudiantes a identificar su propios valores, sensibilizarlos a identificar problemas morales y dilemas, ayudarlos a identificar y entender los alcances del problema, inducirlos a considerar acciones alternativas, prever las consecuencias, trazar un camino moral, escoger una acción que mejor promueva la moralidad e inducirlos a reflexionar sobre su decisión.

En el caso de Instituciones de habla hispana, ya se empieza a impartir de manera formal y seria, aun cuando muchos de los cursos de ética informática todavía no son adecuados a los objetivos reales que se planean alcanzar.

Existen una serie de problemas a los cuales la Ética Informática se sigue enfrentando:

–La bibliografía relacionada con Ética Informática no esta suficientemente acentuada en las teorías éticas, ya sea clásicas o contemporáneas. Esto da como resultado afirmaciones vagas y conceptos que no muestran su totalidad la importante relación entre la Informática y la Ética .

–Mucha de la literatura existente 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.

– La literatura existente es más sociológica que ética; es menos 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 Ética Informática no es solamente proponer análisis sobre "sociología de la informática" o sobre la evaluación social de las tecnologías, 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.

6.5 Psicología del Intruso

El intruso en un sistema informático es una persona cuyos intereses difieren de los objetivos de la organización afectada. Aun cuando el intruso busca obtener los mismos recursos informáticos, el uso final que les da puede ser muy diferente.

Aunque es imposible determinar qué clase de persona es la que está atacando un sistema, en realidad es útil intentar saber las motivaciones y manera de pensar del intruso, pues es el primer paso para determinar qué

clase de acciones realizará para poder penetrar la seguridad impuesta y así tomar las medidas necesarias para evitar su entrada.
La complejidad de la mente humana no es un tema totalmente ajeno a la seguridad informática.

6.6 Códigos de Ética

El Contenido de Ética Informática es importante, por considerarlo como un instrumento que nos facilita reconocer los problemas y resolverlos de acuerdo a los objetivos buscados.
Los códigos de ética, tal como se conocen en el mundo de las empresas, son sistemas de reglas establecidos con el propósito general de guiar el comportamiento de los integrantes de la organización y de aquellos con los cuales ésta actúa habitualmente: clientes, proveedores y contratistas. No obstante la profesión de informática, es una actividad reconocida socialmente y así el futuro ingeniero en informática, debe estar preparado para que un juez o una empresa le solicite un dictamen o peritaje informático y es evidente que este tipo de informes, en la práctica, deben estar firmados por alguien con titulación superior, actuando con rectitud profesional, y obrando según ciencia y conciencia.

6.7 Casos de Estudio

El ataque a Habbo Hotel

Habbo hotel es una red social en línea dirigida principalmente a los usuarios adolescentes, operada por Sulake Corporation.
Habbo Hotel presta servicios de Chat en forma de habitaciones de hotel virtuales así como juegos, decoraciones virtuales y elementos para las páginas de usuario.
Cada usuario tiene un avatar personal llamado Habbo, con el que puede desplazarse por todas las habitaciones virtuales.

En el año del 2006, se presentaron varias quejas por parte de los usuarios sobre prácticas racistas por parte de los moderadores, en respuesta a esta situación, los usuarios de las comunidades en línea de YTMND, 4Chan, y EBaum's organizaron un ataque en conjunto a la comunidad Habbo Hotel.

El 12 de Julio del 2006 se realizó el ataque, que básicamente consistía en aprovechar las mismas características del sistema de navegación de Habbo Hotel para molestar a los demás usuarios.

Dichas prácticas consistían principalmente en:

–Bloquear el acceso a las habitaciones, bloqueando los accesos al colocar los avatares de usuarios en los pasillos, puertas y escaleras virtuales, aprovechando la característica del navegador de que un avatar no puede atravesar el avatar de otro usuario.

–Enviar constantemente mensajes SPAM en las conversaciones públicas, haciendo difícil una comunicación coherente entre los usuarios.

–Inyectar tráfico a servidor, al intentar usar los servicios simultáneamente, y permaneciendo en línea por muchas horas seguidas.
Después de varias horas de realizarse el ataque, el servidor de Habbo Hotel fue saturado, quedándose fuera de servicio por varias horas.
Para poder organizarse mejor, los atacantes se reconocían entre sí modificando la apariencia de su avatar, por la de un hombre de raza negra, una peluca estilo afro y un traje de oficinista.

Aunque el ataque del 12 de Julio es considerado como el "más importante", una serie de ataques se han efectuado desde entonces, aprovechando una vulnerabilidad descubierta durante esas fechas, que permite a los usuarios baneados acceder nuevamente a la comunidad al borrar los archivos temporales de Internet de la pc y los archivos de configuración de macromedia, permitiendo al usuario crear una nueva cuenta.

A partir de estos eventos, los moderadores encargados de la comunidad, han optado una serie de practicas para intentar controlar los abusos por parte de usuarios problemáticos, estas practicas incluyen:

–Reseteo de los foros donde se llevaron a cabo actividades relacionadas con los ataques.

–Deshabilitar los servicios de chat cada vez que sospechan de actividades abusivas.

–Suspensión de cuentas de usuarios de quien se sospecha su participación en estos ataques.

–Baneo inmediato de usuarios cuyos avatares sean similares a los usados por los atacantes.

–Prohibición de una determinada lista de palabras y frases para el uso en los nicks de usuario, dichas palabras y frases forman parte de bromas ofensivas que circulan en Internet. Algunos ejemplos de esta lista incluyen las palabras loli, 4chan, pbear, lulz, hatemachine, raid y partyVan.

Es difícil concluir si estas practicas han sido efectivas para combatir este tipo de ataques, pues hasta se siguen organizando los ataques, los cuales se han convertido en una forma de entretenimiento para los atacantes (todos ellos pertenecientes a comunidades exteriores a los de Habbo Hotel). El ataque efectuado en este caso de estudio, es difícil de controlar, pues no se requieren de grandes conocimientos de sistemas informáticos, pues

consiste mas en realizar una serie de actividades que resultan molestas a otros usuarios, lo que provoca que cualquier usuario pueda convertirse en un atacante, siendo un ejemplo de cómo el factor humano es potencialmente la amenaza mas peligrosa y difícil de controlar para un sistema informático.

Fuentes

http://en.wikipedia.org/wiki/Habbo Hotel
http://lurkmore.com/wiki/Habbo
http://www.encyclopediadramatica.com/Habbo Hotel
http://www.partyvan.info/index.php/Habbo Hotel

Conclusiones

Para finalizar, presento las conclusiones a las que llegué al realizar la presente investigación.

El desarrollo del documento web fue exitosamente concluido. La información relacionada a todos los temas marcados fue recopilada y ordenada de acuerdo a lo establecido por el temario propuesto y la aplicación web fue debidamente codificada y puesta en línea.

La seguridad de un sistema informático no es un raro lujo costoso, sino una necesidad importante que de ser posible debería tomarse en cuenta desde la planeación de un sistema.

Existen diversos métodos, procedimientos, criterios y tecnologías para proteger un equipo de cómputo, pero al final, el elemento mas importante en la Seguridad Informática, es el elemento humano. De la misma manera en que son los humanos los que reciben los beneficios de las tecnologías computacionales, también son los humanos los principales responsables de protegerlas y preservar su buen funcionamiento.

Incluso con el desarrollo de nuevas y mejores tecnologías de seguridad, los sistemas no son entidades concientes que puedan adaptarse a si mismos para trabajar más allá de sus especificaciones establecidas, con el paso del tiempo pueden llegar a ser superados por alguna amenaza contra la cual no están diseñados a afrontar.

La seguridad no es una responsabilidad que recaiga únicamente en los programadores o los administradores, sino de todos los que manipulan y tienen contacto con los equipos de cómputo.

La Seguridad Informática empieza por el ejercicio de buenas practicas por parte de los usuarios.

Los alumnos de la carrera de Ingeniería en Computación (Así como los de carreras afines) deben ser los primeros en tomar conciencia y adquirir los conocimientos necesarios sobre éste importante tema, pues ellos trabajarán con sistemas informáticos como parte de su labor profesional y en muchos casos no será como simples usuarios, sino como desarrolladores, analistas, administradores y otros puestos que requieren un mayor nivel de conocimientos y responsabilidad.

Como en toda materia de estudio, la Seguridad Informática debe estudiarse desde sus temas básicos, pues a partir de estos conocimientos es como se pueden comprender los tópicos mas avanzados del tema. Estos conocimientos elementales son la base sólida a partir de los cuales es posible mejorar la seguridad de un sistema y reducir la probabilidad de que sucedan eventos contraproducentes.

Mantenerse actualizado también es importante. Día a día nuevas tecnologías y tendencias en el campo de la informática van surgiendo, es bueno informarse de las novedades, principalmente en lo referente a la Seguridad Informática, pues los nuevos avances pueden ser elementos benéficos a considerar para mejorar el desempeño de un sistema de seguridad, de la misma manera que también pueden ser amenazas contra las cuales se debe prever una solución.

Si bien aquí finaliza esta tesis, los temas abarcados solo son una parte de lo extenso que es la totalidad del tema. Depende del lector seguir estudiando y adquirir mas conocimientos.

APÉNDICE
Herramientas de edición HTML

Una página web es un documento electrónico que se caracteriza por los hiperenlaces o vínculos que tiene con otros recursos como por ejemplo otra página web o una aplicación en línea.
Toda la estructura de una página web es construida principalmente por medio de un lenguaje de marcado que proporciona información extra de la presentación, estructura y apariencia del documento escrito. El lenguaje de marcas más utilizado para la construcción de páginas web es el HTML Hypertext Markup Language (Lenguaje de Marcas de H ipertexto).

Existen principalmente dos maneras de editar una página HTML:

- Escribiendo el código HTML, esto es, tecleando línea a línea todo el contenido de la página, lo cual requiere conocimiento del lenguaje HTML pero permite un mayor control sobre el contenido y diseño final.
- Modo diseño, esto es, que el desarrollador construya su página web usando una herramienta que le permita generar el código correspondiente al diseño indicado. Este tipo de herramientas facilitan la creación de páginas pues el usuario no necesita conocer el lenguaje HTML para diseñar una página web, presentando un interfaz gráfico que permite visualizar directamente el diseño como página web.

Este tipo de herramientas también es conocido con el acrónimo WYSIWYG What You See Is What You Get (Lo que ves es lo que tienes) porque lo que se ve al trabajar con ellos es lo que posteriormente se mostrará como resultado final en la página.

Análisis comparativo entre herramientas de diseño.

Todas las herramientas de diseño web comparten características comunes como la inserción de etiquetas HTML, estilos de texto, párrafos, enlaces, imágenes, tablas, formularios, soporte para javascript, inserción de archivos multimedia etc.

Por ello el criterio de selección de una herramienta puede enfocarse a otros aspectos entre los que destacan el soporte técnico, la interfaz, la facilidad de manejo, los requerimientos que pide para instalarse, e incluso considerar las desventajas que pudieran resultar inconvenientes para el proyecto.

Frontpage 2003.

Requerimientos:
PC con un procesador Intel Pentium 233-megahertz (MHz) o superior; recomendado a partir de Pentium II.

128 megabytes (MB) de RAM o mayor.
180 MB de espacio disponible en el disco rígido.
Microsoft Windows® 2000 con Service Pack 3 (SP3) o posterior; o Windows XP o posterior.
Monitor Super VGA (800 × 600) o una superior resolución de monitor

Es un editor HTML creado por Microsoft y forma parte del paquete de programas de Microsof Office. Actualmente está descontinuado y fue sustituido por SharePoint y Expression Web.

Frontpage está enfocado para las personas con poca experiencia de diseño web, por lo que sus menús e interfaces son mas fáciles de comprender que en otros editores, en tanto que sus capacidades son semejantes a las de otros como el crear mapas de imágenes, gestionar la arborescencia de las páginas del sitio, etc.

La mayor limitante de Frontpage es que los códigos que genera solo son funcionales para Internet Explorer, generando errores para otros exploradores como Firefox o Netscape lo que presenta un serio inconveniente si lo que se desea es dar a conocer la página a una audiencia más amplia.

GoLive

Requerimientos:

Procesador Intel Pentium a 800 Mhz o equivalente.

64 MB de Ram o mayor.

150MB de espacio libre en disco.

Windows 98/ME/2000/XP

GoLive es un editor html creado por Adobe, el cual tiene entre sus características más importantes la integración de recursos creados con otras aplicaciones de Adobe como Photoshop, Ilustrator, LiveMotion, etc.

GoLive también incluye la herramienta Adobe Web Workgroup Server que facilita la gestión de versiones, del archivo de proyecto y de los recursos compartidos del sitio, así como la administración del sitio y la gestión de permisos.

Con la adquisición de Macromedia por parte de Adobe, ahora Adobe es también dueña de su herramienta Dreamweaver, lo que ha llevado a disminuir su soporte a GoLive.

Dreamweaver MX 2004

Requerimientos:

Procesador Intel Pentium III de 800 MHz (o equivalente) y versiones posteriores.

Windows 2000, Windows XP.

256 MB de memoria RAM.

Pantalla de 16 bits de 1024 x 768.

650 MB de espacio en disco disponible.

Creado por Macromedia, permite trabajar con páginas creadas desde Fireworks manteniendo todas sus características e interactividad, también permite la inserción de elementos interactivos desde su biblioteca sin necesidad de codificar en Java script, también permite la integración con recursos de Flash CS3, hojas de estilo CSS y XML.

Dreamweaver también ofrece la ventaja de ser compatible con Adobe Device Central CS3 lo que permite generar contenido para dispositivos móviles.

Adicionalmente las herramientas visuales de Dreamweaver permiten trabajar al mismo tiempo el diseño visual y la edición de código, permitiendo al programador la opción de editar y depurar el código HTML para un mejor funcionamiento de la versión final de la página.

La herramienta elegida para desarrollar este proyecto, fue Dreamweaver. Su alta compatibilidad le permite importar distintos recursos creados con otras herramientas. Su interfaz gráfico proporciona un ahorro de tiempo en el proceso de diseño, al mismo tiempo que se trabaja en el código HTML para su optimización y mejor funcionamiento en términos de programación. Igualmente es la herramienta a la que actualmente Adobe está dando su apoyo, lo que supone futuras actualizaciones con nuevas opciones que expandirá la capacidad de Dreamweaver como herramienta de diseño, convirtiéndola en una opción a considerar para

Bibliografía y referencias electrónicas

Bibliografía

ANONYMOUS *Maximun Security* 4rd. Edition U.S.A. Sams Publishing, 2003.

DENNING, Dorohty, *Information Warfare and Security,* E.U.A. Adisson Wesley, 2000.

Debra S. Herrmann *Using the common criteria for ITsecurity evaluation,* Boca Raton, FL, USA, CRC Press, Inc. , 2002.

Carballar, José A. *WI-Fi Instalacion, Seguridad y Aplicaciones, Primera edición,* México, Alfaomega Grupo Editor, 2007.

Gómez Vieites, Álvaro, *Enciclopedia de la Seguridad Informática Primera edición,* México, Alfaomega Grupo Editor, 2007.

Zemáneck, Jakub, *Craking sin secretos, Ataque y defensa de softweare,* México, Alfaomega Grupo Editor, 2005.

López Barrientos, M. Jaquelina, *Fundamentos de seguridad informática,* México, UNAM, Facultad de Ingeniería, 2006.

John Chirillo Wiley *Hack Attacks Denied.A complete guide to Network Lockdown,* E.U.A Jhon Wiler & Sons Inc., 2001

Juan José Nombela, *Seguridad Informática,* España, International Thompson Publishing – Paraninfo 1997

Eric A. Fisch, *Secure Computers and Networks. Analysis, Design and Implementation,* E.U.A. Lybrary of Congress Cataloging.

Referencias electrónicas

http://www.jbex.net/seguridad-informatica

http://ciberhabitat.gob.mx/museo/cerquita/redes/seguridad/intro.htm

http://alerta-antivirus.red.es/seguridad/ver_pag.html?tema=S&articulo=4&pagina=1

http://www.dcc.uchile.cl/~cc51d/docs2001/c7-Riesgo_y_vulnerabilidad.pdf

http://www.geocities.com/v.iniestra/apuntes/redes/

http://www.e-ghost.deusto.es/docs/articulo.seguridad.pdf.

http://www.iec.csic.es/criptonomicon/basedatos.html

http://www.dcc.uchile.cl/~jpiquer/Internet/DNS/node2.html

http://multingles.net/docs/jmt/ataques.htm

http://www.rzw.com.ar/seguridad-informatica-429.html

http://www.rzw.com.ar/seguridad-informatica-2100.html

http://www.ucpr.edu.co/auditores/redes/TELE_CELULAR.htm

http://www.pcworld.com.mx/pcw_completo_NOTICIAS.asp?pcwid=2556

http://www.vsantivirus.com/23-08-07.htm

http://www.auditmypc.com/freescan/readingroom/port_scanning.asp
http://www.spitzner.net/audit.html

http://insecure.org/nmap/osdetect/

http://www.segu-info.com.ar/fisica/seguridadfisica.htm

http://www.isa.uniovi.es/docencia/redes/Apuntes/tema8.pdf

http://www.etcetera.com.mx/libro/tres/tres2.htm

http://www.microsoft.com/latam/athome/security/viruses/virus101.mspx

http://www.iec.csic.es/gonzalo/descargas/SeguridadWiFi.pdf

http://www.inf.utfsm.cl/~liuba/iing/trabajos/seguridad_wifi/index.html

http://www.infosecurityonline.org/newsletter/junio/hacking.htm

http://www.alcancelibre.org/article.php/20070403184255131

http://www.elhacker.net/InfoForenseWindows.htm

http://www.alfa-redi.org/rdi-articulo.shtml?x=1304

http://www.segu-info.com.ar/articulos/36-informatica-forense.htm

http://www.bsecure.com.mx/articulo-60-6531-374.html

http://seguridad.internet2.ulsa.mx/congresos/2003/cudi1/impor_bitacoras.pdf

http://www.realidadfutura.com/docu/proyecto_web/node212.html

http://www.segu-info.com.ar/criptologia/criptologia.htm

http://www.virusprot.com/Art28.html

http://www.rediris.es/pgp/firmaweb/

http://www.um.es/docencia/barzana/IAGP/MAGERIT.pdf

http://www.dwheeler.com/secure-programs/Secure-Programs-HOWTO/x641.html

http://www.iec.csic.es/criptonomicon/seguridad/servicio.html

http://www.itpro.cl/Seguridad/ISO27000/tabid/97/Default.aspx

http://seguridadit.blogspot.com/2006/01/norma-iso-17799-vs-iso-27001.html

http://sociedaddelainformacion.wordpress.com/category/seguridad/iso-27000/

http://www.infobaeprofesional.com/interior/home.html

http://www.coresecurity.com/

http://www.kwell.net/ioctave.htm

http://congreso.seguridad.unam.mx/eventos_anteriores/seguridad2004/memorias/ivan/html/img0.html