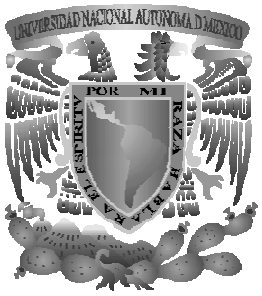


UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA ESCUELA NACIONAL PREPARATORIA No.5 “JOSÉ VASCONCELOS”

T E S I S

QUE PARA OBTENER EL TÍTULO DE
INGENIERO EN COMPUTACIÓN

P R E S E N T A N:

CASTILLO CORONA DULCE MÓNICA
FLORES LOZA MARIBEL

DIRECTORA DE TESIS
M. C. MARÍA JAQUELINA LÓPEZ BARRIENTOS

MÉXICO, D. F. 2008

El éxito no se logra sólo con cualidades especiales. Es sobre todo un trabajo de constancia, de método y de organización.

J.P. Sergent

DEDICO ESTE TRABAJO

A mis padres

Gerardo y Pilar, por sus regaños, consejos, apoyo y por la manera de enseñarme a luchar sin darme por vencida.

A mis hermanos

Gerardo, por estar ahí siempre que te necesite y decirme las palabras exactas en el momento preciso.

Tavo, por comprender mis estados de ánimo y el apoyo.

A mi esposo

Moisés Olea, por tu apoyo y comprensión durante la etapa más importante de nuestras vidas… sin ello no lo hubiéramos logrado.

A mis hijos

Ale y bebé, por que se que algún día apreciaran el esfuerzo con que realice este trabajo por que es por ustedes y para ustedes.

A mi amiga y compañera de Tesis

Maribel Flores por que sin ti no lo hubiera conseguido.

Dulce Mónica Castillo Corona

La constancia es el complemento indispensable de todas las demás virtudes humanas.

Giuseppe Manzini

DEDICO ESTE TRABAJO

A mis padres

Francisco y Juanita por todo su amor, por confiar en mí, por sus regaños y sus consejos, por apoyar y respetar mis decisiones.
¡ Son los mejores padres del mundo !

A mi esposo

Ing. Víctor Ocampo por tu cariño y comprensión en todos estos años juntos. Esto es por y para los dos.
¡ Te amo, corazón !

A mis hermanos

Israel y Adriana, por todas sus palabras de aliento.
¡ Los quiero !

A mi amiga y compañera de Tesis

Mónica Castillo por que con el esfuerzo conjunto se pudo lograr este trabajo.
¡ Gracias por tu paciencia !

Maribel Flores Loza

AGRADECEMOS

A nuestra directora

M. C. Ma. Jaquelina López Barrientos por su enorme paciencia y por compartir con nosotras todos sus conocimientos.
¡Gracias Maestra !

A nuestras amigas y compañeras

A Mayelly Reynoso, Susana Nájera, Paula Bourget y Jessica Martínez por la compañía, los consejos, los regaños y todas las conversaciones que tuvimos.
¡ Gracias por su Amistad !

A la Universidad Nacional Autónoma de México

Nuestra Alma Mater, por la oportunidad que nos brindó al elegirnos y ser parte de ella.
¡ Es un orgullo pertenecer a ti !

A la Facultad de Ingeniería:

Por la formación que nos brindó y por ser nuestra segunda casa en una de las etapas más bonita y significativa de nuestras vidas.

A todos nuestros profesores:

Por compartirnos sus conocimientos y brindarnos su apoyo en todo momento.

Dulce Mónica Castillo Corona
Maribel Flores Loza

ÍNDICE

OBJETIVO

Diseñar e implementar un Sistema de Gestión de Seguridad de la Información que garantice la integridad, confidencialidad y disponibilidad de la información

- Elaborar un estudio de las medidas de seguridad informáticas que tiene la Escuela Nacional Preparatoria plantel 5 “José Vasconcelos”,

- Identificar sus vulnerabilidades y riesgos

- Diseñar e implementar un perfil de protección y políticas de seguridad para la información de la institución.

INTRODUCCIÓN

La información es un bien al cual se le asocia un valor y por lo tanto está sujeta al riesgo. En la actualidad el valor de la información no sólo está asociado al impacto económico de las decisiones que se toman con base en ella, el costo de obtenerla y mantenerla; si no también a lo que esa información representa.

Es por esto que la preocupación por proteger esa información ha recibido considerable atención en los últimos tiempos, sin embargo, ni el valor de la información ni la necesidad de seguridad son asuntos nuevos.

Aún antes de la revolución industrial, la información ha sido un bien valioso. Desde que hay investigación sobre maquinaria, armas secretas, formulas químicas, secretos industriales y estrategias corporativas de mercadeo; aún en esos tiempos, la gente reconocía que cualquiera que controlara cierta información tenía un monopolio útil y por tanto estaba en posición de poder o ventaja competitiva sobre los que no tenían esa información.

El avance de los sistemas informáticos no ha introducido nuevos aspectos en cuanto al valor de la información, si no que ha transformado la naturaleza de los ya existentes. Históricamente, el papel moneda y los metales preciosos estuvieron resguardados en cajas fuertes y bóvedas de acero; hoy, la mayor parte del dinero se almacena en forma electrónica dentro de sistemas de cómputo, que son las nuevas cajas fuertes y bóvedas de seguridad. Por tanto, el enfoque actual es hacer los sistemas informáticos más seguros para proteger, por ejemplo, el dinero electrónico y la información sensible relativa a las organizaciones y a los individuos.

El aumentar de manera extraordinaria el número de sistemas de cómputo, la interacción directa con las computadoras y sus datos se volvió algo rutinario para un gran número de usuarios, hasta para los casuales. Este ambiente abierto, consecuentemente ha aumentado la dificultad para mantener la seguridad. Por otro lado, el hecho de que cada vez más personas cuentan con conocimientos suficientes para manipular sistemas de computo; y que además la información manejada en éstos tenga un valor suficiente como para tentar a algunas personas a tener acceso a ella de manera ilícita, ha originado una mayor preocupación por lograr un nivel satisfactorio de seguridad de los sistemas de cómputo.

En los inicios de los sistemas de cómputo, se crearon medidas para asegurar que la información y el equipo mismo estuvieran a salvo de cualquier deterioro. El constante avance de la tecnología ha dejado esas medidas preventivas obsoletas. Pero el incremento de redes interconectadas, los equipos de cómputo portátiles y la existencia de gente que tiene a su alcance estas herramientas y tiene algún conocimiento en cómputo; ha hecho que el perpetrar los sistemas de cómputo con finalidad de lucro o daño se haya vuelto común; especialmente para personas que

están familiarizadas con el ambiente de cómputo y saben que existen muchas debilidades en los sistemas.

Muchas organizaciones han sido objeto de daños por parte de algún tipo de atacante. Pero muy pocas lo han dado ha conocer en gran parte por la publicidad dañina que les generaría, especialmente si son organizaciones que se dedican al manejo de dinero. Y de las pocas empresas que han puesto demanda por haber sido atacadas en su patrimonio, a nivel jurídico poco o nada se ha podido hacer, debido a que aun no existe ningún esquema jurídico que abarque por completo esta área que todavía es bastante nueva y esta en evolución constante.

Dado lo anterior es claro que la seguridad informática tiene un papel relevante en los sistemas de cómputo, y debe ser un factor a considerar en cualquier organización o por los usuarios que tengan un equipo conectado o no a la red, ya que los diferentes recursos que pueden ser almacenados en los sistemas de cómputo podrían impactar económicamente en caso de pérdida o alteración.

No podemos aceptar esa afirmación simpática que dice: *"el equipo de computo más seguro es aquel que está apagado y, por lo tanto, desconectado de la red".*

La seguridad en nuestros equipos de cómputo no la vamos a lograr si nos limitamos a apagar el equipo y lo desconectamos de la red, habrá que aplicar políticas, metodologías y técnicas de protección de la información.

Así, para garantizar que un sistema es seguro se deben considerar básicamente tres aspectos: Confidencialidad, Integridad y Disponibilidad de la información.

- Confidencialidad indica que los recursos almacenados deben ser accedidos únicamente por los usuarios autorizados a hacerlo.

- Integridad significa que los recursos pueden ser modificados únicamente por los usuarios autorizados y de manera controlada.

- Disponibilidad se refiere a mantener los recursos accesibles a los usuarios autorizados.

Las vulnerabilidades de los sistemas de cómputo, son aquellas grietas en su esquema de seguridad informática las cuales representan amenazas a la información y a los equipos; por medio de éstas puede penetrar personal no autorizado o intrusos y llevar a cabo ataques a los sistemas de información.

Con el incremento del uso de Internet y el aumento de instituciones que utilizan la red para la generación de portales, la protección de la información se convierte en un factor crítico, sobre todo cuando cada vez es más sencillo encontrar herramientas para explotar las vulnerabilidades de los sistemas de información,

las cuales pueden provocar pérdidas en la confidencialidad, integridad o disponibilidad repercutiendo de manera directa o indirecta en pérdidas económicas a los negocios o instancias que sufren de estas incursiones electrónicas.

Si bien es cierto que la incidencia en el volumen de ataques por Internet se ha reducido gracias a un plan de seguridad para los sistemas de información, la severidad y el impacto financiero de dichos ataques se ha incrementado de manera importante. Así, el reto que enfrentan los responsables de la seguridad en las tecnologías de la información se ve cada vez mas complicada.

Durante el ciclo de conferencias World Security Day (Día de la Seguridad), organizado en las instalaciones de la Rectoría General de la Universidad Autónoma Metropolitana celebradas en Noviembre del 2004, en el marco de la celebración del Día Mundial de la Seguridad Informática difundido por Symantec, líder mundial en seguridad Internet.

El ingeniero Gerado Maya, certificado en seguridad de Symantec, afirmó que México ocupa el lugar 15 como generador de ataques vía Internet (encontrar el hueco en la seguridad de las redes, las computadoras y en los programas para dañar, robar o introducir información), mientras que los primeros sitios están ocupados por Estados Unidos, Corea del Sur, China, Alemania, Francia, Taiwan, Canadá, Italia, Gran Bretaña y Japón. Maya señaló que los principales blancos de los ataques en el mundo son las compañías financieras, de energía y electricidad, seguidas de las organizaciones no lucrativas, telecomunicaciones y de alta tecnología.

El ingeniero Gerardo Maya indicó que las empresas menos afectadas por los hackers son las relacionadas con las manufacturas y la salud, mientras que la incidencia de los eventos severos casi se duplicó en las organizaciones de servicios financieros desde diciembre de 2001.

Luego de sostener que el volumen de ataques y los eventos severos se incrementan conforme al tamaño de las empresas y que las más dañadas son las que registran alrededor de 5 mil empleados, subrayó que de acuerdo con el reporte de amenazas, de julio a diciembre del 2002 (información provista por Symantec), se presentan en el mundo entre 20 a 45 ataques por semana, principalmente entre 13 y 21 horas, reduciéndose la incidencia los fines de semana.

Symantec, en México tiene presencia desde 1995, sus principales clientes son 6 de las 10 empresas más importantes en la Ciudad de México, además de secretarías de gobierno. El 70 por ciento del software de seguridad es provisto por esta empresa.

Dado lo anterior, el propósito de la seguridad informática es proteger los recursos de cómputo a través de la implementación apropiada de un Sistema de Gestión de Seguridad de la Información y su entorno; esto es, presentar de manera rigurosa el o los problemas de seguridad que afecte a un sistema; especificar los requerimientos de seguridad que resuelvan ese problema e implementar tales requerimientos.

Así entonces, un Sistema de Gestión de Seguridad de la Información (SGSI) es:

- Un análisis de los recursos de seguridad con los que cuenta una institución.
- Una valoración esos recursos y el impacto que crean en la seguridad de la información, es decir, evaluar si son funcionales o no.
- Diseño de un SGSI tomando en cuenta los aspectos anteriores e implementando mejoras.
- Establecimiento de políticas de seguridad aplicables al objeto de evaluación.

De tal manera que una falta de seguridad informática puede ser solucionada usando un SGSI para buscar solución a sus problemas de seguridad; pero es requisito indispensable que dicho Sistema sea diseñado en base a estándares internacionales para que tengan validez generalizada.

Las instituciones gubernamentales en México, no están exentas de posibles ataques en sus sistemas de información por lo cual este trabajo se centra en analizar y diseñar un Sistema de Gestión de Seguridad de la Información y Políticas de Seguridad para la Escuela Nacional Preparatoria plantel No. 5 “José Vasconcelos” la cual es una institución de educación media-superior y pertenece a la Universidad Nacional Autónoma de México (UNAM).

En el análisis realizado para la tipificación de la información propiedad de la institución, detectamos tres grandes áreas de estudio, que llamaremos Objeto de Evaluación (TOE), estas áreas son:

Centro de Cómputo

En esta área se maneja toda la información relacionada principalmente con dos grandes eventos institucionales como la aplicación del Instrumento de Apoyo a la Superación Académica (IASA) el cual es un software mediante el cual los alumnos pueden “calificar” a los profesores de sus asignaturas; también se lleva a cabo la captura de los informes de actividades de los profesores y sus avances programáticos (3 por año) estos dos eventos se realizan por medio de sistemas enviados por la Dirección General de la Escuela Nacional Preparatoria.

También en esta área los profesores tramitan su certificado digital y pueden hacer la captura de sus calificaciones.

En esta área también se gestiona la red de la Preparatoria No. 5 y provee de señal de Internet a la Escuela Nacional Preparatoria plantel 1 “Gabino Barreda”.

Secretaría Escolar

En esta área se manipula toda la información, trámites y horarios de los alumnos del plantel.

Unidad Administrativa

Aquí se concentra toda la información financiera del plantel, es decir, nóminas, pagos, compras, etc.

Además se maneja toda la información de los empleados del plantel como control de asistencias, permisos, vacaciones, horas extras, horarios, y los contratos de cada uno de ellos.

Para llevar a cabo este proyecto de tesis, hemos tomado en cuenta algunos aspectos importantes y de gran relevancia para la seguridad de la información con la siguiente distribución:

CAPÍTULO I SISTEMAS DE SEGURIDAD

En este capítulo se incluyen conceptos generales de la seguridad de los sistemas de cómputo tales como los servicios básicos de seguridad con los que debe contar como la confidencialidad, integridad, disponibilidad, etc. de la información.

En este capitulo se describen también las vulnerabilidades, amenazas y ataques más comunes que se presentan en los sistemas de Cómputo y el impacto que se espera en los sistemas de cómputo si se llegara a perpetrar un ataque.

Por último se revisan los aspectos legales en los que la información se ve involucrada, tales como derechos de autor, patentes, etc. y el tratamiento que se tiene en México y el mundo para el delito informático.

CAPÍTULO II ESQUEMAS DE SEGURIDAD BASADOS EN ESTÁNDARES INTERNACIONALES

Dando seguimiento al marco teórico del proyecto de tesis en este capitulo se hace referencia a los Sistemas de Seguridad basados en los Estándares Internacionales, los cuales han sido de mucha utilidad a las organizaciones que se basan en ellos para garantizar un nivel aceptable de seguridad en sus sistemas.

En este capítulo se revisarán las normas de seguridad basadas en estándares internacionales como son los Criterios Comunes y los Perfiles de Protección (PP).

También en este apartado, se revisan dos de los estándares sobre los cuales se ha basado en gran medida este proyecto, estos son el estándar ISO/IEC17799 su objetivo de garantizar la seguridad de la información y las áreas de control que considera este estándar, también se revisa el estándar ISO/IEC27001 el cual especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI), se mencionan los beneficios que se obtienen al poner en marcha un SGSI bajo este estándar .

Se verán las funcionalidades de cada una de ellas sus ventajas y desventajas para con ello tomar una como modelo a seguir para el diseño del SGSI para el objeto de evaluación.

CAPÍTULO III CONSIDERACIONES PARA LA ELABORACIÓN DE UN SISTEMA DE GESTIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN (SGSI)

En este capítulo se verán los conceptos que se tomarán a consideración para el diseño de un SGSI basados en la norma ISO/IEC 17799.

En este capítulo se revisan algunas consideraciones que es necesario tomar en cuenta para elaborar un SGSI, como la Administración de riesgos y el Análisis de Riesgos y los aspectos relevantes a tomar en cuenta para evaluar un Esquema de Seguridad que básicamente es realizar una evaluación de la seguridad actual para conocer cómo desarrollar y ejecutar la implantación de un sistema de seguridad.

En este capítulo se define también lo que son las Políticas de Seguridad Informática, las cuales surgen como una herramienta para concienciar a los colaboradores de una organización sobre la importancia y sensibilidad de la información. Y finalmente se verifican algunas de las responsabilidades del personal implicado dentro del diseño de un SGSI.

CAPÍTULO IV CASO PRÁCTICO, SGSI PARA EL OBJETO DE EVALUACIÓN

En este capitulo se describirá a detalle la forma en que se planificó el sistema de Gestión de Seguridad de la Información para el objeto de evaluación.

Primero se describe el análisis del Objeto de Evaluación de este proyecto de tesis; se exponen los motivos por los cuales se diseña un SGSI para la ENP 5 “José Vasconcelos” así como la justificación y objetivos.

Después se describe el entorno físico del objeto de evaluación, considerando todo el software, hardware, usuarios, etc. Es decir, se describen todos y cada uno de los elementos que conforma el objeto de evaluación.

Posteriormente se define a profundidad la Estructura general del objeto de evaluación, su Entorno Físico, se hace un análisis de los usuarios involucrados en

el objeto de evaluación, del Hardware y el Software con el que se cuenta, y se hace un estudio de la Estructura de Red y de la Información que se maneja en la organización.

En este capitulo, también se hace mención de las vulnerabilidades detectadas en el objeto de evaluación y se hace una serie de recomendaciones para cada una de ellas.

CAPÍTULO 5 POLÍTICAS DE SEGURIDAD

Finalmente en este capítulo se describen a detalle las Políticas de Seguridad Informática que se diseñaron para cubrir las vulnerabilidades del Objeto de evaluación.

Para ser posteriormente revisadas y evaluadas por las autoridades pertinentes, tomado en cuenta todas las garantías de los usuarios.

Para llevar a cabo el análisis, diseño y posterior implementación de un Sistema de Gestión de Seguridad de la Información y Políticas de Seguridad de este Objeto de Evaluación, es necesario contar con el apoyo de personas con poder de decisión en estas áreas conjuntamente con el apoyo de la Dirección del plantel, y es de fundamental importancia que ambas partes y los usuarios de la información estén verdaderamente concientes de la importancia de contar con herramientas de seguridad para proteger los bienes informáticos de la institución para crear una cultura de seguridad, y hacer ver a la gente involucrada los peligros a los que esta expuesta cualquier organización relacionada con las redes computacionales.

CAPÍTULO I
SISTEMAS DE SEGURIDAD

1. SISTEMAS DE SEGURIDAD

El incremento en el uso de Internet ofrece una ventaja fundamental en los negocios de hoy, las tecnologías basadas en Internet se han vuelto vitales para cientos de miles de negocios y millones de consumidores alrededor del mundo.

Entender que la tecnología de información (IT) ya no es solamente un soporte para los negocios sino una forma de hacer negocios, está haciendo que las organizaciones cambien su forma de ver a la tecnología y saquen mayor provecho de ella.

Para los usuarios es más fácil realizar las actividades cotidianas; gracias a los servicios de ventas por Internet se logra obtener en minutos diferentes mercancías sin necesidad de salir del hogar, el pago de impuestos a través de pagos en línea evita la molesta espera en la oficina fiscal, es posible pagar los diferentes servicios públicos sin necesidad de desplazarse a los bancos, se puede acceder a todo tipo de información en Internet desde cualquier poblado que cuente con una conexión telefónica rural.

Pero el incremento en el uso de estas tecnologías trae consigo un aspecto conflictivo: la seguridad. Los mensajes pueden ser interceptados y alterados, la información de las organizaciones puede ser copiada o eliminada, los estados de cuenta pueden ser modificados y la información personal almacenada en un equipo de cómputo puede ser alterada. Son estas inseguridades típicas de las redes abiertas la causa del incremento constante de los crímenes computacionales a nivel mundial.

Cualquier persona que esté interesada en aprender sobre diferentes técnicas para ingresar de manera no autorizada a un equipo lo puede lograr en cuestión de minutos, caso contrario a lo que ocurría hace algunos años, cuando las redes estaban en desarrollo. En esos tiempos obtener acceso no autorizado a un sistema requería de un alto nivel de conocimientos de cómputo y era una labor exhaustiva, actualmente el nivel de conocimientos que pueden tener este tipo de personas puede ser escaso y el trabajo involucrado para ingresar de manera no autorizada a un equipo es mínimo.

La seguridad en cómputo es un concepto difícil de definir debido a la gran cantidad de factores que intervienen, pero podría decirse que la seguridad en cómputo es: El conjunto de recursos (metodologías, documentos, programas y dispositivos físicos) destinados a lograr que los activos de una organización sean confidenciales, íntegros, consistentes y disponibles a sus usuarios, autenticados por mecanismos de control de acceso y sujetos a auditoria.

En este capítulo abordaremos las características con las que debe contar un sistema de cómputo seguro, después veremos lo que puede afectar nuestra seguridad, quienes pueden afectar la seguridad de los sistemas y después haremos una descripción de la protección jurídica con que se cuenta en estos momentos.

1.1.Servicios de seguridad de los sistemas de cómputo.

La seguridad de la información es el área que se encarga de reducir los riesgos a que se somete la información desde que es creada, enseguida organizada, después procesada, quizá enviada, y finalmente almacenada etc. "en general en cualquiera de sus modalidades". La seguridad de la información ha sido usada a lo largo de la existencia de la propia información, es decir, en toda la historia de la humanidad.

Hablar de dar seguridad a la información impone poder entender, qué es tener seguridad en la información, y cómo se puede alcanzar esto. De manera simple, tener seguridad es "contar" con un sistema de seguridad de la información, y cómo alcanzarla significa "diseñar" el sistema de seguridad.

Los servicios de seguridad de la información son los servicios de nivel básico que son utilizados para combatir los ataques definidos en el siguiente subtema. Cada uno de los servicios de seguridad combate ataques específicos, y para ello es importante que no sean confundidos con mecanismos de seguridad, ya que los mecanismos son la implementación de los servicios de seguridad.

1.1.1.Confidencialidad

La información debe estar disponible solamente para aquellos usuarios autorizados a accederla. Es prevenir, detectar, impedir el descubrimiento de información. En general la Confidencialidad se refiere a la protección de datos implicados en entornos altamente protegidos, como entornos militares, comerciales, etc.

La confidencialidad se cumple cuando solo las personas autorizadas (podríamos referirnos a los sistemas) pueden conocer los datos o la información correspondiente.

Existen dos tipos de confidencialidad:

- De contenido, la cual se refiere a que la información contenida o almacenada estáticamente en los sistemas de información debe permanecer disponible solamente para ser accedida por usuarios autorizados.

- De flujo, se refiere a que la información no sea descubierta por usuarios ilícitos mientras ésta se encuentra en algún trayecto, o sea en movimiento.

Podemos preguntarnos ¿qué ocurriría si un soporte magnético con los datos los empleados o clientes fuera cedido a terceros? ¿Cuál podría ser su uso final? Podría haber una cadena de ventas incontroladas de esos datos, que podría incluir datos como domicilios o perfil económico, o incluso datos médicos. Como

podemos darnos cuenta el que alguien de manera ilícita pudiera acceder a cierta información de carácter privado pone en riesgo los intereses tanto de las personas como a las empresas.

1.1.2.Integridad

La integridad consiste en que sólo las personas autorizadas pueden variar (modificar o borrar) la información. Además, al hacer esto, deben quedar un registro de cada cambio o movimiento que recibe la información, esto es para control posterior y para auditoria.

La integridad tiene por objeto resguardar la información, de tal forma que no se pueda falsear, así, los datos recibidos (o recuperados) siempre deben ser los mismos que fueron enviados (o almacenados), etc.

Con base en lo anterior podría decirse que la integridad es prevenir, detectar e impedir la modificación inadecuada de información. Por ejemplo en un entorno militar, el mando responsable de un misil no debe ser modificado inadecuadamente. En un entorno comercial, la integridad de los datos es especialmente relevante, puesto que el éxito de una organización depende de lo correctas que son las operaciones que se llevan a cabo y la coherencia en los datos.

Existen dos tipos de integridad:

- De contenido, se refiere a respetar en todo momento las reglas de integridad definidas por las instancias dueñas de la información en el manejo de la misma.

- De secuencia de mensaje, se refiere a garantizar la consistencia de la información con respecto a su uso recurrente, esto deber ser en absoluto orden para no afectar a la información.

Pensemos que alguien varía datos de forma que perdiéramos información de determinadas deudas a cobrar, o que modificara ciertos registros importantes en una base de datos.

Algunas de estas acciones se podrían tardar en detectar, y tal vez las copias de seguridad que se han hecho a lo lago del tiempo como respaldo de información, pudieran estar viciadas, esto haría muy difícil la reconstrucción de la información perdida.

1.1.3.Disponibilidad

El servicio de disponibilidad mantiene la utilidad de la información, permite a los usuarios tener acceso a los sistemas de cómputo, a la información de los sistemas y a las aplicaciones que se realizan sobre la información; todo esto debe ser en el

momento en que los usuarios autorizados lo puedan hacer en el instante en que lo requieran.

La disponibilidad se cumple si las personas autorizadas pueden acceder a la información cuando lo deseen y tantas veces como sea necesario.

El disponer de la información después del momento necesario puede equivaler a la no disponibilidad.

Otro caso grave es la no disponibilidad absoluta que puede haberse producido por algún desastre físico; en este caso a medida que pasa el tiempo el impacto será mayor, hasta llegar a suponer la no continuidad de la información en la organización.

1.1.4.Autenticación

La Autenticación es un servicio que consiste en identificar a los usuarios que entran a un sistema y verificar su autenticidad, de manera que pudiera llevarse a cabo este proceso de diferentes maneras:

- Por lo que se tiene: Esto se puede basar en la posesión de una llave o tarjeta que permita o restrinja el acceso a la información. Un enfoque es usar un elemento físico difícil de copiar, típicamente una tarjeta con una banda magnética. Para mayor seguridad este enfoque se suele combinar con una clave (como es el caso de los cajeros automáticos).

- Por lo que se sabe: Puede ser una clave o password, que permita el acceso a la información. El mecanismo de autenticación más ampliamente usado, se basa en el uso de claves o passwords; es fácil de entender y fácil de implementar.

- La clave también se puede descubrir mirando o filmando cuando el usuario la digita, o, si el usuario hace uso de su clave de manera remota, se puede intervenir la red y observar todos los paquetes que pasan por ella.

- Por último, además de que las claves se pueden descubrir, éstas también se pueden “compartir”, violando las reglas de seguridad. En definitiva, el sistema no tiene ninguna garantía de que quien hizo uso de la clave es realmente el usuario que se supone que es.

- Por lo que se es: Esto es buscar un atributo del usuario, personal e irreproducible como una huella digital. Otra posibilidad es medir características físicas particulares del usuario como la huella digital, el patrón de vasos sanguíneos de la retina, la longitud de los dedos, incluso la firma personal.

Algunas medidas básicas

- Demorar la respuesta ante claves erróneas; aumentar la demora cada vez. Alertar si hay demasiados intentos.

- Registrar todas las entradas. Cada vez que un usuario entra, checar cuándo y desde dónde entró la vez anterior.

- Hacer chequeos periódicos de claves fáciles de adivinar, procesos que llevan demasiado tiempo corriendo, permisos erróneos, actividades extrañas (por ejemplo cuando usuario está de vacaciones).

- Para los más paranoicos: poner trampas para descubrir intentos de uso no autorizado.

1.1.5.Control de acceso

En toda organización es importante implementar y mantener un registro preciso del personal que entra y sale de las instalaciones, lo que nos proporciona un control de acceso y es un auxiliar en materia de seguridad.

Las entradas y salidas del personal a los sistemas de información se monitorean a través de un sistema de control de acceso el cual debe registrar la fecha y la hora en que se producen las entradas y salidas de un sistema.

El tema de Control de Acceso es uno de los ejes principales del estudio de seguridad informática, porque trata de mecanismos que operan en cada máquina de forma aislada, usualmente con una combinación del diseño del sistema de operación y la arquitectura del hardware.

Un Modelo de Control de Acceso de un sistema, se basa en el servicio de Autenticación ya que sirve para identificar a cada usuario, verificar si realmente es quien dice ser y por tanto, que tipo de privilegios o restricciones tiene dentro del sistema.

El control de acceso se lleva a cabo mediante dos tipos de dispositivos:

- Dispositivos Pasivos, los cuales dejan ocurrir las entradas, salidas y movimientos dentro de un sistema de información sin ningún tipo de control, es decir, sin guardar registro de lo que ocurre dentro del sistema.

- Dispositivos Activos, estos dispositivos hacen uso de bitácoras y controlan de manera eficiente el flujo de accesos al sistema debido a que pueden guardar la información de las veces que cada usuario entra al sistema y observa, lee o modifica la información.

Por ejemplo un software de control de acceso en una empresa podría contar con un módulo de reportes que analice automáticamente los ingresos y de acuerdo con los distintos horarios asignados a cada empleado permita conocer las ausencias, incumplimientos de horarios, entre otros.

1.1.6.No repudio

El no repudio es un servicio de seguridad que permite probar la participación de las partes en una comunicación

Previene a los emisores o a los receptores de negar un mensaje transmitido. Por lo que cuando un mensaje es enviado, el receptor puede probar que el mensaje fue enviado por el presunto emisor. Al mismo tiempo, cuando un mensaje es recibido, el remitente puede probar que el mensaje fue recibido por el presunto receptor.

La autenticación aporta seguridad en la identificación de alguien o algo, por otro lado la integridad evita que la información sea alterada o modificada para fines ilícitos.

A pesar de que no se puede conseguir el no repudio sin los servicios de autenticación e integridad, el no repudio consiste en algo más que la autenticidad o integridad de los datos, es la capacidad de probar a una tercera parte que una específica acción ha sido originada, enviada y admitida a una determinada persona.

La firma manuscrita ha permitido certificar el reconocimiento, sobre un documento por parte de cada firmante pese a que pueda ser falsificada, ya que tiene rasgos que la hacen fácil de vincular a quién la realiza. Otros procedimientos se han venido empleando a lo largo de años para conseguir el no repudio de los datos, como por ejemplo el correo certificado con acuse de recibo, los sellos de autoridades públicas etc.

Por ejemplo a través de la firma digital de un mensaje, se podrá conseguir una fuerte prueba de quién firmó (autenticación), qué datos son los que se firmaron (integridad) y finalmente el "no repudio". Esto aporta una prueba frente a la posible negación de los hechos por alguna de las partes.

El no repudio se divide en dos tipos.

- El no repudio en origen, evita o resuelve los conflictos sobre la creación de un mensaje en un momento determinado. Este tipo de no repudio concede a los receptores de los mensajes validez probatoria para resolver posibles conflictos, como por ejemplo que el emisor niegue haber enviado un mensaje, o que el mensaje recibido por el receptor es diferente de lo que el emisor dice haber enviado, así como la discrepancias de la fecha y hora de envío.

- El no repudio en el envío, evita o resuelve conflictos con relación a la recepción de un mensaje y a su envío. Por tanto, lo que hace es proteger al emisor otorgándole valor probatorio frente a posibles reclamaciones futuras, como por ejemplo que el receptor niegue la recepción del mensaje, o el contenido del mismo, o la fecha y hora del envío.

Para conseguir una aplicación adecuada del "no repudio" se deben seguir las siguientes actividades que se deben poner en práctica en el ámbito del comercio electrónico seguro.

- Solicitud del servicio, para conseguir el "no repudio" es necesario que uno o varios de los partícipes en una comunicación estén de acuerdo antes de originar el mensaje y enviarlo, en utilizar los servicios del "no repudio".

- Emisión de una prueba, para ello se utilizará a terceras partes de confianza o autoridades de certificación, o se utilizará la firma electrónica para obtener la prueba.

- Transmisión de la prueba, una vez obtenida la misma, los autores deben transmitir la misma a las partes para que pueda ser verificada.

- Verificación de la prueba, una vez transmitida la prueba corresponderá a su receptor verificar que dicha prueba se ha generado y transmitido correctamente. Aquí las Autoridades de certificación verifican que el emisor es quien dice ser y que la firma electrónica del documento está vigente.

- Conservación de la prueba, para poder obtener el "no repudio" es imprescindible poder demostrar en el futuro que dicha comunicación existió y por tanto, contar con una prueba consistente que demuestre que lo que se aceptó, emitió y envió es altamente vinculante.

1.1.7.Auditoría informática

La Auditoria Informática, también conocida como Auditoria de Sistemas, surge debido a que la información se convierte en uno de los activos más importantes de las empresas, lo cual se puede confirmar si consideramos el hecho de que si se queman las instalaciones físicas de cualquier organización, sin que sufran daños los equipos de cómputo, la entidad podría retomar su operación normal en un menor tiempo, que si ocurre lo contrario. A raíz de esto, la información adquiere gran importancia en la empresa moderna debido a su poder estratégico y a que se invierten grandes sumas de dinero y tiempo en la creación de sistemas de información con el fin de obtener una mayor productividad.

El Departamento de Informática o Sistemas desarrolla diversas actividades y sobre la base de éstas se han establecido las principales divisiones de la Auditoria Informática, las cuales son:

a) Auditoría Informática de Producción o Explotación

Se ocupa de revisar todo lo que se refiere con producir resultados informáticos, listados impresos, ficheros soportados magnéticamente, ordenes automatizadas para lanzar o modificar procesos, etc.

Auditar la producción, operación o explotación consiste en revisar las secciones que la componen y sus interrelaciones, las cuales generalmente son: planificación, producción y soporte técnico.

b) Auditoría Informática de Desarrollo de Proyectos

La función de desarrollo es una evolución del llamado análisis y programación de sistemas, y abarca muchas áreas, como lo son: prerrequisitos del usuario y del entorno, análisis funcional, diseño, análisis orgánico (preprogramación y programación), pruebas entrega a explotación o producción y alta para el proceso.

Estas fases deben estar sometidas a un exigente control interno, ya que en caso contrario, los costos pueden excederse, puede producirse la insatisfacción del usuario.

La auditoria en este caso deberá principalmente comprobar la seguridad de los programas en el sentido de garantizar que lo ejecutado por la máquina sea exactamente lo previsto o lo solicitado inicialmente.

c) Auditoría Informática de Sistemas

Se ocupa de analizar y revisar los controles y efectividad de la actividad que se conoce como técnicas de sistemas en todas sus facetas y se enfoca principalmente en el entorno general de sistemas, el cual incluye sistemas operativos, software básico, aplicaciones, administración de base de datos, etc.

d) Auditoría Informática de Comunicaciones y Redes

Este tipo de revisión se enfoca en las redes, líneas, concentradores, multiplexores, etc. Así pues, la Auditoria Informática ha de analizar situaciones y hechos algunas veces alejados entre sí, y está condicionada a la participación de la empresa telefónica que presta el soporte. Para este tipo de auditoria se requiere un equipo de especialistas y expertos en comunicaciones y redes.

e) Auditoría de la Seguridad Informática

La Auditoria de la seguridad en la informática abarca los conceptos de seguridad física y lógica. La seguridad física se refiere a la protección del hardware y los soportes de datos, así como la seguridad de los edificios e instalaciones que los albergan.

Por su parte, la seguridad lógica se refiere a la seguridad en el uso de software, la protección de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios a la información.

La auditoria en la seguridad informática busca determinar si el esquema de seguridad ha sido implantado correctamente.

f) Auditoría Informática para Aplicaciones en Internet.

En este tipo de revisiones, se enfoca principalmente en verificar los siguientes aspectos, los cuales no puede pasar por alto el auditor informático:

- Evaluación de los riesgos de Internet (operativos, tecnológicos y financieros) y así como su probabilidad de ocurrencia.
- Evaluación de vulnerabilidades y la arquitectura de seguridad implementada.
- Verificar la confidencialidad de las aplicaciones y la publicidad negativa como consecuencia de ataques exitosos por parte de hackers.

1.2.Grietas en la seguridad

La seguridad continuamente se ve expuesta a pérdida, daño total o parcial del sistema de cómputo y en varios casos hasta de la información; algunos ejemplos de estos pueden ser las revelaciones no autorizadas de información (confidencialidad), modificación de los datos (integridad) o negativa al acceder al servicio de cómputo (control de acceso).

En este subtema pretendemos dar a conocer de una manera clara y sencilla tres conceptos, los cuales son las fases para lograr violar la seguridad de un sistema de cómputo. Lo cual es necesario conocer e identificar en las organizaciones para poder determinar de manera clara no solamente qué se desea proteger sino además de qué se desea proteger.

1.2.1.Vulnerabilidades

"Las vulnerabilidades de los sistemas de cómputo, son aquellas grietas en el esquema de seguridad informática las cuales representan amenazas a la información y a los equipos; por medio de éstas pueden penetrar personal no autorizado o intrusos y llevar a cabo ataques a los sistemas de información." [1]

Como vulnerabilidad debemos entender que *"son los puntos débiles del sistema de cómputo, a través de los cuales la seguridad puede ser afectada."*[2]

Nosotros hemos hecho una clasificación de los diferentes tipos de vulnerabilidades, los cuales hemos dividido de la siguiente manera: físicas, naturales, de software y hardware, datos, almacenamiento, de comunicación y humanas.

- FISICAS: Cualquier persona que tenga acceso físico a las instalaciones puede dañar seriamente el equipo.

[1] López Nava Leticia , Sistemas de Seguridad en Cómputo, México, 1998.
[2] Ing. Vega Armando, Seguridad en Bases de Datos, México

- NATURALES: El equipo de cómputo es especialmente sensible a cualquier alteración de su medio ambiente, por ejemplo cambio de temperatura, humedad, polvo, etc.

- SOFTWARE Y HARDWARE: Un dispositivo de almacenamiento que falle o una caída del sistema pueden comprometer la integridad de los datos. En software podemos mencionar al sistema operativo y programas de aplicación. Como hardware nos referimos a la computadora, terminales, impresoras, módems, discos y elementos internos como lo son CD, discos duros, etc.

- DATOS: Los datos son generados de todo lo que la organización realiza. Cuando los intrusos roban datos es como si robaran dinero o equipo, por lo cual podemos decir que los datos son un bien irremplazable.

- ALMACENAMIENTO: Seguridad en cintas y discos de almacenamiento, ya que pueden ser extraviados, dañados o robados.

- DE COMUNICACION: Verificar que las transacciones sean validadas o en su caso de una falla de la red sean desechadas. El conectar una computadora en una red, inevitablemente incrementa la vulnerabilidad de la información almacenada.

- HUMANAS: Si el administrador comete un error, o realiza una acción indebida o desconoce el sistema puede comprometerse la seguridad y la integridad de los datos.

1.2.2.Amenazas y clasificación de amenazas

Los ambientes de cómputo de las organizaciones o de los particulares pueden verse afectados por diversos factores, ya sea de manera accidental o mediante alguna técnica especializada para poder modificar, robar o simplemente dañar la información.

Una amenaza es todo aquello que intenta o pretende destruir y puede producir pérdidas materiales, financieras o de información.

No debemos olvidar que un sistema de cómputo también puede ser afectado por elementos naturales que son impredecibles como los terremotos, inundaciones, incendios, etc.

A continuación se muestra en la tabla 1.1, la clasificación general de amenazas:

CLASIFICACIÓN GENERAL DE AMENAZAS

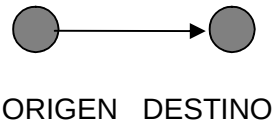
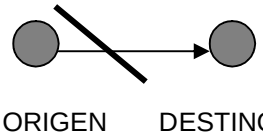
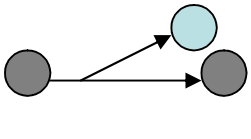
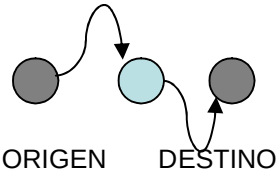
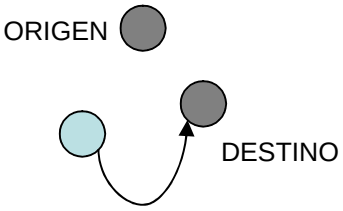
FLUJO NORMAL		En este caso la información fluye de manera normal y segura, presentándose así un sistema seguro y por lo tanto, ideal.
INTERRUPCIÓN		Un recurso del sistema es destruido o interrumpido
INTERCEPCIÓN		Una entidad logra acceder a un recurso y puede ver y/o robar información
MODIFICACIÓN		Una entidad logra acceder a un recurso y manipula la información
SUPLANTACIÓN		Una entidad inserta información falsa en el sistema

TABLA 1.1 CLASIFICACIÓN GENERAL DE AMENAZAS

Agentes de la amenaza

Agentes pueden ser personas desempleadas, hackers, rivales comerciales, terroristas, delincuentes, público en general, compañías que prestan servicio a la organización amenazada, clientes, invitados, desastres físicos, etc.

Algunos de los elementos que pueden amenazar los sistemas de cómputo, su entorno y la información, pueden ser los siguientes.

- Introducción de software malintencionado (de manera intencional) a los sistemas
- Interrupción de las comunicaciones internas o externas
- Escucha furtiva pasiva de comunicaciones internas o externas
- Robo de hardware o software

Algunos de los elementos que pueden amenazar los sistemas de cómputo, su entorno y la información, pueden ser los intrusos que describiremos como aquella persona que obtiene acceso no autorizado a un sistema y que puede ser personal externo o interno de la organización en cuestión; éste puede ser desde un niño de 12 años de cualquier parte del mundo hasta una persona de edad avanzada con acceso a una red.

Tipos de intrusos

- Lamer: Es una persona que no tiene ninguna inquietud por aprender, lo único que busca es tener un usuario y una contraseña ajenas, para formatear el disco duro, y presumir que es un supercracker.
- Newbie o Novato: Es una persona que realmente le interesa aprender de estos temas, pero que necesita tiempo de aprendizaje.
- Phreaker: Es un apasionado del sistema telefónico, investigadores de las telecomunicaciones. Su hobby es conocer el funcionamiento de la redes de telefonía, para después perpetrar ataques en beneficio propio como llamadas gratis, o travesuras como hacer que el vecino pague más, etc.
- Script Kiddies o Ciber Punks: Estos son jóvenes, comúnmente capturados por las autoridades ya que ellos hablan sobre sus ataques en línea. No existe una categoría de edad, adaptan a las computadoras y la tecnología, ellos descargan programas de la red para atacar a los sistemas con intención de vandalismo o interrumpir los sistemas.
- Codificadores y Escritores de Virus: Suelen verse como la elite de los perpetradores, con mucha trayectoria de programación escriben códigos pero no los utilizan ellos mismos. Tienen sus propias redes para experimentar, dejan a otros introducir el código en la Internet.
- Criminales Profesionales: Estos individuos viven irrumpiendo en los sistemas y vendiendo la información. Puede ser que consigan un empleado para espionaje corporativo o del gobierno. Pueden tener también nexos con el crimen organizado.
- Hackers de Vieja Escuela: Estos son gurús al estilo de los años sesenta de Stanford o del MIT para los cuales el término hacking es una divisa de honor. Están interesados en líneas de código y el análisis de los sistemas.

No tienen intensiones malévolas, aunque pueden tener una carencia de preocupación por aislamiento y la información propietaria ya que creen que Internet fue diseñado para un sistema abierto.

- Hacker White Hat: Tienen un conocimiento muy avanzado de programación. Conocen muchos huecos de seguridad de los sistemas operativos, y lo más importante, conocen el por qué de estos huecos de seguridad. Los hackers están buscando información continuamente, y la hacen pública cuando la encuentran, y nunca estropean datos de un sistema intencionalmente.
- Cracker Black Hat: Es una persona que irrumpe dentro de un sistema o viola la integridad del sistema a través de sistemas remotos con ideas maliciosas. Los crackers ganan acceso sin autorización, destruyen o roban datos importantes, incluso vitales, o simplemente causan problemas a sus víctimas. Los crackers pueden ser fácilmente identificados por sus actos maliciosos.

A continuación explicamos algunas amenazas que si no son controladas a tiempo se pueden convertir en ataques.

- **Destrucción de hardware**

Generalmente son empleados molestos o terroristas, los que representan esta amenaza. Como los crackers.

- **Robo de hardware**

Los componentes de hardware son objetivos atractivos para los ladrones especialmente porque pueden ser revendidos fácilmente. Este tipo de robo no solo deshabilita el equipo sino que también puede redundar en pérdida de datos críticos o en robo de mecanismos de almacenamientos.

- **Robo de software**

Puede ser robado en como parte de un robo de computadora o por sí sólo. Los ladrones pueden tomar discos o cintas que contienen copias de software comercial, o peor aún pueden robar copias de software desarrollado por la organización o información valiosa para ésta.

- **Sabotaje por computadora**

La gente que obtiene control sobre los sistemas que controlan la información de la defensa, la transferencia de trillones de dólares diarios por medio de redes de transferencia de fondos, procedimientos médicos, navegación de aerolíneas, etc. Pueden causar mucho daño, tanto a los sistemas como a las personas que dependen de ellos.

Algunos tipos de sabotaje resultan obvios, pero hay otros que no lo son tanto, como son el caso de los virus, que accidentalmente aparecen, y por lo general su

origen es desconocido, por lo que siempre se tomará como accidentalmente los daños que pueden causar.

- **Robo de bienes**

Billones de dólares son robados cada año, por medio de fondos electrónicos de transferencia, almacén, cuentas de pensión y otros varios tipos de fraude.

- **Robo de resultados**

Algunos crímenes simplemente se relacionan recogiendo datos valiosos en un disco, cinta, o papel y llevárselos.

- **Uso no autorizado**

Existen varios tipos de uso no autorizado, el primero se refiere a el uso de una computadora por gente que no esta autorizada a hacerlo. El segundo es el uso de la computadora por empleados para actividades fuera de las labores de la oficina, cada vez que una computadora es encendida y un empleado gasta su tiempo en cuestiones fuera de labores de oficina, le cuesta dinero a la empresa.

- **Desastres**

Este tipo de amenazas puede afectar tanto al hardware, al software y a la información. Los desastres pueden ser naturales (fuego, terremoto, inundación, etc.) que por lo regular son poco frecuentes, no así los accidentes humanos que son los más comunes y van desde derramar líquido sobre algún equipo hasta borrar información valiosa.

Podemos resumir que existen tres tipos de desastres:

  - Naturales: Terremotos, tormentas, fallas en el suministro eléctrico, sobre estos, el personal de las organizaciones no tienen ningún control, pero la información puede ser protegida si se cuenta con planes de contingencia.
  - No intencionales: Muchas veces por falta de cultura informática (desconocimiento del usuario del sistema).
  - Intencionales Externas: Ataques de intrusos, alteración del sistema, comprometimiento de información importante.
  - Intencionales Internas*:* El 80% de los ataques vienen de dentro de la organización.

- **Códigos maliciosos**
  - Caballos de Troya: Son instrucciones introducidas en la secuencia de instrucciones de otros programas legales (de ahí su nombre) y que realizan funciones no autorizadas, destruyen ficheros o capturan información mientras simulan efectuar funciones correctas. Un caso particular de los troyanos son los salami, generalmente utilizados en instituciones financieras, realizan asientos de pequeñas cantidades, como los redondeos de operaciones de cálculo de intereses, par que no

se detecten por su importancia y al final se transfieren a una cuenta bancaria particular.

- Virus y Gusanos: Los virus son programas que modifican otros programas o alteran los ficheros. Antes se propagaban a través de programas en disquetes que al introducirse en los PC, se liberaban y realizaban sus comandos. Hoy día se propagan principalmente a través del correo electrónico, de ahí su gran poder de propagación debido al desarrollo de los e-mails. Se les denomina así debido a su parecido con los virus biológicos ya que necesitan para vivir un cuerpo vivo, el sistema informático y la red en funcionamiento, y además son capaces de reproducirse y de morir, mediante la utilización del software adecuado. Hay dos tipos de virus. Los benignos y los malignos. Los primeros sólo producen efectos molestos como la superposición de mensajes (el virus Marihuana) o movimiento de figuras (virus de la Pelotita) o transposición de los caracteres de la pantalla (virus de la cascada de letras). Los malignos pueden borrar ficheros de datos o alterar el funcionamiento de los programas. Los más conocidos son Viernes 13, Melissa (creado por David L. Smith), Love Letter de Raonel Ramones, Back Orifice de Sir Dyistic, The Tour of de Worm de Morris, y el Chernobyl de Chen Ing-Hou. Hay que destacar que el primer virus de la historia fue construido por el investigador informático Fred Cohen cuando trabajaba en conseguir programas inteligentes que pudieran automodificarse, dando lugar a una rama de la informática, la Informática Evolutiva o Vida Artificial.
- Los gusanos deben a su origen a los investigadores Robert Thomas Morris, Douglas McIlroy y Victor Vysottsky, desarrolladores de un juego de estrategia denominado Corewar (Guerra de la Memoria), que consistía en que ganaba el jugador que era capaz de ocupar más cantidad de memoria. El gusano no necesita, a diferencia de los virus otro programa para funcionar y simplemente se va duplicando y ocupando memoria hasta que su tamaño desborda al sistema informático en que se instala, impidiéndole realizar ningún trabajo efectivo.
- La mejor manera de prevenir virus y gusanos de invadir un sistema es siendo precavido cuando se introducen datos o software a la computadora tener antivirus actualizado en nuestros equipos de cómputo y hacer respaldos continuamente.

1.2.3.Ataques

Puede decirse que un ataque es la actuación de una amenaza dentro de un sistema de cómputo, es decir, cuando un intruso malintencionado ha detectado una vulnerabilidad dentro de un sistema trata de explotarla hasta que tiene oportunidad de lanzar su ataque.

En los últimos años, los ataques se han incrementado y nadie es inmune a la amplia gama de actos maliciosos, por tanto, la seguridad en cómputo debe

apreciarse como un problema de personas y de procesos que puede solucionarse con la conciencia del problema y con la tecnología.

Por otro lado, en términos muy generales, podría decirse que existen tres objetivos primordiales para atacar un sistema o una red, y éstos son: las personas que sin buscar fines maliciosos o criminales, por curiosidad o reto atacan; los intrusos que quieren usar a un sistema determinado como puente de acceso para atacar a otros sistemas; y los intrusos que tienen, como único fin, atacar un sistema para provocar daño a la organización propietaria o que persiguen consultar, copiar, robar y vender datos; existen también el crimen organizado y el espionaje industrial.

Sea cual sea el objetivo, los intrusos siempre causan un daño, voluntario o no, sea en términos de confianza o de un delito grave.

Aunque existen intrusiones mayores y peligrosas, en México, además de la infección por “virus, gusanos y troyanos”, es común en materia de ataques, que los crackers recurran al uso de equipos mexicanos como computadoras personales, servidores, estaciones de trabajo y otros, para atacar a terceros con objeto de usar su infraestructura en cómputo y ancho de banda.[3]

Elementos de los ataques:

- **Motivación**

Son las razones que puede tener un agente para presentar una amenaza hacia el objetivo. Un agente requiere de una motivación para actuar en contra del objetivo, los cuales pueden ser por solo reto, codicia, Intento malintencionado, etc.

Cuando la motivación es revelar la información sin autorización a individuos u organizaciones, la confidencialidad es el blanco. Cuando la amenaza implica modificar la información, el objetivo es la integridad.

- **Capacidad**

Es el nivel y tipo de información que tiene un agente acerca del objetivo. El conocimiento que puede ser útil para un agente incluye lo siguiente:

  - Identificación de usuarios.
  - Contraseñas.
  - Ubicación de archivos.
  - Procedimiento de acceso físico.
  - Nombres de empleados.
  - Número telefónico de acceso.
  - Dirección de red.

[3] Celorio Suárez Mariana, UNAM-CERT organismo especializado en seguridad en cómputo, UNAM, Noviembre 2002, http://www.enterate.unam.mx/Articulos/dos/noviembre/unamcert.htm

- Procedimientos de seguridad.

- **Oportunidad**

Este elemento de los ataques es muy importante ya que en este punto el atacante espera una oportunidad optima para poner en marcha el plan, revisa y monitorea con sumo cuidado el sistema objetivo para encontrar un momento adecuado y exacto para su ataque.

Por ejemplo, un agente tiene oportunidad de ataque cuando un usuario deja abandonado su sitio de trabajo, en ese momento se presenta una oportunidad para comenzar a usar un equipo que no es el suyo.

O bien cuando una red privada no cuenta con un firewall de protección lo suficientemente fuerte, un agente puede encontrar una oportunidad para hackear los equipos.

Etapas de un ataque

- **Preparación**

Cuando un agente ha encontrado una vulnerabilidad en un sistema, traza un plan de acción para poder lanzar su ataque, es decir, se toma su tiempo en buscar la manera más optima y eficaz de destruir, robar o modificar el sistema objetivo.

- **Activación**

En esta etapa, el intruso ha lanzado ya su ataque y está en espera de que sea activado por el sistema objetivo.

- **Ejecución**

En esta última etapa del ataque tiene mucho que ver el sistema objetivo en sí ya que la ejecución de códigos maliciosos, por ejemplo, es responsabilidad de los usuarios finales del sistema en si.

Por ejemplo, cuando en el correo electrónico se envía un archivo que contiene in código malicioso, es responsabilidad del usuario del equipo, revisar todos los archivos que recibe en su correo electrónico, para poder evitar la ejecución de un ataque de este tipo.

Clasificación de ataques

Existen muchos tipos de ataques, sin embargo es importante mencionar que todos esos tipos de ataques a su vez son clasificados en dos grandes clases que son: Ataques pasivos y Ataques activos.

- **Ataques pasivos**

En esta clase de ataques, el atacante o intruso no altera la comunicación, sino que únicamente la escucha o monitorea, para obtener información de lo que se transmite. Sus objetivos son la intercepción de datos y el análisis de tráfico, una

técnica más sutil para obtener información de la comunicación, que puede consistir en:

- Obtención del origen y destino de la comunicación, leyendo las cabeceras de los paquetes monitorizados.
- Control del volumen de tráfico intercambiado entre las entidades monitorizadas, obteniendo así información acerca de actividad o inactividad inusuales.
- Control de las horas habituales de intercambio de datos entre las entidades de la comunicación, para extraer información acerca de los períodos de actividad.

Los ataques pasivos son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos. Sin embargo, es posible evitar su éxito mediante el cifrado de la información.

- **Ataques Activos**

Estos ataques implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos, pudiendo subdividirse en cuatro categorías:

- Suplantación de identidad: el intruso se hace pasar por una entidad diferente. Normalmente incluye alguna de las otras formas de ataque activo. Por ejemplo, secuencias de autenticación pueden ser capturadas y repetidas, permitiendo a una entidad no autorizada acceder a una serie de recursos privilegiados suplantando a la entidad que posee esos privilegios, como al robar la contraseña de acceso a una cuenta.
- Reactuación: uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado, como por ejemplo ingresar dinero repetidas veces en una cuenta dada.
- Modificación de mensajes: una porción del mensaje legítimo es alterada, o los mensajes son retardados o reordenados, para producir un efecto no autorizado. Por ejemplo, el mensaje “Ingresa un millón de pesos en la cuenta A” podría ser modificado para decir “Ingresa un millón de pesos en la cuenta B”.
- Degradación fraudulenta del servicio: impide o inhibe el uso normal o la gestión de recursos informáticos y de comunicaciones. Por ejemplo, el intruso podría suprimir todos los mensajes dirigidos a una determinada entidad o se podría interrumpir el servicio de una red inundándola con mensajes espurios. Entre estos ataques se encuentran los de denegación de servicio, consistentes en paralizar temporalmente el servicio de un servidor de correo, Web, FTP, etc.

1.2.4.Tipos de ataques

Teniendo entendido lo que es un ataque y su clasificación general, a continuación se enuncian los tipos de ataques a los que está expuesto cualquier sistema informático. Sin importar como ocurren los eventos que afecten a la organización, los podemos clasificar de la siguiente forma:

- **Ataques de acceso**

Un ataque de acceso es un intento de obtener información que el atacante no está autorizado a ver. Este tipo de ataque está dirigido contra la confidencialidad de la información, este ataque se puede llevar a cabo mediante:

El fisgoneo el cual consiste en hurgar entre los archivos de información para hallar algo interesante.

Escuchar furtivamente, esto es, si alguien escucha una conversación de la que no forma parte, se dice que escucha furtivamente. Esto ya no solo puede ser físicamente sino también electrónicamente.

- **Ataques de modificación**

Es un intento de modificar la información que una persona no está autorizada. Este tipo de ataque es en contra de la integridad de la información, y se puede llevar a cabo mediante:

Cambios a la información, al hacer cualquier cambio no autorizado, la información es incorrecta puesto que ya no es la información original. Los ataques de cambios a la información pueden ser cuando se agrega información que no existía con anterioridad. O bien borrando la información existente.

- **Ataques de denegación de servicios**

Los ataques de denegación de servicios (DoS, Denial-of-Service) son ataques que niegan el uso de los recursos a los usuarios legítimos del sistema, de la información o de las capacidades. Por lo general los ataques DoS no permiten que el atacante tenga acceso o modifique la información en el sistema de cómputo o en el mundo físico.

Un ataque DoS en contra de la información provoca que dicha información no esté disponible. Esto puede ser causado por la destrucción de la información. Esto también sucede si la información aún existe pero ha sido removida hacia una ubicación inaccesible.

Un ataque de DoS dirigido a una aplicación que manipula o exhibe la información, es en contra de un sistema de cómputo que ejecuta tal aplicación. Si la aplicación no está disponible, la organización no puede realizar las tareas que son desempeñadas por esa aplicación.

Otro ataque DoS está dirigido a derribar sistemas de cómputo. En este tipo de ataque el sistema, junto con todas las aplicaciones que corren en el mismo y toda la información que se encuentra almacenada en él dejan de estar disponibles.

Los ataques DoS en contra de las comunicaciones pueden abarcar desde cortar un alambre para entorpecer las comunicaciones de radio hasta inundar redes con tráfico excesivo. Aquí el objetivo es el medio de comunicación por sí mismo.

Normalmente, los sistemas y la información permanecen ilesos, pero la carencia de comunicaciones evita el acceso a los sistemas y la información

- **Ataques de refutación**

Es un ataque que va en contra de la responsabilidad de la información. Es tratar de transmitir información falsa o de negar que una transacción o evento reales hubieran ocurrido.

Es simplemente negar que la acción se haya realizado como fue registrada. Este tipo de ataque es también conocido como no repudio.

1.3.Aspectos legales de la información y regulaciones

Desgraciadamente la ley en esta materia se desenvuelve muy lentamente ya que las computadoras y su uso son nuevas comparadas con otro tipo de bienes. Debido a esto su lugar dentro de la ley no está muy bien establecido. Conforme se van presentando los casos la ley va avanzando en esta materia. A esto hay que sumarle que los jueces, abogados y policías no están realmente familiarizados con el tema ya que no cuentan con una preparación completa de cómo funciona, de que lo compone y como se desarrolla un sistema informático; por lo que es muy difícil que determinen como la computación se relaciona con otras partes de la ley.

Las leyes referentes a la seguridad en sistemas de cómputo afectan a programadores, diseñadores, desarrolladores y usuarios y a quienes mantienen los sistemas de cómputo, así como a las bases de datos.

1.3.1.El valor de la información

Como hemos mencionado la información es de lo más valioso con lo que cuentan las empresas, bancos, instituciones e incluso los particulares.

En los negocios se paga por un reporte de crédito, un listado de clientes e información interna de los competidores; este tipo de información puede ser vendida y revendida a un sin número de compradores.

La información es un bien que no podemos cuantificar como por ejemplo los libros o los cd’s, los cuales podemos inventariar mientras que a la información solo se le puede determinar clasificar por su calidad.

1.3.2.Comercio de la información

La información tiene un valor y éste puede ser la base de un comercio.

La piratería de software es un ejemplo de esto, aquí nos damos cuenta del valor que puede tener un programa original y el valor del mismo programa pero en versión pirata. Actualmente se está tratando de combatir este delito una de las medidas es asegurar que el desarrollador de software reciba la compensación justa por el uso y distribución del mismo.

1.3.3.Publicación electrónica

Aquí nos enfrentamos al mismo problema que en el punto anterior, al publicar o distribuir programas, documentos, noticias, música, artículos, juegos, etc. Vía Internet nos debemos de asegurar que los autores realmente reciban la compensación justa por su trabajo.

1.3.4.Protección de datos de una base de datos

El objetivo es proteger la Base de Datos contra accesos no autorizados.

La seguridad de los datos se refiere a la protección de estos contra el acceso por parte de las personas no autorizadas y contra su indebida destrucción o alteración.

Seguridad significa el prevenir y/o detectar la publicación de datos de forma no autorizada de información. En general seguridad se refiere a la protección de los datos en diferentes ambientes, tanto en ambientes militares como en ambientes comerciales.

1.3.5.Delitos informáticos

El delito informático implica actividades criminales carácter tradicional, tales como robos o hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje, etcétera. El uso de métodos informáticos ha creado nuevas posibilidades del uso indebido de las computadoras lo que ha propiciado a su vez la necesidad de regulación por parte del derecho.

Para Carlos Sarzana, en su obra Criminales y Tecnología, los crímenes por computadora comprenden "cualquier comportamiento criminal en el cual la computadora ha estado involucrada como material o como objeto de la acción criminal, como mero símbolo[4]".

Nidia Callegari define al delito informático como "aquel que se da con la ayuda de la informática o de técnicas anexas".

María de la Luz Lima dice que el "delito Electrónico" "en un sentido amplio es cualquier conducta criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, el delito informático, es cualquier acto ilícito en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin".

Entonces los delitos informáticos son todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio informático.

- **Sujeto activo**

[4] Sarzana Carlo, "Criminalità e tecnologia" en Computers Crime. Rassagna Penitenziaria e Criminologia. Nos. 1-2 Año 1. Roma, Italia. P.53

Los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informáticos, aún cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten este tipo de delitos.

El nivel típico de aptitudes del delincuente es tema de controversia ya que para algunos en el nivel de aptitudes no es indicador de delincuencia informática en tanto que otros piensan que los posibles delincuentes informáticos son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico, características que pudieran encontrarse en un empleado del sector de procesamiento de datos.

- **Sujeto Pasivo**

El sujeto pasivo o víctima del delito es el objeto sobre el cual recae la conducta de acción criminal que realiza el sujeto activo, y en el caso de los delitos informáticos las víctimas pueden ser individuos, instituciones crediticias, gobiernos, etcétera que usan sistemas automatizados de información, generalmente conectados a enormes redes de computadoras.

El sujeto pasivo, es sumamente importante para el estudio de los delitos informáticos, ya que mediante él podemos conocer las diferentes intrusiones que cometen los delincuentes informáticos, para si poder diseñar un sistema de seguridad y tomar como modelo el modus operandi de los sujetos activos.

1.3.6.Leyes aplicables en México

El sistema legal se ha adaptado en la medida de sus posibilidades a la tecnología de la computación, reutilizando algunas viejas formas de protección legal como los Derechos de Autor y las Patentes, y creando leyes donde las existentes no se pueden adecuar.

Patentes, Derechos de Autor y Secreto de Mercado son mecanismos legales que protegen los derechos de desarrolladores y propietarios de datos y programas. Un aspecto muy importante en la seguridad en cómputo es controlar el acceso a los programas y los datos; tales mecanismos muchas veces son soportados por la ley.

- **Ley modelo**

Las Naciones Unidas a partir de los años 60 ha estado dedicada a facilitar los procedimientos del comercio internacional, agilizando trámites y reduciendo requisitos excesivos. De allí, desde comienzo de los años 90 que se haya estado preocupando del llamado Intercambio Electrónico de Datos, conocido como ***"EDI"*** por su acrónimo en ingles, a través de la Comisión de las Naciones Unidas para el Desarrollo del Derecho Mercantil Internacional (**CNUDMI**), mejor conocida por su también acrónimo en ingles ***UNCITRAL***, la cual Constituyó un Grupo de Trabajo (conocido como el Working Group en Comercio Electrónico) a fin de elaborar leyes modelos que den soporte legal a los mensajes electrónicos. Este esfuerzo ha

producido la recientemente adoptada Ley Modelo de UNCITRAL sobre el Comercio Electrónico.

El proyecto de Ley Modelo, tomó en cuenta la carencia de uniformidad internacional en lo atinente a la regulación de los conocimientos de embarque negociables, acordándose que, siendo la intención de la Ley Modelo la búsqueda de reglas dirigidas a lograr la uniformidad internacional para el uso y práctica de los conocimientos de embarque electrónicos, la mejor solución sería una ley comprensiva que cubriera todos los tipos de conocimientos de embarque.

En la primera parte de la Ley Modelo, compuesta de quince artículos, se establecen principios generales con el fin de dar el soporte legal al comercio electrónico en aquellos países que promulguen las leyes modelos. Estas serían extremadamente útiles en suministrar el necesario apoyo legal a las Reglas de 1990 del CMI sobre Conocimientos de Embarques Electrónicos. Sin embargo, tales artículos no tienen aplicación directa al comercio marítimo, pero son esenciales si el comercio marítimo se realiza en un ambiente electrónico.

a) Capítulo 1°: se refiere a las provisiones generales, ámbito de aplicación, definiciones, interpretación y modificación mediante acuerdos. La característica principal de este articulo en general es que introduce el término "mensaje de datos", es un término jurídico que se quiso utilizar para identificar lo que es un mensaje en un ambiente electrónico, se ha podido manejar únicamente la palabra mensaje o la palabra aviso, pero bueno, a lo mejor no hubiera tenido el contexto, y no se hubiera entendido su significado.
    - La modificación mediante acuerdo está diseñada para facilitar la libertad del contrato, la interpretación para incitar a los eventuales usuarios e intérpretes de la ley modelo, para que tenga una mente amplia en su aplicación e interpretación, dado su origen internacional.
    - Otro punto interesante es lo que se ha llamado la equivalencia funcional, que es realmente tratar de poner dentro del ambiente electrónico, dentro de estos mensajes de datos, una equivalencia que sea igual a las funciones que se producen o que se logran con el documento de papel.

b) Capítulo 2°: se refiere a la aplicación de los requisitos legales de los mensajes de datos, comenzando por su reconocimiento jurídico, al señalar que no se negarán efectos jurídicos, validez o fuerza probatoria al mensaje de datos, por la sola razón de que está siendo conformada por un mensaje de datos. Este reconocimiento evidentemente es necesario y si se quiere darle una base y un soporte legal a este comercio electrónico, se tiene que dar un soporte legal al mensaje de datos, no se puede admitir que se niegue validez, es decir, que se niegue ante un Tribunal, ante una Corte de Justicia o ante las partes, no pueden negar la existencia de un contrato por

el simple hecho de que el contrato está evidenciado en un mensaje de datos.

c) Capítulo 3° se refiere a la formación y validez de los contratos a través de los mensajes de datos, su reconocimiento por las partes, su atribución, su acuse de recibo, su tiempo y lugar de envío y recepción. Mientras que estos artículos no establecen normas directas, ni necesariamente aplican los conocimientos de embarque electrónicos, podrían ser útiles para definir los derechos y responsabilidades que nacen de los mensajes de datos.

En la segunda parte del proyecto de ley, compuesto de dos artículos (16 y 17) referidos a los contratos de transporte de mercancías, se provee la base legal para la negociación de los documentos de transporte electrónicos, redactados de forma tal que sean aplicables a cualquier tipo de transporte.

a) Articulo 16 se describen y especifican los diversos actos relacionados con los contratos de transporte de mercancía, como por ejemplo indicación de las marcas, el número, la cantidad o el peso de las mercancías, declaración de la índole o el valor de las mercancías, etc.
b) Artículo 17 se establece el principio de la singularidad del mensaje de datos, esto es muy importante, porque para que funcione el comercio electrónico y se pueda dar validez a los mensajes de datos, conformando, por ejemplo, un contrato de transporte, específicamente un conocimiento de embarque electrónico, es necesario que ese documento de embarque sea único, de ahí la condición de singularidad, que no pueda ser modificado, salvo por supuesto para hacer una transferencia o una cesión de los derechos, un endoso, este sistema es parte de la aplicación de la teoría de la equivalencia funcional.

La finalidad de la Guía para la incorporación al derecho interno de la ley modelo de la CNUDMI sobre comercio electrónico es orientar tanto a los Estados poco familiarizados con las técnicas de comunicación como a los estudiosos en la materia de los medios electrónicos en los aspectos jurídicos de su empleo, para la incorporación de su régimen al derecho interno. En la información presentada en esta guía se explica cómo las disposiciones incluidas en la ley modelo enuncian los rasgos mínimos esenciales a toda norma legal destinada a lograr los objetivos de la ley modelo. Esta información también puede ayudar a los Estados a determinar si existe alguna disposición de la ley que tal vez convenga modificar en razón de alguna circunstancia nacional en particular.

La ley modelo ha sido redactada en .seis idiomas -árabe, chino, español, francés, inglés y ruso-, es un texto por el cual se puede lograr la admisión legal del comercio.

Las leyes exigen que los conocimientos de embarque se firmen y en este sentido las preguntas que surgen son ¿quién nos firma? y ¿cómo los firma? Esto ha

ocasionado el surgimiento de las firmas digitales, lo que parece muy fácil, pero para ello se requiere de los sistemas criptográficos, pero entonces, se ha desatado una gran competencia entre las grandes empresas de computación, para que el patrón de firma sea la de su propia empresa. Por lo que han acudido empresas apoyadas por Estados para que hagan una ley sobre los patrones de firmas digitales, que no es ninguna ley, sino sencillamente es una forma de que el programa que ellos tienen en esa empresa, sea el que acoja la comunidad internacional.

En el caso de México, que no tiene unificada su legislación mercantil y civil, delimita claramente las remisiones en sus artículos 1o. y 2o. en cuanto que se aplica el Código Civil Federal que rige en toda la República en asuntos del orden federal, como se ve a continuación:

- Artículo 1. Los actos comerciales sólo se regirán por lo dispuesto en este Código y las demás leyes mercantiles aplicables.
- Artículo 2. A falta de disposiciones de este ordenamiento y las demás leyes mercantiles serán aplicables a los actos de comercio las de los derechos comunes contenidos en el Código Civil aplicable en materia federal.

- **Derechos de Autor**

Desde 1976 la ley de Derechos de Autor ha incluido una definición explicita del software de cómputo.

De cualquier forma los Derechos de Autor puede que no sea la mejor manera de proteger los trabajos de cómputo ya que hay que considerar el algoritmo detrás del programa. El algoritmo es una idea, las líneas del programa es la expresión de esa idea.

La protección de los Derechos de Autor se encamina hacia las líneas de programa no al diseño del mismo. Así el hecho de copiar intacto el código de un programa está prohibido pero reimplementar el algoritmo está permitido.

Otro problema es que cuando un programa se protege bajo los Derechos de Autor, el trabajo debe ser publicado. Un programa puede ser publicado distribuyendo copias del código; pero si el objeto fuente no es distribuido, no se considera que haya sido publicado.

Los Derechos de Autor fueron diseñados para proteger la expresión de las ideas, hace énfasis en que una forma de expresar una idea, pertenece al autor y le da el derecho exclusivo de hacer copias de la expresión de su idea y vendérselas al público, pero sólo el puede hacer la venta de copias de su idea.

- **Patentes**

Las patentes protegen los inventos, fueron creadas para aplicarse a resultados de ciencia, tecnología e ingeniería, mientras que los Derechos de Autor se crearon

clásicamente para proteger el arte, la literatura y trabajos escolares. Una patente puede ser válida para algo que es una novedad o es único, así que sólo puede haber una Patente por cada invento.

Un objeto Patentado también debe ser no obvio. Si un invento resulta obvio para una persona que conoce el área de invención, entonces no se puede otorgar la Patente.

Este tipo de protección no es la apropiada para los algoritmos, ya que los algoritmos no difieren en demasía con otros. Además el tiempo y el dinero que se tienen que invertir para obtener y mantener la Patente, resulta difícil para los generadores de software a pequeña escala el obtener esta protección.

- **Secreto de Mercado**

A diferencia de La Patente o los Derechos de Autor, cierta información obtiene su valor si se mantiene en secreto. El Secreto de Mercado es la información que da una compañía sobre sus competidores. La característica principal es que debe mantenerse en secreto. Si alguien obtiene un Secreto de Mercado de manera inapropiada y con ello obtiene beneficios, el dueño del secreto puede demandar para recobrar los beneficios ganados por el otro, así como daños y perjuicios y costos legales.

Este tipo de ley se aplica muy bien a cuestiones de software de cómputo. Un algoritmo nuevo y original, depende de que nadie más lo conozca. La protección del Secreto de Mercado permite la distribución del resultado de un secreto (en este caso la parte ejecutable de un programa) mientras mantiene el diseño del programa en secreto (el código fuente). Pero el Secreto de Mercado protege en igual medida que los Derechos de Autor, así que el software bajo esta protección no puede combatir contra piratas que venden copias del software sin ningún permiso.

La protección del Secreto de Mercado no sirve de mucho cuando alguien infiere el código estudiando las salidas del programa, o bien decodifica el código objeto. Ya que ambas son actividades legítimas y provocan que el Secreto de Mercado Desaparezca.

Casi toda la información que está almacenada o que es transmitida es susceptible de ataques y casi todas las grandes organizaciones han sido afectadas por algún crimen informático. El constante incremento de redes interconectadas hace que los crímenes sean fáciles. Motivos por los cuales hace necesario que los gobiernos presten más atención a este reto tecnológico en el que estamos envueltos.

En México cualquier acceso no autorizado a un sistema de cómputo, puede ser castigado si se siguen los procedimientos adecuados. Al presentarse una intrusión en un sistema de cómputo, se recomienda avisar a las autoridades correspondientes y solicitar apoyo a las organizaciones especializadas como la CERT-México, PGR, PFP. Acudir al ministerio público a denunciar el ilícito.

1.3.7.Tratamiento internacional

Durante los últimos años se ha ido perfilando en el ámbito internacional un cierto consenso en las valoraciones político-jurídicas de los problemas derivados del mal uso que se hace las computadoras.

En 1983, la Organización de Cooperación y Desarrollo Económico (OCDE) inició un estudio de la posibilidad de aplicar y armonizar en el plano internacional las leyes penales a fin de luchar contra el problema del uso indebido de los programas computacionales.

Las conclusiones político-jurídicas desembocaron en una lista de las acciones que pudieran ser consideradas por los Países por regla general, como merecedoras de pena.

La OCDE en 1986 publicó un informe titulado *Delitos de Informática: análisis de la normativa jurídica*, en donde se presentan las normas legislativas vigentes y se recomienda una lista de ejemplos de uso indebido de las computadoras que los países miembros de la OCDE podrían prohibir y sancionar en leyes penales, como por ejemplo el fraude y la falsificación informáticos, la alteración de datos, sabotaje informático, acceso no autorizado, interceptación no autorizada y la reproducción no autorizada de un programa de computadora protegido.

La Comisión Política de Información, Computadoras y Comunicaciones recomienda también que se instituyan protecciones penales contra otros usos indebidos de las computadoras como el espionaje informático, utilización no autorizada de una computadora, utilización no autorizada de un programa protegido, incluido el robo de secretos comerciales y el acceso o empleo no autorizado de sistemas de computadoras.

A nivel de organizaciones intergubernamentales de carácter universal, en Organización de las Naciones Unidas (ONU), en el marco del Octavo Congreso sobre Prevención del Delito y Justicia Penal, celebrado en 1990 en la Habana Cuba, se dijo que la delincuencia relacionada con la informática era consecuencia del mayor empleo del proceso de datos en las economías y burocracias de los distintos países y que por ello se había difundido la comisión de actos delictivos.

En general, se supuso que habría un gran número de casos de delitos informáticos no registrados. Por todo ello, en vista que los delitos informáticos eran un fenómeno nuevo, y debido a la ausencia de medidas que pudieran contrarrestarlos, se consideró que el uso deshonesto de las computadoras podría tener consecuencias desastrosas. A este respecto, el Congreso recomendó que se establecieran normas y directrices sobre la seguridad de las computadoras a fin de ayudar a la comunidad internacional a hacer frente a estas formas de delincuencia.

- **Legislación en otros países**

Pocos son los países que disponen de una legislación adecuada para enfrentarse con el problema de los delitos informáticos, sin embargo existen con objeto de que otros países tomen cartas en el asunto y a su vez tomen en cuenta las medidas adoptadas por estos.

o Alemania

En Alemania para hacer frente a la delincuencia relacionada con la informática a partir del 1 de agosto de 1986, se adoptó la Segunda Ley contra la Criminalidad Económica en la que se contemplan los siguientes delitos:

Espionaje de datos, estafa informática, alteración de datos, Sabotaje informático, utilización abusiva de cheques o tarjetas de crédito.

Sobre los delitos informáticos, estas medidas fueron también adoptadas por los Países Escandinavos y en Austria.

o Austria

Ley de reforma del Código Penal de 22 de diciembre de 1987. Esta ley contempla los siguientes delitos:

Destrucción de datos, estafa informática.

o Francia

Ley número 88-19 de 5 de enero de 1988 sobre el fraude informático.

Acceso fraudulento a un sistema de elaboración de datos, sabotaje informático, destrucción de datos, falsificación de documentos informatizados, uso de documentos informatizados falsos.

o Estados Unidos

La adopción en los Estados Unidos en 1994 del Acta Federal de Abuso Computacional que modificó el Acta de Fraude y Abuso Computacional de 1986.

Con la finalidad de eliminar los argumentos técnicos acerca de qué es y qué no es un virus, un gusano, un Caballo de Troya, etcétera y en que difieren de los virus, la nueva acta proscribe la transmisión de un programa, información, códigos o comandos que causan daños a la

computadora, al sistema informático, a las redes, información, datos o programas. La nueva ley es un adelanto porque está directamente en contra de los actos de transmisión de virus.

El Acta diferencia el tratamiento a aquellos que de manera accidental lanzan ataques de virus de aquellos que lo hacen con la intención de hacer estragos. El castigo es de hasta 10 años en prisión federal más una multa, y para aquellos que lo transmiten sólo de manera imprudencial la sanción fluctúa entre una multa y un año en prisión.

Esta Acta aclara que el creador de un virus no debe escudarse en el hecho que no conocía que con su actuar iba a causar daño a alguien o que él solo quería enviar un mensaje.

En opinión de los legisladores estadounidenses, la nueva ley constituye un acercamiento más responsable al problema de los virus informáticos, no definiendo a los virus sino describiendo el acto para dar cabida en un futuro a la nueva era de ataques tecnológicos a los sistemas informáticos en cualquier forma en que se realicen. Diferenciando los niveles de delitos, la nueva ley da lugar a que se contemple qué se debe entender como acto delictivo.

En el Estado de California, en 1992 se adoptó la Ley de Privacidad en la que se contemplan los delitos informáticos pero en menor grado que los delitos relacionados con la intimidad que constituyen el objetivo principal de esta Ley.

Las enmiendas realizadas a la Sección 502 del Código Penal relativas a los delitos informáticos en la que, entre otros, se amplían los sujetos susceptibles de verse afectados por estos delitos, la creación de sanciones por cada persona afectada y por el acceso imprudencial a una base de datos, etcétera.

El objetivo de los legisladores al realizar estas enmiendas, es la de aumentar la protección a los individuos, negocios, y agencias gubernamentales de la interferencia, daño y acceso no autorizado a las bases de datos y sistemas computarizados creados legalmente. Asimismo, los legisladores consideraron que la proliferación de la tecnología de computadoras ha traído consigo la proliferación de delitos informáticos y otras formas no autorizadas de acceso a las computadoras, a los sistemas y las bases de datos y que la protección legal de todos sus tipos y formas es vital para la protección de la intimidad de los individuos así como para el bienestar de las instituciones financieras, de negocios, agencias, gubernamentales y otras relacionadas con el estado de California que legalmente utilizan esas computadoras, sistemas y bases de datos.

- Chile

  Chile fue el primer país latinoamericano en sancionar una Ley contra delitos informáticos, la cual entró en vigencia el 7 de junio de 1993. Esta ley se refiere a los siguientes delitos: La destrucción o inutilización de los de los datos contenidos dentro de una computadora es castigada con penas de prisión. Asimismo, dentro de esas consideraciones se encuentran los virus. Conducta maliciosa tendiente a la destrucción o inutilización de un sistema de tratamiento de información o de sus partes componentes o que dicha conducta impida, obstaculice o modifique su funcionamiento. Conducta maliciosa que altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información.

- España

  En el Nuevo Código Penal de España, se establece que aquel que cause daños en propiedad ajena, se le aplicará pena de prisión o multa. En lo referente a: La realización por cualquier medio de destrucción, alteración, inutilización o cualquier otro daño en los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos. El nuevo Código Penal de España sanciona en forma detallada esta categoría delictiva (Violación de secretos/Espionaje/Divulgación), aplicando pena de prisión y multa. En materia de estafas electrónicas, el nuevo Código Penal de España, solo tipifica las estafas con ánimo de lucro valiéndose de alguna manipulación informática, sin detallar las penas a aplicar en el caso de la comisión del delito.

CAPÍTULO 2

ESQUEMAS DE SEGURIDAD BASADOS EN ESTÁNDARES INTERNACIONALES

2. ESQUEMAS DE SEGURIDAD BASADOS EN ESTÁNDARES INTERNACIONALES

En la actualidad la seguridad de la información ha tenido un gran auge dentro de las pequeñas y grandes organizaciones así como la preocupación de los usuarios de los sistemas de cómputo por mantener seguros sus equipos es cada vez mayor pero para lograr esto y homogeneizarlos, se crearon estándares a nivel mundial, para con ello cumplir con la necesidad de tener un modelo en común.

2.1. Criterios Comunes (CC)

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

CCIT-SE (Common Critería for Information Technology Security Evaluation) mejor conocido como CC versión 2.1, aprobada en agosto de 1999, fue adoptada por ISO como Criterios Comunes para la Evaluación de las Tecnologías de Información (ISO/IEC 15408) en diciembre de 1999.

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

En la evaluación de las propiedades de seguridad de los productos, existen tres grupos que tienen interés general en la misma: los consumidores, los desarrolladores y evaluadores como lo observaremos en la Tabla 2.1.

	Consumidores	Desarrolladores	Evaluadores
Parte 1 : Introducción y Modelo general	Como información referencial	Como información referencial para definir requerimientos y formular especificaciones de seguridad para TOE's.	Como información referencial. Como estructura de soporte para ST's y PP's.
Parte 2 : Requerimientos de Seguridad Funcional	Como soporte y referencia en la formulación y declaración de requerimientos de funciones de seguridad	Como referencia cuando se interpretan las declaraciones de requerimientos y la formulación de especificaciones funcionales de las TOE's	Criterios de evaluación mandatorios para determinar si un TOE presenta efectivamente las funciones de seguridad
Parte 3 : Requerimientos de aseguramiento	Como soporte para determinar los niveles de aseguramiento requeridos	Como referencia para interpretar requerimientos de aseguramiento y determionar los alcances de aseguramiento de los TOE's	Criterios de evaluación mandatorios para determinar el aseguramiento de los TOE's y para evaluar los PP's y ST's

TABLA 2.1 " INTRODUCCIÓN A LOS CRITERIOS COMUNES"

Donde:

TOE (Target of evaluation) es el producto o sistema de TI que se quiere evaluar. ST (Security Target) es el objetivo de seguridad, es decir, es una estructura formal que comprende las amenazas al TOE, los requisitos de seguridad y el resumen de las especificaciones de las funciones de seguridad y medidas de aseguramiento implementadas en el TOE. El ST es la base para un acuerdo contractual entre desarrolladores, evaluadores y consumidores.

PP (Protection Profile) es un perfil o estructura formal que especifica, el entorno donde se usará el TOE, los ST y los requisitos de seguridad que el TOE debe satisfacer para alcanzar los ST.

La evaluación parte de la descripción de los requisitos de seguridad de un determinado sistema o componente y puede realizarse de manera genérica o particular para un ST. Una categoría de productos o sistemas de TI tienen una serie de requisitos, objetivos y amenazas respecto a su seguridad, los mismos que se encuentran descritos en el PP, un perfil de protección (PP) responde a las demandas de los consumidores en lo que respecta a la seguridad. Un cliente o consumidor de TI puede utilizar las evaluaciones como ayuda para decidir si un producto o sistema satisface sus necesidades de seguridad, los CC proporcionan una estructura formal para estas necesidades, es decir el PP.

Paralelamente un desarrollador usa un ST, estructura formal aplicable a un producto específico con el que identifica los requisitos satisfechos por su TOE. Los CC describen el conjunto de acciones generales que el evaluador debe llevar a cabo y los procedimientos a seguir se encuentran especificados en el Common Evaluation Methodology (CEM).

Los Criterios Comunes (versión 2.1) están formados básicamente por tres partes: introducción y modelo general, requerimientos de seguridad funcional y requerimientos de garantía de seguridad

Parte 1. Introducción y modelo general

Esta parte está dirigida a las personas que tienen nociones acerca de la evaluación de seguridad ya que introduce los conceptos generales y el formato de los Criterios Comunes. Aquí se describe cómo fueron establecidos los CC y para quiénes están destinados. Además, elabora sobre la definición de funcionalidad de seguridad, requisitos de confiabilidad y las estructuras de perfiles de protección y metas de seguridad.

Parte 2. Requerimientos de seguridad funcional

Estos requerimientos están destinados a los usuarios y desarrolladores, pues establecen un conjunto de componentes de seguridad funcional como un estándar el cual expresa los requerimientos de seguridad funcional para los productos IT. Los componentes funcionales presentados son para utilizarse en los perfiles de protección y metas de seguridad.

Los requerimientos funcionales están organizados en once clases, denominadas clases de requerimientos funcionales y cada una de ellas cubre las necesidades de un área muy particular de la seguridad, a su vez, cada clase funcional se descompone en una o más familias funcionales, las cuales tratan de forma específica los diferentes aspectos que conforman en su totalidad a la clase en cuestión. Así, las familias funcionales contienen uno o más componentes, y cualquiera de ellos puede seleccionarse para incluirlo en el perfil de protección.

El propósito de esta sección es proporcionar información a los usuarios para la selección de un componente funcional apropiado, una vez que la clase y a su vez la familia ha sido identificada como un ente necesario o parte útil de sus requerimientos de seguridad. Las operaciones permitidas son:

- Iteración: permite a un componente ser usado más de una vez con operaciones variables.
- Asignación: permite la especificación de un parámetro identificado.
- Selección: permite la especificación de uno o más elementos de una lista.
- Refinamiento: permite la adición de detalles.

Para alcanzar los objetivos de seguridad identificados, el objeto de seguridad debe incluir requerimientos funcionales que especifiquen las funcionalidades de seguridad que deben implementarse en el producto o sistema evaluado.

Estos requerimientos están agrupados, en la segunda parte de los Criterios Comunes, en once rubros genéricos:

1. Clase FAU: Auditoría de seguridad

Auditar la seguridad involucra reconocimiento, registro, almacenamiento y análisis de información relacionada a las actividades relevantes de la seguridad. El resultado de los registros de la auditoría puede ser examinado para determinar cuáles actividades relevantes de seguridad ocurrieron y qué usuario es responsable de ellas. Sus familias son:

- FAU_ARP (Respuesta automática de auditoría de seguridad).
- FAU_GEN (Generación de datos de auditoría de seguridad
- FAU_SAA (Análisis de auditoría de seguridad).
- FAU_SAR (Revisión de la auditoría de seguridad).
- FAU_SEL (Selección del evento de auditoría de seguridad).
- FAU_STG (Almacenamiento del evento de auditoría de seguridad

2. Clase FCO: Comunicación

Esta clase proporciona dos familias que aseguran la identidad de un grupo participante en el intercambio de datos. Estas familias están destinadas a garantizar la identidad del creador de la información transmitida (prueba de origen) y de igual forma, probar la identidad del receptor de la información transmitida (prueba de receptor). Estas familias aseguran que un creador no puede negar haber enviado el mensaje, ni el receptor puede negar haberlo recibido.

- FCO_NRO (No repudio de origen).
- FCO_NRR (No repudio de receptor).

3. Clase FCS: Soporte de cifrado

Las funciones de seguridad de la TOE pueden emplear operaciones de cifrado para ayudar a satisfacer requerimientos de seguridad de alto nivel. Estos incluyen: identificación y autenticación, no repudio, camino confiable, canal confiable y separación de datos.

Esta clase se utiliza cuando el objeto de evaluación implanta funciones de cifrado, la implantación de las cuales podría ser en hardware, firmware o software.

- FCS_CKM (Administración de claves de cifrado).
- FCS_COP (Operación de cifrado).

4. Clase FDP: Protección de datos de usuario

Esta clase contiene familias relacionadas con los requisitos para las funciones de seguridad de la TOE y las políticas de función de seguridad relacionadas con la protección de datos de usuario. FDP está dividida en cuatro grupos.

- Políticas de función de seguridad de protección de datos de usuario
  - FDP_ACC (Política de control de acceso).
  - FDP_IFC (Política de control de flujo de información).

- Formas de protección de datos de usuario
  - FDP_ACF (Funciones de control de acceso).
  - FDP_ACC, la cual especifica el ámbito de control de la política en cuestión.
  - FDP_IFF (Funciones de control de flujo de información).
  - FDP_ITT (Transferencia TOE interna).
  - FDP_RIP (Protección de información residual
  - FDP_ROL (Retroceso).
  - FDP_SDI (Integridad de datos almacenados).

- Almacenamiento, importación y exportación a distancia en línea
  - FDP_DAU (Autenticación de datos).
  - FDP_ETC (Exportación al exterior del control de las funciones de segundad del objeto de evaluación).
  - FDP_ITC (Importación del exterior del control de las funciones de seguridad del objeto de evaluación).

- Comunicación entre las funciones de seguridad del objeto de evaluación
  - FDP_UCT (Protección de transferencia de confidencialidad de datos de usuario entre las funciones de seguridad del objeto de evaluación).
  - FDP_UIT (Protección de transferencia de integridad de datos de usuario entre las funciones de seguridad del objeto de evaluación).

5. Clase FIA: Identificación y autenticación

Esta clase está dedicada a los requerimientos de funciones para establecer y verificar una identidad de usuario. En esta parte se les da atributos de seguridad a los usuarios, ya que es fundamental para la puesta en marcha de las políticas de seguridad definidas. Las familias que componen esta clase son:

- FIA_AFL (Fallas de autenticación).
- FIA_ATD (Definición de atributos de usuario).-
- FIA_SOS (Especificación de secretos).
- FIA_UAU (Autenticación de usuario).

- FIA_UID (Identificación de usuario).
- FIA_USB (Enlace usuario-sujeto).

6. Clase FMT: Administración de la seguridad

Esta clase se ha desarrollado para especificar la administración de varios aspectos de las funciones de seguridad de los objetos de evaluación: atributos de seguridad, datos de las funciones de seguridad, y las funciones mismas.

- FMT_MOF (Administración de funciones en TSF).
- FMT_MSA (Administración de atributos de seguridad).
- FMT_MTD (Administración de datos de las funciones de seguridad del objeto de evaluación).
- FMT_REV (Revocación).
- FMT_SAE (Vigencia de atributos de seguridad).
- FMT_SMR (Perfiles de administración de la seguridad).

7. Clase FPR: Privada

Esta clase contiene los requerimientos de privacía, los cuales proporcionan a un usuario protección contra la revelación y mal uso de la identidad por parte de otros usuarios. Sus familias son:

- FPR_ANO (Anonimato).
- FPR_PSE (Pseudonimia).
- FPR_UNL (Imposibilidad de asociación).
- FPR_UNO (Inobservabilidad).

8. Clase FPT: Protección de las funciones de seguridad del objeto de evaluación

Las familias que se mencionan a continuación relacionan la integridad y la administración de los mecanismos que proporcionan las funciones de seguridad de la TOE (independientemente de las políticas de seguridad específicas) y a la integridad de los datos de las funciones de seguridad (independientemente de los contenidos específicos de los datos de las políticas de seguridad). En cierto sentido, puede parecer que las familias en esta clase duplican componentes de la clase FDP (Protección de datos de usuario), las cuales pueden ser regularmente implantadas usando los mismos mecanismos, no obstante, FDP se enfoca a la protección de datos de usuario, mientras que FPT se enfoca a la protección de datos de las funciones de seguridad del objeto de evaluación, de hecho, los componentes de la clase FPT son necesarios para proporcionar requerimientos de las políticas de seguridad en el objeto de evaluación y que no pueden ser alteradas o eludidas.

Los datos de las funciones de seguridad, son la base de los datos administrativos y son éstos los que se refieren a la puesta en vigor de las políticas de seguridad.

Las familias que constituyen esta clase son:

- FPT_AMT (Prueba de la máquina abstracta subyacente).

- FPT_FLS (Seguro ante fallas).
- FPT_ITA (Disponibilidad de datos exportados de las funciones de seguridad del objeto de evaluación).
- FPT_ITC (Confidencialidad de datos exportados de las funciones de seguridad del objeto de evaluación).
- FPT_ITI (Integridad de datos TSF exportados).
- FPT_ITT (Transferencia interna de datos objeto de evaluación-funciones de seguridad).
- FPT_PHP (Protección física de las funciones de seguridad del objeto de evaluación).
- FPT_RCV (Recuperación confiable).
- FPT_RPL (Detección de retransmisión).
- FPT_RVM (Medición de referencia)
- FPS_SEP (Separación de dominio)
- FPT_SSP (Protocolo de sincronía de estado)
- FPT_STM (Sellos de tiempo)
- FPT_TDC (Consistencia de datos de funciones de seguridad entre funciones de seguridad).
- FPT_TRC (Consistencia de retransmisión de datos de funciones de seguridad dentro del objeto de evaluación).
- FPT_TST (Autoverificación de las funciones de seguridad del objeto de evaluación)

9. Clase FRU: Utilización de los recursos

Esta clase proporciona tres familias que fundamentan la disponibilidad de recursos requeridos tales como capacidad de procesamiento y capacidad de almacenamiento.

- FRU_FLT (Tolerancia a fallas)
- FRU_PRS (Prioridad de servicio)
- FRU_RSA (Asignación de recursos)

10. Clase FTA: Acceso a la TOE

Esta clase especifica los requerimientos funcionales para controlar la sesión del usuario. Las familias que las componen son:

- FTA_LSA (Limitación en el ámbito de atributos seleccionables)
- FTA_MCS (Limitación en sesiones concurrentes múltiples)
- FTA_SSL (Cierre de sesión)
- FTA_TAB (Banderas de acceso del objeto de evaluación)
- FTA_TAH (Historia de acceso del objeto de evaluación)
- FTA_TSE (Establecimiento de sesión del objeto de evaluación)

11. Clase FTP: Caminos / Canales confiables

En esta clase se proporcionan los requerimientos necesarios para establecer un camino de comunicación confiable entre los usuarios y las funciones de seguridad, y así mismo con otros productos IT.

Debemos entender por canal confiable es un medio en el cual se puede iniciar la comunicación por ambos extremos del canal y el cual proporcionará características de no repudio con respecto a la identidad de los extremos del canal.

Y un camino confiable es el medio en donde los usuarios ejecutan funciones a través de la interacción directa garantizada con las funciones de seguridad. Por lo regular se utilizan para que el usuario realice actividades de identificación inicial o autenticación.

- FTP_ITC (Canal confiable entre funciones de seguridad)
- FTP_TRP (Camino confiable)

2.1.1. Los requerimientos de aseguramiento

Los requerimientos de aseguramiento definen los criterios que hay que aplicar para la evaluación del producto o sistema. Estos requerimientos han sido extraídos de la parte 3 de los Criterios Comunes.

1. Clase ACM (Administración de la configuración)

Esta clase permite asegurar que se ha preservado la integridad de la TOE mediante el requerimiento de disciplina y control en los procesos de refinamiento y modificación del objeto de evaluación y cualquier otra información relacionada; también, previene de modificaciones no autorizadas, adiciones o supresiones a la TOE, y de esta manera, se garantiza que el objeto de evaluación y la documentación empleada para su evaluación están listas para ser distribuidas.

2. Clase ADO (Distribución y operación)

Define los requerimientos para las medidas, procedimientos, y estándares relacionados con la distribución segura, instalación y uso operacional del objeto de evaluación, asegurando que la protección de seguridad ofrecida por el objeto de evaluación no ha sido comprometida durante su transferencia, instalación, inicialización, y operación.

3. Clase ADV (Desarrollo)

Se explican los requerimientos para el refinamiento de las funciones de seguridad paso a paso, desde la especificación del objeto de evaluación hasta llegar a su implantación actual. Cada una de las representaciones de las funciones de seguridad resultantes proporcionan información para ayudar al evaluador a determinar si los requerimientos funcionales del objeto de evaluación fueron considerados y reunidos.

4. Clase AGD (Documentos guía)

La clase de garantía AGD define requerimientos que se refieren a la comprensión, la cobertura y la documentación operacional proporcionada por el desarrollador. Esta documentación, proporciona dos categorías de información, para usuarios y para administradores, las cuales son un factor importante en la operación segura de un objeto de evaluación.

5. Clase ALC (Soporte del ciclo de vida)

Se definen los requerimientos de garantía a través de la adopción de un modelo de ciclo de vida bien definido para todos los pasos del desarrollo de la TOE, incluyendo procedimientos y políticas que permitan solucionar posibles fallas o daños, técnicas para el correcto uso de herramientas, y las medidas de seguridad usadas para proteger el entorno de desarrollo.

6. Clase ATE (Pruebas)

La clase de garantía ATE indica los requerimientos de prueba que demuestran que las funciones de seguridad satisfacen los requerimientos funcionales de seguridad del objeto de evaluación.

7. Clase AVA (Evaluación de la vulnerabilidad)

Esta clase define los requerimientos que se refieren a la identificación de vulnerabilidades explotables. Específicamente, se refiere a aquellas vulnerabilidades introducidas en la construcción, operación, mal uso, o configuración incorrecta del objeto de evaluación.

2.1.2. Niveles de Garantía

El nivel de aseguramiento (EAL) corresponde a una selección particular de requerimientos de aseguramiento.

El resultado de la evaluación es una confirmación o una refutación de que el objeto de evaluación satisface sus objetivos de seguridad con la confianza correspondiente al nivel de evaluación pretendido. El descubrimiento de una vulnerabilidad aprovechable en el nivel considerado origina un resultado negativo de la evaluación.

El organismo de certificación otorga la certificación cuando todas las tareas de evaluación han permitido establecer que el producto o sistema cumple con los objetivos de seguridad y no posee vulnerabilidades aprovechables.

Los CC definen 7 niveles de evaluación de aseguramiento (EAL, Evaluation Assurance Level), para cuya evaluación se exige un rigor y formalismo progresivos en el diseño y la construcción del TOE, se tiene en cuenta además la fortaleza de

los mecanismos de seguridad del TOE, según el tipo de ataque que se espere contra él. Los EAL son los siguientes:

- EAL1 - functionally tested - Este nivel proporciona una evaluación del TOE, en las condiciones en que éste se encuentra disponible al cliente, incluye un chequeo de las especificaciones y también de la documentación de soporte que entregue el proveedor. Se pretende que la evaluación EAL1 pueda ser llevada a cabo de manera satisfactoria sin la asistencia del desarrollador del TOE y con un mínimo presupuesto. Esta evaluación es aplicable cuando se requiere evidencia de si el TOE funciona de una manera consistente con su documentación, pero las amenazas a su seguridad no son vistas como algo serio, el análisis se basa en el chequeo independiente de las funciones de seguridad del TOE. El EAL1 proporciona un incremento significativo de aseguramiento sobre un producto o sistema de TI no evaluado.
- EAL2 - structurally tested - Este nivel proporciona aseguramiento mediante el análisis de las funciones de seguridad usando las especificaciones, la documentación de soporte y diseño de alto nivel del TOE, para comprender el comportamiento de su seguridad. El EAL2 representa un incremento significativo de aseguramiento comparado con el EAL1, por los requerimientos de chequeo del desarrollador, el análisis de vulnerabilidad y la evaluación de la funcionalidad basada en, especificaciones mas detalladas del TOE. Es aplicable cuando desarrolladores o usuarios requieren un nivel de bajo a moderado de aseguramiento. La inversión de costo y tiempo no se incrementa sustancialmente.
- EAL3 - methodically tested and checked - Este nivel proporciona aseguramiento a través del uso de controles del ambiente de desarrollo, manejo de la configuración del TOE y evidencia de procedimientos de entrega seguros, el análisis es soportado por el chequeo independiente de las funciones de seguridad del TOE, evidencias de las pruebas del desarrollador basadas en especificaciones funcionales y diseño de alto nivel, análisis de funciones y de vulnerabilidades. El incremento de aseguramiento sobre el EAL2 está dado por los requerimientos de una cobertura mas amplia de chequeo de funciones, mecanismos y procedimientos de seguridad del TOE, que proporcionan confianza en que no habrá interferencias durante el desarrollo.
- EAL4 - methodically designed, tested and reviewed - Una evaluación EAL4 proporciona un análisis soportado por el diseño de bajo nivel de los módulos del TOE y una parte de la implementación. El test se basa en un análisis de vulnerabilidades, y aunque es riguroso no requiere de manera sustancial conocimientos especiales u otros recursos. Los controles de desarrollo se basan en el modelo de ciclo-de-vida, identificación de herramientas y el manejo automático de configuración. El EAL4 es el más alto nivel en el que es económicamente posible reajustar una línea de productos existente.
- EAL5 - semiformally designed and tested - Proporciona un análisis que incluye la implementación completa. El aseguramiento es incrementado por

un modelo formal de las políticas de seguridad del TOE, una presentación semiformal de las especificaciones funcionales y del diseño de alto nivel, y una demostración semiformal de la correspondencia entre éstos. En este nivel de evaluación se requiere el diseño modular del TOE y el análisis de covert channels (canales ocultos o canales ilícitos de flujo de información). El análisis de vulnerabilidades debe asegurar resistencia a la penetración de atacantes cuya fortaleza sea moderada.

- EAL6 - semiformally verified design and tested - El EAL6 es aplicable al desarrollo de TOE's especialmente seguros, para situaciones de alto riesgo en las que el valor de los recursos protegidos justifica los costos adicionales. La evaluación se basa en un análisis modular y por capas del diseño, el análisis de vulnerabilidades debe asegurar resistencia a la penetración de atacantes cuya fortaleza sea alta, la búsqueda de covert channels debe ser sistemática.
- EAL7 - formally verified design and tested - Es aplicable al desarrollo de TOE's para aplicaciones en situaciones de extremado riesgo, y cuando el valor de los recursos a proteger justifica los altos costos. Para una evaluación EAL7 se requiere una presentación formal de las especificaciones funcionales y del diseño de alto nivel, y que exista correspondencia entre ambos, el análisis incluye todo lo necesario para los niveles anteriores y además la validación de un análisis sistemático de covert channels.

Los EAL's de CC han sido desarrollados con el objetivo de preservar los conceptos de aseguramiento bosquejados en los Criterios que los anteceden y que son su base, de esta manera los resultados de evaluaciones previas a los CC continúan siendo relevantes. En la tabla 2.2 que se presenta a continuación, se establece una equivalencia entre niveles de distintos Criterios, equivalencia que no hay que tomar al pie de la letra pues los niveles de aseguramiento no son tratados de la misma manera en los distintos criterios y por tanto una semejanza directa exacta no existe.

Common Criteria	US TCSEC	European ITSEC
-	D: Protección Mínima	EO
EAL1	-	-
EAL2	CI: Seguridad Discrecional	EI
EAL3	C2: Acceso Controlado	E2
EAL4	BI: Seguridad Etiquetada	E3
EAL5	B2: Protección Estructurada	E4
EAL6	B3: Dominios de Seguridad	E5
EAL7	AI: Seguridad Verificada	E6

TABLA 2.2 "INTRODUCCIÓN A LOS CRITERIOS COMUNES "

Este acuerdo, denominado Arrangement (Arreglo) tiene un impacto previsible reflejado en los datos sobre el mercado de TI que proporciona el EITO (European Information Technology Observatory). El conjunto de los países miembros del Arreglo representaban más del 65% del mercado mundial, esto en 1999.

Este Arreglo se gestiona por un Comité, cuya primera presidencia corresponde a Alemania y fue firmado en coincidencia con la Primera Conferencia Internacional de Criterios Comunes a la que asistieron expertos de 23 países.

El Arreglo parte de la premisa de que la utilización de productos y sistemas de TI, cuya seguridad ha sido certificada, es una de las salvaguardas principales para proteger la información y los sistemas que la manejan.

Los Organismos de Certificación reconocidos son los encargados de expedir certificados de seguridad a productos o sistemas de TI, o a perfiles de protección, que hayan sido previamente evaluados por Servicios de Evaluación, conforme a los CC, y cuyo resultado haya sido satisfactorio.

El Arreglo consta de 18 artículos, 11 anexos y un apéndice, a lo largo de los cuales especifica con detalle los requisitos que han de cumplir los Certificados de

CC, los Organismos de Certificación y los Servicios de Evaluación, esto entre otros aspectos.

Los CC establecen un conjunto de requisitos que permiten definir las funciones de seguridad de productos y sistemas de TI y de los criterios necesarios para evaluar su seguridad, el proceso de evaluación garantiza que las funciones de seguridad de dichos productos y sistemas reúnen los requisitos que declaran. Los resultados y las evaluaciones realizadas por Servicios de Evaluación independientes entre sí, son equivalentes en su totalidad.

Entre los objetivos del Arreglo, figuran:

- Asegurar que las evaluaciones realizadas a productos y/o sistemas de TI, o a perfiles de protección (adecuados a cada caso), hayan sido hechas bajo normas rigurosas y consistentes.
- Propiciar el incremento de los productos y sistemas de TI, y de los perfiles de protección evaluados, con nivel de seguridad en aumento, disponibles en el mercado.
- Que gracias a la aceptación internacional de los certificados, se elimine la carga, en distintos países, que acarrea la duplicación de las evaluaciones de productos y sistemas de TI, y/o perfiles de protección.
- Disminuir los gastos de evaluación y certificación de productos y sistemas de TI, y/o perfiles de protección, en razón de la economía de escala.

2.2.Perfiles de Protección (PP)

La finalidad de un Perfil de Protección es la de ser reutilizada y definir requerimientos de la TOE (objeto de evaluación) que se sabe son útiles y efectivos en la reunión de los objetos identificados, además contiene los fundamentos de los objetivos y requerimientos de seguridad.

a) Propósito

- Presentar en forma rigurosa un problema de seguridad que afecte a un conjunto o colección de sistemas.
- Especificar lo requerimientos de seguridad que resolverán dicho problema.
- La implementación de esos requerimientos.

b) Definición

Es un conjunto estándar de requerimientos de seguridad que pueden ser satisfechos por uno o más productos, por sistemas que tienen un fin común dentro de una organización.

Se puede orientar a un entorno u objetivo específico (sistema operativo, bases de datos, firewalls, etc.), o también a un conjunto de productos agrupados en un sistema (redes de datos, área de cómputo, laboratorios, etc.).

En resumen podemos decir que un PP es una explicación de lo que quiere proteger un usuario y de lo que quiere llegar a lograr, un documento de diseño de seguridad, y un camino que nos lleve del “qué es” al “cómo lograrlo”.

El lector primario de un PP es el dueño de la misión/organización, pero también es de gran utilidad a los usuarios, desarrolladores, evaluadores y auditores, ya que los requerimientos son en base a las necesidades de los usuarios.

Como principalmente se trata de una explicación de las necesidades de seguridad que requiere la organización, el esquema de seguridad que se desarrolle le pertenece al dueño de la información.

El analista y experto de seguridad, debe comprender completamente la misión de la organización y en este sentido puede decir tanto lo que espera como lo que no, del entorno.

c) Uso

Ya que se trata de una explicación detallada lo que requiere el usuario el lenguaje deberá ser claro.

Al plasmar una necesidad y explicarla claramente puede ser satisfecha mediante diversos productos, de manera que una organización puede usar uno o varios PP para solucionar sus problemas, pero es requisito indispensable que dichos perfiles sean redactados según indican los criterios comunes (CC) para que sean validos.

2.2.1. Estructura de los perfiles de protección

Los Criterios Comunes tienen como finalidad evaluar si un PP es completo, consistente, y técnicamente válido para que sea conveniente utilizarlo como un informe de requerimientos para un entorno de seguridad.

Así, un PP deberá presentarse como un documento dirigido al usuario donde deberá ajustarse a los lineamientos de los CC.

La estructura que se presenta a continuación, es la forma en cómo se ha construido la metodología de perfiles de protección y la cual se basa en el seguimiento de los puntos contemplados de manera general en el Diagrama 1.

a) Introducción

1. En el documento administrador se identificará al PP que nos proporcionará la información necesaria y descriptiva para identificar, clasificar, registrar y cruzar referencias en un PP.

2. Panorama del PP, esta parte deberá ser lo suficientemente detallada a manera que el lector desde que empiece a leer la introducción para poder determinar sin que quepa la menor duda que el PP descrito se adecua a los intereses para la organización. En general esta parte debe contener un resumen ejecutivo (lo que el dueño o directivo de la organización tiene que ver), una explicación clara y concisa del problema

ha resolver y como se dará solución al mismo. También contendrá una síntesis clara sobre el contenido técnico del PP.

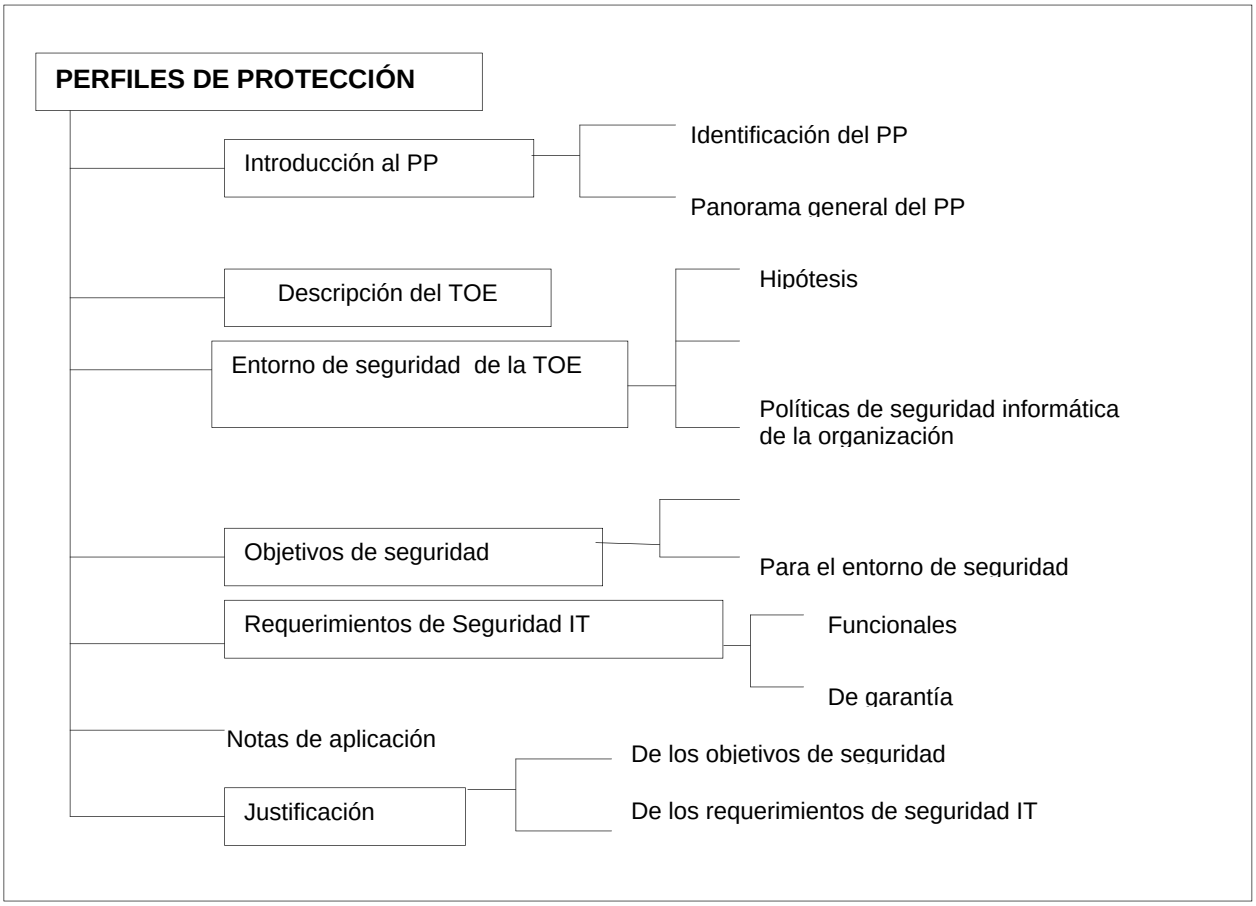


DIAGRAMA 2.1 CONTENIDO DEL PERFIL DE PROTECCIÓN

b) Descripción del objeto de la evaluación

A fin de saber cuáles son los requerimientos de seguridad que necesitan. Al mismo tiempo la información presentada se irá revisando para verificar si existe inconsistencia alguna, en caso de que las haya. Como un PP por lo regular hace referencia a una implantación específica, se pueden asumir las características que se describen en este apartado. Aparte de esto si la TOE es un producto o sistema el cual su principal función es la seguridad. Esta parte del PP la podemos utilizar para describir el amplio contexto de aplicación dentro del cual se aplicará. Dentro de esta parte también se debe añadir ¿Qué es el objeto de evaluación y cuál es su entorno?.

Este documento va dirigido principalmente al técnico administrador, incluye una descripción funcional, la cual debe ir más allá de la descripción de características de seguridad (a menos que la TOE sea un producto que sirve en especifico para la seguridad). Debe contener una descripción que informe los límites de la TOE, lo

que quiere decir que debe aclarar que esta dentro de la TOE y que esta fuera de sus alcances.

c) Entorno de seguridad

Aquí se describirá todo lo referente a la seguridad del entorno en la que se pretende utilizar la TOE y la forma como se espera éste sea empleado, de manera que debe contener los siguientes datos a describir hipótesis, amenazas, las políticas de seguridad organizacional. Se deberá considerar todo aquello que interactúe con la TOE y su entorno por ejemplo: los sistemas físicos y lógicos, tipos de usuarios, hardware y software.

En resumen el entorno de seguridad debe estar enfocado a las necesidades del usuario para facilitar la definición de requerimientos, sin olvidar que se deben considerar los diversos factores con los que interactúa, así como los alcances que tendrá sobre el entorno tomando en cuenta las que no se resolverán en otros ámbitos. También identifica las amenazas a las que está expuesto la TOE y determina las políticas de seguridad que deberán operar para resguardar el entorno.

d) Hipótesis

Por medio de la hipótesis se mostrarán aspectos de seguridad del entorno, o cual debe incluir: información de cómo se utilizará la TOE, información acerca del entorno E Lo que querremos decir es que en base al entorno y a la interacción con los diversos elementos se establece la hipótesis, donde se considerará como debe comportarse de manera segura la TOE. No se deben incluir detalles de las funciones de seguridad en la definición de hipótesis. Cada hipótesis deberá tener su nombre o etiqueta para facilitar las referencias.

e) Amenazas

Primero debemos tomar en cuenta aquellas que atentan contra los bienes de la organización y contra las cuales queremos protegernos haciendo énfasis en la TOE y su entorno de tal forma que el apartado correspondiente a amenazas deberá contener aquellas amenazas que los usuarios y todo aquel que haga uso del esquema de seguridad quieran ver explícitamente tomadas en cuenta; las amenazas que sean relevantes, determinando cuáles son los bienes que requieren protección, contra qué métodos de ataque o contra qué eventos indeseables hay que protegerlos, y quiénes o cuáles son los agentes amenazadores; la descripción de las amenazas de forma explícita y concisa; las descripciones de las amenazas de manera concisa, evitando el traslape de éstas; las amenazas que pongan en riesgo a los bienes informáticos.

f) Políticas de seguridad de la organización

A través de las políticas de seguridad se identificará, y si es necesario explicará, cualquier enunciado de política de seguridad organizacional y las normas con las cuales el objeto de evaluación debe cumplir.

Se deberán determinar las políticas de seguridad informática para la organización, así como los requisitos que no se puedan satisfacer sólo mediante el estudio de las amenazas y definir las políticas como conjuntos de reglas que deben ser implementadas por la TOE. Se deberán tomar los rubros que se muestran en el Diagrama 2.2 .

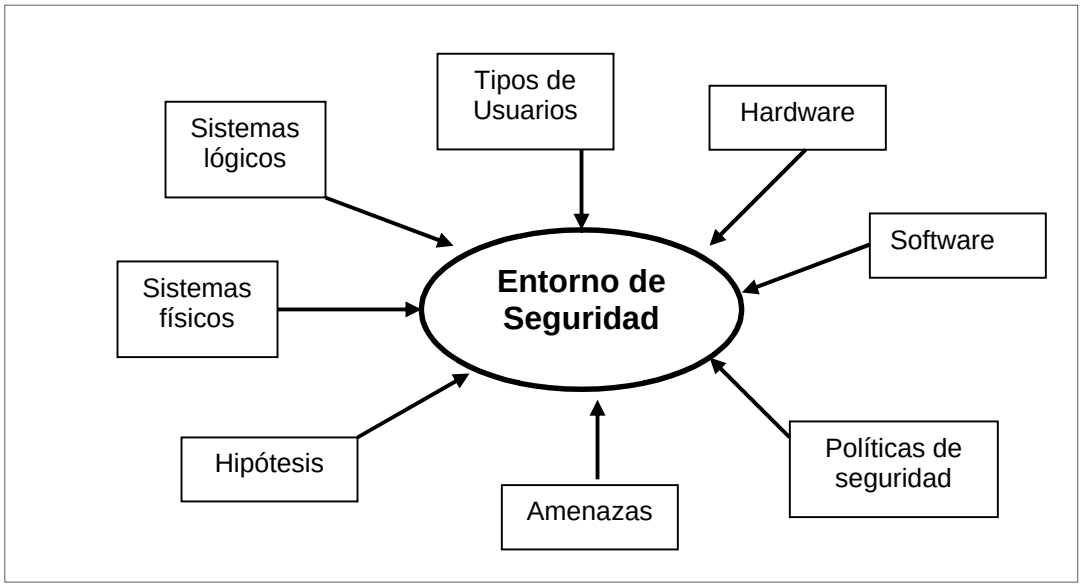


DIAGRAMA 2.2. “ANÁLISIS DEL ENTORNO DE SEGURIDAD”

g) Objetivos

Con base en las hipótesis, amenazas y políticas de seguridad determinadas durante la fase de análisis del entorno de seguridad, se procederá a establecer los objetivos de seguridad. El informe de los objetivos de seguridad definirá los objetivos de seguridad para la TOE y su entorno:

- Objetivos de seguridad para la TOE, los cuales deberán estar claramente documentados y referidos a los aspectos de las amenazas identificadas para que puedan ser contrarrestadas por el objeto de evaluación y por las políticas de seguridad organizacional.
- Objetivos de seguridad para el entorno, los cuales deberán estar claramente documentados y referidos a los aspectos de las amenazas identificadas no contrarrestadas completamente por el objeto de evaluación y las políticas de seguridad organizacional o hipótesis no completamente reunidas.

Así, los objetivos de seguridad deberán indicar el cómo se hará frente a las amenazas y a las políticas desde el punto de vista de las hipótesis; grado de efectividad; enfoque particular de cada objetivo y relación entre el objetivo, las políticas y las amenazas; se deberá plantear un objetivo de seguridad para cada requerimiento funcional; los objetos de la TOE deben ser afirmaciones concisas de la respuesta esperada para satisfacer los requerimientos de seguridad; a que tipo

pertenece cada objetivo si es de tipo preventivo, de detección o correctivo.(ver Diagrama 2.3).

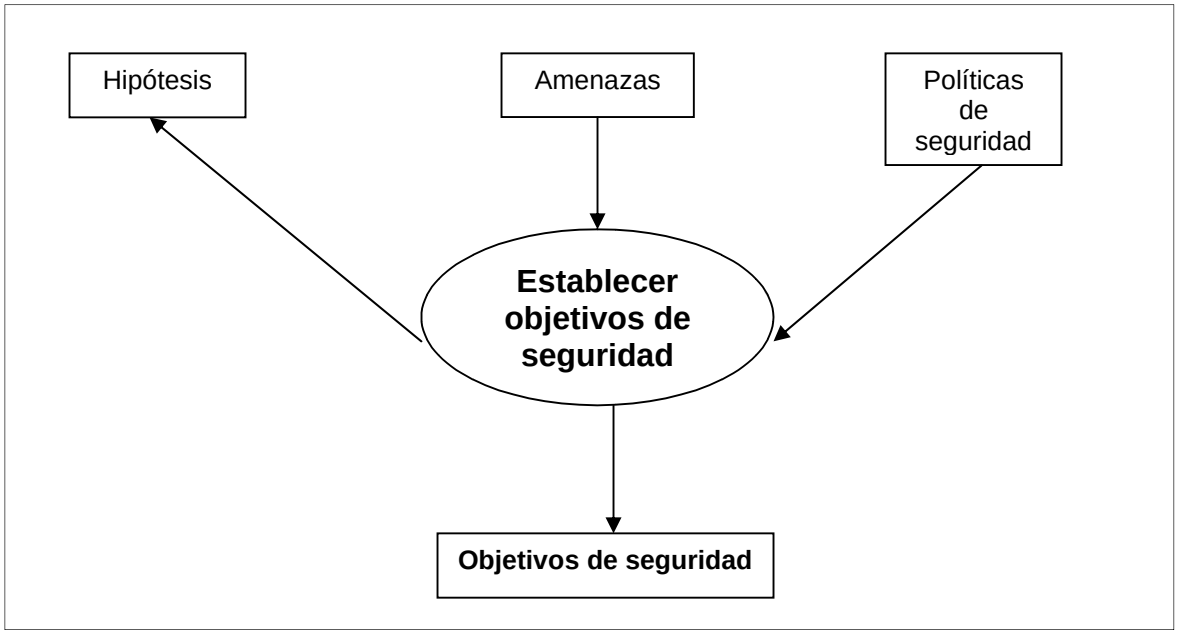


DIAGRAMA 2.3." DETERMINACIÓN DE OBJETIVOS DE SEGURIDAD"

h) Requerimientos

En esta parte del PP se definen detalladamente los requerimientos de seguridad IT que deberán ser cubiertos por la TOE o por su entorno, a fin de determinar el nivel de seguridad y de garantía necesarios y seleccionar los requerimientos de garantía de la tecnología de la información con base en el valor de los activos que se desean proteger, los riesgos a los que están expuestos dichos activos, la factibilidad técnica, los costos probables y los tiempos disponibles, y entonces definir los requerimientos de seguridad IT necesarios, considerando los catálogos de requerimientos incluidos en CC. .(ver Diagrama 2.4).

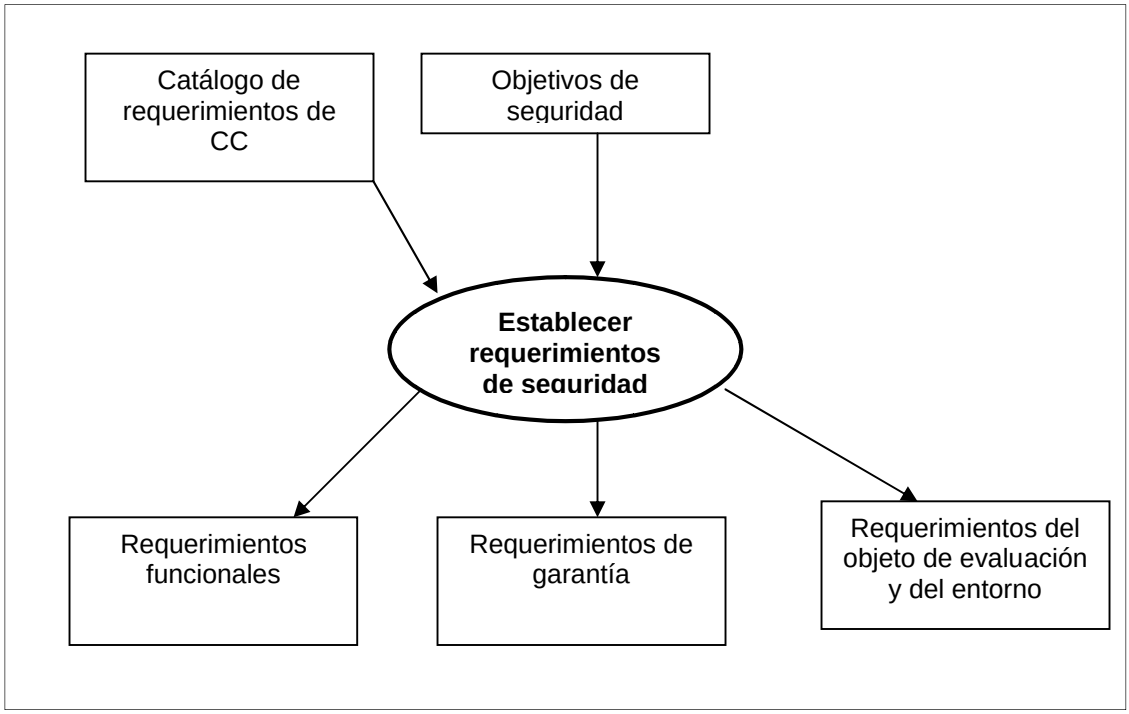


DIAGRAMA 2.4 .”ESTABLECER REQUERIMIENTOS DE SEGURIDAD”

El informe de los requerimientos de seguridad definirá éstos en dos vertientes: la primera se refiere a todo aquello que requiera el objeto de evaluación a fin de que éste opere funcione de manera segura, a este tipo de requerimientos se les denomina requerimientos funcionales; la segunda se refiere a aquello que garantice que el objeto de evaluación es seguro y por lo tanto el usuario de éste lo considere confiable, a este tipo de requerimientos se les denomina requerimientos de garantía. Los requerimientos de seguridad TOE deberán informar lo siguiente: qué funciones debe realizar el objeto de evaluación; qué funciones debe realizar en su conjunto el entorno; las garantías y motivos para tener confianza; las garantías en cuanto a la calidad de las tecnologías de la información desde el punto de vista de la seguridad; la garantía final, que depende del desarrollador y del operador del esquema de seguridad; los requerimientos funcionales de seguridad que lograrán cada uno de los objetivos de seguridad de la TOE; la lista de requerimientos funcionales, en la que se indiquen aquellos que apoyan a los requerimientos dedicados específicamente a algún objetivo; el nivel de seguridad necesario de acuerdo a su importancia en el logro de los objetivos y su factibilidad técnica.

i)Justificación

En esta parte del PP se presenta la evidencia que justifica el trabajo desarrollado. Esta evidencia es el soporte de que el PP desarrollado es un conjunto completo y cohesivo de requerimientos y que proporcionará un conjunto efectivo de medidas

de defensa de seguridad IT para el objeto de evaluación dentro de su entorno de seguridad.

La justificación debe realizarse considerando dos aspectos fundamentales: los objetivos de seguridad y los requerimientos de seguridad; el primero demostrará que el conjunto de los objetivos de seguridad es fácil de seguir para todos los aspectos identificados en el entorno de seguridad del objeto de evaluación y que es conveniente cubrirlos, y el segundo, demostrará que será de gran utilidad reunir el conjunto de requerimientos de seguridad, y que es fácil de seguir para alcanzar los objetivos planteados.

En este apartado se deberá demostrar que el PP está completo, correcto y es internamente consistente; a cada objetivo asignarle una amenaza, política y su hipótesis mediante un esquema o tabla donde nos mostrará que el riesgo, política e hipótesis estarán cubiertos por al menos un objetivo de seguridad; explicar en cada riesgo, política e hipótesis porqué los objetivos señalados son los adecuados; demostrar que los CC se cumplen y que los requerimientos seleccionados no están en conflicto, es decir, que se ha procurado que un requisito funcional no permita que otro requisito sea evitado, alterado o desactivado.

j)Definición de la arquitectura

Con la plena confianza y certidumbre que los requerimientos seleccionados son los necesarios y por lo tanto son los que permitirán alcanzar los objetivos de seguridad y nos ayudarán a hacer cumplir las políticas y contrarrestar las amenazas, se define la arquitectura de seguridad, esto es, se seleccionan los mecanismos y las herramientas necesarios y se lleva a cabo su implantación. Para ello se deberá diseñar la arquitectura de seguridad basándonos en los requerimientos identificados. Hacer la selección de herramientas que logren alcanzar los objetivos planteados, hacer que se cumplan las políticas de seguridad y contrarresten las amenazas identificadas. Por último y no por ello menos importante se deberán buscar soluciones que protejan la TOE, así como el software, el hardware y el firmeware asociados al entorno de seguridad y con lo que las compañías y proveedores de servicios de seguridad están comprometidos a fin de detener, evitar y contrarrestar ataques de seguridad IT.

k)Implementación

Finalmente, el proceso de implementación, en el cual se lleva a cabo la instalación de las herramientas de seguridad, siguiendo las indicaciones dadas por el fabricante a través de los manuales y configurándolas de acuerdo con las políticas de seguridad, pero no debemos olvidar que se instalarán las herramientas seleccionadas, la configuración de las herramientas se hace siguiendo al pie de la letra las políticas de seguridad que creamos, hacer pruebas y por último nuestro esquema de seguridad esta en producción .(ver Diagrama 2.5).

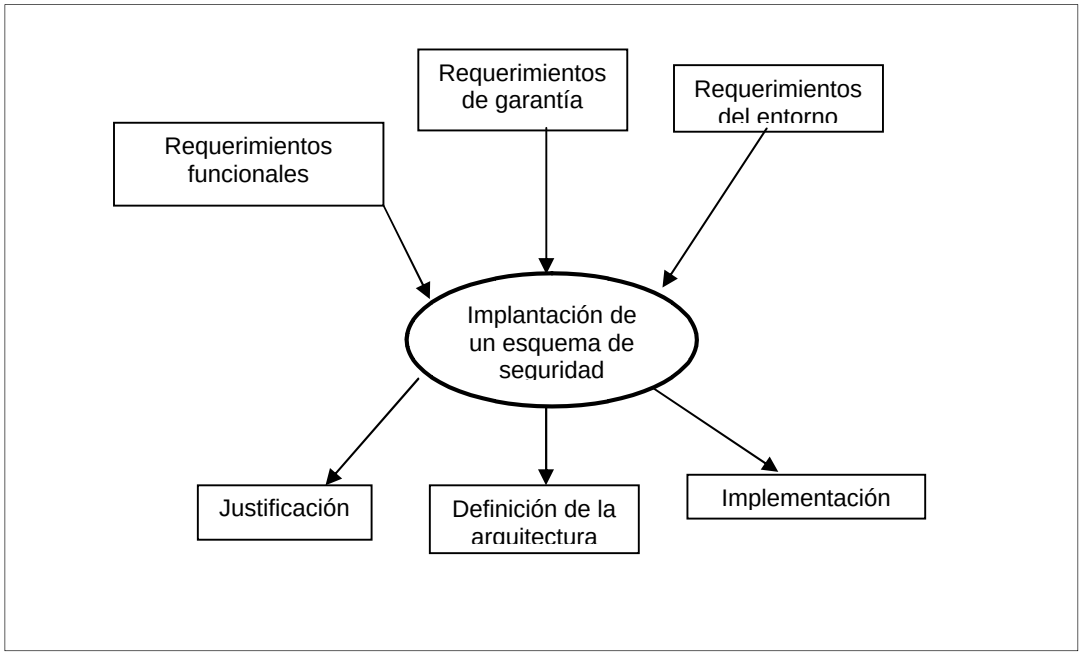


DIAGRAMA 2. 5.” IMPLEMENTACIÓN DEL ESQUEMA DE SEGURIDAD”

2.2.2.Administración de la seguridad

Para finalizar nuestro esquema de seguridad, debemos considerar el llevar a cabo la administración de la seguridad. Y para ello se recomienda contar con un Departamento de Seguridad en Cómputo, el cual deberá estar conformado por el personal responsable en cada área o entorno y por personal especializado en seguridad informática; así, este equipo de trabajo se encargará de administrar la seguridad informática de la empresa u organización.

El objetivo principal de la administración de la seguridad es gestionar y dirigir todas las acciones que se lleven a cabo a fin de proteger la información, hacer uso lícito de ésta, la protección de los recursos con que cuenta la empresa u organismo. Para cumplir estos objetivos en su totalidad no basta con haber desarrollado un esquema de seguridad, esto es solo el comienzo ya que después se debe de trabajar en un plan de acción el cual consta de cuatro etapas.

Etapa 1: Planeación

Se debe llevar a cabo una revisión periódica a las políticas de seguridad, por lo que es menester revisar en su totalidad el esquema de seguridad desarrollado para identificar si se requiere desarrollar nuevas políticas, suprimir algunas y modificar las que ya existen. Al respecto se recomienda que se lleve a cabo el proceso de revisión al menos cada dos años.

Etapa 2: Protección

Después de revisar y actualizar las políticas de seguridad del entorno, se debe reforzar la seguridad con base en éstas y hacer uso de las nuevas tecnologías, ya que éstas permiten nuevas formas de protección con las cuales se eleva el nivel de seguridad del entorno en cuestión.

Etapa 3: Detección

También es necesario contar con sistemas que estén monitoreando continuamente la información, asía como las áreas y sistemas que sean considerados dentro de las políticas como de gran importancia; también se debe considerar que estos sistemas nos proporcionen reportes que permitan detectar cualquier actividad extraña que se presente a fin de tomar las medidas pertinentes, y, reaccionar adecuadamente.

Etapa 4: Reacción

Aquí se van a tomar las decisiones pertinentes las cuales su objetivo principal es el de proteger los bienes informáticos de la organización, basándonos en la información obtenida en la etapa anterior, como hemos mencionado esto nos va a ayudar a hacer un análisis de manera continua para poder tomar la decisión del cambio. Estos cambios pueden ser de muchos tipos desde actualizar la tecnología empleada con la que protegemos nuestra información, modificar esquemas de seguridad, llevar acabo una revisión extraordinaria a las políticas, etc.

2.3.Norma ISO/IEC 17799

Toda organización o empresa que tenga interés en proteger algún bien, requiere de un modelo de seguridad para lo cual se hace un análisis de riesgo, sin embargo, sabemos que existen estándares de seguridad los cuales sirven como "guía" a los desarrolladores de esquemas de seguridad para elaborar cada uno de ellos. Tal es el caso de la norma ISO/IEC 17799 la cual está diseñada para garantizar y certificar la seguridad de la información en las organizaciones.

2.3.1. Historia de ISO/IEC 17799

Los orígenes de ISO-17799 están en BS7799[5]. En mayo de 1987 un grupo dedicado a la seguridad de la información. "Centro Comercial de Seguridad en Cómputo del Departamento Británico de Comercio e Industria" (CCSC - DTI) cuyas tareas principales eran:

[5] "BS 7799 es una norma que presenta los requisitos para un Sistema Administrativo de Seguridad de la Información. Ayudará a identificar, administrar y minimizar la gama de amenazas a las cuales está expuesta regularmente la información" http://www.bsiamericas.com

- Brindar ayuda a los vendedores de productos de seguridad TI mediante el establecimiento de un conjunto de criterios de evaluación de seguridad reconocidos internacionalmente.
- Brindar ayuda a los usuarios mediante un código de buenas prácticas de seguridad dando origen al “Código de prácticas para usuarios” publicado en 1989. El “Código de prácticas para usuarios” retomado y desarrollado por NCC (Centro Nacional de Cómputo) por un grupo de usuarios de la industria británica para asegurar que el código fuera significativo y práctico desde el punto de vista del usuario.

En febrero de 1993 se publican los resultados como un documento guía del estándar británico (BS). Recibe el nombre “PD 0003: código de prácticas para el manejo de seguridad de la información”. Trabajo que da lugar a la primera versión del estándar británico BS7799, publicándose y poniéndose en circulación en 1995.

En 1998 se crea el BSI (Instituto Británico de Estándares) el cual es programa para acreditar a las firmas auditoras: cuerpos de certificación y auditores individuales para auditar organizaciones con base en el estándar BS7799

El objetivo es proveer un nivel de confianza alto a las organizaciones y a sus socios comerciales buscando la seguridad de sus activos y recursos TI.

El cual fue de gran aceptación de la norma británica por: Australia, Sudáfrica, Nueva Zelanda, Holanda y Noruega el gobierno del Reino Unido recomendó como parte de su “Ley de Protección a la Información de 1998” (que entró en vigor el 1° de marzo de 2000) que las compañías británicas utilizaran el estándar BS7799 como método de cumplimiento de esa ley

Mientras algunas organizaciones utilizaron el estándar BS7799, otras expresaron la necesidad de un estándar común.

Esta demanda condujo al rápido seguimiento del estándar BS7799 dando origen al lanzamiento realizado por la ISO en Diciembre de 2000 y teniendo como nombre ISO/IEC 17799:2000.

ISO 17799 es el único estándar de alto nivel y de naturaleza conceptual dedicado al manejo de la seguridad de la información en un campo manejado por “Principios” y “Buenas Prácticas”.

2.3.2. Objetivo de ISO/IEC 17799

Este estándar define a la información como un activo o recurso que existe de muchas formas y que tiene amplio valor para una cierta organización.

El objetivo principal de este estándar es garantizar la seguridad de la información, es proteger este recurso de manera oportuna y conveniente de un rango muy amplio de vulnerabilidades, de tal manera que se asegure la continuidad del

negocio, se minimicen los daños y se maximicen las ganancias de las inversiones y las oportunidades de negocio.

ISO 17799 define la seguridad de la información como la conservación de:

- Confidencialidad
- Integridad
- Disponibilidad
- Autenticidad

Como objetivos particulares de este estándar, podemos tomar en cuenta los siguientes:

- Capacitar a las organizaciones para implementar apropiadamente seguridad de las TI.
- Proveer una guía común de mejores prácticas.
- Facilitar el comercio entre compañías dando confianza en la seguridad de las TI compartida.
- Brindar a los profesionales en TI anteproyectos para desarrollar políticas y procesos de seguridad empresarial.

La seguridad de la información se logra implementando un conjunto de controles, los cuales pueden ser políticas, prácticas, procedimientos, estructuras organizacionales y funciones de software. Estos controles necesitan ser establecidos para asegurar que se alcancen los objetivos específicos de seguridad de la organización.

Tipos de Controles

- Basados sobre requerimientos legislativos (aspecto legal): Protección de datos y privacidad de información personal, resguardado de registros organizacionales y derechos de propiedad intelectual.
- Los considerados a ser la mejor práctica para la seguridad de la información: Información sobre la documentación de las políticas de seguridad, distribución de responsabilidades en la seguridad de la información, educación y entrenamiento en seguridad de la información, reporte de incidentes de seguridad, dirección de continuidad de negocios.

2.3.3.Áreas de control

Política de seguridad

Se necesita una política que refleje las expectativas de la organización en materia de seguridad a fin de suministrar administración con dirección y soporte. La política también se puede utilizar como base para el estudio y evaluación en curso.

Organización de la seguridad

Sugiere diseñar una estructura de administración dentro la organización que establezca la responsabilidad de los grupos en ciertas áreas de la seguridad y un proceso para el manejo de respuesta a incidentes.

Control y clasificación de los recursos de información

Necesita un inventario de los recursos de información de la organización y con base en este conocimiento, debe asegurar que se brinde un nivel adecuado de protección.

Seguridad del personal

Establece la necesidad de educar e informar a los empleados actuales y potenciales sobre lo que se espera de ellos en materia de seguridad y asuntos de confidencialidad. También determina cómo incide el papel que desempeñan los empleados en materia de seguridad en el funcionamiento general de la compañía. Se debe tener implementar un plan para reportar los incidentes.

Seguridad física y ambiental

Responde a la necesidad de proteger las áreas, el equipo y los controles generales.

Manejo de las comunicaciones y las operaciones

Conservar la integridad y disponibilidad del procesamiento y la comunicación de la información protegiéndola en las redes e infraestructura de soporte

Control de acceso

Establece la importancia de monitorizar y controlar el acceso a la red y los recursos de aplicación para proteger contra los abusos internos e intrusos externos.

Desarrollo y mantenimiento de los sistemas

Recuerda que en toda labor de la tecnología de la información, se debe implementar y mantener la seguridad mediante el uso de controles de seguridad en todas las etapas del proceso.

Manejo de la continuidad de la empresa

Aconseja estar preparado para contrarrestar las interrupciones en las actividades de la empresa y para proteger los procesos importantes de la empresa en caso de una falla grave o desastre.

Cumplimiento

Imparte instrucciones a las organizaciones para que verifiquen si el cumplimiento con la norma técnica ISO 17799 concuerda con otros requisitos jurídicos, como la Directiva de la Unión Europea que concierne la Privacidad, la Ley de Responsabilidad y Transferibilidad del Seguro Médico (HIPAA por su sigla en Inglés) y la Ley Gramm-Leach-Billey (GLBA por su sigla en inglés).

Esta sección también requiere una revisión a las políticas de seguridad, al cumplimiento y consideraciones técnicas que se deben hacer en relación con el proceso de auditoria del sistema a fin de garantizar que las empresas obtengan el máximo beneficio.

2.3.4.Organización de la Seguridad

Infraestructura de seguridad de la información

Objetivo: Administrar la seguridad de la información dentro de la organización.

- *Coordinación de seguridad de la información*: En una organización grande debe estar conformado un foro por representantes de partes relevantes de la organización para implementar controles de seguridad. Este foro asigna responsabilidades, establece metodologías de seguridad, revisión de incidentes, etc.
- *Asignación de responsabilidades de seguridad de la información*: Deben ser definidas responsabilidades para cada bien y para realizar procesos de seguridad específicos. Niveles de autorización deben ser definidos y documentados.
- *Consejo de especialistas en seguridad de la información*: Debe ser proporcionado por un consejero o asesor experimentado.
- *Cooperación entre organizaciones*: Contactos apropiados con autoridades legales, cuerpos regulatorios, proveedores de servicio y operadores de telecomunicaciones, para asegurar que una acción apropiada puede ser tomada rápidamente en un incidente de seguridad.
- *Revisión independiente de seguridad de la información*: Es recomendable que sea realizada por un administrador independiente o una organización externa especialista en auditorias.
- *Seguridad de Acceso de Terceras Personas*: Mantener la seguridad de la información organizacional accedida por terceras personas.
- *Identificación de Riesgos del Acceso de Terceras Personas*: Saber si la organización va a dar el acceso a terceras personas tenemos que saber a que estamos expuestos, otorgando permisos restringidos.
- *Tipos de acceso*: se debe considerar el acceso físico y el lógico, requerimientos de seguridad en contratos de terceras personas, términos que deben ser considerados en el contrato, política general sobre seguridad de la información, descripción de cada servicio disponible, niveles inaceptables de servicio, obligaciones respectivas de las partes del contrato, responsabilidades legales, derechos de propiedad intelectual y acuerdos de control de acceso.

Control y Clasificación de los Bienes Informáticos

- Contabilidad de Bienes

Objetivo: Mantener protección apropiada de bienes organizacionales.

- *Inventario de bienes*: La organización necesita identificar sus bienes y el valor relativo e importancia; con esta información la institución puede proporcionar niveles de protección de acuerdo a los distintos valores de bienes; cada bien debe ser identificado y documentado, junto con su localización actual.

Seguridad del Personal

- Definición de Seguridad en el Trabajo y Recursos

Objetivo: Reducir los riesgos de error humano, fraude o mal uso.

- *Responsabilidades de seguridad en el trabajo*: Las responsabilidades deben estar documentadas apropiadamente.
- *Resguardo de personal y políticas*: Disponibilidad de referencias satisfactorias; verificación de currículos de los aspirantes; confirmación de calificaciones académicas y profesionales; verificación independiente de identidad; acuerdos de confidencialidad, términos y condiciones de empleo:

Entrenamiento del Usuario

Objetivo: Asegurar que los usuarios están conscientes de las amenazas y están preparados para soportar las políticas.

Respuesta a Incidentes y mal Funcionamiento

Objetivo: Minimizar el daño de los incidentes de seguridad y mal funcionamiento.

- *Reporte de incidentes de seguridad*: Deben ser reportados por los canales apropiados tan rápido como sea posible. Incluye el procedimiento de reporte y el procedimiento a la respuesta al incidente.
- *Reporte de malfuncionamiento de SW*: Se deben establecer procedimientos por mal funcionamiento de SW.
- *Proceso disciplinario*: Debe establecerse para los empleados que han violado políticas de seguridad.

Seguridad Física y del Entorno

- Áreas de Seguridad

Objetivo: Prevenir acceso no autorizado, daño e interferencia.

- *Perímetro de seguridad física*: La protección física puede ser lograda creando algunas barreras físicas a los sistemas de información.
- *Controles de entrada física*: Las áreas de seguridad deben estar protegidas por controles apropiados de entrada para asegurar que solo personal autorizado tiene acceso.
- *Seguridad en oficinas, salas y facilidades*: La selección y diseño de un área segura debe tomar en cuenta las posibilidades de amenazas naturales o humanas.
- *Trabajo en áreas seguras*: El personal debe estar consciente de la

existencia de áreas de seguridad; debe ser evitado el trabajo no supervisado en áreas de seguridad; no debe permitirse fotos, video, audio; sólo con autorización.

- Seguridad del Equipo

Objetivo: Prevenir pérdida, daño o compromiso de bienes e interrupción de actividades.

- *Colocación del equipo y protección*: Debe ser colocado o protegido para reducir riesgos de amenazas del ambiente, humanas y oportunidades de acceso no autorizado.
- *Suministro de energía*: El equipo debe estar protegido de fallos de energía y anomalías.
- *Seguridad del cableado*: Cableado de energía y de telecomunicaciones debe estar protegido de intercepción o daño. Se sugiere el uso de fibra óptica para sistemas críticos, rutas o medios de transmisión alternativos.
- *Mantenimiento del equipo*: Mantenimiento basado en especificaciones y normas. Realizado por personal autorizado.

Administración de Comunicaciones y Operaciones

- Procedimientos Operacionales y Responsabilidades

Objetivo: Corroborar que las operaciones se lleven a cabo de manera segura y correcta brindando facilidades de procesamiento de información.

- *Documentación de procedimientos de operación*: Los procedimientos de operación deben ser documentados y mantenidos, los cambios deben ser autorizados por la dirección.
- *Control de cambio organizacional*: Los cambios a las facilidades de procesamiento de información deben ser controlados.
- *Procedimientos de dirección de incidentes*: Cubrir todos los tipos potenciales de incidentes de seguridad. Acciones para recuperación y corrección de fallos deben ser controlados.

- Planeación del Sistema y Aceptación

Objetivo: Minimizar el riesgo de fallo de sistemas.

- *Capacidad de planeación:* Las demandas de capacidad deben ser monitoreadas y proyecciones de requerimientos de capacidad futuros deben ser hechos para asegurar disponibilidad.
- *Aceptación del sistema:* Criterios de aceptación para nuevos sistemas de información y nuevas versiones deben ser establecidos, acordados y documentados, así como las pruebas pertinentes.

- Protección Contra Software Malicioso

Objetivo: Proteger la integridad de software e información.

- *Controles contra software malicioso*: Políticas para licencias de software y prohibir el uso de software no autorizado; control sobre instalaciones,

actualizaciones, vacunas y reparación; revisiones regulares de software y contenido de datos, procedimientos contra protección de virus y ataques.

- Respaldos

Objetivo: Mantener la integridad y disponibilidad de la información.

  - *Respaldo de información y Registros de operación.*

- Administración de Red

Objetivo: Asegurar el resguardo de información en la red.

  - *Controles de red*: Los administradores deben implementar controles para asegurar la seguridad de los datos en red y la protección de servicios.

- Manejo de Medios y Seguridad

Objetivo: Prevenir daños a bienes e interrupciones.

  - *Administración de medios removibles:* Procedimientos para la administración de medios removibles, su copia, lectura y almacenamiento.
  - *Seguridad de documentación del sistema*: Controles para proteger documentación del sistema de acceso no autorizado.

- Intercambio de Información y SW

Objetivo: Prevenir pérdida, modificación o mal uso en el intercambio de información entre organizaciones.

  - *Acuerdos de intercambio de información y software:* procedimientos para transmisión y recepción; estándares de identificación y responsabilidades.
  - *Seguridad de medios en tránsito:* Debe ser usado transporte o correo confiable; controles especiales para información sensitiva como firmas digitales o encriptación; deben establecerse controles para amenazas del comercio electrónico como la autenticación, autorización.
  - *Seguridad de correo electrónico:* ataques, protección, consideraciones legales, responsabilidades de proveedores y empleados, uso de criptografía.

- Acceso del Usuario

Objetivo: Prevenir el acceso no autorizado a los sistemas de información.

Los procedimientos formales deben controlar la asignación de los derechos de acceso a los sistemas y a los servicios de información.

Los procedimientos deben cubrir todas las etapas que comprenden al acceso del usuario, del registro inicial de nuevos usuarios al registro final de los usuarios que solo requieren el acceso a los sistemas y a los servicios de información.

- Responsabilidades del Usuario

Objetivo: Prevenir el acceso de usuario no autorizado.

La cooperación de usuarios autorizados es esencial para la seguridad afectiva. Los usuarios deben ser enterados de sus responsabilidades de mantener controles de acceso eficaces, particularmente con respecto al uso de contraseñas y a la seguridad del equipo del usuario.

- Control de Acceso a los Sistemas Operativos

Objetivo: Prevenir el acceso no autorizado a la computadora.

Las instalaciones de la seguridad en el sistema operativo ya no se deben utilizar para restringir el acceso a los recursos de la computadora. Estas instalaciones deben ser capaces de lo siguiente:

Identificar y verificar la identidad del usuario. Abastecimiento de los medios apropiados para la autentificación. Cuando sea apropiado, restringir los tiempos de conexión de usuarios.

- Control de Acceso al uso de Sistemas

Objetivo: Prevenir el acceso no autorizado a la información en los sistemas.

Las instalaciones de Seguridad se deben utilizar para restringir el acceso dentro del uso de sistemas. El acceso al software y a la información se debe restringir a los usuarios no autorizados

- Supervisión al Acceso y uso del Sistema

Objetivo: Detectar actividades no autorizadas.

Los sistemas se deben supervisar para detectar cualquier anomalía del control de acceso y para registrar acontecimientos.

La supervisión del sistema permite la eficacia de controles adoptados para ser comprobado.

- Desarrollo y Mantenimiento

Objetivo: Corroborar que la seguridad sea sólida en los sistemas de información.

Todos los requerimientos de seguridad se deben identificar antes del desarrollo de los sistemas de información.

- Seguridad en el uso de los Sistemas

Objetivo: Prevenir pérdida, modificación o el uso erróneo de los datos del usuario en el uso de los sistemas.

Los controles apropiados se deben diseñar en el uso de los sistemas. Éstos deben incluir la validación de los datos de entrada, del proceso interno y los datos de la salida.

- Control de Acceso de Red

Objetivo: Protección de servicios de red.

Todo acceso y servicios de red deben ser controlados. Esto es necesario para asegurarse de que los usuarios que tienen acceso a las redes y a los servicios de red no comprometan la seguridad de estos servicios de red. Esto se logra a través de:

  - Interfaces apropiadas entre la red de la organización y las redes poseídas por otras organizaciones, o redes públicas.
  - Mecanismos apropiados de la autentificación para los usuarios y el equipo.
  - Control del acceso del usuario a los servicios informativos.

- Seguridad de los ficheros del Sistema

Objetivo: Asegurarse de que la ayuda sea de una manera segura, todo acceso a los ficheros del sistema debe ser controlado y la integridad del sistema debe ser mantenida por el usuario.

  - Seguridad de los Procesos de Desarrollo y de la ayuda

Objetivo: Mantener la seguridad del software del sistema y del uso de la información.

Los procesos del proyecto y de la ayuda deben ser controlados. Los encargados responsables del uso del los sistemas deben también ser responsables de la seguridad del proyecto. Deben resguardar la seguridad del sistema.

2.4.Norma ISO/IEC 27001

El estándar para la seguridad de la información ISO/IEC 27001 (Information technology - Security techniques - Information security management systems - Requirements) fue aprobado y publicado como estándar internacional en Octubre de 2005 por International Organization for Standardization y por la comisión International Electrotechnical Commission.

Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI).

En 2002, se revisó BS 7799-2 para adecuarse a la filosofía de normas ISO de sistemas de gestión. En 2005, y con más de 1700 empresas certificadas en BS7799-2, este esquema se publicó por ISO como estándar 27001. También en ese año, se revisa ISO17799.

En Marzo de 2006, posteriormente a la publicación de la ISO27001:2005, BSI publicó la BS7799-3:2006, centrada en la gestión del riesgo de los sistemas de información. Este servirá de base a la ISO 27005, que tardará aún algún tiempo en editarse.

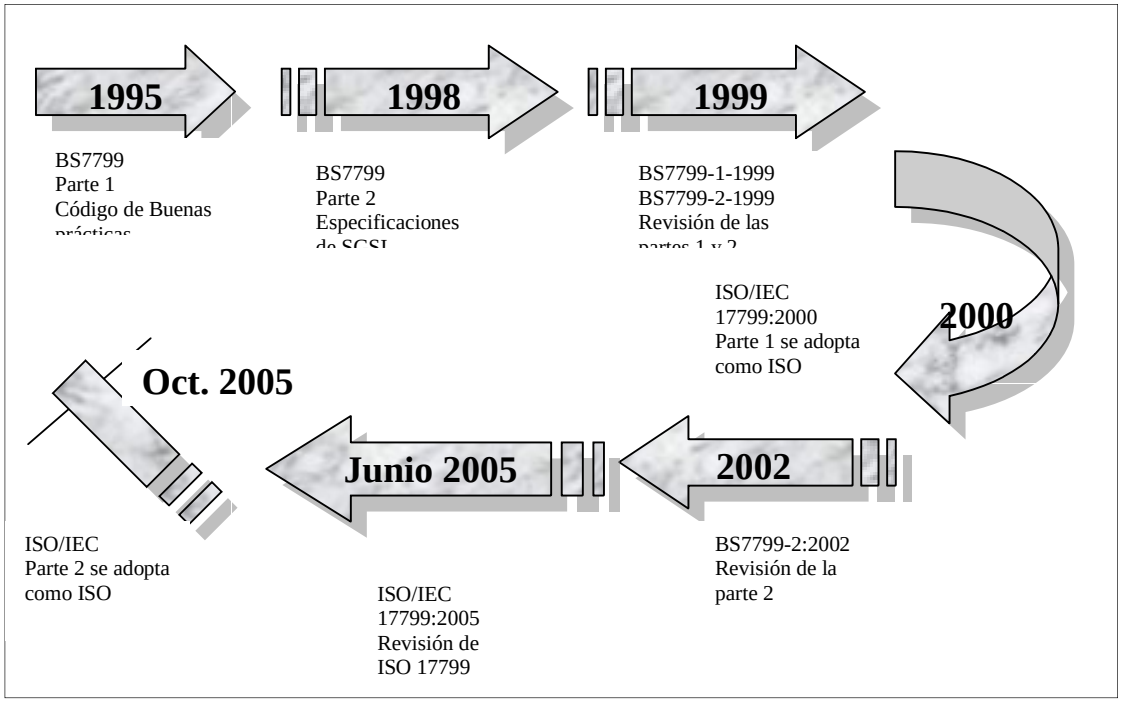


DIAGRAMA 2.5 "HISTORIA DE ISO 27001 "

2.4.1.La serie 27000

A semejanza de otras normas ISO, la 27000 es realmente una serie de estándares.

- ISO 27000: Contiene términos y definiciones que se emplean en toda la serie 27000.
- ISO 27001: Es la norma principal de requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 y es la norma con arreglo a la cual se certifican por auditores externos los SGSI de las organizaciones. Fue publicada e!15 de Octubre de 2005 y sustituye a la BS 7799-2, habiéndose establecido unas condiciones de transición para aquellas empresas certificadas en esta última. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO17799:2005 (futura ISO27002), para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados.
- ISO 27002 (ISO 17799): Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información.
- ISO 27003: En fase de desarrollo; probable publicación a finales de 2008. Contendrá una guía de implementación de SGSI.

- ISO 27004: En fase de desarrollo; probable publicación a lo largo de 2008. Especificará las métricas y las técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles relacionados.
- ISO 27005: En fase de desarrollo; probable publicación a finales de 2007 ó principios de 2008. Consistirá en una guía para la gestión del riesgo de la seguridad de la información y servirá, por tanto, de apoyo a la ISO27001 y a la implantación de un SGSI.
- ISO 27006: Publicada en Febrero de 2007. Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información.

A continuación se explican cada uno de los apartados que contiene la norma ISO 27001

- Introducción: generalidades e introducción al método PDCA.
- Campo de aplicación: se especifica el objetivo, la aplicación y el tratamiento de exclusiones.
- Referencias normativas: otras normas que sirven de referencia.
- Términos y definiciones: breve descripción de los términos más usados en la norma.
- Sistema de gestión de la seguridad de la información: cómo establecer, implementar, monitorizar, revisar, mantener y mejorar el SGSI; requerimientos de documentación y su control.
- Responsabilidades de la Dirección: en cuanto a compromiso con el SGSI, provisión de recursos y formación y concienciación del personal.
- Auditorías internas del SGSI: cómo realizar las auditorías internas de control.
- Revisión del SGSI por la dirección: cómo gestionar el proceso de revisión constante del SGSI.
- Mejora de SGSI: mejora continua, acciones correctoras y acciones preventivas.
- Resumen de controles: anexo que enumera los objetivos de control y controles que se encuentran detallados en la norma ISO 17799:2005.
- Relación con los Principios de la OCDE: correspondencia entre los apartados de la ISO 27001 y los principios de buen gobierno de la OCDE.
- Correspondencia con otras normas: tabla de correspondencia de puntos con ISO 9001 y 14001.
- Bibliografía: normas y publicaciones de referencia.

Desde finales de 2005 las organizaciones ya pueden obtener la certificación ISO/IEC 27001 en su primera certificación con éxito o mediante su recertificación periódica correspondiente cada tres años, puesto que la certificación BS 7799-2 ha quedado reemplazada.

Esta norma tiene como misión desarrollar todos los aspectos que deben ser considerados para poder “medir” el cumplimiento de la norma ISO 27001. Ésta hace especial hincapié en el concepto de SGSI y en la aplicación de controles, los cuales son los que en definitiva le dan vida a este ciclo permanente de gestión. El principio básico es que si no se puede medir, entonces no sirve de nada. Con lo

que queremos dar a entender es que la idea de medición es muy amplia y en definitiva, va desde la medición más simple hasta la combinación de varios niveles o instancias de ellas para poder ofrecer datos que lleven a un verdadero “cuadro de mando de la seguridad”, que sería el objetivo último de todo SGSI, y a través del cual, los diferentes niveles jerárquicos de la organización, podrán acceder a la información de seguridad, que a su nivel le hace falta conocer y en base a esta adoptar las decisiones correspondientes.

ISO/IEC 27001:2005 es una norma que establece los requisitos de los sistemas de gestión de la seguridad de la información. Ayuda a identificar, gestionar y minimizar el abanico de amenazas a las que está sometida siempre la información. Esta norma esta diseñada para asegurar la selección de los controles de seguridad adecuados y proporcionados para proteger la información y dar la confianza a partes interesadas incluyendo a los clientes de una empresa.

Es conveniente para diferentes tipos de uso empresarial, incluyendo los siguientes:

- Formulación de exigencias y objetivos para la seguridad
- Asegurar la gestión mas rentable de los riesgos
- Asegurar el cumplimiento legal
- Desarrollar un proceso para la puesta en práctica y la gestión de controles para asegurar el conocimiento de los objetivos de seguridad específicos de una empresa.
- Identificación y clarificación de los procesos existentes en la gestión de la seguridad de la información.
- Puede ser usado por la dirección para determinar el estado de las actividades de la gestión de la seguridad de la información.
- Como herramienta de auditores internos y externos para determinar el grado de cumplimiento con la política, directivas y normas adoptadas por una empresa.
- Para proporcionar información relevante sobre la política de la seguridad de la información, directivas, normas y procedimientos dentro del mercado.
- Para proporcionar información relevante sobre seguridad de la información a clientes.

Una empresa que utilice ISO/IEC 27001:2005 como base para su SGSI podrá obtener la certificación a través de BSI, lo que le permitirá demostrar a las partes interesadas que su SGSI satisface todos los requisitos de la norma.

ISO/IEC 27001:2005 es una norma que establece los requisitos de los sistemas de gestión de la seguridad de la información. Ayuda a identificar, gestionar y minimizar el abanico de amenazas a las que está sometida siempre la información. Esta norma esta diseñada para asegurar la selección de los controles de seguridad adecuados y proporcionados para proteger la información y dar la confianza a partes interesadas incluyendo a los clientes de una empresa.

Es conveniente para varios tipos diferentes de uso empresarial, incluyendo lo siguiente:

- Formulación de exigencias y objetivos para la seguridad
- Asegurar la gestión mas rentable de los riesgos
- Asegurar el cumplimiento legal
- Desarrollar un proceso para la puesta en práctica y la gestión de controles para asegurar el conocimiento de los objetivos de seguridad específicos de una empresa.
- Identificación y clarificación de los procesos existentes en la gestión de la seguridad de la información.
- Puede ser usado por la dirección para determinar el estado de las actividades de la gestión de la seguridad de la información.
- Como herramienta de auditores internos y externos para determinar el grado de cumplimiento con la política, directivas y normas adoptadas por una empresa.
- Para proporcionar información relevante sobre la política de la seguridad de la información, directivas, normas y procedimientos dentro del mercado.
- Para proporcionar información relevante sobre seguridad de la información a clientes.

2.4.2.Beneficios

- Establecimiento de una metodología de gestión de la seguridad clara y estructurada.
- Reducción del riesgo de pérdida, robo o corrupción de información.
- Los clientes tienen acceso a la información a través de medidas de seguridad.
- Los riesgos y sus controles son continuamente revisados.
- Confianza de clientes y socios estratégicos por la garantía de calidad y confidencialidad comercial.
- Las auditorías externas ayudan cíclicamente a identificar las debilidades del sistema y las áreas a mejorar.
- El sistema se integra con otros sistemas de gestión (ISO9001, ISO14001).
- Continuidad de las operaciones necesarias de negocio tras incidentes de gravedad.
- Conformidad con la legislación vigente sobre información personal, propiedad intelectual y otras.
- Imagen de empresa a nivel internacional y elemento diferenciador de la competencia.
- Proporciona confianza y reglas claras a las personas de la organización.
- Reduce costos y mejora los procesos y servicio.
- Aumenta la motivación y satisfacción del personal.
- Seguridad garantizada con base en la gestión de procesos en vez de en la compra sistemática de productos y tecnologías.

¿Cómo adaptarnos?

Para adaptarse a la nueva norma ISO 27001 se ha adaptado un diagrama (ver diagrama 2.6) el cual indica que hacer en cada fase desde el arranque del proyecto hasta cuales son las acciones a tomar en cada fase del mismo.

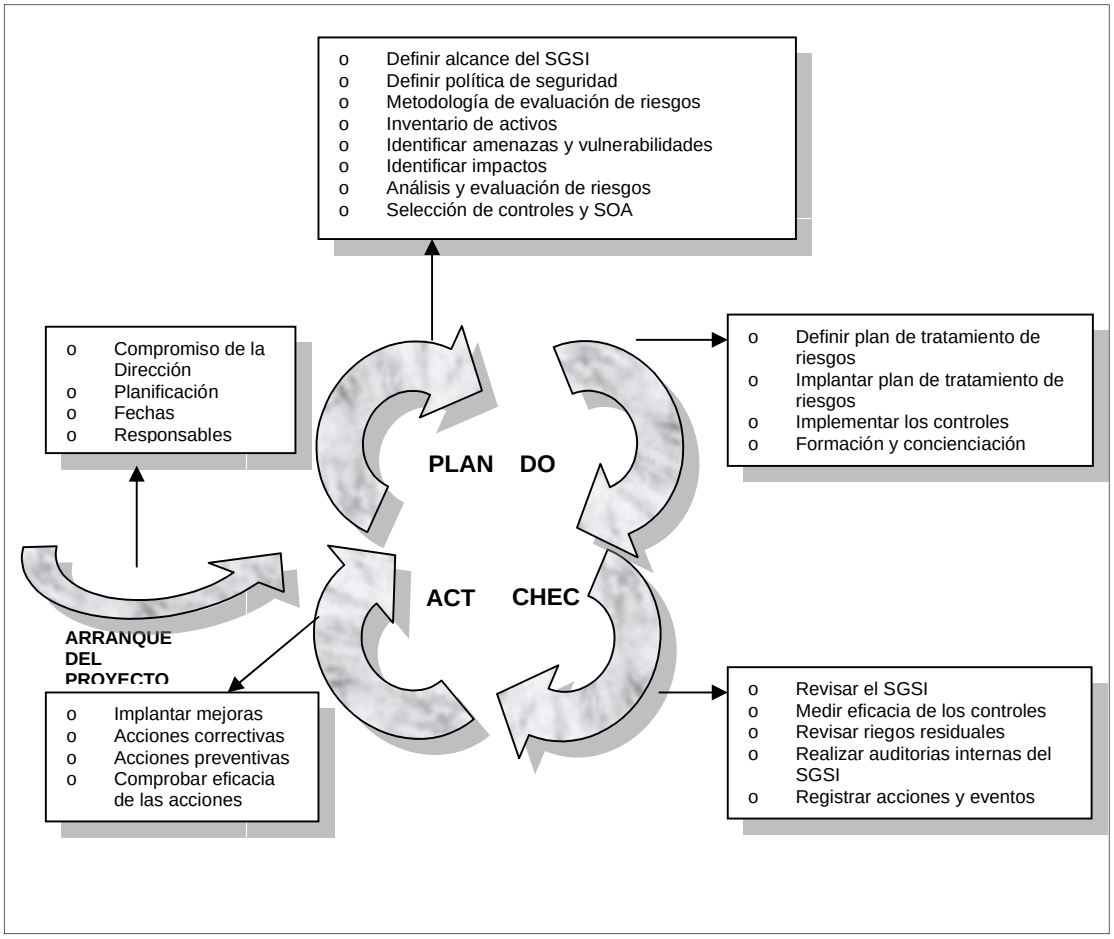


DIAGRAMA 2.6 FASES DE ADAPTACIÓN DEL PROYECTO A LA NORMA 27001

Arranque del proyecto…

A continuación se muestra el diagrama (ver diagrama 2.7) que nos indica el arranque del proyecto así como:

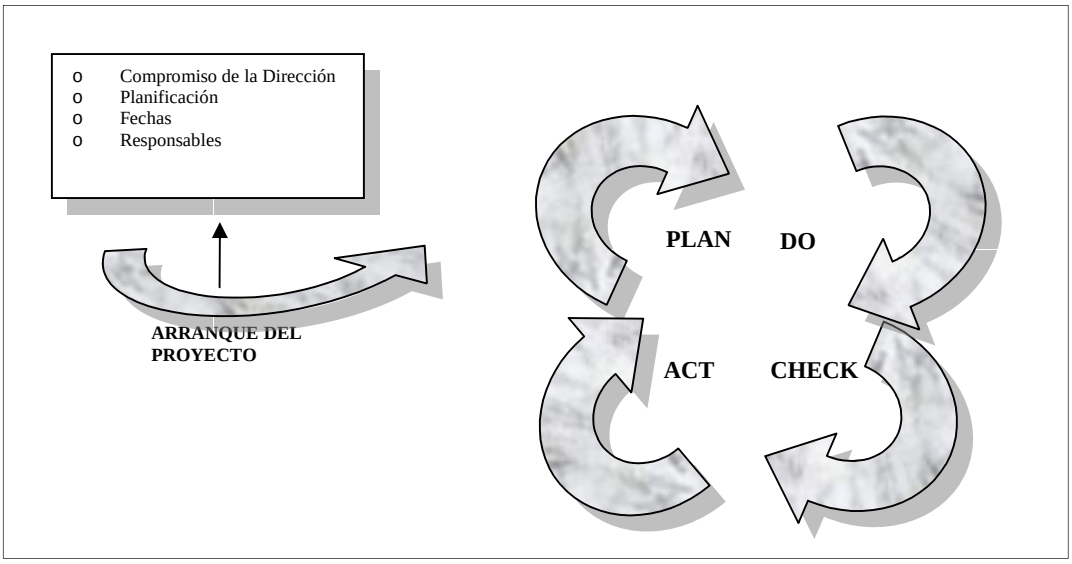


DIAGRAMA 2.7 ARRANQUE DEL PROYECTO

- Compromiso de la Dirección: una de las bases fundamentales sobre las que se inicia un proyecto de este tipo es el apoyo claro y decidido de la Dirección de la organización. No sólo por ser un punto contemplado de forma especial por la norma sino porque el cambio de cultura y concienciación que lleva consigo el proceso hacen necesario el impulso constante de la Dirección.
- Planificación, fechas, responsables: como en todo proyecto de envergadura, el tiempo y el esfuerzo invertidos en esta fase multiplican sus efectos positivos sobre el resto de fases.

Planificación

En esta parte se va a definir que alcance va a tener nuestro proyecto, en otras palabras cual es la misión a seguir. Identificación de las amenazas y valoración de los riegos, etc. (ver diagrama 2.8)

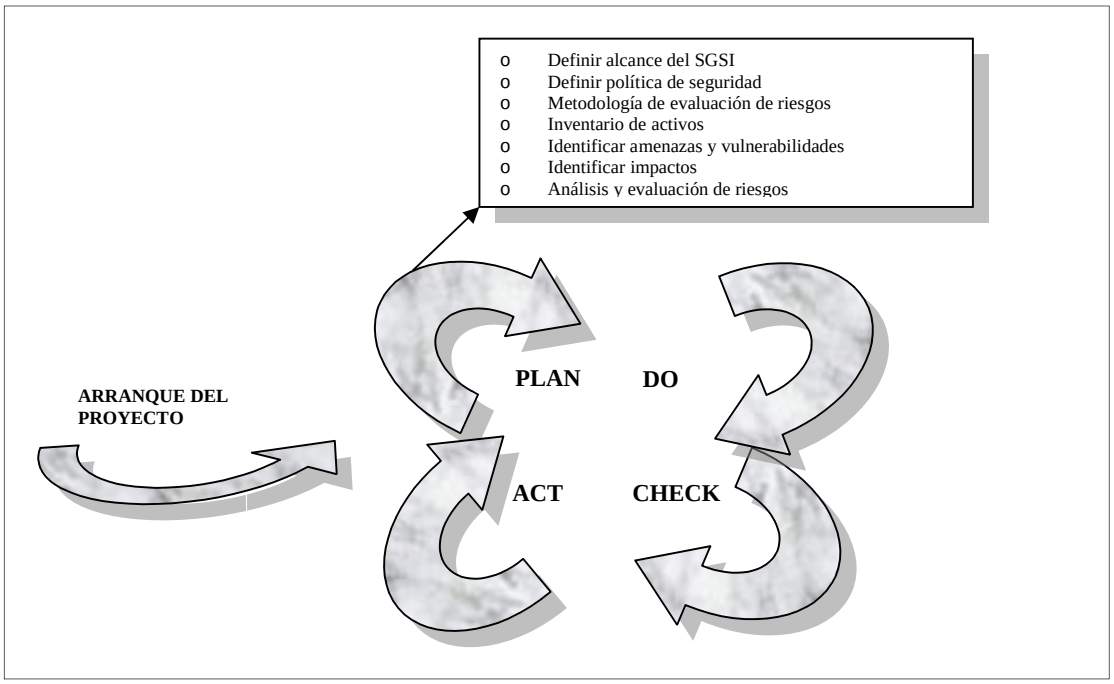


DIAGRAMA 2.8 PLANIFICACIÓN DEL PROYECTO

- Definir alcance del SGSI: en función de características del negocio, organización, localización, activos y tecnología, definir el alcance y los límites del SGSI (el SGSI no tiene por qué abarcar toda la organización; de hecho, es recomendable empezar por un alcance limitado).
- Definir política de seguridad: que incluya el marco general y los objetivos de seguridad de la información de la organización, tenga en cuenta los requisitos de negocio, legales y contractuales en cuanto a seguridad, esté alineada con la gestión de riesgo general, establezca criterios de evaluación de riesgo y sea aprobada por la Dirección. La política de seguridad es un documento muy general, una especie de "declaración de intenciones" de la Dirección, por lo que no pasará de dos o tres páginas.
- Definir el enfoque de evaluación de riesgos: definir una metodología de evaluación de riesgos apropiada para el SGSI y las necesidades de la organización, desarrollar criterios de aceptación de riesgos y determinar el nivel de riesgo aceptable. Existen muchas metodologías de evaluación de riesgos aceptadas internacionalmente la organización puede optar por una de ellas, hacer una combinación de varias o crear la suya propia. ISO 27001 no impone ninguna ni da indicaciones adicionales sobre cómo definirla. El riesgo nunca es totalmente eliminable -ni sería rentable hacerlo-, por lo que es necesario definir una estrategia de aceptación de riesgo.

- Inventario de activos: todos aquellos activos de información que tienen algún valor para la organización y que quedan dentro del alcance del SGSI.
- Identificar amenazas y vulnerabilidades: todas las que afectan a los activos del inventario.
- Identificar los impactos: los que podría suponer una pérdida de la confidencialidad, la integridad o la disponibilidad de cada uno de los activos.
- Análisis y evaluación de los riesgos: evaluar el daño resultante de un fallo de seguridad (es decir, que una amenaza explote una vulnerabilidad) y la probabilidad de ocurrencia del fallo; estimar el nivel de riesgo resultante y determinar si el riesgo es aceptable (en función de los niveles definidos previamente) o requiere tratamiento.
- Identificar y evaluar opciones para el tratamiento del riesgo: el riesgo quede reducido (mitigado mediante controles), eliminado (p. Ej., eliminando el activo), aceptado (de forma consciente) o transferido (p. Ej., con un seguro o un contrato de outsourcing).
- Selección de controles: seleccionar controles para el tratamiento el riesgo en función de la evaluación anterior y otros controles adicionales si se consideran necesarios.
- Aprobación por parte de la Dirección del riesgo residual y autorización de implantar el SGSI: hay que recordar que los riesgos de seguridad de la información son riesgos de negocio y sólo la Dirección puede tomar decisiones sobre su aceptación o tratamiento. El riesgo residual es el que queda, aún después de haber aplicado controles (el "riesgo cero" no existe prácticamente en ningún caso).
- Confeccionar una Declaración de Aplicabilidad: la llamada SOA (Statement of Applicability) es una lista de todos los controles seleccionados y la razón de su selección, los controles actualmente implementados y la justificación de cualquier control. Es, en definitiva, un resumen de las decisiones tomadas en cuanto al tratamiento del riesgo.

Implementación

En esta parte se definirá como se deberán tratar los riesgos, se creará conciencia entre el personal de la institución y se pondrá en marcha el SGSI (ver diagrama 2.9).

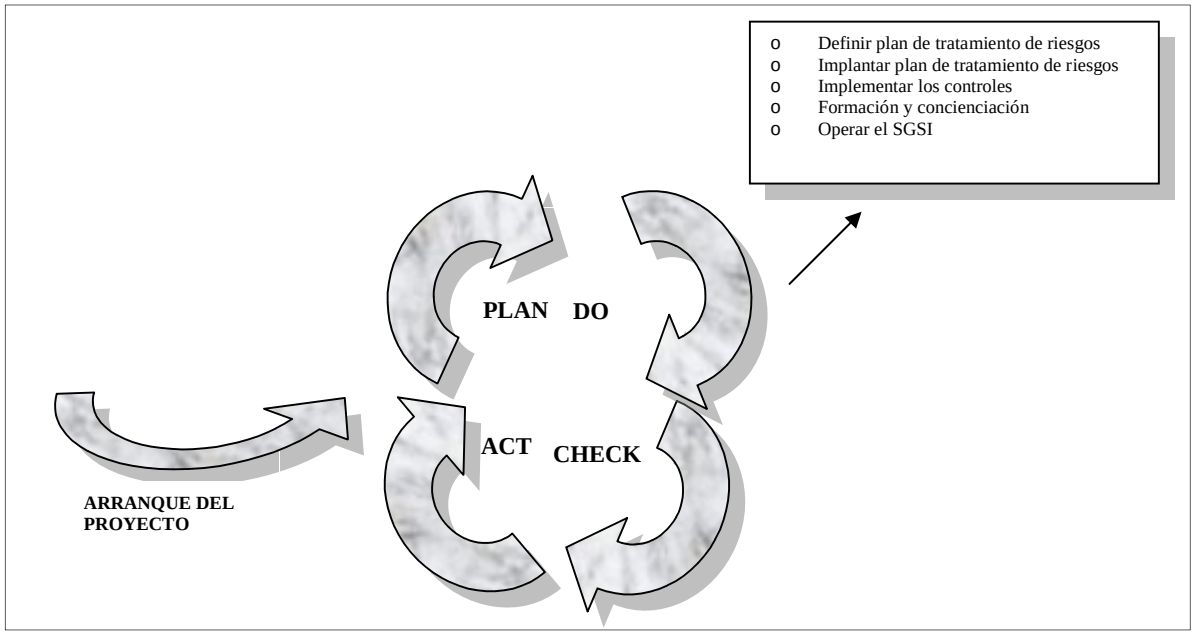


DIAGRAMA 2.9 IMPLEMENTACIÓN DEL PROYECTO

- Definir plan de tratamiento de riesgos: que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información.
- Implantar plan de tratamiento de riesgos: con la meta de alcanzar los objetivos de control identificados.
- Implementar los controles: todos los que se seleccionaron en la fase anterior.
- Formación y concienciación: de todo el personal en lo relativo a la seguridad de la información.
- Desarrollo del marco normativo necesario: normas, manuales, procedimientos e instrucciones.
- Gestionar las operaciones del SGSI y todos los recursos que se le asignen.

Monitorización

Aquí lo que se hará es vigilar que este siendo efectiva la implementación de nuestro SGSI, que los riesgos se hallan minimizado y auditar internamente nuestro sistema (ver diagrama 2.10).

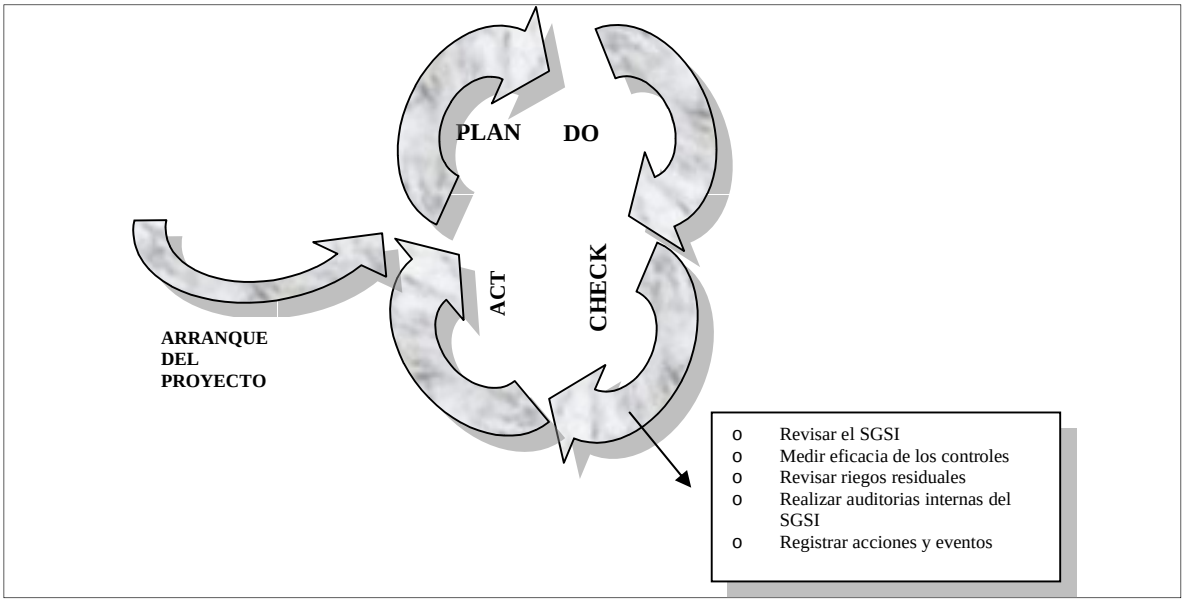


DIAGRAMA 2.10 MONITORIZACIÓN DEL PROYECTO

- Ejecutar procedimientos y controles de monitorización y revisión: para detectar errores en resultados de procesamiento, identificar brechas e incidentes de seguridad, determinar si las actividades de seguridad de la información están desarrollándose como estaba planificado, detectar y prevenir incidentes de seguridad mediante el uso de indicadores y comprobar si las acciones tomadas para resolver incidentes de seguridad han sido eficaces.
- Revisar regularmente la eficacia del SGSI: en función de los resultados de auditorías de seguridad, incidentes, mediciones de eficacia, sugerencias y feedback de todos los interesados.
- Medir la eficacia de los controles: para verificar que se cumple con los requisitos de seguridad.
- Revisar regularmente la evaluación de riesgos: los cambios en la organización, tecnología, procesos y objetivos de negocio, amenazas, eficacia de los controles o el entorno tienen una influencia sobre los riesgos evaluados, el riesgo residual y el nivel de riesgo aceptado.
- Realizar regularmente auditorías internas: para determinar si los controles, procesos y procedimientos del SGSI mantienen la conformidad con los requisitos de ISO 27001, el entorno legal y los requisitos y objetivos de seguridad de la organización, están implementados y mantenidos con eficacia y tienen el rendimiento esperado.
- Revisar regularmente el SGSI por parte de la Dirección: para determinar si el alcance definido sigue siendo el adecuado, identificar mejoras al proceso del

SGSI, a la política de seguridad o a los objetivos de seguridad de la información.

- Actualizar planes de seguridad: teniendo en cuenta los resultados de la monitorización y las revisiones.
- Registrar acciones y eventos que puedan tener impacto en la eficacia o el rendimiento del SGSI: sirven como evidencia documental de conformidad con los requisitos y uso eficaz del SGSI.

Mejora continua

En esta parte de nuestro proyecto se harán las correcciones que hagan falta para mejorar y optimizar nuestro sistema, así como acciones preventivas y comprobar la eficacia de las acciones tomadas (ver diagrama 2.11).

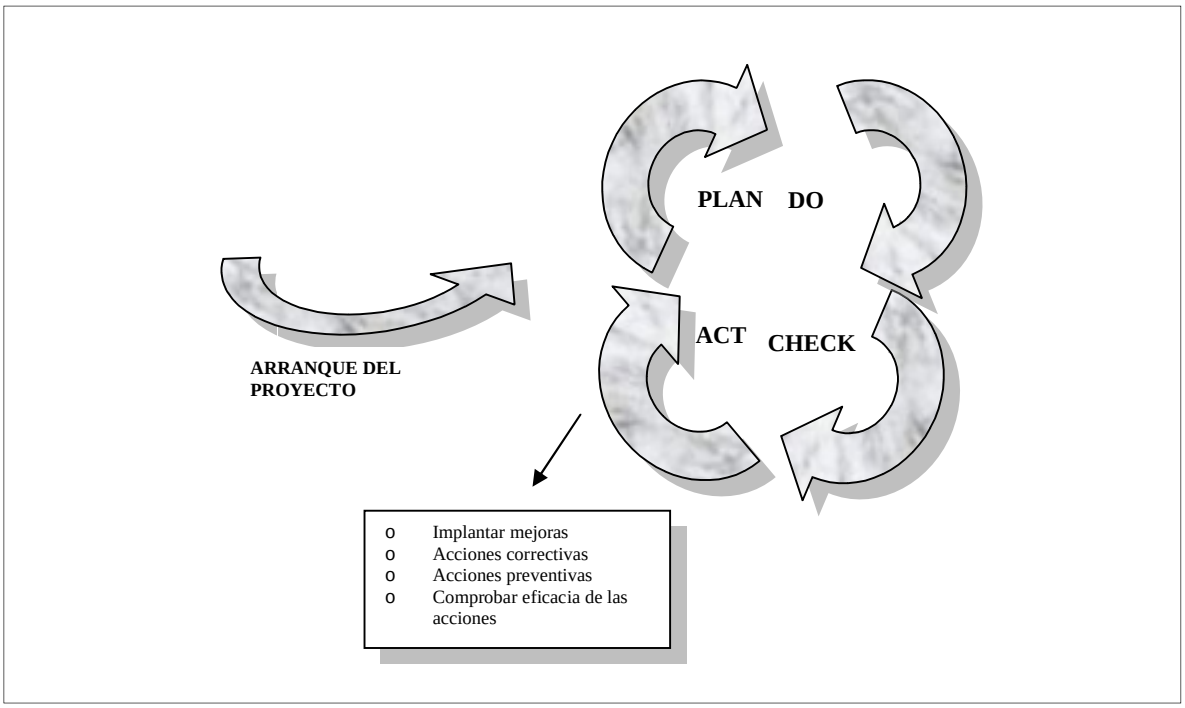


DIAGRAMA 2.11MEJORA CONTINUA DEL PROYECTO

- Implantar mejoras: poner en marcha todas las mejoras que se hayan propuesto en la fase anterior.
- Acciones correctivas: para solucionar no conformidades detectadas.
- Acciones preventivas: para prevenir potenciales no conformidades.
- Comunicar las acciones y mejoras: a todos los interesados y con el nivel adecuado de detalle.
- Asegurarse de que las mejoras alcanzan los objetivos pretendidos: la eficacia de cualquier acción, medida o cambio debe comprobarse siempre.

2.4.3.Aspectos Clave

Fundamentales

- Compromiso y apoyo de la Dirección de la organización.
- Definición clara de un alcance apropiado.
- Concienciación y formación del personal.
- Evaluación de riesgos exhaustiva y adecuada a la organización.
- Compromiso de mejora continua.
- Establecimiento de políticas y normas.
- Organización y comunicación. Integración del SGSI en la organización.

Factores de éxito

- La concienciación del empleado por la seguridad. Principal objetivo a conseguir.
- Realización de comités de dirección con descubrimiento continuo de no conformidades o acciones de mejora.
- Creación de un sistema de gestión de incidencias que recoja notificaciones continuas por parte de los usuarios (los incidentes de seguridad deben ser reportados y analizados).
- La seguridad absoluta no existe, se trata de reducir el riesgo a niveles asumibles. La seguridad no es un producto, es un proceso.
- La seguridad no es un proyecto, es una actividad continua y el programa de protección requiere el soporte de la organización para tener éxito.
- La seguridad debe ser inherente a los procesos de información y del negocio.

Riesgos

- Exceso de tiempos de implantación: con los consecuentes costos descontrolados, desmotivación, alejamiento de los objetivos iniciales, etc.
- Temor ante el cambio: resistencia de las personas.
- Discrepancias en los comités de dirección.
- Delegación de todas las responsabilidades en departamentos técnicos.
- No asumir que la seguridad de la información es inherente a los procesos de negocio.
- Planes de formación y concienciación inadecuados.
- Calendario de revisiones que no se puedan cumplir.
- Definición poco clara del alcance.
- Falta de comunicación de los progresos al personal de la organización.

Consejos básicos

- Mantener la sencillez y restringirse a un alcance manejable y reducido: un centro de trabajo, un proceso de negocio clave, un único centro de proceso de datos o un área sensible concreta; una vez conseguido el éxito y observados los beneficios, ampliar gradualmente el alcance en sucesivas fases.
- Comprender en detalle el proceso de implantación: iniciarlo con base en cuestiones exclusivamente técnicas es un error frecuente que rápidamente sobrecarga de problemas la implantación; adquirir experiencia de otras implantaciones, asistir a cursos de formación o contar con asesoramiento de consultores externos.

- La autoridad y compromiso decidido de la Dirección de la empresa -incluso si al inicio el alcance se restringe a un alcance reducido- evitarán un muro de excusas para desarrollar las buenas prácticas, además de ser uno de los puntos fundamentales de la norma.
- La certificación como objetivo: aunque se puede alcanzar la conformidad con la norma sin certificarse, la certificación por un tercero asegura un mejor enfoque, un objetivo más claro y tangible y, por lo tanto, mejores opciones de alcanzar el éxito.
- No reinventar la rueda: aunque el objetivo sea ISO 27001, es bueno obtener información relativa a la gestión de la seguridad de la información de otros métodos y marcos reconocidos.
- Servirse de lo ya implementado: otros estándares como ISO 9000 son útiles como estructura de trabajo, ahorrando tiempo y esfuerzo; es conveniente pedir ayuda e implicar a auditores internos y responsables de otros sistemas de gestión.
- Reservar la dedicación necesaria diaria o semanal: el personal involucrado en el proyecto debe ser capaz de trabajar con continuidad en el proyecto.
- Registrar evidencias: deben recogerse evidencias al menos tres meses antes del intento de certificación para demostrar que el SGSI funciona adecuadamente.

CAPÍTULO 3

CONSIDERACIONES PARA LA ELABORACIÓN DE UN SISTEMA DE GESTIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN (SGSI)

3. CONSIDERACIONES PARA LA ELABORACIÓN DE UN SISTEMA DE GESTIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN (SGSI)

3.1. Administración de riesgos

Como ya se ha mencionado, dentro de una empresa o institución lo más importante que se tiene es la información por lo cual debemos tener técnicas que nos aseguren no solo la seguridad física sino también la información que se almacena dentro de nuestros equipos. A este tipo de seguridad se le llama lógica la cual nos va a brindar la aplicación de "barreras " o "procedimientos" que va a permitir el acceso solo a aquellas personas que estén autorizadas para hacerlo.

"La administración de riesgos es una aproximación científica del comportamiento de los riesgos, anticipando posibles pérdidas accidentales con el diseño e implementación de procedimientos que minimicen la ocurrencia de pérdidas o el impacto financiero de las pérdidas que puedan ocurrir"[1].

3.1.1. Clasificación de los riesgos

"Ninguna empresa tiene suficiente dinero y personal para eliminar por completo todos sus posibles riesgos asociados a IT"[2]*, señala George Kurtz, vicepresidente senior de Administración de riesgos de McAfee. "Por ello, se debe ser capaz de cuantificar los riesgos que enfrenta y asignar prioridad a sus inversiones en seguridad de acuerdo con ellos."*[3]

A fin de cuantificar los riesgos y asignar prioridad a las medidas de corrección, Kurtz, propone un modelo que permite medir el riesgo según tres factores: valor de los activos, vulnerabilidad de los activos y amenazas reales.

- **Valor de los activos**

Un servidor que procesa transacciones equivalentes a miles de dólares cada minuto obviamente constituye un activo más vital que el computador de un representante de atención al cliente. De esta forma, una estrategia de reducción de riesgos inteligente exige tener una clara noción del valor que los diferentes

[1] Kurtz George, vicepresidente senior de Administración de riesgos de McAfee (http://www.mcafee.com/mx/enterprise/security_insights/measuring_risk_gauge_vulnerability.html)

[2] Kurtz George, vicepresidente senior de Administración de riesgos de McAfee (http://www.mcafee.com/mx/enterprise/security_insights/measuring_risk_gauge_vulnerability.html)

[3] Kurtz George, vicepresidente senior de Administración de riesgos de McAfee (http://www.mcafee.com/mx/enterprise/security_insights/measuring_risk_gauge_vulnerability.html)

activos de IT en la empresa tienen para el negocio.

- **Vulnerabilidad de los activos**

Además de poseer diferente valor para el negocio, los activos de IT poseen distintos niveles de vulnerabilidad inherente. Un sistema del que dependen páginas Web públicas resulta más vulnerable que uno que no está conectado a Internet. Y un interruptor asegurado en un gabinete de cables eléctricos está menos expuesto que un equipo portátil que se encuentra a miles de kilómetros del perímetro de seguridad de la empresa.

- **Amenazas reales**

Finalmente, los equipos de seguridad deben tener una idea clara de las amenazas reales a las que se expone un activo determinado. Los exploits se dirigen más hacia los sistemas operativos populares en términos comerciales, por ejemplo, que a los sistemas más antiguos. Por ello, si bien las aplicaciones más antiguas que se ejecutan en aquellos sistemas anteriores pueden tener un alto valor para la empresa, también constituyen el objetivo de menos amenazas y, por lo tanto, plantean un riesgo substancial menor para la empresa que las aplicaciones que se ejecutan en Microsoft Windows o Linux™.

Estos tres elementos pueden ser ilustrados en la siguiente diagrama (ver diagrama 3.1).

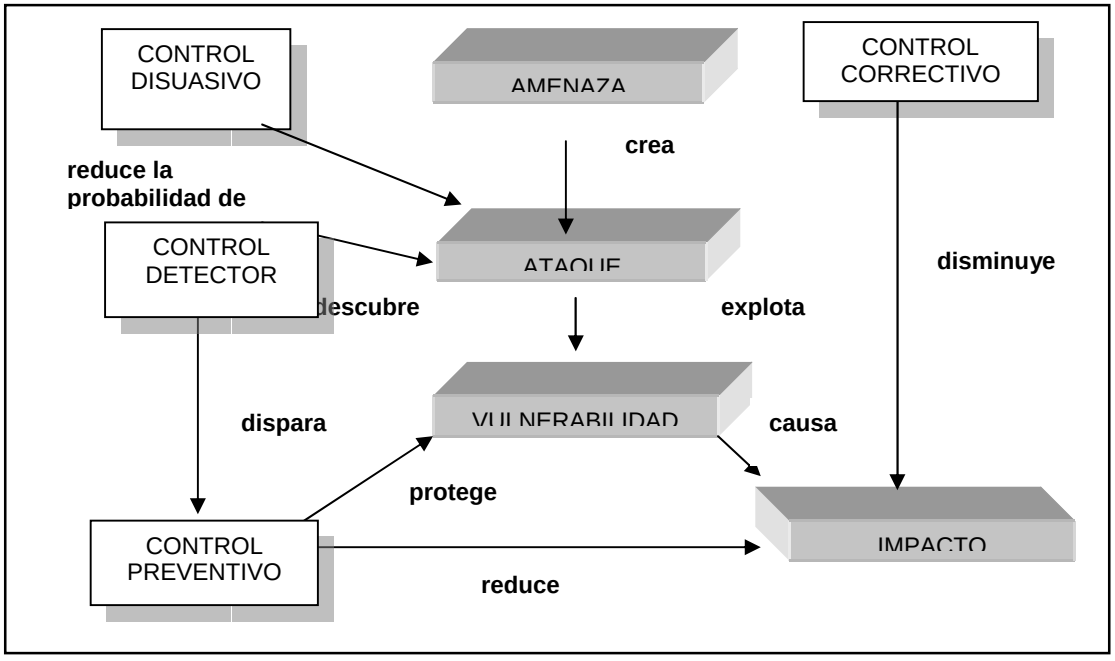


DIAGRAMA 3.1 MODELO RELACIONAL SIMPLE

"Es posible calcular el riesgo según el valor comercial del activo, su vulnerabilidad inherente y la intensidad de las amenazas a las que realmente se ve sometido."[4]

3.1.2.Estrategias de administración de riesgos

Además de comprender los niveles específicos de riesgo, los equipos de seguridad pueden incrementar de manera importante su efectividad al ampliar su perspectiva en cuanto a cómo es posible superar los riesgos asociados a IT. Kurtz señala cuatro posibles estrategias de administración de riesgos: reducción de riesgos, aceptación de riesgos, transferencia de riesgos y prevención de riesgos.

Reducción de riesgos: normalmente, ésta es la primera respuesta que viene a la mente ante un riesgo. Incluye todas las contramedidas que adoptan los equipos de seguridad contra amenazas, entre las que se encuentran firewalls, detección de intrusos y antivirus.

Aceptación de riesgos: si el costo de superar un riesgo es mayor que el del riesgo mismo, o si superar dicho riesgo absorberá recursos que se utilizarían para superar un riesgo mucho más serio, la medida más conveniente es limitarse a aceptar el riesgo.

Transferencia de riesgos: en algunos casos, una medida más prudente es transferir el riesgo a un tercero, como una empresa de seguros, que asignarlo a recursos limitados, cuyos esfuerzos por reducirlo probablemente serán infructuosos.

Prevención de riesgos: existen situaciones en las que el nivel de riesgo y el costo de superarlo son simplemente inadmisibles. En tales casos, resulta más conveniente evitar el riesgo, ya sea al retirar el sistema afectado o simplemente al no implementarlo.

"Si piensa que debe mitigar cada riesgo que enfrenta, agotará sus recursos antes de eliminar las posibilidades de exposición"[5]*, afirma Kurtz. "Debe utilizar una combinación de estrategias basada en la naturaleza de su entorno de IT y en el tamaño de su presupuesto de seguridad."* [6]

Los equipos de seguridad pueden incrementar su eficacia al automatizar la mayor cantidad posible de procesos de administración de riesgos, desde el

[4] Kurtz George, vicepresidente senior de Administración de riesgos de McAfee (http://www.mcafee.com/mx/enterprise/security_insights/measuring_risk_gauge_vulnerability.html)
[5] Kurtz George, vicepresidente senior de Administración de riesgos de McAfee (http://www.mcafee.com/mx/enterprise/security_insights/measuring_risk_gauge_vulnerability.html)

[6] Kurtz George, vicepresidente senior de Administración de riesgos de McAfee (http://www.mcafee.com/mx/enterprise/security_insights/measuring_risk_gauge_vulnerability.html)

descubrimiento de activos y la evaluación del riesgo asociado a ellos a verificar que los procedimientos de reparación se hayan ejecutado correctamente y generen los resultados esperados.

De acuerdo con la empresa de investigación de IT Gartner, las organizaciones que implementan procesos y tecnologías de administración de riesgos apropiados para descubrir, organizar por prioridad y corregir las vulnerabilidades tienen un 90% menos de probabilidad de ser víctimas de un ataque exitoso.

"El gran mito popular es que para contar con suficiente seguridad basta sólo instalar un firewal"[7]*, comenta Kurtz. "La realidad es que su nivel de seguridad depende en gran medida de lo bien que comprende y administra el riesgo en todas sus diversas formas y con cuanta eficiencia concentra sus limitados recursos donde serán más útiles."* [8]

3.2. Análisis de Riesgos

El Consejo Superior de Informática y para el impulso de Administración Electrónica da la siguiente definición de Análisis de Riesgos:

”Identificación de las amenazas que acechan a los activos (componentes pertenecientes o relacionados con el sistema de información) y determinación de la vulnerabilidad de los activos ante esas amenazas. Con lo anterior se estima el impacto o grado de perjuicio que una seguridad insuficiente puede tener para la organización a partir del cual se calcula el riesgo que se corre.”[9]

El objetivo general del análisis de riesgos es identificar sus causas potenciales, en el siguiente diagrama se muestran los principales riesgos que amenazan el entorno informático (ver diagrama 3.2).

[7] Kurtz George, vicepresidente senior de Administración de riesgos de McAfee (http://www.mcafee.com/mx/enterprise/security_insights/measuring_risk_gauge_vulnerability.html)

[8] Kurtz George, vicepresidente senior de Administración de riesgos de McAfee (http://www.mcafee.com/mx/enterprise/security_insights/measuring_risk_gauge_vulnerability.html)

[9] Consejo Superior de Informática y para el impulso de Administración Electrónica

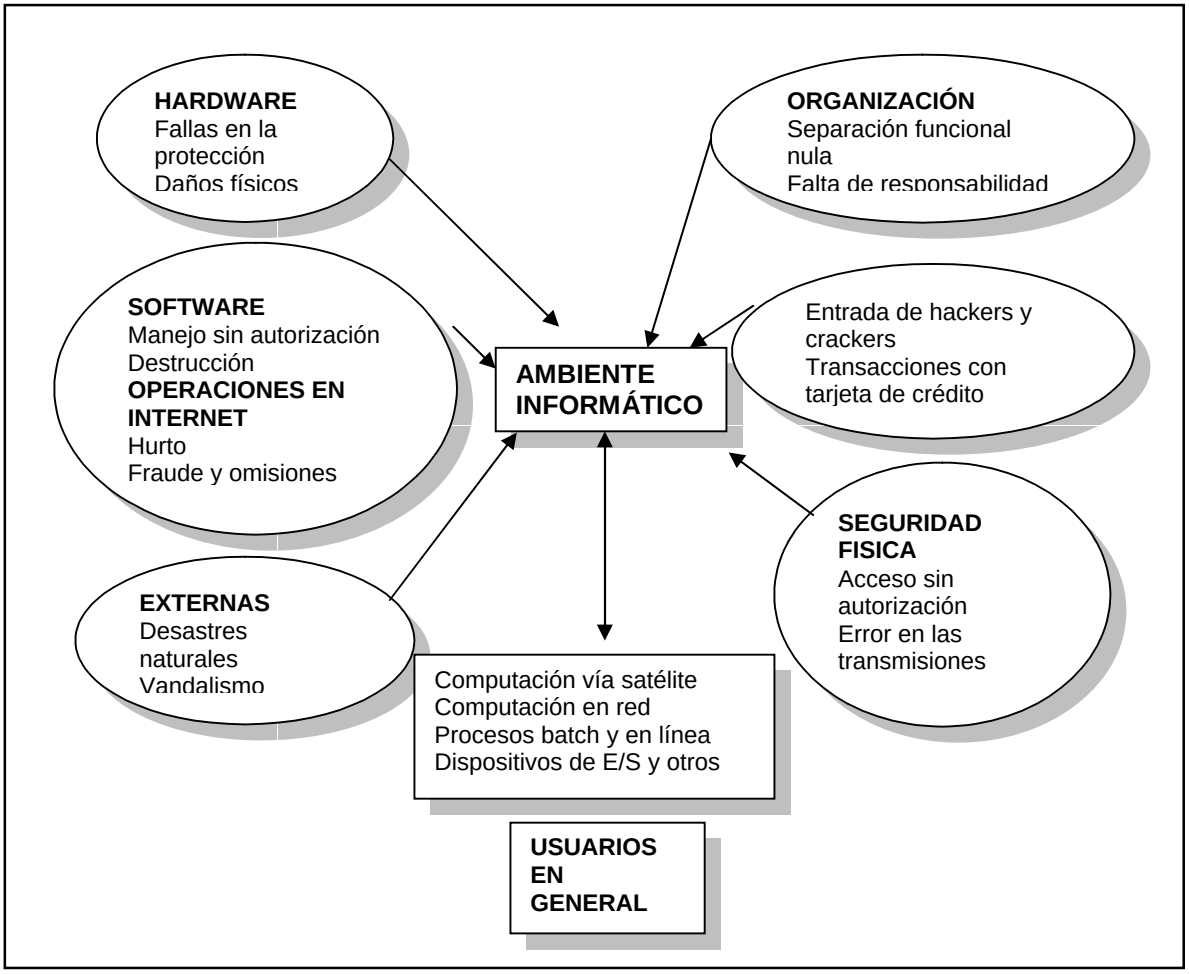


DIAGRAMA 3.2 "PRINCIPALES AMENAZAS QUE AFECTAN A UN AMBIENTE INFORMÁTICO"

El análisis de riesgos debe cumplir los siguientes objetivos:

- Analizar el tiempo, esfuerzo y recursos disponibles y necesarios para atacar los problemas.
- Llevar a cabo un minucioso análisis de los riesgos y debilidades.
- Identificar, definir y revisar los controles de seguridad.
- Determinar si es necesario incrementar las medidas de seguridad.

Cuando se identifican los riesgos, los perímetros de seguridad y los sitios de mayor peligro, nos permiten hacer el mantenimiento del sistema más fácilmente.

Antes de realizar el análisis de riesgos debemos tomar en cuenta los siguientes aspectos:

- Las políticas y las necesidades de la organización así como la colaboración
- Los nuevos avances tecnológicos y la astucia de intrusos expertos.

- Tomar en cuenta los costos $^{v}_{s}$ la efectividad del programa, en el que se va a desarrollar los mecanismos de control.
- El comité o la junta directiva de toda organización debe incluir en sus planes y presupuesto los gastos necesarios para el desarrollo de programas de seguridad, así como tener en cuenta que esta parte es fundamental de todo proceso de desarrollo de la empresa, especificar los niveles de seguridad y las responsabilidades de las personas relacionadas, las cuales son complemento crucial para el buen funcionamiento de todo programa de seguridad.
- Otro aspecto que se debe tener en cuenta es la sobrecarga adicional que los mecanismos y contramedidas puedan tener sobre el entorno informático, sin olvidar los costos adicionales que se generan por su implementación.
- El análisis de riesgos utiliza el método matricial llamado MAPA DE RIESGOS, para identificar la vulnerabilidad de un servicio o negocio a riesgos típicos, este método contiene los siguientes pasos:

    o Localización de los procesos en las dependencias que intervienen en la prestación del servicio (Ver tabla 3.1).

PROCESOS	DEPENDENCIAS			
	DIVISION FINANCIERA	SISTEMAS	CARTERA	CONTABILIDAD
Gestión de centros de transaccionales	X	X	X	
Administración de sistemas		X		
Atención al cliente		X	X	
Conciliación de cuentas	X			X

TABLA 3.1MATRIZ DE DEPENDENCIAS VS PROCESOS

    o Localización de los riesgos críticos y su efecto en los procesos del Negocio. En este paso se determina la vulnerabilidad de una actividad a una amenaza. Para asignar un peso a cada riesgo se consideran tres categorías de vulnerabilidad (1 baja, 2 media, 3 alta) que se asignan a cada actividad de acuerdo a su debilidad a una amenaza (causa de riesgo). Por ejemplo, si afirmamos que el riesgo a una Decisión equivocada tiene alto riesgo de vulnerabilidad, entonces tendría alta prioridad dentro de nuestras políticas de seguridad (Ver tabla 3.2).

RIESGO	(%) Obtenido	Vulnerabilidad
Decisiones equivocadas	**59**	ALTA
Fraude	**55**	MEDIA
Hurto	**54**	MEDIA

TABLA 3.2 "MATRIZ DE RIESGOS VS. VULNERABILIDAD "

Dentro del entorno informático las amenazas (causas de riesgo) se pueden clasificar así:

- Naturales

Incluyen principalmente los cambios naturales que pueden afectar de una manera u otra el normal desempeño del entorno informático; por ejemplo, la posibilidad de un incendio en el sitio donde se encuentran los concentradores de cableado dado que posiblemente están rodeados de paredes de madera es una amenaza natural.

- Accidentales

Son las más comunes que existen e incluyen:

  - Errores de los usuarios finales: El usuario tiene permisos de administrador y posiblemente sin intención modifica información relevante.
  - Errores de los operadores: El operador tenía una sesión abierta y olvidó salir del sistema; alguien con acceso físico a la máquina en cuestión puede causar estragos.
  - Error administrativo: Las Instalaciones y configuraciones no cuentan con mecanismos de seguridad para su protección.
  - Errores de salida: Impresoras u otros dispositivos mal configurados.
  - Errores del sistema: Daños en archivos del sistema operativo.
  - Errores de comunicación: Permitir la transmisión de información violando la confidencialidad de los datos.

- Deliberadas

Estas amenazas pueden ser: activas (accesos no autorizados, modificaciones no autorizadas, sabotaje) o pasivas (son de naturaleza mucho más técnica, como: emanaciones electromagnéticas y/o microondas de interferencia).

  - Localización de los riesgos críticos en las dependencias de la empresa y procesos que intervienen en el negocio (Ver tablas 3.3 y 3.4).

Proceso / Riesgo	Decisiones equivocadas	Fraude	Hurto
Gestión de centros transaccionales		X	X
Administración de sistemas		X	X
Atención al cliente		X	X
Conciliación de cuentas	X	X	X

TABLA 3.3 MATRIZ DE PROCESOS $^{V}_{S}$ RIESGO

Riesgos ^{V}s Dependencias.	División Financiera	Sistemas	Cartera	Contabilidad
Decisiones equivocadas	X			X
Fraude	X	X	X	X
Hurto	X	X	X	X

TABLA 3.4 MATRIZ DE RIESGO $^{V}_{S}$ DEPENDENCIA

- Identificar los controles necesarios

En este paso se precisan los controles, los cuales son mecanismos que ayudan a disminuir el riesgo a niveles mínimos o en algunos casos eliminarlos por completo. Se debe tener en cuenta que dichas medidas tienen tres diferentes capacidades que incluyen: mecanismos de prevención, mecanismos de detección y mecanismos de corrección; y que dentro de un proceso ó negocio funcionan como se describe en la diagrama 3.3 En este paso se incluye la funcionalidad y utilidad del control, y se identifican las personas responsables de la implantación de los controles.

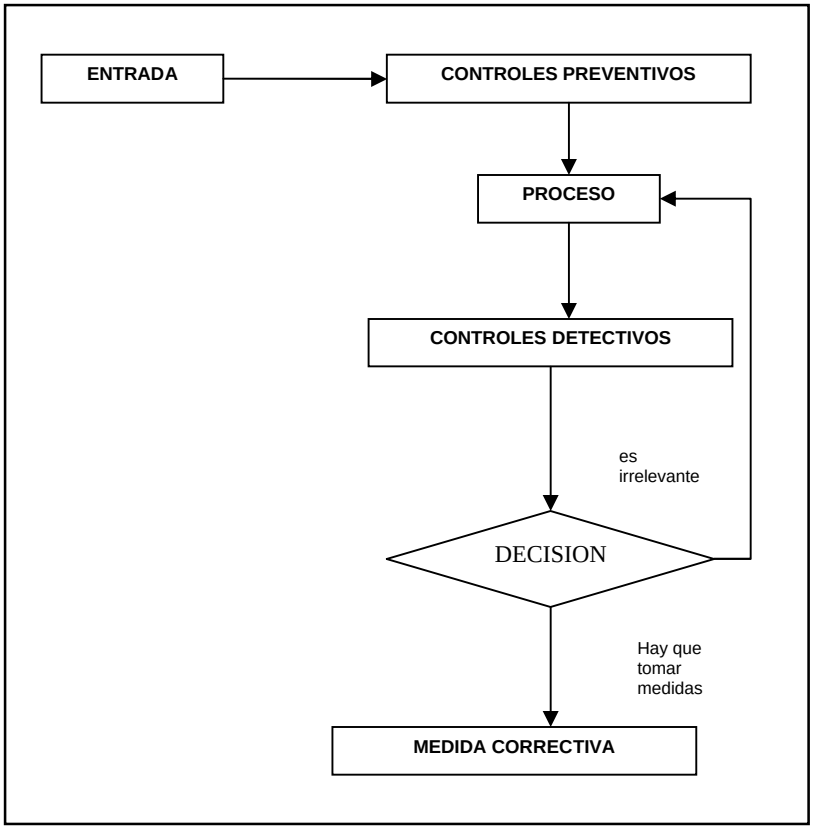


DIAGRAMA 3.3 FUNCIÓN DE LAS MEDIDAS DE CONTROL PREVENTIVAS, DE DETECCIÓN Y CORRECTIVAS.

- Diseñar los controles definitivos

En este paso se tienen los productos necesarios para iniciar el proceso de implantación de los controles utilizados o bien para empezar la construcción de dichos mecanismos.

Los siguientes criterios permiten evaluar los mecanismos de control:

o Confidencialidad

Se refiere a la protección de la información principalmente de accesos no autorizados. Información del personal, investigaciones y reportes de desarrollo son algunos de los ejemplos de información que necesita confidencialidad.

o Integridad

Es el servicio ofrecido por el departamento de informática. Debe ser adecuado, completo y auténtico en el momento de ser procesada, presentada, guardada o transmitida la información.

- Disponibilidad

Indica la disponibilidad que pueden tener en un determinado momento las actividades informáticas. Esta disponibilidad debe ser inmediata.

- Resultados del análisis de riesgos

Los resultados del análisis de riesgos, deben dados a conocer oportunamente para que sean incorporados, desde las primeras fases del proceso.

- Verificar por parte de la auditoria informática, la incorporación oportuna de los controles

La auditoria informática debe conocer el resultado del análisis de riesgos y verificar su implantación oportuna, para asegurar los mejores niveles de calidad, seguridad y efectividad de los procesos informáticos.

3.2.1.Pasos del análisis de riesgos

Para llevar a cabo un análisis de riesgo es necesario tomar en cuenta algunos aspectos, los cuales son el nivel actual de riesgo, las consecuencias que podrían acarrear dichos riesgos y qué hacer en caso de que el riesgo llegue a ser alto.

Los pasos a seguir para realizar este análisis son los siguientes:

1. **Identificar y evaluar los activos**

Para comenzar debemos saber cuál es el valor de los activos que necesitamos proteger. Este valor es de gran importancia ya que no solo es monetario también se basa en diferentes características como son; su costo, sensibilidad, misión crítica o la misma combinación de estas propiedades. El valor del activo será utilizado más tarde para determinar la magnitud de pérdida cuando la amenaza ocurra.

2. **Identificación de amenazas**

Ya que identificamos los activos que requieren de protección ahora corresponde a las amenazas a estas las tenemos que identificar y examinar para determinar el grado de pérdida en caso de que dichas amenazas se presenten. Aquí tendremos que observar qué amenazas afectan al sistema o la red y con que frecuencia ocurren, debemos considerar en este punto, que entren al sistema personas no autorizadas, que se pueda tener acceso a información confidencial, que el acceso esté bloqueado, la desconfiguración de la red o sistema, errores internos del software utilizado.

3. Identificar y describir las vulnerabilidades

La relación entre las amenazas y las vulnerabilidades nos va a determinar el nivel de riego que existe en el sistema. Por lo general para que exista un riesgo, las amenazas van ligadas a una vulnerabilidad, pero hay ocasiones en que existen áreas que son altamente vulnerables pero no tienen consecuencias al no existir amenaza alguna.

4. Determinación del impacto de la ocurrencia de una amenaza

Cuando una amenaza se lleva a cabo, los activos sufren grandes daños, en donde las pérdidas son catalogadas en áreas de impacto, las cuales citaremos a continuación:

- *Revelación*: cuando la información es procesada y se pierde la confidencialidad.
- *Modificación*: cuando el activo o contenido a sido cambiado de su estado original sin permiso alguno.
- *Destrucción*: cuando se pierde por completo el activo o su contenido.
- *Denegación de servicio*: Cuando el sistema no permite el acceso a éste por determinado tiempo.

5. Controles en el lugar

El tener los controles debidamente identificados va a permitir recolectar los datos durante el análisis de riesgo. Dos de estos tipos son:

- Controles requeridos

Estos controles los podemos agrupar en una o más reglas escritas. La manera en que almacenemos y ordenemos nuestros datos y su almacenamiento en el sistema o en la red y el modo en el que opera determinará las reglas a aplicar, cuales son lo controles que se requieren.

- Controles discrecionales

Los controles requeridos en muchas ocasiones no disminuyen el nivel de vulnerabilidad a un nivel aceptable, por lo que los administradores recurren a los controles direccionales para lograrlo.

6. Determinar los riegos residuales (conclusiones)

Al final siempre va a existir un riego residual pero debemos determinar que tan aceptable es o no. El riesgo residual al final va a tomar 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.
- Todas los controles que no están dentro del lugar.

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

7. Identificar los controles adicionales (recomendaciones)

Ya que se determinó el nivel de riesgo residual existente. Ahora se debe saber la manera más efectiva y menos costosa para reducir el riesgo. La relación una vez que el riesgo residual haya sido determinado, el siguiente paso es identificar la forma más efectiva y menos costosa para reducir el riesgo a un nivel aceptable. Una relación entre costo, conveniencia, tiempo debe llevarse a cabo al mismo tiempo que los controles adicionales son implementados. Las recomendaciones son:

- *Recomendación de controles requeridos*: Comenzar a evaluar cuales son los controles con los que no contamos y que son obligatorios o requeridos.
- *Recomendación de controles discrecionales*: Esta recomendación va dirigida a los controles que son necesarios par reducir el nivel de riego.

8. Preparar un informe del análisis del riesgo

El análisis de riesgo tiene como objetivos identificar a los activos con riesgo, tomar en cuenta las medidas protectoras y minimizar los efectos del riesgo, asignar un costo a cada control. Este proceso también determina si los controles son efectivos. Cuando el análisis está completo, un informe de la evaluación del riesgo debe prepararse. Los detalles técnicos del reporte deben incluir como mínimo:

- Niveles de vulnerabilidad.
- Amenazas correspondientes y su frecuencia.
- El ambiente usado.
- Conexión del sistema.
- Nivel o niveles de sensibilidad de 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 un método formal para investigar los riesgos de un sistema informático y recomendar las medidas apropiadas que deben adoptarse 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. Este análisis es fundamental para cualquier organización que valore su información.

3.3.Evaluación de un Esquema de Seguridad

Cuando hablamos de realizar una evaluación de la seguridad es importante conocer cómo desarrollar y ejecutar la implantación de un sistema de seguridad.

Desarrollar un sistema de seguridad significa planear, organizar, coordinar, dirigir y controlar las actividades relacionadas destinadas a mantener y garantizar la integridad física y lógica de los recursos implicados en la función informática, así como el resguardo de los activos de la empresa.

Las consideraciones de un sistema integral de seguridad deben contemplar:

- Definir elementos administrativos
- Definir políticas de seguridad (a nivel departamental e institucional).
- Organizar y dividir las responsabilidades
- Contemplar la seguridad física del centro de cómputo contra catástrofes naturales.
- Definir prácticas de seguridad para el personal.
- Desarrollar Plan de emergencia, plan de evacuación, uso de recursos de emergencia.
- Definir el tipo de pólizas de seguros.
- Definir elementos técnicos de procedimientos.
- Definir las necesidades de sistemas de seguridad para hardware y software poniendo atención al flujo de energía dentro del centro de cómputo y a los cableados locales y externos.
- Aplicar Aplicación de los sistemas de seguridad incluyendo datos y archivos.
- Atender Atendiendo a la creación de políticas de destrucción de basura, copias, fotocopias, etc.
- Planificar Planificación de los papeles de los auditores internos y externos.
- Planificar Planificación de programas de desastre y sus pruebas (simulación).
- Planificar Planificación de equipos de contingencia con carácter periódico.
- Controlar Control de desechos de los nodos importantes del sistema.

Para dotar de medios necesarios al elaborar un sistema de seguridad se deben considerar los siguientes puntos:

- Sensibilizar a los ejecutivos de la organización en torno al tema de seguridad
- Realizar un diagnóstico de la situación de riesgo y seguridad de la información en la organización a nivel software, hardware, recursos humanos y ambientales.
- Elaborar un plan para desarrollar el programa de seguridad.

Plan de Seguridad

Un plan de seguridad es un documento que describe cómo una organización plantea sus necesidades de seguridad. El plan debe sujetarse a revisiones periódicas, según las necesidades de seguridad vayan cambiando.

Un buen plan de seguridad es un documento oficial de las prácticas de seguridad vigentes en una organización. También debe contemplar el hacer cambios o mejorar las prácticas de seguridad de una manera estructurada. Por lo que también puede ser útil para medir el efecto de los cambios y sugerir otras mejoras.

El plan debe identificar y organizar las actividades de seguridad para un sistema de cómputo; además de abarcar la situación actual y los cambios proyectados a través de los aspectos que a continuación se mencionan.

3.3.1.Políticas

Las políticas de seguridad informática surgen como una herramienta organizacional para concienciar a los colaboradores de una organización sobre la importancia y sensibilidad de la información. Ante esta situación, el proponer o identificar una política de seguridad requiere un alto compromiso con la organización, agudeza técnica para establecer fallas y debilidades, y constancia para renovar y actualizar dicha política en función del dinámico ambiente que rodea las organizaciones modernas.

Una política de seguridad informática es un conjunto de reglas que indican de manera clara y concisa qué es lo que está permitido realizar dentro de la organización, así como imponer las sanciones correspondientes para cualquier violación a las normas establecidas. De esta manera se permite una comunicación con los usuarios, ya que las políticas establecen un canal formal de actuación del personal, en relación con los recursos y servicios informáticos de la organización.

No se puede considerar que una política de seguridad informática es una descripción técnica de mecanismos, ni una expresión legal que involucre sanciones a conductas de los empleados, es más bien una descripción de los que deseamos proteger y el por qué de ello, pues cada política de seguridad es una invitación a cada uno de sus miembros a reconocer la información como uno de sus principales activos. Por tal razón, las políticas de seguridad deben concluir en una posición consciente y vigilante del personal por el uso y limitaciones de los recursos y servicios informáticos.

Elementos de una Política de Seguridad Informática

Como una política de seguridad debe orientar las decisiones que se toman en relación con la seguridad, se requiere la disposición de todos los miembros de la organización para lograr una visión conjunta de lo que se considera importante.

Las Políticas de Seguridad Informática deben considerar principalmente los siguientes elementos:

- Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica.
- Objetivos de la política y descripción clara de los elementos involucrados en su definición.
- Responsabilidades por cada uno de los servicios y recursos informáticos aplicado a todos los niveles de la organización.
- Requerimientos mínimos para configuración de la seguridad de los sistemas que abarca el alcance de la política.
- Definición de violaciones y sanciones por no cumplir con las políticas.
- Responsabilidades de los usuarios con respecto a la información a la que tiene acceso.

Las políticas de seguridad informática, también deben ofrecer explicaciones comprensibles sobre por qué deben tomarse ciertas decisiones y explicar la importancia de los recursos. Igualmente, deberán establecer las expectativas de la organización en relación con la seguridad y especificar la autoridad responsable de aplicar los correctivos o sanciones.

Otro punto importante, es que las políticas de seguridad deben redactarse en un lenguaje sencillo y entendible, libre de tecnicismos y términos ambiguos que impidan una comprensión clara de las mismas, claro está sin sacrificar su precisión.

Por último, las políticas de seguridad, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes, como son: el aumento de personal, cambios en la infraestructura computacional, alta rotación de personal, desarrollo de nuevos servicios, regionalización de la empresa, cambio o diversificación del área de negocios, etc.

Parámetros para establecer Políticas de Seguridad

Es importante que al momento de formular las políticas de seguridad informática, se consideren por lo menos los siguientes aspectos:

- Efectuar un análisis de riesgos informáticos, para valorar los activos y así adecuar las políticas a la realidad de la empresa.
- Reunirse con los departamentos dueños de los recursos, ya que ellos poseen la experiencia y son la principal fuente para establecer el alcance y definir las violaciones a las políticas.
- Comunicar a todo el personal involucrado sobre el desarrollo de las políticas, incluyendo los beneficios y riesgos relacionados con los recursos y bienes, y sus elementos de seguridad.

- Identificar quién tiene la autoridad para tomar decisiones en cada departamento, pues son ellos los interesados en salvaguardar los activos críticos su área.
- Monitorear periódicamente los procedimientos y operaciones de la empresa, de forma tal, que ante cambios las políticas puedan actualizarse oportunamente.
- Detallar explícita y concretamente el alcance de las políticas con el propósito de evitar situaciones de tensión al momento de establecer los mecanismos de seguridad que respondan a las políticas trazadas.

Razones que impiden la Aplicación de las Políticas de Seguridad Informática

A pesar de que un gran número de organizaciones canalizan sus esfuerzos para definir directrices de seguridad y concretarlas en documentos que orienten las acciones de las mismas, muy pocas alcanzan el éxito, ya que la primera barrera que se enfrenta es convencer a los altos ejecutivos de la necesidad y beneficios de buenas políticas de seguridad informática.

Esta situación ha llevado a que muchas empresas con activos muy importantes, se encuentren expuestas a graves problemas de seguridad y riesgos innecesarios, que en muchos casos comprometen información sensitiva y por ende su imagen corporativa. Ante esta situación, los encargados de la seguridad deben confirmar que las personas entienden los asuntos importantes de la seguridad, conocen sus alcances y están de acuerdo con las decisiones tomadas en relación con esos asuntos.

Si se quiere que las políticas de seguridad sean aceptadas, deben integrarse a las estrategias del negocio, a su misión y visión, con el propósito de que los que toman las decisiones reconozcan su importancia e incidencias en las proyecciones y utilidades de la compañía.

Finalmente, es importante señalar que las políticas por sí solas no constituyen una garantía para la seguridad de la organización, ellas deben responder a intereses y necesidades organizacionales basadas en la visión de negocio, que lleven a un esfuerzo conjunto de sus actores por administrar sus recursos, y a reconocer en los mecanismos de seguridad informática factores que facilitan la formalización y materialización de los compromisos adquiridos con la organización.

Estado Actual

Esto es, describir el estado de la seguridad de la organización al momento de iniciar la elaboración de un plan de seguridad. Esta situación incluye una lista de los bienes de la organización que necesitan ser protegidos, las posibles amenazas y las medidas precautorias.

El plan debe definir límites de responsabilidad: especificar los bienes que deben ser protegidos; qué grupos son excluidos, en el caso de que sea una empresa que tiene contacto con otras organizaciones vía red; y el perímetro de protección de la organización

3.3.2.Recomendaciones y requerimientos

Al realizar la evaluación de la seguridad es importante también conocer cómo desarrollar y ejecutar el implantar un sistema de seguridad.

Desarrollar un sistema de seguridad significa: planear, organizar coordinar dirigir y controlar las actividades relacionadas a mantener y garantizar la integridad física de los recursos implicados en la función informática, así como el resguardo de los activos de la empresa, en este caso se considera la información como uno de los bienes mas importantes a resguardar.

Plan de Seguridad Ideal (o Normativo)

Un plan de seguridad para un sistema de seguridad integral debe:

- Asegurar la integridad y exactitud de los datos
- Permitir identificar la información que es confidencial
- Contemplar áreas de uso exclusivo
- Proteger y conservar los activos de desastres provocados por la mano del hombre y los actos abiertamente hostiles
- Asegurar la capacidad de la organización para sobrevivir accidentes
- Cuidar a los empleados de tentaciones o sospechas innecesarias
- Tomar en cuenta la administración contra acusaciones por imprudencia

Consideraciones para con el Personal

Es de gran importancia la elaboración del plan considerando el personal, pues se debe propiciar una conciencia de seguridad para obtener una auto evaluación honesta de su comportamiento con respecto al sistema, que lleve a la persona a:

- Asumir riesgos
- Cumplir promesas
- Innovar

Para apoyar estos objetivos se deben cumplir los siguientes pasos:

1. Motivar

Se deben desarrollar métodos de participación reflexionando sobre lo que significa la seguridad y el riesgo, así como su impacto a nivel empresarial, de cargo e individual.

2. Capacitación General

En un principio a los ejecutivos con el fin de que conozcan y entiendan la relación entre seguridad, riesgo y la información, y su impacto en la empresa. El objetivo de este punto es que se podrán detectar las debilidades y potencialidades de la organización frente al riesgo. Este proceso incluye como práctica necesaria la implantación la ejecución de planes de contingencia y la simulación de posibles delitos.

3. Capacitación de Técnicos

Se deben formar técnicos encargados de mantener la seguridad como parte de su trabajo y que estén capacitados para instruir y habilitar a otras personas en lo que es la ejecución de medidas preventivas y correctivas.

4. Ética y Cultura

Se debe establecer un método de educación estimulando el cultivo de elevados principios morales, que tengan repercusión a nivel personal e institucional. De ser posible realizar conferencias periódicas sobre: doctrina, familia, educación sexual, relaciones humanas, etc.

- Etapas para Implantar un Sistema de Seguridad

Introducir el tema de seguridad en la visión de la empresa y hacer que el plan entre en vigor y los elementos empiecen a funcionar y se observen y acepten las nuevas instituciones, leyes y costumbres del nuevo sistema de seguridad se recomienda seguir los siguientes siete pasos:

  - Definir los procesos de flujo de información y sus riesgos en cuanto a todos los recursos participantes.
  - Capacitar a los gerentes y directivos, contemplando el enfoque global.
  - Designar y capacitar supervisores de área.
  - Definir y trabajar sobre todo las áreas donde se pueden lograr mejoras relativamente rápidas.
  - Mejorar las comunicaciones internas.
  - Identificar claramente las áreas de mayor riesgo corporativo y trabajar con ellas planteando soluciones de alto nivel.

- Capacitar a todos los trabajadores en los elementos básicos de seguridad y riesgo para el manejo del software, hardware y con respecto a la seguridad física.

3.3.3. Responsabilidades dentro de un sistema de seguridad

- Dirección Administrativa

Es la entidad cuyo propósito es establecer las directrices y autorizar las estrategias que permitan fortalecer en la Organización, las medidas de seguridad informática y cuyas funciones son:

- Establecer directrices en materia de seguridad informática.
- Autorizar estrategias, políticas y programas de acción en este aspecto.
- Revisar los resultados de los diferentes programas de acción implantados.
- Solucionar los problemas de seguridad informática.

- Gerencias

Los gerentes de las áreas, departamentos o unidades organizacionales para fines de la protección de la información, son los responsables de la misma, cumpliendo lo que a continuación se detalla:

- Introducir e involucrar los conceptos, medidas y mecanismos de seguridad informática dentro de su ámbito de responsabilidad y en la normatividad y procedimientos que realicen para apoyar su función.
- Vigilar y supervisar el cumplimiento de las políticas y normas de seguridad informática.
- Apoyar y dar información para la realización de diagnósticos de riesgos y minimización de los mismos.
- Atender y dar seguimiento a los riesgos detectados por el Departamento de Seguridad Informática y en su caso se asuma o acepte, deberá constar por escrito en un documento avalado con su firma.
- Realizar pruebas que identifiquen el esquema de seguridad bajo el cual trabajan los sistemas automatizados.
- Promover la difusión de las medidas y mecanismos de seguridad para consolidar la confianza con el personal, clientes y proveedores mediante la protección de los activos propiedad de la Organización.
- Con base en las instrucciones del Departamento de Seguridad Informática, mediante un estudio específico, tomar dediciones de seguridad relativas a la protección de los activos de información.
- Delegar responsabilidad operacional para la protección de los activo de información.

- Considerar en la evaluación de su personal el cumplimento de las políticas de seguridad en la información, definidas en al normatividad vigente.
- Implantar y dar seguimiento a los programas para formar conciencia de la importancia de la seguridad informática que se establezcan para garantizar el uso de las herramientas para tal fin.
- Detectar y plantear problemas sobre seguridad de información al Departamento de Seguridad Informática.

- Personal en General

Todo el personal, independientemente de su función y jerarquía, deberá impulsar y promover la seguridad en la institución en todas y cada una de sus actividades y acatar las disposiciones al respecto, aceptando las consecuencias laborales y legales por no cumplirlas; dentro de estas disposiciones destacan las siguientes:

- Conocer y acatar la normatividad aplicable en materia de seguridad informática.
- No divulgar ni modificar información confidencial sin autorización expresa de acuerdo con las facultades conferidas, no permitir a otra persona el acceso a la misma.
- Cooperar en al realización de Campañas para hacer conciencia, que en materia de seguridad informática se realicen en la Organización, proporcionando información que se le solicite y con actitud positiva.
- Emprender todas las medidas de seguridad informática aplicables a su función y que de manera enunciativa, mas no limitativa, se enuncian:

    - Utilizar con seguridad y responsabilidad sus claves de acceso.
    - Respetar el acceso a los lugares de cómputo.
    - Realizar eficientemente los respaldos de su información.
    - Utilizar el software autorizado sin hacer copias ilegales.
    - Utilizar el equipo sólo de acuerdo con las facultades asignadas
    - Apegarse a la normatividad establecida para manejar de manera segura la información en todos sus medios y formas.
    - Dar seguimiento a las medidas y mecanismos de seguridad informática.
    - Reportar irregularidades detectadas en las instalaciones de trabajo al supervisor de área o jefe inmediato y atender las indicaciones establecidas en la normatividad de seguridad informática.
    - Reconocer la propiedad de la Organización sobre todos los productos, aplicaciones e información desarrollada por los empleados.
    - Aplicar el código de ética existente en la Organización.

Si algunos o todos los procedimientos de implementación son muy complicados, pueden ser implementados gradualmente. Así mismo, algunos procedimientos de

control pueden requerir que el personal encargado de la administración de la seguridad dé entrenamiento a los usuarios finales.

El plan de seguridad deberá especificar el orden en que los procedimientos de seguridad serán implementados, de tal forma que las amenazas más serias o latentes sean cubiertas primero. Esta actividad permite controlar el progreso de las medidas implementadas.

3.4.Desarrolladores de esquemas de seguridad

3.4.1.Dirección de tecnología y seguridad informática

Esta área se encarga de mantener los equipos y el software actualizado ya que día a día se presentan nuevas amenazas, también verifica que el sistema responda de manera segura.

Funciones:

- Coordinar la creación y actualización de la normatividad de protección a la información.
- Verifica el cumplimiento de la normatividad, políticas y prácticas sanas de protección a la información.
- Supervisa el monitoreo constante de las herramientas tecnológicas de seguridad y del inventario de activos informáticos de la institución.
- Supervisa los procesos de Diagnóstico de vulnerabilidades tecnológicas en los sistemas de la institución.
- Evalúa y autoriza el desarrollo y mantenimiento de sistemas en base a los requerimientos de seguridad y protección de la información.
- Coordina la interacción con sistemas de información externas.
- Lleva a cabo el desarrollo de infraestructura y sistemas de seguridad informática.

3.4.2.Gerencia de seguridad informática

Tiene a su cargo, la definición de políticas de seguridad, medidas de seguridad y dar apoyo en este aspecto a todas las áreas de la Organización.

Funciones:

- Establece y mantiene las políticas y normas generales en materia de seguridad informática.
- Realiza evaluaciones y diagnósticos de riesgos para identificar vulnerabilidades y señalar acciones de solución.
- Investiga tecnología de vanguardia para la protección de la información en todos sus medios y formas en conjunto con las áreas involucradas.

- Propone, define y fija mecanismos y medidas para fortalecer la seguridad de la información.
- Promueve en la organización, programas de concienciación y capacitación en materia de seguridad informática.
- Evalúa los requerimientos de Seguridad de la institución, investiga y propone la Tecnología, estándares y controles de seguridad acordes a las necesidades de la institución.
- Acuerda con las áreas encargadas de la difusión y capacitación que se den a conocer los aspectos relevantes al personal de la institución, para mantener la disciplina, ética profesional y hábitos adecuados de seguridad y protección de los activos de la tecnología de información.
- Supervisa los accesos a los sistemas y a las aplicaciones, de acuerdo a las políticas definidas por los dueños de la información.

3.4.3.Departamento de administración de recursos

Tiene a su cargo la administración de los accesos de los usuarios, dándoles a éstos privilegios y/o restricciones de uso de los sistemas, de las aplicaciones y las plataformas tecnológicas.

Funciones:

- Controlan la asignación de los accesos y otorgamiento de facultades a los usuarios y atributos en el medio ambiente aplicativo y técnico, si así corresponde.
- Dan mantenimiento y actualizan los parámetros y catálogos utilizados por los esquemas de acceso y facultades.
- Establecen y vigilan la continuidad, recuperación y actualización oportuna de los usuarios y recursos.
- Dan seguimiento a situaciones de excepción en actividades relacionadas con la seguridad, reportando éstas a sus niveles de Dirección y al Departamento de Seguridad Informática.
- Plantean y detectan problemas referentes a la seguridad de la información.
- Verifican el control de acceso a los sistemas y las aplicaciones, aplicando las políticas definidas por los dueños de la información.
- Actualizan los parámetros para el control de acceso a los sistemas.
- Realizan monitoreo y estadísticas de seguridad.
- Llevan el control de la administración de los indicadores de seguridad.
- Realizan la administración y seguimiento de incidentes.

3.4.4.Departamento de servicios técnicos de seguridad

Este departamento se encarga de verificar que todos los procesos de seguridad en una organización sean diseñados bajo las normatividades correspondientes, además se encargan de hacer las pruebas necesarias de las herramientas de seguridad propuestas.

Funciones:

- Aseguran que se cumplan las normas, los procedimientos y estándares vigentes en seguridad informática que se encuentren dentro de su ámbito de responsabilidad.
- Investigan y evalúan herramientas tecnológicas de seguridad informática con apego a los requerimientos de la Gerencia de Seguridad Informática.
- Realizan los procesos de diagnóstico de vulnerabilidades tecnológicas en los sistemas de la institución.
- Configuran herramientas y aplicaciones según políticas de la arquitectura de seguridad.
- Llevan a cabo el análisis de las bitácoras de las herramientas de monitoreo para identificar posibles incidentes o riesgos futuros.
- Análisis forense de incidentes.
- Elaboran las metodologías e instructivos de operación.

3.4.5.Departamento de seguimiento y control

Aquí se encargan de seguir muy de cerca que el personal de la Organización se apegue a la reglas y cumpla con las políticas de seguridad establecidas; en caso de que se presente un eventualidad este departamento se encarga de darle seguimiento además de diseñar y ejecutar planes de capacitación orientados a que el personal este lo mas informado posible en cuanto a seguridad se refiere.

Funciones:

- Supervisar que las áreas den cumplimiento de la normatividad, políticas y prácticas sanas de protección de la información.
- Dar seguimiento a la corrección por parte de las áreas operativas y técnicas de las vulnerabilidades detectadas.
- Participar en el desarrollo y mantenimiento de sistemas en base a los requerimientos de seguridad y protección de la información.
- Realizar campañas de difusión y hacer conciencia de las políticas institucionales de seguridad informática.
- Realizar las actividades de capacitación como cursos, seminarios, pláticas y presentaciones que contribuyan a la difusión y hacer conciencia de la seguridad informática.
- Llevar a cabo las Auditorías de seguridad informática.
- Coordinar los planes de contingencia.

3.4.6.Departamento de análisis y desarrollo

Esta área se encarga de mantener la actualización de herramientas de seguridad y de software, para poder así estar protegidos ante nuevas amenazas.

Funciones:

- Desarrollo e implementación de nuevos sistemas y software de seguridad.
- Coordinan y mantienen programas de actualización para los sistemas de servicios externos como el portal de Internet, y de nuevos desarrollos que requieren de niveles más altos de seguridad.
- Desarrollan e implementan software de infraestructura y estándares técnicos de seguridad informática conforme a los lineamientos establecidos por la Gerencia de Seguridad Informática.
- Garantizan la correcta instalación y liberación de los esquemas y herramientas de seguridad informática.
- Dan mantenimiento y soporte a esquemas y herramientas requeridos y sustentados en las normas y políticas institucionales de seguridad informática.
- Coordinan el desarrollo de nuevas tecnologías.

3.4.7.Departamento de enlace

Tiene a su cargo auditar constantemente la aplicación y funcionalidad de las políticas de seguridad, mantiene al día las bitácoras de estadística de mantenimiento y soporte. También agenda, para su ejecución, todos aquellos asuntos que deban ser solucionados a la brevedad.

Funciones:

- Audita el cumplimiento y suficiencia de las políticas y normas de seguridad informática, informando sobre el apego a las mismas por parte de los involucrados.
- Revisa y evalúa lo controles de seguridad y los esfuerzos en desarrollo para la implementación de los mismos.
- Proporciona logística y soporte técnico a las auditorias de seguridad
- Monitorear los sistemas externos y reportar los incidentes al área de seguridad.
- Mantiene la estadística de eventos, reportes y mantenimiento.
- Lleva el control de seguimiento de los asuntos pendientes.

CAPÍTULO 4
DISEÑO DEL SGSI PARA EL OBJETO DE EVALUACIÓN

4. DISEÑO DEL SGSI PARA EL OBJETO DE EVALUACIÓN.

4.1.Exposición de motivos

En la actualidad son miles las instituciones que se han visto sujetas a los ataques en sus instalaciones, tanto desde el interior como del exterior de las mismas, basta decir que cuando la institución se encuentra sujeta a un ataque un grupo de personas se involucran y están pendientes de éste, tratando de contrarrestar y anular estas amenazas reales.

La carencia de recursos humanos involucrados en seguridad, la escasa concienciación de los usuarios, la falta de visión y las limitantes económicas han retrasado el diseño e implementación de un plan rector de seguridad.

El objetivo principal de la Gerencia de Seguridad Informática en una organización es brindar a los usuarios de la institución, los recursos informáticos en la cantidad y calidad que demandan, esto es, que en la institución se tenga continuidad confiable en el servicio todos los días del año.

La seguridad de las instituciones se ha convertido en una cuestión de seguridad nacional, por ello contar con un documento de políticas de seguridad es imprescindible, en este se deben plasmar los mecanismos confiables que con base en una política institucional proteja los activos de la institución.

Así pues, ante este panorama surge el siguiente proyecto de políticas de seguridad que harán que esta institución pueda disponer de los ejes de proyección que en materia de seguridad la Institución requiere.

El presente capítulo, es nuestra propuesta del Perfil de Protección y Políticas de Seguridad que en materia cómputo, informática y comunicaciones digitales hemos elaborado como proyecto de tesis para la Coordinación de Cómputo de la Escuela Nacional Preparatoria Nº 5 “José Vasconcelos” la cual se encuentra ubicada en Calzada del Hueso Nº 729 Col. Ex Hacienda de Coapa en la Delegación Tlalpan con C.P. 14300, y con la ayuda conjunta del Coordinador del Centro de Cómputo de esta institución, el L.A. David Alejandro Rodríguez Abad quien es el principal responsable de las cuestiones en materia de informática y cómputo de esta institución, para normar a la institución en estos rubros.

Esta propuesta ha sido detenidamente planteada, analizada y revisada a fin de no violar las garantías de los individuos que laboran en la institución, y no pretende ser una camisa de fuerza, más bien muestra una buena forma de operar los sistemas con la debida seguridad que esto implica, respetando los estatutos y reglamentos de la Institución.

4.2.Objetivo del proyecto

Esta propuesta surge en respuesta a la preocupación del personal que labora en el departamento de cómputo e informática de la ENP 5 “José Vasconcelos” por mantener los

activos de información y sus sistemas seguros contra cualquier forma de ataque. Y pretende no solo establecer una filosofía de seguridad, sino forjar una educación y un hábito en usuarios, administradores y el personal en general que conlleve a un ambiente más seguro tanto dentro de la institución como fuera de ella.

4.3. Objeto de evaluación

4.3.1. Antecedentes

La ENP (Escuela Nacional Preparatoria) desde su origen es una Institución de carácter público y modelo educativo de la enseñanza media superior, respondiendo satisfactoriamente a los retos y demandas de la sociedad en su conjunto. Forma parte del sistema educativo mexicano y es uno de los dos sistemas de bachillerato de la UNAM (Universidad Nacional Autónoma de México).

La ENP consta de nueve planteles distribuidos en el área metropolitana, los cuales recibieron nombres de maestros de la preparatoria tales como:

- Plantel 1 "Gabino Barreda"
- Plantel 2 "Erasmo Castellanos Quinto"
- Plantel 3 "Justo Sierra"
- Plantel 4 "Vidal Castañeda y Nájera"
- Plantel 5 "José Vasconcelos"
- Plantel 6 "Antonio Caso"
- Plantel 7 "Ezequiel A. Chávez"
- Plantel 8 "Miguel E. Shulz"
- Plantel 9 "Pedro de Alba"

La ENP cuenta con la infraestructura necesaria para el desarrollo y atención de la comunidad preparatoriana, donde actualmente asisten a sus nueve planteles cerca de 48,000 alumnos y 2,400 profesores.

Misión de la ENP

Educar hombres y mujeres que mediante una formación integral, adquieran una pluralidad de ideas, la comprensión de los conocimientos necesarios para acceder con éxito a estudios superiores, así como una mentalidad analítica, dinámica y crítica que les permita ser conscientes de su realidad y comprometidos con la sociedad. Además, tener la capacidad de adquirir constantemente nuevos conocimientos, destrezas y habilidades para enfrentarse a los retos de la vida de manera positiva y responsable.

Realizar investigación educativa para desarrollar y aplicar nuevos métodos y técnicas avanzadas de enseñanza, que eleven la calidad de los procesos de enseñanza y aprendizaje.

4.3.2.Estructura general del objeto de evaluación

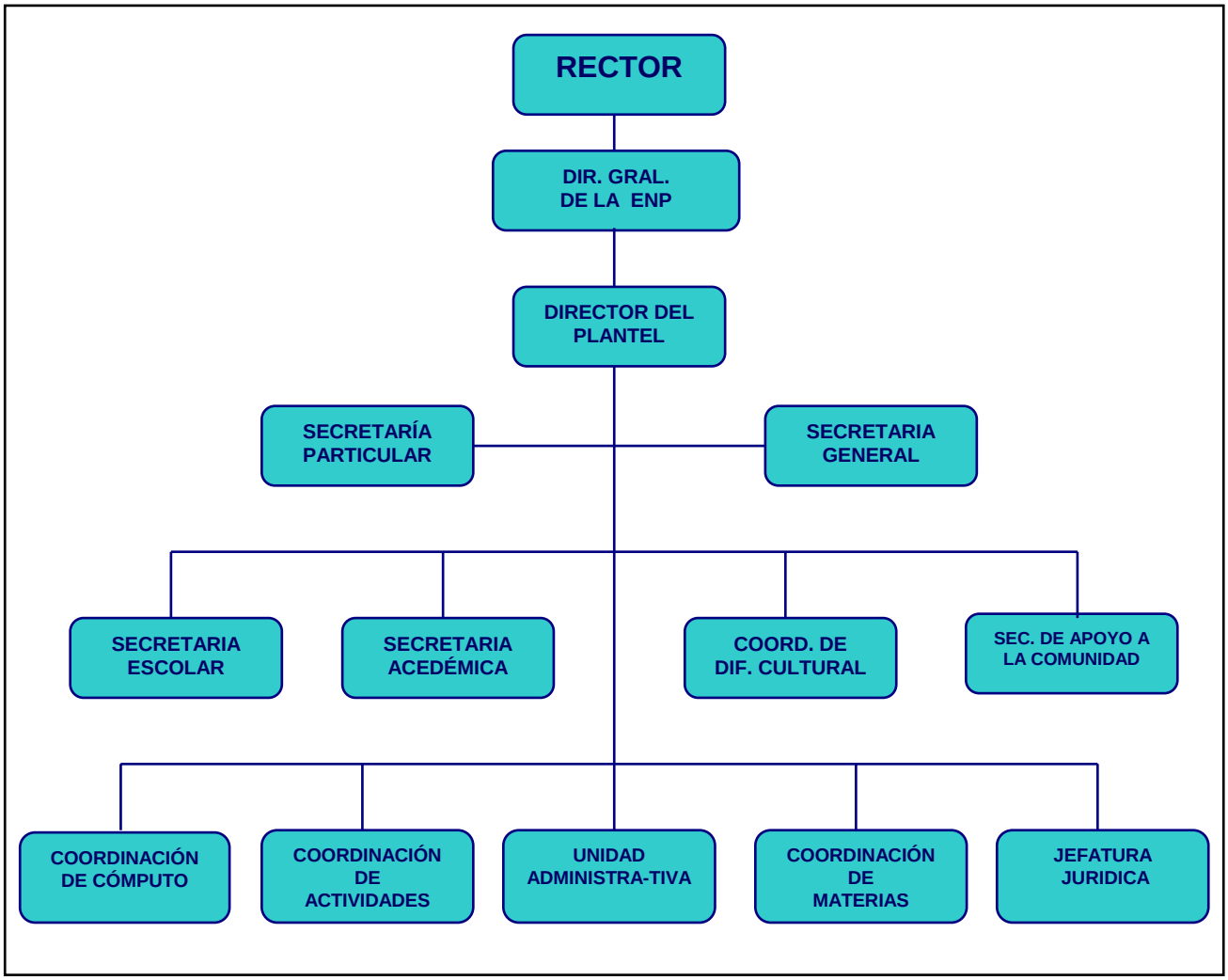


FIGURA 4.1 ORGANIGRAMA DEL OBJETO DE EVALUACIÓN

En casi todas las secretarías, coordinaciones y jefaturas del plantel antes mencionadas se cuenta con equipo de cómputo y se maneja información con distintos niveles de sensibilidad. Nuestra propuesta del Perfil de Protección y Políticas de Seguridad abarca en la medida de lo posible las siguientes áreas: Secretaría Escolar, Unidad Administrativa y Centro de Cómputo.

Se tomaron en cuenta solo estas áreas debido a que en ellas existe una gran concentración de información y es aquí en donde se distribuye la mayoría de la red local de la institución.

Para llevar acabo esta propuesta es necesario contar con el apoyo de personas con poder de decisión dentro de la institución como el Director, los Funcionarios, Jefes y en mayor medida el apoyo del Coordinador de Cómputo del plantel, esto es fundamental para el éxito del proyecto, ya que estas personas son un conjunto de elementos relacionados entre sí para lograr la seguridad total de la institución y crear una cultura de seguridad haciendo ver a la

gente involucrada los peligros a los que esta expuesta cualquier organización en sus activos de información.

4.3.3.Entorno físico del objeto de evaluación.

Ubicación

El Objeto de Evaluación de esta propuesta se encuentra en la Ciudad de México y tiene la siguiente dirección:

Coordinación de Cómputo de la Escuela Nacional Preparatoria Plantel Nº 5 “José Vasconcelos”. Calzada del Hueso Nº 729., Col. Ex Hacienda de Coapa, Del. Tlalpan, C.P. 14300.

Este plantel es uno de los más grandes de su tipo en la Ciudad de México y en América Latina, cuenta con instalaciones suficientes para atender las demandas de su comunidad. Tiene una población estudiantil de alrededor de 9,000 alumnos activos y aproximadamente cuenta con 475 empleados Académicos y 450 empleados Administrativos también cuenta con una plantilla de aproximadamente 35 funcionarios y empleados de confianza.

Se conforma de tres grandes edificios de aulas para clase denominados Edificio A, Edificio B y Edificio D y actualmente se inauguró una biblioteca la cual es un edificio independiente.

Existe también un edificio para Gobierno, en éste se encuentran las oficinas de la Dirección, y las oficinas de las Secretarías General, Particular, Académica, Escolar y Apoyo a la Comunidad así como la oficina de la Coordinación de Difusión Cultural y Unidad Administrativa.

Existe un edificio más denominado Edificio C o Centro de Cómputo, aquí se encuentra la oficina de la Coordinación de Cómputo y la concentración mas alta de equipos de cómputo en todo el plantel. También en este edificio se encuentra montada toda la estructura de distribución de la red para todo el plantel.

Como ya se mencionó debido al tipo de información que se manipula dentro del plantel el Objeto de Evaluación de este proyecto se reduce al análisis de las siguientes áreas: secretaría escolar, unidad administrativa y centro de cómputo.

Para poder describir correctamente el acceso al entorno físico del objeto de evaluación es necesario mencionar de manera general la forma en que los usuarios de los sistemas de cómputo acceden al plantel ya que las diferentes áreas de análisis se encuentran dispersas en todo el campus.

Para ingresar al plantel en las entradas se encuentran al menos dos vigilantes los cuales tienen como función dar el acceso a los alumnos previa identificación con la credencial interna de la institución; si se trata de una persona que no labora en el plantel y tampoco es alumno debe identificarse y comunicar al vigilante hacia qué área se dirige, para llevar un control de acceso de estas personas se cuenta con una bitácora de visitas en la cual se debe anotar el nombre, el área a la que se dirige y registrar la hora de entrada, adicional a esto la visita debe dejar una identificación oficial en el control de entrada. El personal de vigilancia

provee de un gafete de identificación a la persona en cuestión, el cual deberá portar durante todo el tiempo que se encuentre dentro de la institución.

A los trabajadores Académicos y Administrativos del plantel, el personal de vigilancia les da libre acceso a la institución confiando en un reconocimiento visual de la persona lo cual no es garantía de que esta persona pertenezca a la plantilla laboral de la institución.

A los equipos de cómputo que se encuentran en la Unidad Administrativa y las oficinas de Secretaría Escolar tienen acceso únicamente los custodios o responsables del equipo.

Para acceder al Centro de Cómputo el personal lo hace después de un reconocimiento visual por parte del vigilante esto es debido a que en este edificio es muy pequeña la cantidad de personas que labora. El acceso de los alumnos es un tanto mas complicado ya que no se les permite la entrada a las aulas de cómputo con ningún tipo de bolsa o mochila, el alumno debe dejar su mochila en unos anaqueles en la entrada del al Centro y después entrar a su salón.

El Centro de Cómputo cuenta con seis aulas de clase y solo en dos de ellas se tiene implementada la red, una oficina en donde se concentra el personal, un cuarto para los dispositivos de red, baños y bodega.

La disposición física de los equipos en las aulas está debidamente organizada, sin embargo el cableado de red de los salones que cuentan con este servicio, está implementado de manera errónea ya que no existe un sistema de clasificación de cableado.

En el área o cuarto de servidores de red se observan los dispositivos sin la protección debida ya que están aglutinados en un rincón, las instalaciones de cables no son adecuadas ya que no tienen ningún sistema de identificación tanto de cables como de dispositivos, así mismo están en riesgo constante por estar expuestos a sufrir o provocar accidentes.

No se cuenta con un adecuado equipo de ventilación pues el calor generado por las máquinas se puede percibir inmediatamente.

El objeto de evaluación cuenta con tres servidores uno de ellos llamado VASCONCELOS está localizado en la oficina de la Secretaría Escolar y provee los servicios de red local a los usuarios. Los usuarios de este servidor son los Secretarios Escolares y el personal a su cargo, es decir, las secretarias de servicios escolares.

El otro par de servidores se encuentran en el Centro de Cómputo y son conocidos con el nombre de PREPA5 y proveen de los servicios de red local a las aulas que cuentan con estructura de red del Centro de Cómputo, uno de estos servidores provee el servicio de Internet al Plantel Nº 1 “Gabino Barreda”[1] por medio de un enlace telefónico.

[1] El plantel 1 "Gabino Barreda" se localiza en Av. de las Torres y Calle Prolongación de Aldama s/n. Tepepan Xochimilco. CP 16020. México D.F.

4.3.4.Usuarios del objeto de evaluación

Los usuarios del objeto de evaluación se clasifican en los siguientes grupos de acuerdo a su área.

- **Grupo Administrador:** Los usuarios que pertenecen a este grupo son personal de mayor nivel como los jefes de departamento, y coordinadores.
    - Privilegios: tienen acceso exclusivo a su pc, en la cual cuentan con los privilegios siguientes; leer, escribir, borrar y modificar la información. Todos los recursos de internet y red local son permitidos.
- **Grupo Trabajadores:** Los usuarios de este grupo son personal administrativo; secretarias y personal de confianza.
    - Privilegios: Tienen acceso exclusivo a su PC, en la cual cuentan con los privilegios siguientes: leer, consultar y escribir. Todos los recursos de Internet son permitidos.
- **Grupo Coordinación de Cómputo:** Este grupo engloba a todos los encargados del sistema, administradores de redes y soporte técnico.
    - Privilegios: A los empleados de este género se les otorgan los privilegios y permisos correspondientes según los criterios de su jefe inmediato y de los propietarios de la información.
- **Grupo Profesores y Alumnos:** Son los usuarios del equipo de cómputo asignado al Centro de Cómputo.
    - Privilegios: Los usuarios de este tipo no cuentan con permisos para manipular información sensible propiedad de la institución, sólo pueden realizar consultas a cierta información y cuentan con todos los recursos de Internet, dentro del Centro de Cómputo bajo restricciones de la cuenta de invitado de Windows XP. Es decir, no pueden hacer instalaciones de software no autorizado.

4.3.5.Hardware del objeto de evaluación

Equipo con el que cuenta el objeto de evaluación:

Doscientos setenta y uno equipos de cómputo en total, de diferentes marcas entre Hewlett Packard (HP), Compaq y DELL. Los cuales están distribuidos de la siguiente manera:

Unidad Administrativa: Seis equipos HP y tres DELL.

Secretaría Escolar: Diecinueve equipos Compaq y dos HP.

Oficina del Centro de Cómputo: Cinco equipos DELL para uso del personal que pertenece a esta oficina.

Salón 1: Veinticinco equipos HP.

Salón 2: Treinta y nueve equipos HP.
Salón 3: Seis equipos DELL y treinta y cuatro Compaq.
Salón 4: Quince equipos HP, un equipo DELL y veintiuno Compaq.
Salón 5: Cuarenta y cinco HP
Salón 6: Cuarenta equipos Compaq y diez HP

Estos equipos son de características estándar para uso personal, a excepción de los tres servidores y los dos equipos de los secretarios Escolares y Coordinación de Cómputo.

Los equipos de uso general como los de las secretarias de Secretaría Escolar son marca Compaq con capacidad de HD de 10 GB y memoria de 128MB, procesador Intel Celeron a 1GHz.

Los equipos que son utilizados en el centro de cómputo son de diferentes marcas que varían en cuanto a capacidad de Disco Duro, memoria y procesador, estos son equipos Compaq, Hewlett Packard y DELL. Aproximadamente cada año se recibe equipo de nueva adquisición el cual en su mayoría es marca Hewlett Packard y se distribuye hacia diferentes sectores del plantel quienes lo han requerido con anterioridad.

El Servidor Prepa 5 (véase FOTO 4.2) también se encuentra dentro del centro de cómputo y es un equipo marca DELL con una capacidad de cuatro discos duros de 120GB con dos procesadores Intel Pentium IV a 3.2GHz con memoria RAM de 3GB. En este servidor se encuentra montada la página de la ENP No. 5 http://www.prepa5.unam.mx y a ésta se tiene acceso desde el exterior. Este servidor está montado sobre una plataforma Linux.

FOTO 4.2 SERVIDOR PREPA 5

Este servidor es el más poderoso dentro del plantel y tuvo un costo aproximado de 80 mil pesos, el Secretario Escolar es la persona que se encarga de dar mantenimiento y actualizar el sitio web del plantel.

En este servidor se almacena toda la información de los alumnos inscritos en el plantel y se realizan respaldos de información con una frecuencia diaria en época de inscripciones y de exámenes extraordinarios. El resto del año se hace un respaldo de manera automática pero con una frecuencia de una vez por semana.

El servidor Vasconcelos (FOTOS 4.3 Y 4.4) se encuentra ubicado en la Secretaría Escolar y cuenta con una capacidad de almacenamiento en dos discos duros uno de 100GB y otro de 150 GB con memoria RAM de 1.5GB y procesador Intel Pentium IV.

FOTOS 4.3 Y 4.4. SERVIDOR VASCONCELOS

Existe un servidor más (ver FOTO 4.5), el cual trabaja en conjunto con el servidor *Prepa 5* para elaboración de respaldos y filtrado de información este equipo es de marca Compaq con capacidad de almacenamiento en disco duro de 40 GB y procesador Intel Celeron a 1.2 GHz además tiene una memoria RAM de 512 MB. Es decir, sirve como un "puente" entre el servidor *Vasconcelos* y el servidor *Prepa 5*.

FOTO 4.5 SERVIDOR "PUENTE" PARA PREPA 5

Otros dispositivos de hardware

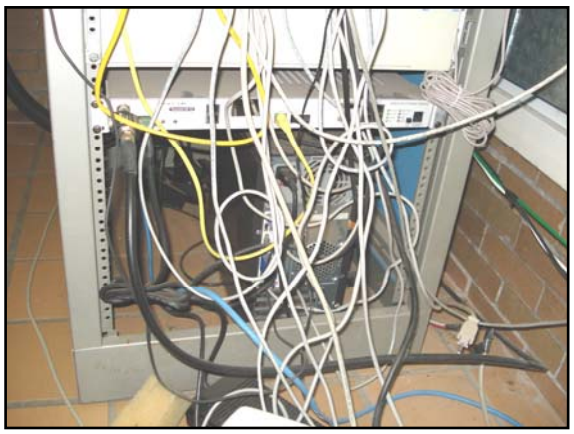
- Se cuenta con 18 impresoras láser, 12 de ellas están destinadas al centro de cómputo, 2 a la secretaría escolar y 6 a la unidad administrativa. Hay una impresora mas en la unidad administrativa, pero ésta es de matriz y funciona para la impresión de los contratos de los trabajadores entre otras cosas.
- Se cuenta con 2 scanner, en el centro de cómputo.
- Tres fotocopiadoras, una para cada área.
- Algunas de las PC´s cuentan con su propio quemador de discos.
- Dos reguladores para el área de red del centro de cómputo.
- Se cuenta con una planta generadora de energía.
- Dispositivos de red para el centro de cómputo y secretaría escolar.

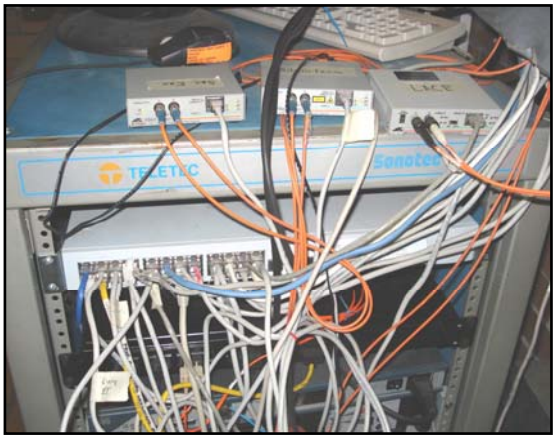
En las siguientes fotografías (4.6 - 4.14) se aprecian las condiciones en que se encuentra el cuarto de servidores, el cual muestra la falta de atención, no cumple con un adecuado mantenimiento, protección contra catástrofes y otros servicios.

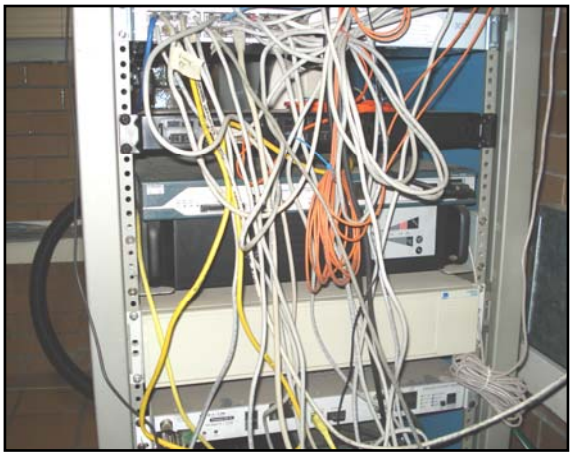
FOTO 4.6 AIRE ACONDICIONADO DEL ÁREA DE RED

FOTO 4.7 CABLEADO DE RED

FOTO 4.8 CENTRO DE CARGA GENERAL

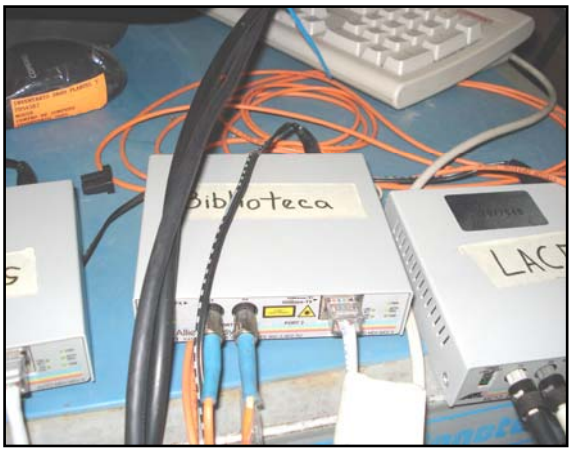






FOTOS 4.9, 4.10 Y 4.11 DISPOSITIVOS DE RED

FOTO 4.12 REGULADOR PARA EL ÁREA DE RED



FOTOS 4.13 Y 4.14 TRANSCEIVERS (TRANSFORMADORES DE MEDIOS) DESDE EL ÁREA DE RED HASTA SECRETARÍA ESCOLAR, BIBLIOTECA Y LACE RESPECTIVAMENTE

Cableado estructurado del laboratorio 1

Se muestra a continuación de las fotos 4.15 a la 4.17, las condiciones en las que se encuentra el cableado en le laboratorio 1 así como el equipo con el que cuenta.

FOTO 4.15 HUB DE 24 NODOS PARA EL LABORATORIO 1

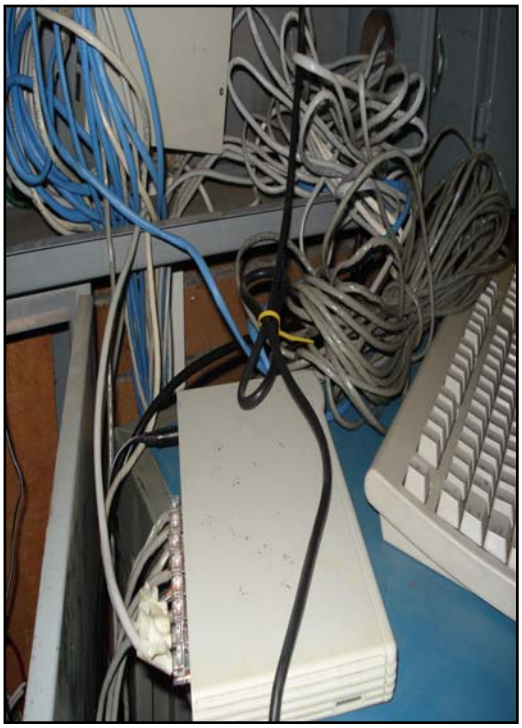


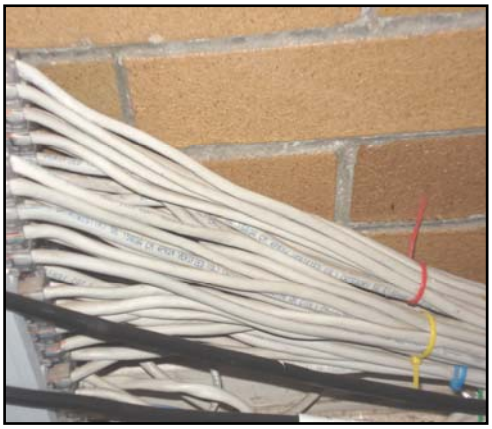
FOTO 4.16 HUB DE 8 NODOS PARA EL LABORATORIO 1

FOTO 4.17 ANTENA DE RED INALÁMBRICA PRIVADA

Cableado estructurado para el laboratorio 2

En seguida de la fotos 4.18 a la 4.21 se muestran las condiciones en las que se encuentra el cableado en le laboratorio 2 así como el equipo con el que cuenta.

FOTOS 4.18 Y 4.19 SWITCHES 2X24 PARA EL LABORATORIO 2



FOTOS 4.20 Y 4.21 CABLEADO DEL LABORATORIO 2 SIN CANALETA

Como podemos observar aquí se tiene un orden en el cableado lo contrario al laboratorio 1.

Cableado estructurado para Secretaria Escolar

En las siguientes fotografías (4.22 - 4.24) observamos la instalación del cableado estructurado que se encuentra en la Secretaría Escolar.

FOTO 4.22 ESTRUCTURA DE CABLEADO PARA LA SECRETARIA ESCOLAR.

FOTO 4.23 SWITCHES DE SECRETARÍA ESCOLAR 2X24

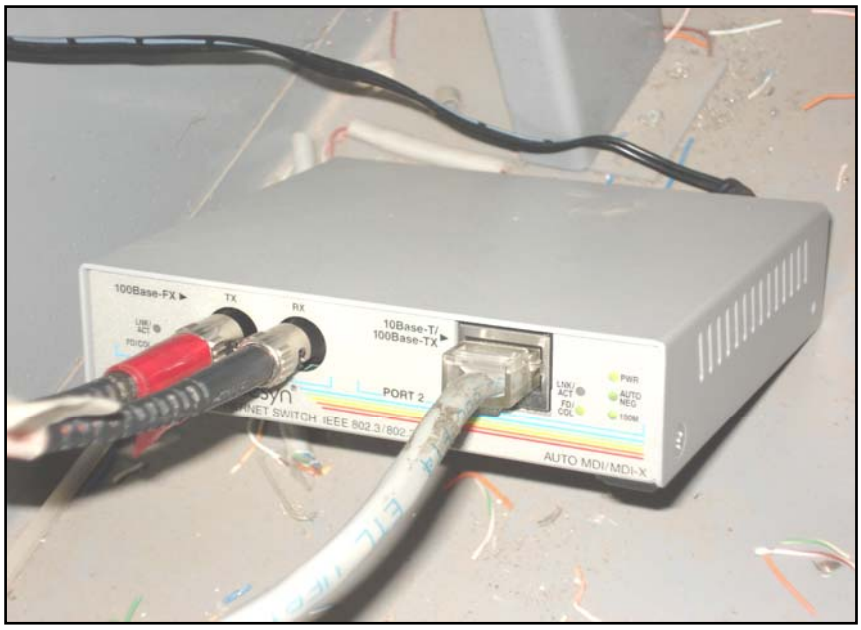


FOTO 4.24 TRANSFORMADOR DE MEDIOS PARA SECRETARÍA ESCOLAR

4.3.6.Software

- Los Servidores de Prepa5 están montados sobre el sistema operativo LINUX
- El servidor Vasconcelos cuenta con Windows 2000 Server.
- No se cuenta con software de control de acceso a la red
- Las herramientas de seguridad que se tiene son las ofrecidas por el sistema operativo Linux.
- Los equipos de uso general cuentan, en su mayoría con Windows XP Profesional. Todas ellas deben tener el antivirus de libre distribución Grisoft AVG 7.5.

4.3.7.Estructura de red

La red interna de la ENP No. 5 “José Vasconcelos” se conforma de la siguiente manera:

Cuenta con un enlace de microonda directamente con DGSCA a través de una antena, la cual se encuentra localizada en la azotea del edificio de Gobierno o Dirección. De esta antena sale un enlace mediante Fibra Óptica que recorre una distancia aproximadamente de 65 metros hasta el Centro de Cómputo.

En el centro de cómputo se cuenta con un Puente de red o Bridge2 (ver foto 4.25), debido a que la red prepa5 pertenece a Red UNAM, DGSCA enlaza mediante este puente a la red prepa5 con Red UNAM.

FOTO 4.25 PUENTE DE RED CON CONEXIÓN DE FIBRA OPTICA

El puente se conecta directamente a un Router3 Cisco el cual fue configurado previamente por el personal de DGSCA con las tablas de ruteo necesarias para que la red local de la preparatoria 5 trabaje correctamente.

De este Router, sale una conexión con cable UTP directamente a un Switch4 3Com de 24 puertos (ver foto 4.26), se puede decir que este es el “Switch Principal” ya que del correcto funcionamiento de este dispositivo, depende toda la red de la escuela.

[2] Un puente o bridge es un dispositivo de interconexión de redes que opera en el nivel de enlace de datos del modelo OSI (capa 2). Este interconecta dos segmentos de red haciendo el pasaje de datos de una red para otra, con base en la dirección física de destino de cada paquete. Un bridge conecta dos segmentos de red como una sola red usando el mismo protocolo de establecimiento de red

[3] Dispositivo de hardware para interconexión de redes que opera en la capa tres o nivel de red del modelo OSI. A través de sus tablas de enrutamiento configurados previamente, los routers pasan los paquetes para la red o router con el rango de direcciones que corresponde al destino del paquete. Se utilizan máscaras de red para definir las subredes interconectadas

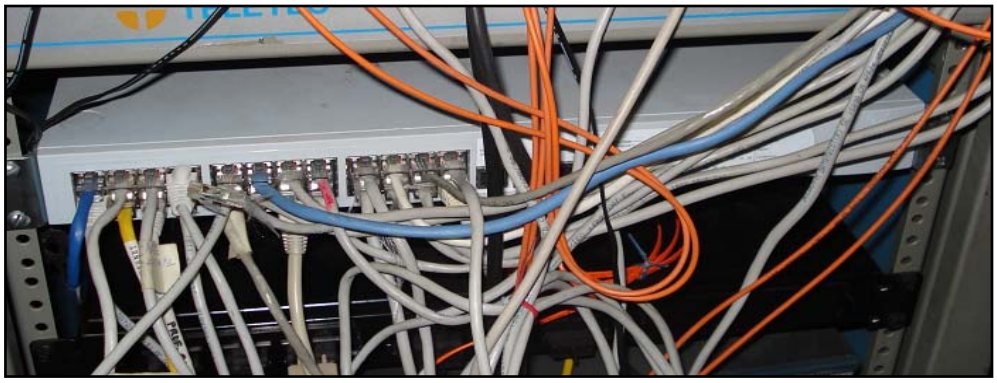


FOTO4.26 SWITCH A PRINCIPAL

De este Switch salen conexiones con cable UTP a todas y cada una de las áreas del plantel y por supuesto dentro de esas áreas se encuentra nuestro objeto de evaluación.

Para la Secretaría Escolar y la Unidad Administrativa del plantel, se cuenta con una conexión de UTP directamente del "Switch A Principal" a un convertidor de medios o Transceiver, el cual tiene como función convertir la señal de entrada de cable UTP a una señal de salida apta para viajar en Fibra Óptica. (ver foto4.27).

Una vez que la señal de red llega por medio de Fibra óptica a las oficinas de la Secretaría Escolar es recibida por un convertidor de medios más, para transformarla nuevamente a una señal apta para viajar por cable UTP.

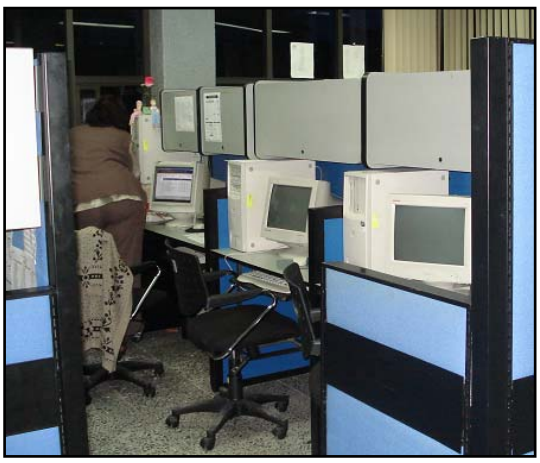
FOTO 4.27 CONVERTIDOR DE MEDIOS EN LA SECRETARÍA ESCOLAR

[4]Un switch o conmutador es un dispositivo electrónico de interconexión de redes que opera en la capa 2 (nivel de enlace de datos) del modelo OSI. Un conmutador interconecta dos o más segmentos de red, funcionando de manera similar a los puentes (bridges), pasando datos de un segmento a otro, de acuerdo con la dirección MAC de destino de los datagramas en la red

Esta señal se conecta a dos Switch de 24 nodos (ver foto4.28) cada uno para dotar de señal a todos los usuarios de la Secretaría Escolar, el servidor VASCONCELOS y la Unidad Administrativa mediante cables UTP.

FOTO 4.28 CONEXIÓN TRANSCEIVER CON SWITCH

En el Centro de Cómputo (ver fotos 4.29 y 4.30) la red está conectada de manera similar, sólo que como la distancia entre el Switch Principal y los laboratorios es mucho menor, la conexión se hace mediante cable UTP.



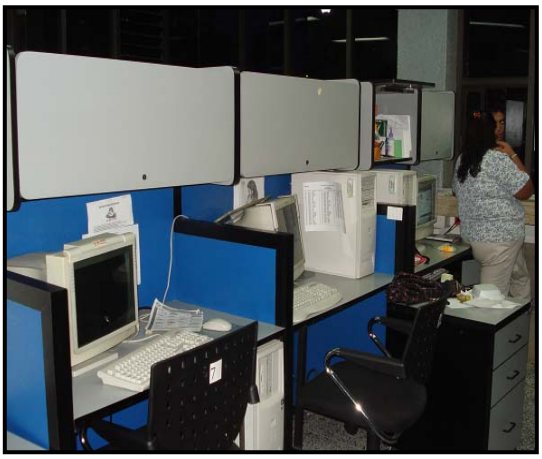


FOTO 4.29 y 4.30 USUARIOS DE SECRETARIA ESCOLAR

Para el Laboratorio 1 sale una conexión del switch principal a un Hub de 24 nodos éste a su vez se conecta con otro Hub de 8 nodos mediante un cable UTP cross over a manera de cascada. De este par de dispositivos sale un cable UTP para cada una de las computadoras que se encuentra en este laboratorio (ver fotos 4.31 - 33).

FOTO 4.31 HUB DE 24 NODOS

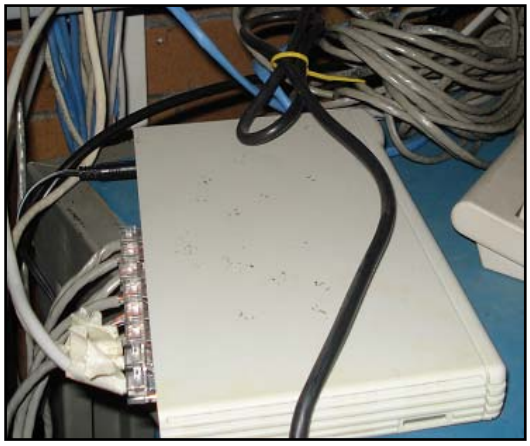


FOTO 4.32 HUB DE 24 NODOS

FOTO 4.33 EQUIPOS EN EL LABORATORIO 1

Para el Laboratorio 2, se tiene una conexión con cable UTP que sale directamente del switch principal y éste viaja desde el área de red hasta el laboratorio 2 literalmente “pegado” sobre la pared del centro de cómputo, para llegar a un par de switches conectados en cascada mediante un cable UTP cross over, dentro del laboratorio(ver fotos 4.34 – 4.36)

FOTOS 4.34 y 4.35 CABLE DE RED PARA EL LABORATORIO 2

FOTOS 4.36. CONEXIÓN EN CASCADA DE SWITCH PARA EL LABORATORIO 2

FOTO 4.37 EQUIPOS EN EL LABORATORIO 2

4.3.8.Información

La información se clasifica como secreta, confidencial y pública, la información secreta es aquella que se maneja en la Unidad Administrativa del Plantel y por obvias razones no puede ser vista por mas de las personas que están autorizadas. La información confidencial son los resultados de las evaluaciones de los profesores que es parte de la información que se maneja en el Centro de Cómputo y la información pública son las calificaciones e información general dirigida a los alumnos por parte de la Secretaría Escolar.

La información que se maneja tanto en la red local como a través de Internet, no es sometida a ningún proceso de encriptación ya que la mayoría de los usuarios de la institución son trabajadores administrativos y no están capacitados para someter la información a algún proceso de este tipo.

En su lugar, toda la información manejada en la institución es enviada en la red local al jefe del departamento en cuestión; entonces éste se encarga de clasificarla y seleccionarla según su delicadeza e importancia.

La disponibilidad de la información se ve algunas veces afectada, esto debido a las malas condiciones climáticas, ya que el servicio de Internet de alta velocidad en el plantel llega vía microonda desde DGSCA[5].

Debido a la incorrecta instalación del cableado estructurado y la no adecuada clasificación de los dispositivos de red, en una contingencia es imposible restablecer el servicio del Centro de Cómputo de manera inmediata.

Ahora bien, los servicios de red local, funcionan sin mayor complicación, sin embargo el hecho de que haya empleados con una pobre instrucción en materia de informática; hace que en ocasiones los servicios de red local tengan una abrupta interrupción.

Esto es en verdad un gran problema ya que si el personal no cuenta con el conocimiento para darle una solución rápida y eficaz el problema empeora; por ejemplo en el servicio de impresión en red, se envían documentos a imprimir sin darse cuenta de que el servicio no está disponible en ese momento.

Otro gran problema es que la gente especializada en soporte técnico, no coincide con los horarios de los demás trabajadores, y cuando se presenta alguna anomalía en algún equipo, el problema persiste hasta que la persona especializada acude a darle solución.

El uso del software propio de la organización está autorizado únicamente para las personas que laboran en las áreas específicas del plantel, como una medida para garantizar este hecho se propone a los trabajadores la creación de claves a sus cuentas de sesión tanto en los equipos de cómputo como en las sesiones de los sistemas especializados. Al no contar con un generador de claves y confiar en el juicio de los usuarios para generar sus propias contraseñas, se está agrandando una enorme grieta en la seguridad, ya que por lo regular las contraseñas proporcionadas de esta manera tienen un nivel de seguridad muy bajo y son muy propensas a plagios.

[5] Cicuito Escolar de Ciudad Universitaria C.P. 04510. Frente a la Facultad de Contaduría y Administración

Esto representa una enorme amenaza para la información ya que si no se cuenta con claves verdaderamente confiables, pueden presentarse ataques de índole interno.

4.4.Vulnerabilidades y Recomendaciones

A continuación se presentan y describen de forma general los problemas y consideraciones que afectan directa o indirectamente la seguridad del la institución, y con base en éstas más adelante se formulan las políticas de seguridad.

4.4.1. Falta de control de los recursos de cómputo

Si se pretende que el plantel cuente con un sistema que garantice en gran medida, que los activos de la institución estarán seguros; es recomendable tener un control total y absoluto de los recursos de cómputo con los que se cuenta.

Por experiencia se ha observado en los últimos meses que no se cuenta con un registro debidamente inventariado y organizado de todos y cada uno de los recursos de cómputo que han sido asignados al plantel. Esto representa un gran riesgo ya que si se ha omitido el registro de alguno o algunos de los recursos, no se puede hacer un debido análisis de riesgos de los activos de la institución, y por consecuencia no se podría diseñar un sistema que garantice la seguridad del plantel.

También es importante tener muy en cuenta la ubicación física de los equipos en todas las áreas ya que si por algún motivo se presenta la necesidad de cambiarlo de ubicación, se tendrá el control exacto del inventario de los equipos en cuestión.

A continuación se dan las ventajas por las cuales es importante dicho control.

- **Software:**
  - Permite la fácil localización de un Software cuando este es requerido.
  - Se evitan gastos innecesarios compartiendo software y licencias entre departamentos.
  - Permite mantener actualizadas las versiones de los sistemas operativos, utilerías, servicio de red y cualquier otro software.
- **Hardware:**
  - Permite tener un conocimiento del total del equipo de cómputo.
  - En base a ese conocimiento se prevé la utilización de mecanismos que aporten cierto nivel de seguridad.
  - Ante cualquier amenaza, se conoce cuales son los recursos críticos que deben ser primordialmente resguardados, y en caso de pérdida se conoce el monto total de los daños.
  - Permite un mayor control para el mantenimiento preventivo y correctivo del equipo de cómputo.
  - Permite tener un control para la actualización del equipo de cómputo.
- **Incidentes de Seguridad:**
  - Permite conocer que tan vulnerables son los sistemas.

- Permite saber cuales son los huecos de seguridad más explotados y en base a ello tomar las medidas de seguridad necesarias para controlar incidentes.
- Se lleva un historial de los incidentes presentados para que puedan posteriormente servir de referencia en respuesta a nuevos ataques.
- Permite a la Coordinación de Cómputo, en base a los reportes de incidentes enviados y a la experiencia de los administradores elegir y definir un procedimiento estándar que solucione de forma más rápida y definitiva el problema.
- Las experiencias, retroalimentación e información son compartidas entre los administradores
- Se cuenta con información detallada y disponible para cualquier tipo de estudio sobre la seguridad en cómputo de la institución.

La Coordinación de Cómputo en conjunto con el departamento de Compras e inventarios de la unidad administrativa, es responsable de la administración de los recursos de cómputo de la institución como parte de sus actividades básicas deben llevar el control del software y hardware que pertenecen a la institución y de los incidentes de seguridad ocurridos en el mismo.

Solución:

Para acelerar y facilitar el proceso de control del equipo y sistemas de cómputo de plantel, los administradores de cada área, deben mantener un control de sus recursos tanto de hardware como de software y reportarlos a través de formatos establecidos específicamente para este fin.

A continuación, se presenta el contenido de dos de los formatos que serán utilizados por las diferentes áreas del plantel, en los cuales se detalla la información requerida a los Administradores de área para su concentración.

Ver Capítulo 5 del apartado de“Políticas del equipo de cómputo” incisos a) y d)

Formato de control de Incidentes de Seguridad

Reporte Nº _____
Fecha _____
Departamento _____

Antecedentes

1) Descripción del incidente
    a) Cómo se detectó
    b) Como se analizó el incidente
2) Describir lo que se encontró (Nombre del Software y versión, archivos, herramientas, etc.)
3) Consecuencias o daños del incidente
4) Primeras medidas en respuesta al incidente

Respuesta al Incidente

5) Recursos comprometidos (S. O, Servicios de Red, hardware, etc.)
6) ¿Se detectó al intruso, interno y/o externo ? (describir como se detectó)
7) ¿Se implementó algún recurso que bloqueara definitivamente la posibilidad de ocurrencia de dicho incidente?. Describa lo que se hizo.
8) Observaciones

No. de INVENTARIO	
AREA	
FECHA	

USUARIO	**C P U**					**MONITOR**			
	INV-UNAM	**No.SERIE**	**WINDOWS**	**MARCA**	**MODELO**	**INV-UNAM**	**SERIE**	**MARCA**	**MODELO**

MOUSE			**TECLADO**			**SOFTWARE**		**HARDWARE**		
INV-UNAM	**SERIE**	**MARCA**	**INV-UNAM**	**SERIE**	**MARCA**	**S. O.**	**OFFICE**	**PROC**	**RAM**	**H. D.**

FORMATO PARA CONTROL DE INVENTARIO DE HARDWARE Y SOFTWARE

4.4.2.Mantenimiento y actualización

Al no contar con este tipo de servicio se incrementan las posibilidades de que exista una falla que ocasione alteraciones en el software y la información puede no estar disponible si se presenta un caso.

Si el equipo no es de nueva adquisición, éste es revisado por los Técnicos Académicos de cómputo para emitir un diagnóstico y en lo posible, solucionar la falla. Este servicio se da sin la seguridad de que la información contenida en los equipos no será robada por el o los técnicos en cuestión.

Solución:

Cuando el equipo es de nueva adquisición y presenta algún problema, se hace valer la garantía del equipo y el servicio de mantenimiento se brinda por personas ajenas a la institución, es decir, el proveedor. En caso contrario, el mantenimiento del equipo es efectuado por los Técnicos Académicos de Cómputo.

Ver Capítulo 5 del apartado de"Políticas del equipo de cómputo"incisos b) y c)

4.4.3.Libre acceso a las salas de cómputo

- Usuarios: Actualmente la institución solo se basa en la visualización por parte del personal de vigilancia confiando en el aspecto y apariencia de las personas que entran o salen, pero esto no es suficiente para garantizar que entran solo las personas que realmente tienen acceso y que nadie extraerá o hará uso indebido de los sistemas de cómputo y de sus recursos.

  Este problema origina que cualquier persona de cualquier área o incluso externa a la institución pueda sustraer, dañar, hacer mal uso de los recursos de cómputo o utilizar las cuentas y los huecos de seguridad en ellas para comprometer los sistemas o información de lo usuarios. Debido a esto se han tenido incidentes de seguridad como el robo parcial de recursos en el Centro de Cómputo que aunque esto no trae consecuencias directas como la destrucción, revelación e integridad de la información si afecta a la Institución. Algunos otros problemas tienen que ver con la oportunidad de acceso de cualquier hacker a las salas de cómputo así como el acceso al resto de los equipos. Esta es precisamente la justificación para definir y establecer que los sistemas y recursos de cómputo deben estar en lo posible resguardados de cualquier atentado ocasionado por la falta de restricción en el acceso a las Salas de Cómputo.

Solución:

Se podría poner en marcha es que, todos y cada uno de los usuarios a los cuales se les conceda el acceso a las instalaciones, ya sean alumnos, profesores o trabajadores en general, sean debidamente identificados por el personal de vigilancia, así mismo, deberán registrarse en un bitácora de control de accesos, y presentar de manera física una identificación que los acredite como miembros de la institución, sea cual sea su cargo.

- Visitas: Generalmente las personas que no pertenecen a la Institución pueden entrar una vez registradas en un formato de control. Algunas ocasiones se les da un gafete de visita y en ocasiones no, pero una vez entrando a las instalaciones, prácticamente se encuentran libres y fácilmente pueden hacerse pasar por cualquier persona que labore dentro de las oficinas, en caso de que hayan tenido acceso a las salas de cómputo abiertas y/o nadie les haya preguntado ¿Qué hacen dentro del área sin autorización?,

Solución:

Asignar y obligar a que se porte un gafete que debe ser proporcionado a la entrada del plantel, con un color distintivo dependiendo del lugar a donde se dirijan. Por ejemplo si la visita se dirige oficialmente al Centro de Cómputo o Secretaría Escolar así lo deberá indicar su gafete y en caso de que se le sorprenda estando en algún otro departamento, será fácil identificar en primer lugar, que se trata de una visita y en segundo que no está en el lugar correcto, esto solo será derivado por dos causas, por que se perdió en el plantel o definitivamente por que esta husmeando.

Ver Capítulo 5 del apartado de "Políticas de control de accesos" inciso a).

4.4.4. Acceso al equipo de cómputo, la red y sistemas administrativos.

Los usuarios de los equipos de cómputo tienen acceso a los mismos de distintas maneras dependiendo del área en que se encuentren.

En la Unidad administrativa y en la Secretaría Escolar, solo tienen acceso el personal custodio de los equipos, es decir, cada usuario tiene una PC que es responsabilidad suya y de nadie más.

En el Centro de Cómputo es un tanto distinto, los usuarios "alumnos" tienen el derecho implícito de utilizar un equipo de cómputo durante el tiempo que permanezca dentro del laboratorio asignado para sus clases de Informática. De esta manera es entonces el profesor en cuestión, el responsable de todo lo que ocurra dentro del laboratorio en materia de equipo de cómputo.

Para poder hacer uso de una PC dentro del centro de Cómputo, los usuarios profesores deben expresar su deseo de esto al personal encargado del centro de cómputo, y sólo bajo su autorización podrá hacer uso del mismo. Algo similar sucede con los alumnos que quieran trabajar en un equipo fuera de su horario de clase.

En muchas ocasiones, cuando los usuarios consiguen el acceso a los equipos aprovechan para elaborar trabajos que en poco o nada tienen que ver con asuntos académicos, por ejemplo navegan por páginas restringidas, descargan software no autorizado, juegan y hasta maltratan o hurtan en el peor de los casos, el equipo de cómputo que les fue asignado.

Solución:

Una solución es que exista en todo momento una persona que verifique el buen uso de los equipos de cómputo, es decir, tener un vigilante que dé aviso del mal uso, mutilación o robo del equipo de cómputo. O bien, publicar en todos los lugares visibles para los usuarios, las responsabilidades que acarrea el uso de un equipo así como las consecuencias a las que se hace sujeto si se detecta un mal uso del mismo.

Ver Capítulo 5 del apartado de "Políticas de control de accesos" inciso b) al f).

4.4.5. Ignorancia en el uso básico del sistema y la importancia en la seguridad.

Parte de la información básica en cada cuenta son los archivos de configuración que definen aspectos importantes sobre el comportamiento del sistema frente a otros sistemas y usuarios. Uno de estos archivos por ejemplo, permite al usuario especificar que cuentas o usuarios pueden acceder a sus sistemas casi sin ningún tipo de autenticación. Esta es una forma práctica y rápida para el manejo de conexiones remotas, aunque esta facilidad también

puede generar grandes huecos de seguridad si el usuario por ignorancia no las define de forma correcta.

Por otra parte, los usuarios, por ser los que trabajan diariamente con los sistemas, son los que con mayor posibilidad pueden detectar anomalías en su cuenta o sobre la red, pero si no saben o no asumen esa responsabilidad encontraran siempre otras cosas más importantes que hacer, que simplemente avisar a los encargados acerca del problema. Esta es ciertamente otra desventaja para localizar al momento cualquier problema o inconsistencia que pueda comprometer al sistema.

Por tal motivo es claro que si no se tiene una educación en seguridad para los usuarios nunca creerán importante, necesario ni obligatorio asumir el compromiso de formar parte activa en la procuración de seguridad desde su propio lugar, comenzando por la creación adecuada de contraseñas.

Solución:

Concienciar a los usuarios sobre los aspectos básicos de seguridad en el uso del sistema con la impartición de cursos básicos para el manejo de la PC, y los aspectos más relevantes de seguridad. Estos cursos se impartirán anualmente y todo usuario estará obligado a participar en ellos. La capacitación es una medida indispensable también para los administradores de los sistemas en el fortalecimiento de cualquier mecanismo de seguridad incluyendo las políticas de seguridad.

Sin embargo este punto podrá darse en la medida en que la institución esté conciente y preparada para realizar cambios y ajustes que mejoren la seguridad en sus sistemas de cómputo, cuando se tiene planteadas políticas o al menos una filosofía de seguridad dentro de la institución, será necesario como primera acción capacitar a cada usuario y administrador según estos lineamientos de seguridad.

Ver Capítulo 5 del apartado de “Políticas de acceso a cuentas de usuario”

4.4.6.Utilización de los recursos de red

La red en la E.N.P. 5 la cual es parte de la Red UNAM es una subred local clase C con disponibilidad de 255 nodos para conexión de equipos. Como se describió anteriormente, la instalación de la red en general es deficiente ya que no se cuenta con una estructura debidamente identificada en el “cerebro” de la red el cual se encuentra en el área de red del Centro de Cómputo.

No se cuenta con ventilación adecuada, y tampoco se tiene personal destinada al aseo de esta área.

Los cables de conexión no cuentan con ningún tipo de identificación ni protección, los dispositivos de hardware de red se encuentran en una disposición física que hace muy difícil determinar, en caso de falla, cual de los dispositivos es realmente el que no está funcionando.

Por ejemplo, si ocurre una interrupción en el servicio de red, lo que se procede a hacer es desconectar físicamente dispositivo por dispositivo y volverlos a conectar con lo que las fallas se solucionan a prueba y error.

Solución:

Cumplir con los estándares de las normas internacionales para la construcción de los centros de computo, que contempla; instalaciones eléctricas, sistemas de tierras, análisis de calidad de energía, aire acondicionado, cableado estructurado, detección y extinción de incendios, control de acceso, circuito cerrado de televisión, seguridad, automatización y monitoreo local y remoto, piso falso, falso plafón y acabados, muros contra incendio, proyectos llave en mano.

Ver Capítulo 5 del apartado de "Políticas de recursos de red"

4.4.7.Revelación de contraseñas y cuentas compartidas

La revelación de contraseñas y el compartir de cuentas son problemas de seguridad cotidianos en la mayoría de los departamentos de la institución, e independientemente de la razón por la cual estas actitudes sean permitidas (como desarrollo de un mismo proyecto o confianza) lo que si es real, es que se están creando grandes huecos de seguridad no solo a nivel departamento sino además en todo el sistema de información del plantel. Es claro que existen muchos otros métodos y herramientas de los intrusos para explotar cualquier hueco en los sistemas, pero las contraseñas y cuentas estrictamente personales pueden minimizar y evitar problemas potenciales.

Sin embargo la situación no termina aquí, si la contraseña es revelada a una persona externa, o incluso interna, y ésta tiene intereses secundarios, una vez teniendo el acceso a una puerta del sistema o bien una cuenta, se tiene con mayor posibilidad otros privilegios que pueden comprometer la información de terceros, el sistema mismo, o servir de puente para un intruso.

Solución:

Convocar a los usuarios a tomar pláticas informativas y de concienciación para exponer los riesgos que conlleva la compartición de claves y cuentas de usuario; fincar responsabilidades y establecer sanciones para los infractores.

Ver Capítulo 5 del apartado de "Políticas de acceso a cuentas de usuario"

4.4.8.Falta de ética en seguridad en cómputo

Es válido considerar que la falta de ética suele ser el origen de muchos problemas de toda índole, que ciertamente todo se mueve con respecto a los intereses personales de cada individuo. En materia de cómputo, la ética tiene que ver con muchos aspectos que involucran a la seguridad.

La intimidad por ejemplo es un derecho que con los medios de comunicación tradicionales como el correo postal o correo certificado; está hasta cierto punto garantizado, en cambio

con el uso generalizado de los sistemas de comunicación electrónicos, la intimidad y el anonimato de las personas resultan crecientemente amenazadas.

Aunque hablar de ética es un tema muy difícil de tratar por ser demasiado interno y particular a cada persona, es evidente que actuar con ética es lo mínimo que todo individuo le debe a otro o a una institución.

Solución:

Independientemente de cualquier situación, toda persona debe respetar los derechos de intimidad, confidencialidad y propiedad de terceros, esto implica desde no entrometerse en información crítica como el teclear una contraseña o password, hasta intimidar, insultar o molestar a otros mediante los mecanismos de comunicación electrónicos.

Ver Capítulo 5 del apartado de “Políticas de respeto a los derechos de los demás”

4.4.9.Adquisición, Instalación, Actualización del software y licencias

El software que se usa dentro del plantel, por lo general es por procedencia ilegal, a menos de que se trate de algún sistema operativo (Windows) ya que debido a que el equipo que se adquiere es de marca cuenta con la licencia de Microsoft para Windows.

En cuanto a procesadores de texto, tablas, etc. El resto del software que es instalado es de procedencia ilegal o bien pirata, a excepción del software propiedad de la institución, el cual se envía directamente a las áreas que lo requieren desde la Dirección General de la Escuela Nacional Preparatoria o de la Dirección General de personal.

El software antivirus que fue adoptado por el plantel, a petición de la Coordinación de Cómputo, es el Grisoft AVG el cual es un software de libre distribución.

Muchas veces, el software es instalado de manera errónea y por personas que no tiene el conocimiento necesario para hacerlo, esto repercute en un mayor índice de fallas en los sistemas.

Esto representa un gran riesgo para la seguridad de los sistemas ya que por no contar con las licencias necesarias para el uso del software se pueden dejar de recibir ciertas actualizaciones y parches importantes para la navegación segura en Internet. O bien, en el caso del software institucional no se respetaría la propiedad intelectual haciendo copias no autorizadas de software.

Solución:

Una solución a este problema es que el plantel cuente con un presupuesto destinado específicamente para la adquisición de software original, y que se ponga en marcha. Así mismo es recomendable que el software sea instalado por una persona capacitada para hacerlo de la manera correcta.

También se propone que aquel software, propiedad de la institución quede protegido bajo la propiedad intelectual y los derechos de autor.

Ver Capítulo 5 del apartado de "Políticas de software y políticas de uso de licencias"

4.4.10.Uso irresponsable de los recursos de cómputo

Desde hace tiempo, la institución ha sido víctima en diversas ocasiones de usos indebidos de los recursos de cómputo que la Coordinación de Cómputo asigna al personal para el desarrollo de sus actividades. Usos irresponsables los hay desde atentados físicos, hasta utilizar el equipo como medio para comprometer sistemas de cómputo local o remoto.

Comenzando con los atentados físicos, muchas de las veces el equipo de cómputo es dañado o robado parcialmente, y aunque esto no atenta en amplio grado la seguridad de los sistemas y la información, si lo hace indisponible.

Ahora hablando del uso inadecuado de los recursos de cómputo, poco tiempo antes de la elaboración de esta propuesta, en algunas áreas del plantel se trató de controlar el uso de los recursos de impresión para uso personal con sanciones. Sin embargo este tipo de actos son un tanto difíciles de controlar, y como dato interesante que cabe mencionar, la cantidad de recursos directos invertidos anualmente a la impresión asciende a varios miles de pesos.

Otro problema que se ha encontrado en la áreas de estudio de la institución, es el uso ilegal de los discos duros, para diversos fines, por ejemplo, el almacenamiento no autorizado de software del servicio de red, por ejemplo los programas de charla en línea (chats) o archivos ejecutables para juegos o música. Obviamente esto genera en amplio grado indisponibilidad en operaciones de entrada y salida en los sistemas, pero debemos recordar que la mayoría de los virus entran a nuestras máquinas por medio de este tipo de archivos.

Solución:

Cualquier situación problemática que se presente con el equipo, debe ser inmediatamente reportada a los administradores para convocar a las personas encargadas, su solución.

Ver Capítulo 5 del apartado de "Políticas del uso responsable del equipo de cómputo"

Algunos otros problemas en cómputo que atentan contra la seguridad de los sistemas es la creación de cuentas ilegales con las cuales se logran accesos ilícitos, comprometiendo el sistema. De hecho se han encontrado en varias ocasiones archivos de contraseñas o passwords almacenados en directorios ocultos o en cuentas de usuarios, que han obligado a tomar medidas de emergencia.

Las sesiones abiertas no controladas y las cuentas compartidas son un hueco fácil de ataques, pues mientras la sesión se encuentre abierta y el usuario ausente, el tiempo puede ser suficiente para que un intruso pueda comprometer el sistema u obtener información crítica del mismo. Al parecer estos motivos no han sido hasta el momento un blanco de incidentes de seguridad grave, pero si es necesario aclarar que aunque no existan pérdidas de información visibles para el propietario de la cuenta, la información está disponible para ser accesada y visualizada rápidamente, incluyendo información confidencial y cuyo propietario puede ser hasta la misma institución.

Solución:

Cada usuario tiene la obligación de cuidar y usar de forma responsable los recursos asignados, y en base a que todo recurso de cómputo pertenece a la institución, el uso solo se hará con fines legales y relacionados a la misión de la misma, esto es que el usuario siempre y cuando mantenga una relación oficial con la institución, puede utilizar el equipo y los sistemas de cómputo única y exclusivamente para lo que debe y se le está permitido hacer.

Ver Capítulo 5 del apartado de “Políticas del uso responsable de los recursos de cómputo” y “Políticas de respeto a los derechos de los demás”

4.4.11.Respaldos de información y planes de contingencia

Las catástrofes (naturales o artificiales) son la amenaza menos probable contra los entornos habituales: simplemente por su ubicación geográfica, a nadie se le escapa que la probabilidad de sufrir un terremoto o una inundación que afecte a los sistemas. Sin embargo, el hecho de que las catástrofes sean amenazas poco probables no implica que contra ellas no se tomen unas medidas básicas, ya que si se produjeran generarían los mayores daños.

Un subgrupo de las catástrofes es el denominado de riesgos poco probables. Obviamente se denomina así al conjunto de riesgos que, aunque existen, la posibilidad de que se produzcan es tan baja (menor incluso que la del resto de catástrofes) que nadie toma, o nadie puede tomar, medidas contra ellos. Ejemplos habituales de riesgos poco probables son un ataque nuclear contra el sistema, el impacto de un satélite contra la sala de operaciones. Nada nos asegura que este tipo de catástrofes no vaya a ocurrir, pero la probabilidad es tan baja y los sistemas de prevención tan costosos que no vale la pena tomar medidas contra ellas.

Al no contar con un esquema de elaboración y clasificación de respaldos, se corre el riesgo de no disponer de la información en caso de contingencia. Alguna vez en el Centro de Cómputo se observó que el archivo que contiene el control de inventario de equipos de ésta área fue dañado por un virus informático; y precisamente en aquellas fechas se acercaba la comisión de Auditoria de la Dirección General de Preparatoria Nacional. Como no se contaba con ningún respaldo de esta información, se tuvo que trabajar a marchas forzadas y sin interrupción en el registro y captura de los números de inventario de todos y cada uno de los dispositivos de hardware que se encontraban en ése momento en el centro de cómputo. Un trabajo bastante exhaustivo.

Solución:

Como sea, es importante contar con respaldos de información, al menos, para poder responder ante alguna catástrofe que dañara el estado actual del sistema.

Contar con procedimientos de respuesta para eventos radicales, y desde luego contar con medidas para eventos más probables como un incendio en las instalaciones, con equipos contra incendio que puedan evitar un daño total.

Ver Capítulo 5 del apartado de “Política de elaboración de respaldos y planes de contingencia”

4.5.Desarrollo de las Políticas de Seguridad

El objeto de evaluación quedó conformado por las áreas de Secretaría Escolar, Unidad Administrativa y Centro de Cómputo. Las personas encargadas de que la información y los recursos fluyan constantemente son principalmente el personal del Centro de Cómputo, estos se encargan de brindar servicio directo al usuario, por el ámbito de competencia que tiene cada uno de ellos en materia de informática, desde el equipamiento, instalación, alteración, cambio de lugar, programación, etc.

Para crear una política de seguridad en cómputo también es necesario determinar cuales son actualmente los problemas y las causas que están generando deficiencias en el desarrollo computacional, esto permite definir de forma real, las medidas que solucionen de forma directa y eficaz los problemas que en seguridad se desean resolver.

La política principal de seguridad en cómputo de la institución se define bajo dos premisas:

- Como medida correctiva en solución a los problemas de seguridad en cómputo que han surgido y de los que actualmente son motivo potencial de incidentes de seguridad.
- Como medida preventiva de nuevos ataques que si bien no han ocurrido se desean evitar hasta el mayor grado posible.

A lo largo de esta tesis, se ha llevado a cabo un análisis minucioso de la situación en cuanto a seguridad informática en la que se encuentra la ENP 5 destacando los aspectos más sensibles y por ende más importantes para el desarrollo de las políticas de seguridad, a continuación se describen de forma global las principales partes que fueron consideradas.

- Con el objeto de conocer el contexto en el cual se desarrolla este proyecto, se realizó un estudio de la estructura de la red de la Secretaría Escolar, Unidad Administrativa y el Centro de Cómputo de la Escuela Nacional Preparatoria Plantel 5 “José Vasconcelos”, los recursos y sistemas de cómputo, servicios de red, entre otros.
- Después, se trató la situación actual de la seguridad de cómputo en las áreas de análisis, los problemas y necesidades de seguridad, los incidentes que se han suscitado, etc.
- Posteriormente se definieron los recursos con los cuales se contaba para el desarrollo de las políticas y posteriormente para los procedimientos de seguridad, los recursos humanos, recursos técnicos así como herramientas y dispositivos de seguridad.
- Se procedió con la definición de las políticas de seguridad.
- Finalmente una vez que éstas fueron definidas, se derivó como acción secundaria desarrollar el plan de seguridad y se dieron algunas sugerencias para la implementación y evaluación de dichas políticas.

4.6. Seguridad en los sistemas

Expertos en seguridad afirman que “Ningún Sistema de Cómputo puede estar completamente seguro sino hasta que éste se encuentre apagado y físicamente bien resguardado”. Ciertamente tratar asuntos sobre la implementación de seguridad en los sistemas suele ser muy extenso, no solo por la diversidad de métodos y herramientas que actualmente existen para implementar seguridad, sino además por la cantidad de métodos y técnicas de ataque que los intrusos innovan para comprometer sistemas. Es necesario tener en mente que la complejidad de la seguridad puede crecer exponencialmente con el número de servicios proporcionados, y que entre más comunicada se encuentre una máquina mayores serán los riesgos y los requerimientos de seguridad.

Las herramientas y dispositivos de seguridad pueden ser un mecanismo útil en la seguridad del sistema, generalmente cada herramienta está diseñada para cubrir objetivos específicos.

Un aspecto básico a considerar antes de la implementación de cualquier herramienta de seguridad, es conocer cuáles son actualmente los huecos de seguridad o los puntos débiles del sistema que pueden ser explotados con mayor facilidad, y con base en ese estudio, elegir las herramientas más convenientes.

Este particular interés se fundamenta en que no existe actualmente dentro del plantel medidas de seguridad que establezcan el uso de herramientas que mejoren la seguridad de los sistemas, generalmente solo hay instalado un antivirus en los equipos y debido a que se trata de software libre, no provee de protección confiable a los sistemas de información.

Las herramientas de seguridad no pueden considerarse como una medida extra de seguridad sino el medio posible que hace lo que un administrador no puede hacer, monitorear día y noche todos y cada uno de los sistemas, verificar si alguno de ellos en sus múltiples directorios tiene algún archivo intruso, o si existe alguna contraseña o password débil en los sistemas que deba ser cambiado, etc. En fin estas son actividades que pueden fungir como excelentes vigilantes y generadores de información que pueda ser posteriormente interpretada por el administrador para la toma de decisiones.

Existen otros dispositivos de seguridad que igualmente pueden fortalecer la seguridad de los sistemas. La implementación de cualquier mecanismo de seguridad surge con base en el nivel de seguridad requerido y a los problemas de seguridad que se deseen tratar.

La Coordinación de Cómputo debe tomar el control de estas decisiones. Cada mecanismo a implantar, debe ser estudiado, definido, reglamentado y ejecutado periódicamente a nivel institucional como se crea pertinente.

A los administradores de área como responsables de la seguridad de los sistemas, les concierne la acción de echar a andar herramientas y mecanismos de seguridad que necesiten ser implementados y todo aquello que sea necesario para su adaptación y funcionamiento.

Además como medida de seguridad indispensable, se deben normar y auditar periódicamente los archivos de configuración y los permisos de acceso a los sistemas, especialmente en las cuentas de servicios de red de la institución, con el objeto de evitar que deficiencias en este rubro, puedan ser utilizadas por intrusos para irrumpir la seguridad de los sistemas.

Ahora bien, como parte de un SGSI se integran la elaboración, publicación y puesta en marcha de las Políticas de Seguridad Informática de la institución, las cuales serán vistas y revisadas ampliamente en el siguiente capítulo.

CAPÍTULO 5
POLÍTICAS DE SEGURIDAD INFORMÁTICA DE LA ENP No.5 “JOSÉ VASCONCELOS”

5. POLÍTICAS DE SEGURIDAD INFORMÁTICA DE LA ENP No.5 “JOSÉ VASCONCELOS”

5.1. Introducción

Conforme a transcurrido el tiempo a partir de la segunda década de los ’80, los incidentes de seguridad, comenzaron a acaparar la atención de propios y extraños, los medios masivos de comunicación descubrieron una nueva “mina de oro “ al dar a conocer al público los detalles, a veces inventados de algunos de los más conocidos problemas en este campo, como el tan conocido ataque a la Fuerza Aérea de los Estados Unidos considerado como el más organizado y sistemático que hasta el momento ha sufrido el Pentágono, y como estos, una infinidad de ataques de los cuales una mayoría son publicados por Agencias de Seguridad computacional a través de Internet, y otras tantas, ni siquiera son detectados.

Aunque estos incidentes han servido como entretenimiento al público, también han servido para ir despertando la conciencia tanto de la misma gente como de los Administradores y Usuarios de Sistemas de Cómputo, de que la seguridad debe ser actualmente una preocupación real. Las situaciones que antes pertenecían a las historias de Ciencia ficción ahora se encuentran en la vida real con una frecuencia cada vez mayor.

Sin embargo la Seguridad en Cómputo va mucho más allá de impedir que los intrusos se roben la información y se la vendan al enemigo. También implica proteger a los usuarios contra sus propios errores, o sugerir a los administradores realizar a tiempo sus respaldos. Los problemas cotidianos son mucho menos “atractivos” que la persecución de un espía a través de redes de cómputo, pero son igual de importantes, de manera que es necesario estar preparados para hacerles frente.

5.2. Objetivo del proyecto

Este proyecto surge en respuesta a la preocupación por mantener los sistemas y la información del Centro de Cómputo seguros contra cualquier forma de ataque. Pretende no solo establecer una filosofía de seguridad, sino forjar una educación y un hábito en usuarios y administradores que conlleve a un ambiente mas seguro tanto en los sistemas internos como hacia al mundo entero.

5.3. Razón de las Políticas de Seguridad

Este documento representa una propuesta de políticas de seguridad que pretende alcances institucionales que permita crear y establecer una educación y una filosofía sobre la postura que en materia de seguridad en cómputo debe tener el Centro de Cómputo de la Preparatoria 5 “José Vasconcelos” respecto a las amenazas que lo rodean.

5.4. Objetivo de las Políticas de Seguridad

Como norma interna, y considerando que la ignorancia no debe ser tomada como una excusa, esta propuesta de políticas define ciertos lineamientos que establecen un límite entre lo que está permitido a los usuarios dentro y fuera del Centro de Cómputo y lo que no está,

esto es con el propósito de proteger la información almacenada en los sistemas y el acceso a los mismos.

El principio básico de seguridad es “Lo que no se permite expresamente, está prohibido”.

5.5.Vigencia

Estas políticas entrarán en vigor a partir del momento en que las Autoridades del Plantel conjuntamente con la Coordinación de Cómputo lo determinen y su vigencia se dará dependiendo de la funcionalidad de cada una de ellas y de las necesidades posteriores del Centro de Cómputo.

5.6.Políticas generales

1. Los problemas que se presenten de forma cotidiana y el método particular de uso de los sistemas y recursos de cómputo estará plasmado en un reglamento. Llamado “Reglamento Interno para el Centro de Cómputo de la Escuela Nacional Preparatoria plantel 5 José Vasconcelos”.

2. Las diferentes áreas que operen con sus propias redes o computadoras pueden agregar con la aprobación de las autoridades del plantel y la Coordinación de Cómputo las políticas expuestas en este documento y/o solicitar un estudio para el diseño de guías particulares, pero no pueden bajo ninguna circunstancia contradecir tales políticas.

3. Estas políticas deben ser revisadas anualmente por la Coordinación de Cómputo para su constante actualización.

4. Cada uno de los departamentos fuera del Centro de Cómputo deberán emitir, con la asesoría conjunta del personal de cómputo, los planes de contingencia que correspondan a las actividades que realicen.

5. Debido al carácter confidencial de la información, el personal del Plantel y el Centro de Cómputo deberá de conducirse de acuerdo a los códigos de ética profesional y las normas y procedimientos ya establecidos.

5.7.Políticas del equipo de cómputo.

a) De la ubicación del equipo de cómputo.

1. Todo el equipo de cómputo (computadoras, estaciones de trabajo, supercomputadoras, y equipo periférico), que esté o sea conectado a la Red, o aquel que en forma autónoma se tenga y que sea propiedad de la UNAM debe de sujetarse a las normas y procedimientos de instalación básica que emite el Centro de Cómputo del plantel.

2. El departamento de Compras e Inventarios en conjunto con la Coordinación de Cómputo deberá tener un registro debidamente ordenado e inventariado de todos los equipos asignados al plantel.

3. El equipo que sea de propósito específico y tenga una misión crítica asignada (servidores, dispositivos de red, etc.), requiere estar ubicado en un área que cumpla con los requerimientos de: seguridad física, condiciones ambientales, alimentación eléctrica, y acceso que la Coordinación de Cómputo tiene establecido en los procedimientos de este tipo.

4. Los Técnicos Académicos responsables de las áreas de apoyo deberán, en conjunción con la Coordinación de Cómputo dar cabal cumplimiento a los procedimientos de instalación, notificaciones correspondientes de actualización, reubicación, reasignación, y todo aquello que implique movimiento de equipos en su ubicación.

5. La protección física de los equipos corresponde a quienes en un principio se les asigna, y corresponde notificar los movimientos en caso de que existan, a las autoridades correspondientes del Centro de Cómputo o del departamento de Compras e Inventarios u otras de competencia.

b) Del mantenimiento de equipo de cómputo.

1. A la Coordinación del Centro de Cómputo del plantel, corresponde la asignación de equipos de nueva adquisición, la realización del mantenimiento preventivo y correctivo y la verificación de la seguridad física. Para tal fin debe emitir los procedimientos y excepciones respectivas.

2. En el caso de los equipos atendidos por terceros como proveedores de soporte técnico externos; la Coordinación de Cómputo deberá verificar, valorar, y justificar la utilización del servicio e informar a la autoridad correspondiente del requerimiento de servicio con un proveedor externo.

3. El personal técnico de apoyo interno de los departamentos académicos se apegará a los requerimientos establecidos en las normas y procedimientos que el Centro de Cómputo emita.

4. Los Técnicos Académicos de Cómputo pueden otorgar mantenimiento preventivo y correctivo a los equipos, a partir del momento en que sean autorizados por la Coordinación de Cómputo del Plantel.

5. Corresponde al Administrador de la Red (Coordinación de Cómputo) asignar las direcciones IP a los equipos que conforman la Red, así como presentar a las personas bajo su cargo las listas de los usuarios académicos y administrativos, que puedan tener acceso a los equipos y a los servicios de mantenimiento básico, a excepción de los atendidos por terceros.

6. Por motivos de normatividad expedidos por la SECODAM en materia de adquisiciones, arrendamiento y servicios, queda estrictamente prohibido dar mantenimiento a equipo de cómputo que no es propiedad de la institución.

7. El plantel, debe tener debidamente documentados los acuerdos y contratos con las empresas de mantenimiento contratados para su ejecución en el tiempo mínimo.

8. Todo servicio de mantenimiento y/o reparación de los equipos de cómputo que no sea de nueva adquisición, será ejecutado por los Técnicos Académicos de Cómputo previa autorización de la Coordinación de Cómputo y del usuario en cuestión. Además estos servicios serán debidamente documentados en un formato destinado para este efecto.

c) De la actualización del equipo.

1. Todo el equipo de cómputo (computadoras personales, estaciones de trabajo y demás relacionados), y los de telecomunicaciones que sean propiedad del plantel y de la institución, debe procurarse sea actualizado tendiendo a conservar e incrementar la calidad del servicio que presta, mediante la mejora sustantiva de su desempeño.

d) De la reubicación del equipo de cómputo.

La reubicación del equipo de cómputo se realizará satisfaciendo las normas y procedimientos que el Centro de Cómputo emita para ello.

1. El equipo de cómputo a reubicar sea del Centro de Cómputo o de las áreas del plantel externas se hará bajo la autorización de la Coordinación de Cómputo y el acuerdo con el responsable actual del equipo, contando el lugar a donde se hará la ubicación con los medios necesarios para la instalación del equipo.

5.8.Políticas de control de acceso

a) De acceso del personal y visitas a las instalaciones

1. Se consideran usuarios autorizados aquellos que requieren el uso de los recursos de cómputo y de red del Centro de Cómputo, y que se encuentran realizando alguna actividad oficial relacionada con la misión de la institución. Usuarios autorizados son: Técnicos Académicos, Personal Administrativo y Docente, Estudiantes y prestadores de Servicio Social entre otros.

2. El acceso de personal se llevará acabo de acuerdo a las normas y procedimientos que dicta la Coordinación de Cómputo.

3. Todo Técnico Académico de cómputo sin excepción debe portar constantemente el gafete dentro del Centro de Cómputo y solo con el puede tener acceso al mismo.

4. El control de acceso a las salas de cómputo de profesores y alumnos debe ser preferentemente bajo los procedimientos del reglamento del centro de Cómputo.

5. Debido a la naturaleza de estas áreas se llevará un registro permanente del tráfico de personal, sin excepción.

6. El Departamento de Compras e Inventarios deberá proveer de insumos y equipo con base a los requerimientos específicos de cada área.

7. Las visitas que hayan sido previamente autorizadas deben portar un gafete que les será proporcionado en la oficina del Centro de Cómputo con el color adecuado dependiendo del lugar donde se dirijan, pudiendo acceder a las salas de cómputo siempre y cuando la visita se encuentre acompañada por el usuario del Centro de

Cómputo por quien procede, y habiendo previamente solicitado el permiso de acceso a los encargados existiendo una razón suficiente que amerite el acceso a las mismas.

b) Del control de acceso al equipo de cómputo.

1. Todos y cada uno de los equipos son asignados a un usuario, por lo que es de su competencia hacer buen uso de los mismos.

2. Las áreas donde se tiene equipo de propósito general cuya misión es crítica estarán sujetas a los requerimientos que la Coordinación de Cómputo emita.

3. Las áreas de cómputo de los departamentos donde se encuentre equipo cuyo propósito reúna características de imprescindible y misión crítica, deberán sujetarse también a las normas que establezca la Coordinación de Cómputo.

4. Dada la naturaleza insegura de los sistemas operativos y su conectividad en la red, la Coordinación de Cómputo tiene la facultad de acceder a cualquier equipo de cómputo que no esté bajo su supervisión directa.

c) Del control de acceso local a la red.

1. La Coordinación de Cómputo es responsable de proporcionar a los usuarios el acceso a los recursos informáticos.

2. La Coordinación de Cómputo es la responsable de difundir el reglamento para el uso de la red y de procurar su cumplimiento con la ayuda conjunta de los jefes de los departamentos correspondientes.

3. Dado el carácter unipersonal del acceso a la Red Prepa5, el departamento de Cómputo verificará el uso responsable, de acuerdo al Reglamento para el uso de la red.

4. El acceso lógico a equipo especializado de cómputo (servidores, routers, bases de datos, equipo de supercómputo centralizado y distribuido, etc.) conectado a la red, es administrado por la Coordinación de Cómputo.

5. Todo el equipo de cómputo que esté o sea conectado a la Red Prepa5, o aquellas que en forma autónoma se tengan y que sean propiedad de la institución, debe de sujetarse a los procedimientos de acceso que emite el departamento de Cómputo.

d) De control de acceso remoto.

1. La Coordinación de Cómputo es la responsable de proporcionar el servicio de acceso remoto y las normas de acceso a los recursos informáticos disponibles.

2. Para el caso especial de los recursos de supercómputo a terceros deberán ser autorizados por la Dirección General de Preparatorias o por la Dirección del plantel.

3. El usuario de estos servicios deberá sujetarse al Reglamento de uso de la Red Prepa5 y en concordancia con los lineamientos generales de uso de Internet.

4. El acceso remoto que realicen personas ajenas a la institución deberá cumplir las normas que emite la Coordinación de Cómputo del plantel.

e) De acceso a los sistemas administrativos.

1. Tendrá acceso a los sistemas administrativos solo el personal del plantel que es titular de una cuenta de usuario orientada a este efecto o bien tenga la autorización del responsable si se trata de personal de apoyo administrativo o técnico.

2. El manejo de información administrativa que se considere de uso restringido deberá ser cifrada con el objeto de garantizar su integridad.

3. La instalación y uso de los sistemas de información se rigen por el reglamento de uso de la Red Prepa5 y por las normas y procedimientos establecidos por el departamento de Cómputo.

f) De la WWW.

1. La Coordinación de Cómputo es responsable de verificar la correcta instalación de los servidores World Wide Web. Es decir, sólo se permiten servidores de páginas autorizadas.

2. El departamento de Cómputo deberá emitir las normas y los requerimientos para la instalación de servidores de páginas locales, de bases de datos, del uso de la Intranet institucional, así como las especificaciones para que el acceso a estos sea seguro.

3. Los accesos a las páginas de Web a través de los navegadores deben sujetarse a las normas que previamente se manifiestan en el Reglamento de acceso a la Red Prepa5.

4. A los responsables de los servidores de Web corresponde la verificación de respaldo y protección adecuada.

5. Toda la programación involucrada en la tecnología Web deberá estar de acuerdo con las normas y procedimientos que la Coordinación de Cómputo emita.

6. El material que aparezca en la página de Internet de LA PREPARATORIA No. 5 deberá ser aprobado por la Secretaría Escolar y la Coordinación de Cómputo, respetando la ley de propiedad intelectual (derechos de autor, créditos, permisos y protección, como los que se aplican a cualquier material impreso).

7. Con referencia a la seguridad y protección de las páginas, así como al diseño de las mismas deberá referirse a las consideraciones de diseño de páginas electrónicas establecidas por el departamento de Cómputo.

8. La Coordinación de Cómputo tiene la facultad de llevar a cabo la revisión periódica de los accesos a los servicios de información, y conservar información del tráfico.

5.9.Políticas de los recursos de la red

1. Los recursos disponibles a través de la Red serán de uso exclusivo para asuntos relacionados con las actividades sustantivas de la institución.

2. La Coordinación de Cómputo es responsable de emitir el Reglamento, y los Jefes de las áreas correspondientes verificar su fiel seguimiento al Reglamento para el uso de la Red.

3. El uso de Internet y del servicio de correo electrónico es para uso exclusivamente académico.

4. De acuerdo con las disposiciones de la SECODAM[1], corresponde a la Coordinación de Cómputo dar aviso a DGSCA[2] para administrar, mantener y actualizar la infraestructura de la Red Prepa5.

5. Se comisionará un área encargada de supervisar las instalaciones del centro de cómputo para informar a las autoridades correspondientes de las anomalías, daños, desperfectos y necesidades relacionadas con las instalaciones.

5.10.Políticas de acceso a cuentas de usuario

a) Uso autorizado

1. Las cuentas de ingreso a los sistemas y los recursos de cómputo son propiedad de la institución y se usarán exclusivamente para actividades relacionadas con la misma.

2. Para que un usuario sea autorizado para trabajar en un equipo, debe contar con la instrucción suficiente que lo capacite como conocedor del uso de un equipo de cómputo.

3. El usuario tiene la obligación de revisar la guía básica sobre el uso del sistema que le será entregado una vez que su cuenta sea creada.

4. Ninguna cuenta de usuario podrá ser usada para propósitos ilegales, criminales o no éticos.

5. Las cuentas en los sistemas son estrictamente personales e intransferibles.

6. Se agendarán cursos de capacitación dirigidos a los trabajadores que tengan acceso a los equipos y sistemas de cómputo.

7. Para la creación o modificación de contraseñas de acceso, no se deberán utilizar nombres de familiares y conocidos, fechas especiales, nombres en forma invertida, o cualquier palabra que sea fácil de deducir.

8. Para reforzar la seguridad de la información de la cuenta, el usuario bajo su criterio

[1] Secretaría de Contraloría y Desarrollo Económico
[2] Dirección General de Servicios de Cómputo Académico

deberá hacer respaldos de su información dependiendo de la importancia y frecuencia del cambio de la misma.

b) Tiempo de uso de las cuentas

1. Se prohíbe dejar sesiones abiertas sin control alguno.
2. Cuando el usuario deje de tener alguna relación oficial con la institución o la cuenta deje de ser utilizada por un tiempo definido por los administradores, esta debe ser removida.
3. Cuando el usuario deje de laborar o de tener una relación con la institución, este debe notificarlo al administrador de sistemas para proceder y tomar las medidas pertinentes con su información y cuenta de acceso.

5.11.Políticas de respeto a los derechos de los demás

1. Todo usuario debe respetar la intimidad, confidencialidad y derechos individuales de los demás.
2. Nadie puede ver, copiar, alterar o destruir la información de un usuario sin el consentimiento explícito del afectado.
3. Los administradores no podrán remover del sistema ninguna información de cuentas individuales, a menos que la información sea de carácter ilegal, o ponga en peligro el buen funcionamiento de los sistemas, o se sospeche ser de algún intruso utilizando una cuenta ajena.

5.12.Políticas de software

a) Coordinación de Cómputo

1. La Coordinación de Cómputo debe llevar un control total del software y su ubicación física.
2. La Coordinación de Cómputo es la encargada de suministrar medidas de seguridad razonables contra la intrusión o daños a la información almacenada en los sistemas, la instalación de cualquier herramienta, dispositivo o versión de software que refuerce la seguridad de los sistemas. Sin embargo debido a la amplitud y constante innovación de los mecanismos de ataque no se garantiza una seguridad total.
3. La Coordinación de Cómputo debe estar pendiente de la instalación de cualquier parche de software que refuerce la seguridad de los sistemas de cómputo del Plantel.
4. La Coordinación de Cómputo debe monitorear constantemente el tráfico de paquetes sobre la red a fin de determinar y solucionar anomalías, usos indebidos o cualquier falla que provoque problemas de comunicación.
5. La Coordinación de Cómputo es la encargada de agendar y organizar al personal encargado del mantenimiento preventivo y correctivo del equipo de cómputo del

plantel.

b) Administradores de sistemas

1. La instalación del software se hará únicamente por los administradores bajo estricta licencia, a excepción de lo que corresponde al dominio público.

2. Los administradores deben hacer respaldos mensuales de la información de las máquinas que tengan a su cargo, siempre y cuando se cuente con dispositivos de respaldo.

3. El administrador debe mantener informada a la Coordinación de Cómputo de cada software adquirido e instalado.

4. Cada máquina debe estar registrada en el patrón único de control de equipo de cómputo y red de la Coordinación de Cómputo.

5. El administrador debe auditar periódicamente los sistemas y los servicios de red, para verificar que no existen archivos no autorizados, configuraciones inválidas o permisos extras que pongan en riesgo la seguridad de la información.

6. Los incidentes de seguridad deben ser reportados en el formato de control de incidentes y enviados a la Coordinación de Cómputo, junto con cualquier experiencia o información que ayude a fortalecer la seguridad de los sistemas de cómputo.

7. Los administradores de cómputo deben realizar la instalación o adaptación de sus sistemas de cómputo en materia de seguridad.

8. Es responsabilidad del administrador revisar periódicamente las bitácoras de los sistemas a su cargo.

c) De la adquisición de software.

1. Del presupuesto de los proyectos que se otorga a las diferentes áreas del plantel, una cantidad deberá ser aplicada para la adquisición de programación con licencia.

2. La Dirección del Plantel, propiciará y autorizará la adquisición de licencias, licencias flotantes, licencias por empleado y de licencias en cantidad, para obtener economías de escala y de acorde al plan de austeridad del Gobierno de la República.

3. Corresponderá a la Coordinación de Cómputo emitir las normas para el tipo de licenciamiento, cobertura, transferibilidad, certificación y vigencia.

4. De acuerdo a los objetivos globales del departamento de Cómputo se deberá propiciar la adquisición y asesoramiento en cuanto a software de vanguardia.

5. En cuanto a la paquetería sin costo deberá respetarse la propiedad intelectual intrínseca del autor.

6. La Coordinación de Cómputo promoverá y propiciará que la adquisición de software de dominio público provenga de sitios oficiales y seguros.

d) De la instalación de software.

1. Corresponde al departamento de Cómputo emitir las normas y procedimientos para la instalación y supervisión del software básico para cualquier tipo de equipo.

2. En los equipos de cómputo, de telecomunicaciones y en dispositivos basados en sistemas de cómputo, únicamente se permitirá la instalación de software con licenciamiento apropiado y de acorde a la propiedad intelectual.

3. El departamento de Cómputo es responsable de brindar asesoría y supervisión para la instalación de software informático.

4. La instalación de software que desde el punto de vista de la Coordinación de Cómputo pudiera poner en riesgo los recursos de la institución no está permitida.

5. Con el propósito de proteger la integridad de los sistemas informáticos y de telecomunicaciones, es imprescindible que todos y cada uno de los equipos involucrados dispongan de software de seguridad (antivirus, vacunas, privilegios de acceso, y otros que se apliquen).

6. La protección lógica de los sistemas corresponde a quienes en un principio se les asigna y les compete notificar cualquier movimiento al departamento de Cómputo.

e) De la actualización del software.

1. La adquisición y actualización de software para equipo especializado de cómputo y de telecomunicaciones se llevará a cabo de acuerdo a la agenda que sea propuesta por la DGSCA.

2. Corresponde a la Coordinación de Cómputo proponer la adquisición y actualización del software.

3. El usuario deberá mantener actualizadas y habilitadas permanentemente las herramientas oficiales de exploración y eliminación de virus.

4. Las actualizaciones del software de uso común o más generalizado se llevarán a cabo de acuerdo al plan de actualización desarrollado por la Coordinación de Cómputo.

f) Del software propiedad de la institución.

1. Toda los programas adquiridos por la institución sea por compra, donación o cesión es propiedad de la institución y mantendrá los derechos que la ley de propiedad intelectual le confiera.

2. El departamento de Cómputo deberá tener un registro de todos los paquetes de programación propiedad del plantel.

3. Todos los sistemas programáticos (programas, bases de datos, sistemas operativos, interfases) desarrollados con o a través de los recursos del plantel se mantendrán como propiedad de la institución respetando la propiedad intelectual del mismo.

4. Es obligación de todos los usuarios que manejen información masiva, mantener el respaldo correspondiente de la misma ya que se considera como un activo de la institución que debe preservarse.

5. Las bases de datos, la información generada por el personal y los recursos informáticos de la institución deben estar resguardados.

6. Corresponderá a la Coordinación de Cómputo promover y difundir los mecanismos de respaldo.

7. La Coordinación de Cómputo administrará los diferentes tipos de licencias de software y vigilará su vigencia en concordancia con la política informática.

5.13.Política de uso de licencias

1. Está prohibido inspeccionar, copiar y almacenar programas computacionales, software y demás fuentes que violen la ley de derechos de autor.

2. Todas las licencias del software de adquisición legal por parte de la institución, deberán ser renovadas y actualizadas año con año o conforme a contrato con el proveedor.

5.14.Políticas de uso responsable de los recursos de cómputo

1. Se prohíbe dañar, sustraer o hacer mal uso de los recursos de cómputo y red de la institución.

2. Por ningún motivo está permitido resetear, desconectar periféricos o provocar interrupciones eléctricas en cualquier equipo de cómputo y/ o de red.

3. Todo software de comunicación a Internet ajeno a la institución se considerará fuera de norma y al responsable de su instalación se le aplicarán las medidas disciplinarias correspondientes.

4. Los recursos de cómputo no pueden ser usados directa o indirectamente por visitas ni para fines personales, a excepción de aquellas que así lo requieran y que hayan previamente solicitado el permiso a los encargados.

5. Es deber del usuario, reportar cualquier problema que se detecte en el equipo para que las personas encargadas, den solución inmediata.

5.15.Políticas de elaboración de respaldos y planes de contingencia

1. Es responsabilidad del Administrador del área cumplir con la política de respaldos de información establecida en este apartado.

2. Los procedimientos y frecuencia de respaldo de información o aplicaciones deberán

considerar la cantidad, clasificación e importancia de la información a respaldar.

3. Para mayor seguridad los respaldos se conservarán en dos lugares: un área dentro de las instalaciones del plantel y otra en una ubicación externa al plantel.

4. Cada área deberá contar con una bitácora para el registro y control de respaldos, la cual deberá contener los siguientes datos: fecha y contenido del respaldo, nombre y firma de quien lo elaboró, visto bueno de su inmediato superior.

5. Cuando se vaya a realizar un servicio de mantenimiento a los equipos, deberá generarse el respaldo correspondiente, si el mantenimiento es de tipo preventivo o correctivo deberá hacerse con la anticipación necesaria.

6. Mantener vigentes, con respecto a las normas y leyes, los planes de contingencia en caso de cualquier catástrofe.

7. Tanto los edificios como las instalaciones deben estar debidamente protegidas contra cualquier tipo de catástrofe.

8. Difundir de manera obligatoria y por escrito los planes de contingencia a todos los empleados.

9. Realizar simulacros

5.16.Políticas de sanciones

1. Cualquier acción detectada que vaya en contra de estas políticas será sancionada en base al criterio de una comisión conformada por el Coordinador de Cómputo y un Técnico Académico para solucionar el caso.

2. Cualquier violación a las políticas y normas de seguridad deberá ser sancionada de acuerdo al reglamento vigente del Centro de Cómputo.

3. Las sanciones pueden ser desde una llamada de atención o informar al usuario hasta la suspensión del servicio dependiendo de la gravedad de la falta y de la malicia o perversidad que ésta manifiesta.

4. Corresponderá al Centro de Cómputo hacer las propuestas finales sobre las sanciones a quienes violen las disposiciones en materia de seguridad informática de la institución.

5. Todas las acciones en las que se comprometa la seguridad de la Red y que no estén previstas en esta política, deberán ser revisadas por la Coordinación de Cómputo y el personal de Cómputo para dictar una medida sujetándose al estado de derecho.

5.17.Políticas de supervisión y evaluación

1. Cada uno de los departamentos de la Institución donde esté en riesgo la seguridad en la operación, servicio y funcionalidad del departamento, deberá emitir las normas y los procedimientos que correspondan.

2. Las auditorías de cada actividad donde se involucren aspectos de seguridad lógica y física deberán realizarse periódicamente y deberá sujetarse al calendario que establezca el departamento de Cómputo del plantel y/o el grupo especializado de seguridad.

3. Para efectos de que la institución disponga de una red con alto grado de confiabilidad, será necesario que se realice un monitoreo constante sobre todos y cada uno de los servicios que las tecnologías de la Internet e Intranet disponen.

4. Los sistemas considerados críticos, deberán estar bajo monitoreo permanente.

5.18.Políticas de seguimiento y control

1. Esta política de seguridad deberá seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes: crecimiento de la planta de personal, cambio en la infraestructura computacional, desarrollo de nuevos servicios, entre otros.

2. El documento que contiene la política de seguridad deber ser difundido a todo el personal involucrado en la definición de estas políticas.

La presente Política de Seguridad Informática constituye un documento normativo y de consulta, los administradores de área o jefes de los departamentos involucrados son responsables de su difusión entre el personal bajo su cargo, por lo que formará parte de los instrumentos permanentes de trabajo de dichas áreas.

La Coordinación de cómputo del plantel y las personas designadas por ésta, son responsables de las actualizaciones a esta política, requeridas por modificaciones al los sistemas, equipos o la red del plantel. La dirección del plantel y la Coordinación de Cómputo son las áreas depositarias de ésta Política y queda bajo su responsabilidad la guarda y custodia de la misma, así como el control de eventuales actualizaciones.

Así mismo, las áreas usuarias son co-responsables del contenido de este documento y, por tanto, cuando en el transcurso de la operación, identifiquen aspectos que requieran modificaciones, éstas deberán hacerse del conocimiento de la Coordinación de Cómputo del plantel para que se proceda a su actualización.

CONCLUSIONES

El objetivo de la tesis se cumplió, ya que gracias estudio de las medidas de seguridad que tiene la Escuela Nacional Preparatoria plantel 5 “José Vasconcelos”, se detectaron muchas deficiencias y por consecuencia los puntos más vulnerables y los riesgos de las tres áreas del Objeto de Evaluación, y puesto que son amenazas para el sistema de información de la institución se logró el diseño de Políticas de Seguridad Informática para mitigar, y en algunos casos eliminar, posibles daños en los bienes informáticos de la institución.

Gracias a la implantación de estas Políticas de Seguridad se podrá mitigar el impacto en los bienes del la institución para que sea lo mas bajo posible y en caso de sufrir algún ataque, la institución este prevenida con un plan de recuperación que garantice la integridad, confidencialidad y la disponibilidad de la información.

Sabemos y estamos concientes de que algunas de las Políticas de Seguridad propuestas no se podrán llevar a cabo por cuestiones políticas de la misma institución, pero sin embargo se deberán adaptar a las necesidades de la misma con la intención de no dañar al sistema y mantenerlo seguro.

Esta propuesta del SGSI ya se ha presentado a la Coordinación de Cómputo y a la Dirección del plantel, y ambas autoridades están haciendo una seria consideración para ponerla en marcha a la brevedad posible ya que se ha estado haciendo conciencia de la importancia de la seguridad de los bienes de la institución y de la falta de control que se tiene hasta el día de hoy.

Dentro del Centro de Cómputo se ha estado fomentando la cultura de la seguridad informática comenzando por el personal que labora de planta en esta área, quienes han conformado una “Comisión de Seguridad Interna” la cual tiene como objetivo realizar un estudio más profundo del estado actual de la seguridad en esta área, para así poder detectar otras posibles vulnerabilidades y proponer mas Políticas de Seguridad para controlarlas.

En la Unidad Administrativa no se han implementado las Políticas aún, sin embargo, gracias a las entrevistas que se les hicieron para la realización de este proyecto, el personal de esta área se ha dado a la tarea de realzar algunos respaldos de información y han hecho conciencia de la falta de control que se tiene en esta área.

Después de obtener las autorizaciones pertinentes se implementará y pondrá en práctica el sistema de Gestión de Seguridad de la Información y las Políticas de Seguridad propuestas en este proyecto de tesis en el objeto de evaluación; y la Coordinación de Cómputo se asegurará del cumplimiento tanto de la

política de seguridad como el uso correcto de las herramientas de seguridad que se hayan elegido para tal fin.

De igual manera se pretende que a futuro se impartan cursos de capacitación para el personal de la institución, esto con el fin de que se instruyan en el uso correcto de los sistemas de cómputo; con esto se pretende que al tener personal calificado se mitiguen los errores en los sistemas.

Este proyecto pretende inicialmente atacar las amenazas de seguridad de las tres áreas del objeto de evaluación , sin embargo, debido al profundo interés que demuestra tanto la Dirección del plantel como la Coordinación de Cómputo se pretende a largo plazo implementar este proyecto de tesis en todas y cada una de las áreas del plantel.

Y finalmente que sea posible trascender las puertas de éste plantel, elaborando una propuesta a la Dirección General de la Escuela Nacional Preparatoria para que sea implementado un Sistema de Gestión de Seguridad de la Información en cada uno de los nueve planteles bajo su Dirección, atendiendo a las necesidades particulares de cada uno de ellos.

APÉNDICE I.

HERRAMIENTAS DE SEGURIDAD

Una vez identificadas las potenciales amenazas y las vulnerabilidades existentes, resulta mucho más fácil ordenar las políticas de seguridad y los resguardos apropiados. Las organizaciones cuentan con una gran variedad de tecnologías desde paquetes de software, antivirus hasta hardware dedicado a la seguridad de la red como los IDS[1], servidores de seguridad (kerberos) o firewalls, a fin de brindar protección a todas las áreas de la red.

Al igual que un edificio, una red requiere varios niveles de protección para ser completamente segura. Una vez establecidas estas soluciones, se pueden implementar herramientas que periódicamente detecten las vulnerabilidades en la seguridad de la red y contrarresten las amenazas latentes garantizando una seguridad continua. Además, se pueden contratar consultores profesionales de seguridad de redes para que brinden asesoramiento en el diseño de la solución.

I. Paquete Antivirus

El software de protección contra virus viene con muchas computadoras y puede detener muchas amenazas de virus si se realiza una actualización periódica del mismo y su mantenimiento es óptimo.

La industria de los antivirus se basa en una amplia red de usuarios que le suministra advertencias oportunas ante la presencia de nuevos virus, de manera tal que se puedan desarrollar y distribuir los antídotos rápidamente. Debido a que todos los días se generan miles de virus nuevos, es de vital importancia que la base de datos que contiene el nombre de los virus se mantenga actualizada. El paquete de antivirus contiene una lista de los virus conocidos cuando intentan atacar. Los proveedores del software publican en sus sitios Web las últimas novedades en antídotos y el software relacionado con estos.

La política de seguridad debe estipular que todas las computadoras de la red estén actualizadas y preferentemente que todas tengan instalado el mismo paquete antivirus, por compatibilidad, y para que los costos de mantenimiento y actualización sean mínimos.

[1] Un sistema de detección de intrusos (o IDS de sus siglas en inglés *Intrusion Detection System*) es un programa usado para detectar accesos desautorizados a un computador o a una red. Estos accesos pueden ser ataques de habilidosos hackers, o de Script Kiddies que usan herramientas automáticas.

II. Certificados Digitales

Los certificados digitales, o los certificados de claves publicas, son los equivalentes electrónicos de los pasaportes o las licencias de conducir, y se emiten por autoridades certificadoras (CA) específicas.

Los certificados digitales comúnmente se usan para identificación al establecer túneles seguros por Internet.

En la ENP, así como en la UNAM entera, el sistema calificaciones se maneja con este tipo de certificados digitales.

III. PEM: Privacy Enhanced Mail

PEM es un conjunto de mecanismos que dan soporte a la criptografía, autenticación e integridad de mensajes de correo electrónico. PEM utiliza llaves públicas de algoritmos RSA[2] para autenticación, y por lo tanto necesita mecanismos para distribuir en forma confiable la llave pública a todos los participantes.

Por ejemplo, cuando el participante *A* desea obtener la llave pública de *B*, una manera de hacerlo es vía un certificado de alguien en quien *A* confíe (*CA*) y que diga: “la llave publica de *B* es *K* Firma *CA*”.

En lugar de buscar una autoridad central como el ejemplo anterior, PEM especifica una jerarquía de árbol para que el proceso de certificación sea más escalable. La autoridad PEM puede delegar su autoridad a otro *CA* que esté mas bajo en el árbol. Esto significa que *CA*, en lugar de firmar certificados para individuos, firma certificados para otro *CA*, por ejemplo *CA2*.

Asumiendo que se conoce la llave pública de *CA*, se puede aprender de manera confiable la clave pública de *CA2*.

[2] El sistema criptográfico con clave pública RSA es un algoritmo asimétrico cifrador de bloques, que utiliza una clave pública, la cual se distribuye (en forma autenticada preferentemente), y otra privada, la cual es guardada en secreto por su propietario.

Ahora si *CA2* firma un certificado para *B*, se puede confiar que se trata de la llave pública de *B*. Delegando repetidamente la autoridad es posible construir un árbol como el siguiente (ver figura 1).

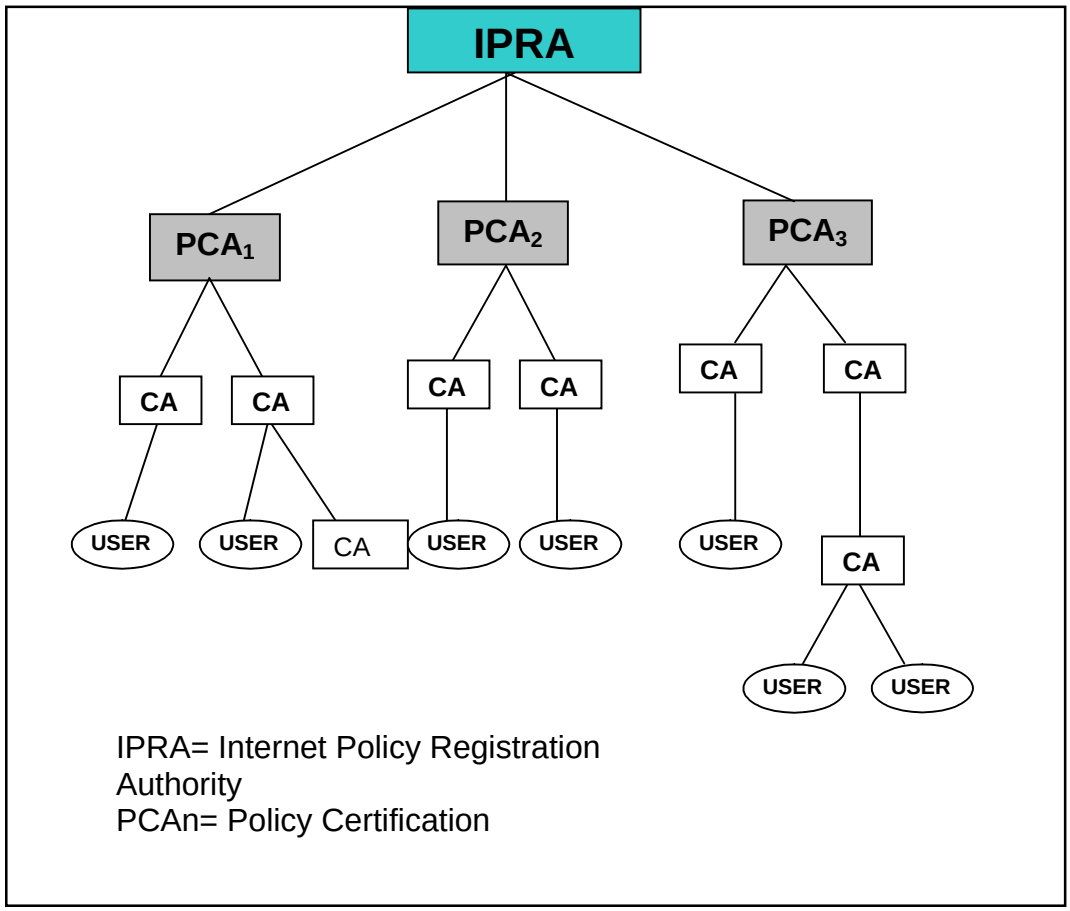


FIGURA 1

Comenzando con la llave pública de la raíz, se puede conocer la llave pública de cualquier hoja a través de un conjunto de certificados.

El problema de este tipo de delegación es la confianza de un *CA* a otro. El hecho de que *CA1* firme el certificado de *CA2* me da bastante confianza en que tengo la clave publica legítima de *CA2* (ya que confío en que *CA1* hace muy bien su trabajo), pero no me da confianza en los certificados que emite *CA2* ya que *CA2* podría ser sobornado.

¿Qué hacer ante esto?... La autoridad raíz (*IPRA*), conoce mas de cerca de cada *CA*, y no sólo su identidad, por ejemplo conoce los procedimientos que *CA* utiliza para generar certificados. La jerarquía PEM permite diferentes tipos de *CA* los cuales son certificados por diferentes autoridades (*PCA*). Cada *PCA* tiene un conjunto de políticas públicas que utiliza para delegar autoridad. Por ejemplo *PCA*1 podría tener un conjunto de políticas muy estrictas y PCA2 menos estrictas.

Para encriptar un mensaje, *A* primero debe conocer la llave pública de *B*, la cual has sido enviada a *A* vía un correo electrónico usando los certificados apropiados. Después *A* elige una llave aleatoria con la cual encripta la llave pública de *B* y se incluye en el mensaje.

La llave generada se utiliza para criptografiar el mensaje utilizando cierto algoritmo (DES[3]). Al recibir, B usa su llave privada para extraer la llave generada de la manera siguiente, (ver figura 2):

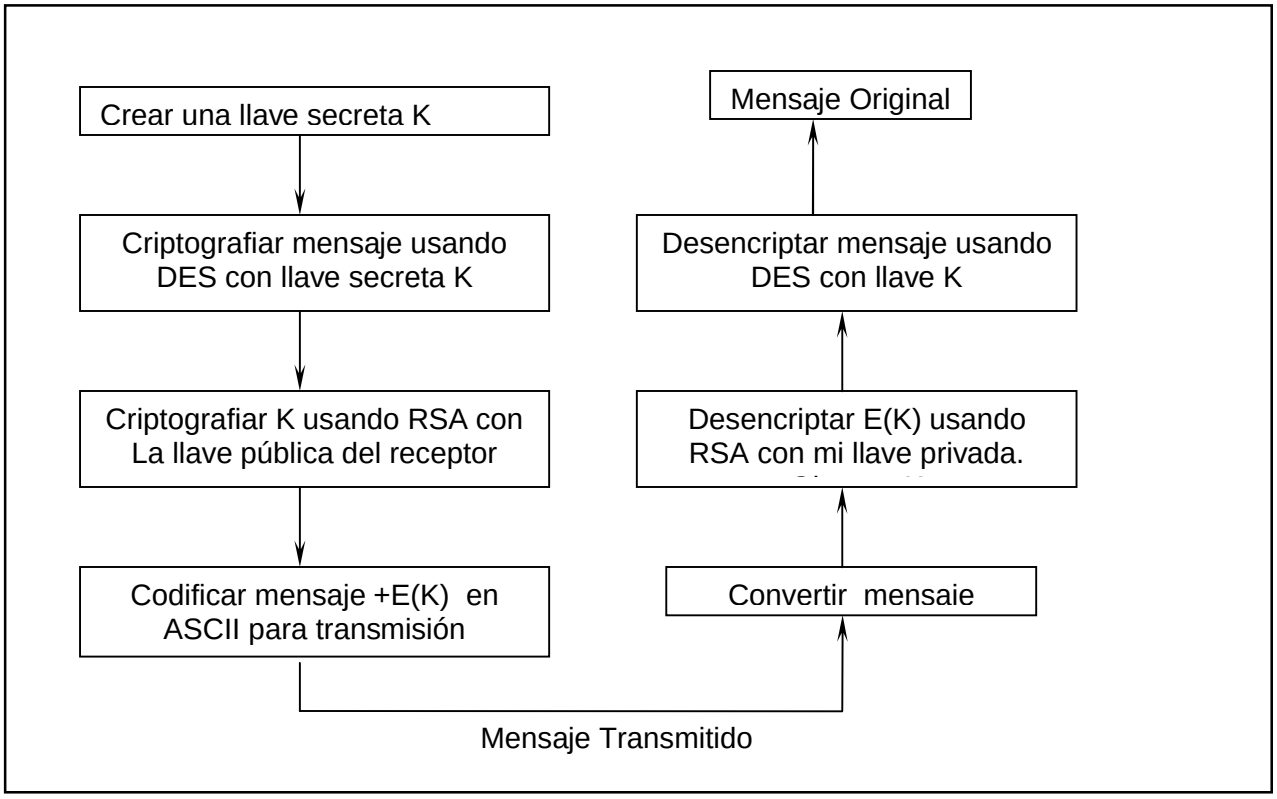


FIGURA 2

IV. PGP: Pretty Good Privacy

Cumple la misma función que PEM. Difiere en pequeños detalles; los más significativos están en la forma como se manejan los certificados: PEM utiliza una fuerza jerárquica estricta y PGP admite mallas arbitrarias de *CA*. PGP parte de la base en que cada usuario maneja sus propios criterios, es decir esta fundado a base de confianza.

[3]Data Encryption Standard (DES) es un algoritmo de cifrado, es decir, un método para cifrar información, escogido como FIPS en los Estados Unidos en 1976, y cuyo uso se ha propagado ampliamente por todo el mundo. El algoritmo fue controvertido al principio, con algunos elementos de diseño clasificados, una longitud de clave relativamente corta, y las continuas sospechas sobre la existencia de alguna puerta trasera para la National Security Agency (NSA).

Por ejemplo, si una persona *A*, que conozco muy bien me entrega personalmente su llave pública, confío en que pertenece a ella. Si *A* me da un certificado de *B* firmado por *A* puedo dudar. También puedo confiar que *A* me pueda dar certificados de personas que trabajan con ellos.

PGP reconoce que el problema de la confianza es de índole personal y entrega a los usuarios el material suficiente para que ellos tomen sus propias decisiones.

Phil Zimmerman desarrollador de PGP dice "*PGP es para personas que prefieren doblar su paracaídas ellas mismas*" . La operación es similar a PEM, pero permite que diferentes algoritmos sean usados en distintas funciones.

PGP, puede proteger de un modo fácil y seguro la privacidad de los mensajes de correo electrónico y archivos adjuntos, cifrándolos de modo que solamente los destinatarios puedan leerlos. También se pueden firmar digitalmente mensajes y archivos, asegurando su autenticidad. Un mensaje firmado verifica que la información en él no ha sido adulterada de ningún modo.

Uno de los modos más convenientes de usar PGP es a través de una de las aplicaciones de correo electrónico que soporte PGP. Con estas aplicaciones, se puede cifrar y firmar, así como descifrar y verificar mensajes, mientras se redacta y se lee el mensaje de correo.

Si no se cuenta con el servicio de correo electrónico que soporte PGP, se puede usar PGPtools para realizar las funciones PGP en archivos. También se puede usar PGP para cifrar y firmar archivos del disco duro para guardarlos en forma segura de modo que datos sensibles no puedan ser recuperados por otros.

PGP está basado en una tecnología de cifrado conocida como criptografía de clave pública, en la cual dos claves complementarias llamadas par de claves, son usadas para mantener comunicaciones seguras. De ellas, una es una clave privada a la cual solamente el propietario tiene acceso, y la otra es una clave pública que puede ser compartida libremente con otros usuarios PGP.

Para enviar a alguien un mensaje de correo electrónico privado, se usa una copia de la clave pública de esa persona para cifrar la información, la cual solamente podrá ser descifrada usando la clave privada de esa persona. PGP puede usarse para cifrar o firmar archivos que son guardados en el disco duro del equipo, para autenticar que no han sido alterados.

La clave privada puede usarse también para firmar el correo electrónico dirigido a otros o para firmar archivos para autenticarlos. Los destinatarios pueden entonces usar una copia de la clave pública de origen para asegurarse que fue realmente el generador del archivo quien envió el mensaje de correo electrónico, y que no fue alterado mientras estaba en tránsito. Cuando alguien envía un mensaje de correo electrónico con una firma digital, se tiene que generar una copia de la clave pública de la persona quien generó el mensaje para comprobar la firma digital y asegurarse que nadie haya adulterado el contenido del mensaje.

Con el programa PGP se pueden crear y administrar fácilmente las claves y acceder a todas las funciones para cifrar y firmar, así como descifrar y verificar sus mensajes de correo electrónico, archivos, y archivos adjuntos.

Antes de empezar a usar PGP, se deben generar un par de claves. El par de claves PGP está compuesto de una clave privada a la cual solamente el propietario de la misma tiene acceso, y una clave pública, la cual puede ser copiada y hacerla disponible libremente a cualquiera con quien se quiera intercambiar información.

La clave pública es un simple bloque de texto, de modo que es fácil intercambiar claves con cualquiera, ésta se puede incluir en un mensaje de correo electrónico, copiarla a un archivo, o publicarla en un servidor de claves público o corporativo donde cualquiera pueda obtener una copia cuando la necesite.

Los requerimientos de sistema para instalar PGP Versión 5.5 son:

- Windows 95 o NT
- 8 MB de RAM
- 15 MB de espacio en el disco duro

V. SISTEMAS DE DETECCIÓN DE INTRUSOS (IDS)

Una intrusión es cualquier conjunto de acciones que puede comprometer la integridad, confidencialidad o disponibilidad de una información o un recurso informático. Los intrusos pueden utilizar debilidades y brechas en la arquitectura de los sistemas y el conocimiento interno del sistema operativo para superar el proceso normal de autenticación.

Hoy día existen en el mercado una buena cantidad de productos conocidos como Sistemas de Detección de Intrusos o en inglés IDS (Intrusión Detection System).

Estos sistemas basan su funcionamiento en la recolección y análisis de información de diferentes fuentes, que luego utilizan para determinar la posible existencia de un ataque o penetración de intrusos.

En caso de que exista la suficiente certeza de la detección de un incidente, el IDS tiene como función principal alertar al administrador o personal de seguridad, para que tome acciones al respecto. Otras implementaciones más complejas son capaces de ir más allá de la notificación de un posible ataque, es decir pueden ejecutar acciones automáticas que impidan el desarrollo de éste.

Arquitectura de un IDS

Normalmente la arquitectura de un IDS está formada por:

- La fuente de recogida de datos. Estas fuentes pueden ser un log, un dispositivo de red, o el propio sistema

- Reglas que contienen los datos y patrones para detectar anomalías de seguridad en el sistema.
- Filtros que comparan los datos espiados de la red o de logs con los patrones almacenados en las reglas
- Detectores de eventos anormales en el tráfico de red.
- Dispositivo generador de informes y alarmas. En algunos casos con la sofisticación suficiente como para enviar alertas vía correo electrónico.

Clasificación de IDS

Según sus características es posible clasificar a los IDS´s en tres tipos:

- HIDS (Host IDS): proteje contra un único servidor, PC host. Monitorean gran cantidad de eventos analizando actividades con una gran precisión, determinando de esta manera qué procesos y usuarios se involucran en una determinada acción. Recaban información del sistema como archivos, recursos, etc, para su posterior análisis en busca de posibles incidencias. Todo ello en modo local, dentro del propio sistema.
- NIDS (Net IDS): Protege un sistema basado en red. Actúan sobre una red capturando y analizando paquetes de red. Luego analizan los paquetes capturados, buscando patrones que supongan algún tipo de ataque. Bien ubicados, pueden analizar grandes redes y su impacto en el tráfico suele ser pequeño. Actúan mediante la utilización de un dispositivo de red configurado en modo promiscuo (analizan o ven todos los paquetes que circulan por un segmento de red aunque estos vayan dirigidos a un determinado equipo). Analizan el tráfico de red, normalmente, en tiempo real. No sólo trabajan a nivel TCP/IP, también lo pueden hacer a nivel de aplicación.
- DNIDS (Distributed NIDS): Este tipo de IDS, más que proteger, monitoriza la actividad entre varias redes. Tiene una visión global. El carácter distribuido da al sistema la escalabilidad y adaptabilidad necesarias para que pueda ajustarse a las necesidades de rendimiento de cualquier red. Una característica deseable actualmente en los Sistemas de Detección de Intrusiones basados en Red, es que sean adaptables a distintos tipos de redes (en topología y tamaño) y que sean capaz de evolucionar con la red en la que son implantados, pudiendo adaptarse a sus necesidades crecientes .
- IDS Pasivos: Son aquellos IDS que notifican a la autoridad competente o administrador de la red mediante el sistema que sea, alerta, etc., pero no actúan sobre el ataque o atacante.

- IDS Activos: Generan algún tipo de respuesta sobre el sistema atacante o fuente de ataque como cerrar la conexión o enviar algún tipo de respuesta predefinida en nuestra configuración.

Métodos de detección

Los IDS pueden clasificarse en base a varios aspectos: método de detección, tipo de monitoreo y forma de recolección y análisis de la información.

Según el método de detección, los hay de detección de mal uso y detección de anomalías.

El modelo de detección de mal uso consiste en observar cualquier proceso que intente explotar los puntos débiles de un sistema en específico. Las diferentes acciones, que integran el mencionado proceso, comúnmente se denominan patrones o firmas del ataque.

Una ventaja de este método es que permite centralizar las labores de detección en el conjunto de firmas que posee el IDS, minimizando así, la carga de procesamiento del sistema. Muchos productos comerciales utilizan este enfoque e inclusive periódicamente proporcionan actualizaciones de éstas firmas.

En cambio, el modelo de detección de anomalías se basa en monitorear constantemente el sistema para así detectar cualquier cambio en los patrones de utilización o el comportamiento del mismo. Si algunos de los parámetros monitoreados sale de su regularidad, el sistema generará una alarma que avisará al administrador de la red sobre la detección de una anomalía.

Este tipo de detección es bastante compleja, debido a que la cuantificación de los parámetros a observar no es sencilla y a raíz de esto, se pueden presentar los siguientes inconvenientes:

- Pueden generarse falsas alarmas si el ambiente cambia repentinamente, por ejemplo, cambio en el horario de trabajo.

- Un atacante puede ir cambiando lentamente su comportamiento para así engañar al sistema.

Según el tipo de monitoreo, hay IDS´s con detección orientada al host o detección orientada a la red.

El modelo orientado al host se basa en el monitoreo y análisis de información, que refleja el estado del host donde éste reside. La mayoría de la información que este tipo de sistema recopila es obtenida a través del sistema operativo del host. Esto último causa complicaciones debido a que la información que se procesa no contiene registros del comportamiento, de bajo nivel, de la red.

Los IDS que utilizan el modelo orientado a red, fundamentan su monitoreo en información recolectada de la red. Generalmente, ésta información es capturada mediante mecanismos de "sniffing[4]".

Características deseables de un IDS

Debe ejecutarse continuamente sin intervención o supervisión de un operador humano. Ser lo suficientemente confiable, como para ejecutarse en background, pero no debe ser una caja negra, es decir, que su funcionamiento interno pueda ser examinado. Ser capaz de tolerar fallas, en el sentido de que pueda sobrevivir a una caída del sistema, sin tener que reconstruir su base de datos de conocimientos al reiniciarse. El sistema debe tener la capacidad de automonitorearse para asegurar su correcto funcionamiento.

Debe ser ligero, es decir su ejecución no debe cargar al sistema de una manera tal que le impida ejecutar otras tareas con relativa normalidad

Debe observar desviaciones del comportamiento estándar.

Debe poder adaptarse al comportamiento cambiante del sistema, es decir, si la configuración del sistema cambia, el IDS se adaptará.

Debe ser difícil de engañar.

IDS SNORT

Snort es un sniffer de paquetes y un detector de intrusos basado en red (se monitoriza todo un dominio de colisión). Es un software muy flexible que ofrece capacidades de almacenamiento de sus bitácoras tanto en archivos de texto como en bases de datos abiertas. Implementa un motor de detección de ataques y barrido de puertos que permite registrar, alertar y responder ante cualquier anomalía previamente definida. Así mismo existen herramientas de terceros para mostrar informes en tiempo real (ACID) o para convertirlo en un sistema detector y preventor de intrusos (ver figura 3).

[4] En informática, un packet sniffer es un programa de captura de las tramas de red. Generalmente se usa para gestionar la red con una finalidad docente, aunque también puede ser utilizado con fines maliciosos.

Es algo común que, por topología de red y necesidad material, el medio de transmisión (cable coaxial, UTP, fibra óptica etc.) sea compartido por varias computadoras y dispositivos de red, lo que hace posible que un ordenador capture las tramas de información no destinadas a él. Para conseguir esto el sniffer pone la tarjeta de red o NIC en un estado conocido como "modo promiscuo" en el cual en la capa de enlace de datos (ver niveles OSI) no son descartadas las tramas no destinadas a la MAC address de la tarjeta; de esta manera se puede obtener (sniffar) todo tipo de información de cualquier aparato conectado a la red como contraseñas, e-mails, conversaciones de chat o cualquier otro tipo de información personal (por lo que son muy usados por crackers, aunque también suelen ser usados para realizar comprobaciones y solucionar problemas en la red de modo legal).

Este IDS implementa un lenguaje de creación de reglas flexible, potente y sencillo. Durante su instalación ya nos provee de cientos de filtros o reglas para backdoor, DDoS, finger, FTP, ataques web, etc.

Puede funcionar como sniffer ya que podemos ver en la consola y en tiempo real qué ocurre en nuestra red y todo nuestro tráfico, el registro de paquetes ya que permite guardar en un archivo los logeos para su posterior análisis, un análisis offline o como un IDS normal, en este caso NIDS. Cuando un paquete coincide con algún patrón establecido en las reglas de configuración, se logea. Así se sabe cuando, de donde y cómo se produjo el ataque.

Aún cuando tcpdump (bitácora de SNORT) es considerada una herramienta de auditoría muy útil, no se considera un verdadero IDS puesto que no analiza ni señala paquetes por anomalías. Tcpdump imprime toda la información de paquetes a la salida en pantalla o a un archivo de registro sin ningún tipo de análisis. Un verdadero IDS analiza los paquetes, marca las transmisiones que sean potencialmente maliciosas y las almacena en un registro formateado, así, Snort utiliza la librería estándar libcap y tcpdump como registro de paquetes en el fondo.

Snort está disponible bajo licencia GPL[5], gratuito y funciona bajo plataformas Windows y UNIX/Linux. Dispone de una gran cantidad de filtros o patrones ya predefinidos, así como actualizaciones constantes ante casos de ataques, barridos o vulnerabilidades que vayan siendo detectadas a través de los distintos boletines de seguridad.

La característica más apreciada de Snort, además de su funcionalidad, es su subsistema flexible de firmas de ataques. Snort tiene una base de datos de ataques que se está actualizando constantemente y a la cual se puede añadir o actualizar a través de la Internet.

Los usuarios pueden crear firmas, basadas en las características de los nuevos ataques de red y enviarlas a la lista de correo de firmas de Snort, para que así todos los usuarios de Snort se puedan beneficiar. Esta ética de comunidad y compartir ha convertido a Snort en uno de los IDSes basados en red más populares, actualizados y robustos.

[5] General Public License o licencia pública general

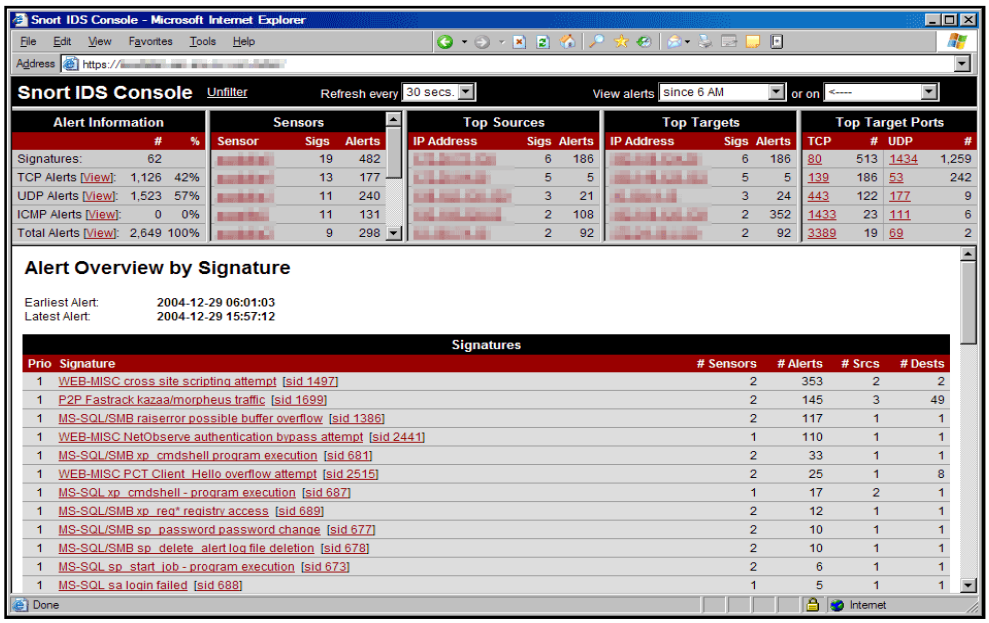


FIGURA 3 Consola Snort

VI. Secure Sockets Layer SSL

Tanto el protocolo SSL como TLS manejan la seguridad en la Capa de Transporte, sus sucesores, son los nuevos protocolos criptográficos que proporcionan comunicaciones seguras en Internet.

Secure Sockets Layer (SSL) es un protocolo estándar industrial que hace un uso sustancial de la tecnología de llave pública. SSL fue desarrollado por Netscape Communications en 1994 y incluyendo la autentificación. Netscape tomó una licencia de la tecnología criptográfica de llave pública RSA[6] y la usó para desarrollar dicho protocolo. Esta capa estándar está localizada entre TCP/IP (la capa de comunicación) y HTTP (la capa de aplicación).

El SSL es soportado por las aplicaciones de clientes populares (Netscape Navigator, Microsoft Internet Explorer), la mayoría de las aplicaciones de servidores (Netscape, Microsoft, Apache, Oracle, etc.) y Autoridades Certificadoras como VeriSign. SSL es ampliamente utilizado a través de Internet para cuestiones de seguridad.

[6] El sistema criptográfico con clave pública RSA es un algoritmo asimétrico cifrador de bloques, que utiliza una clave pública, la cual se distribuye (en forma autenticada preferentemente), y otra privada, la cual es guardada en secreto por su propietario.

En la tabla 1 se presentan los servicios fundamentales de seguridad que SSL provee, todos ellos utilizan las técnicas de llave pública:

Servicio	Tecnología Aplicada	Protección contra:
Privacidad	Encriptación	Crackers/Hackers
Integridad	Funciones Hash	Vándalos
Autenticación	Certificados X.509	Impostores

TABLA 1: SERVICIOS FUNDAMENTALES DE SEGURIDAD EN SSL

- Privacidad: Esta se alcanza a través de una combinación de la encriptación por medio de la llave pública y llave simétrica. Toda comunicación entre el servidor SSL y el cliente SSL se encripta usando una llave y un algoritmo de encriptación. La comunicación encriptada hace que sea inútil y no legible para aquellos que llegaran a capturarla.

- Integridad: Asegura que la información transmitida durante una comunicación SSL no sea modificada y llegue hasta su destino final. SSL utiliza una combinación de unas funciones matemáticas secretas compartidas llamadas funciones hash[7] para proveer el servicio de Integridad.

- Autenticación: Este es el proceso en el cual el servidor se convence de la identidad del cliente y viceversa (opcionalmente). Estas identidades son codificadas en la forma de Certificados de llave pública[8], donde los certificados son verificados por Autoridades Certificadoras confiables.

SSL implica una serie de fases básicas:

- Negociar entre las partes el algoritmo que se usará en la comunicación

- Intercambio de claves públicas y autenticación basada en certificados digitales

- Cifrado del tráfico basado en cifrado simétrico

[7] Hash se refiere a una función o método para generar claves o llaves que representen de manera casi unívoca a un documento, registro, archivo, etc., resumir o identificar un dato a través de la probabilidad, utilizando una *función hash* o *algoritmo hash*

[8] Es la pieza central de la infraestructura PKI (infraestructura de clave pública o en inglés, Public Key Infrastructure), y es la estructura de datos que enlaza la clave pública con los datos que permiten identificar al titular.

El protocolo SSL intercambia registros, cada registro puede ser comprimido, cifrado y empaquetado con un código de autentificación del mensaje (MAC). Cada registro tiene un campo de content_type que especifica el protocolo de nivel superior que se está usando.

Cuando se inicia la conexión, el nivel de registro encapsula otro protocolo, el protocolo handshake, que tiene el content_type.

El cliente envía y recibe varias estructuras handshake:

- Envía un mensaje ClientHello especificando una lista de conjunto de cifrados, métodos de compresión y la versión del protocolo SSL más alta permitida. Éste también envía bytes aleatorios que serán usados más tarde (llamados Challenger de Cliente o Reto). Además puede incluir el identificador de la sesión.

- Después, recibe un registro ServerHello, en el que el servidor elige los parámetros de conexión a partir de las opciones ofertadas con anterioridad por el cliente.

- Cuando los parámetros de la conexión son conocidos, cliente y servidor intercambian certificados (dependiendo de las claves públicas de cifrado seleccionadas). Estos certificados son actualmente X.509, pero hay también un borrador especificando el uso de certificados basados en OpenPGP.

- El servidor puede requerir un certificado al cliente, para que la conexión sea mutuamente autenticada.

- Cliente y servidor negocian una clave secreta común llamada master secret, simplemente cifrando una clave secreta con una clave pública que es descifrada con la clave privada de cada uno. Todos los datos de claves restantes son derivados a partir de este master secret (y los valores aleatorios generados en el cliente y el servidor), que son pasados a través una función pseudo aleatoria cuidadosamente elegida.

VII. Secure Shell SSH Y OPENSSH

Cuando se realiza una conexión a un servidor remoto usando por ejemplo el comando telnet o ftp, el login (usuario) y password (contraseña) son transmitidos en la red de forma clara, lo cual representa un gran riesgo si llega a existir sobre la red un programa que capture la información, basándose en el modo promiscuo de las redes ethernet (comúnmente llamado sniffer), ocasionando obtener tanto el login como el password y pudiendo posteriormente irrumpir en el servidor con esta información.

Este tipo de comunicación en claro se muestra en la siguiente ilustración (ver figura 4):

FIGURA 4t

Este tipo de problemáticas ha llevado al diseño de herramientas que permitan evitar estas situaciones siendo el caso de Secure Shell (ssh), desarrollado por Tatu Ylonen en la Universidad Tecnológica de Helsinki en Finlandia y OpenSSH, que nace del proyecto de un sistema operativo orientado con la filosofía de la seguridad en mente como lo es OpenBSD.

Secure Shell y OpenSSH permiten realizar la comunicación y transferencia de información de forma cifrada proporcionando fuerte autenticación sobre el medio inseguro. Este tipo de conexión se muestra en la ilustración siguiente (ver figura 5):

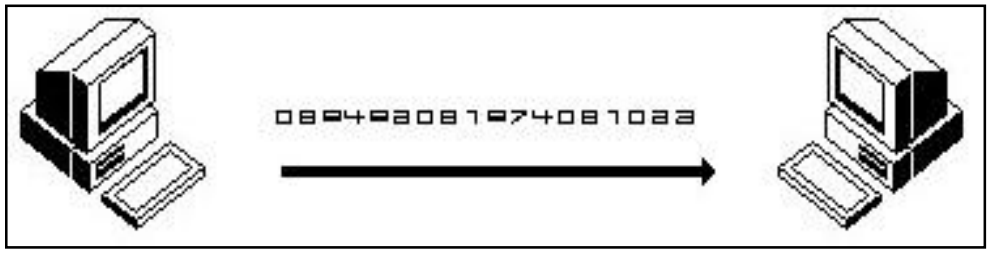


FIGURA 5

Secure Shell (ssh) es un programa que permite realizar conexiones entre máquinas a través de una red abierta de forma segura, así como ejecutar programas en una máquina remota y copiar archivos de una máquina a otra. Proporciona una exhaustiva autenticación y comunicaciones seguras en redes no seguras.

SSH provee fuerte autenticación y comunicación segura sobre un canal inseguro y nace como un reemplazo a los comandos telnet, ftp, rlogin, rsh, y rcp, los cuales proporcionan gran flexibilidad en la administración de una red, sin embargo, presenta grandes riesgos en la seguridad de un sistema. Adicionalmente, SSH provee seguridad para conexiones de servicios X Windows y envío seguro de conexiones arbitrarias TCP.

La ventaja más significativa de ssh es que no modifica mucho las rutinas. En todos los aspectos, iniciar una sesión de ssh es tan sencillo como iniciar una sesión de telnet. Tanto el intercambio de llaves, la autenticación, así como el posterior cifrado de sesiones son transparentes para los usuarios.

Debido a la promiscuidad de la interfaz ethernet, se genera una problemática sobre los siguientes servicios de red usados en la actualidad, tales como: Telnet, ftp, http, rsh, rlogin y rexec.

Ello representa un problema importante, ya que, incluso en un entorno de red cerrado, debe existir como mínimo un medio seguro para poder desplazar archivos, hacer copia de archivos, establecer permisos, etc., a través de medios seguros.

Por ello para evitar que determinadas personas capturen el trafico diario de la red, es conveniente instalar el Secure Shell (SSH). Entre los ataques más comunes que nos previenen Secure Shell están:

- Sniffering (Captura de trafico)
- IP Spoofing
- MACpoofing
- DNS Spoofing
- Telnet Hickjacking
- ARP Spoofing
- ARP Spoofing
- IP Routing Spoofing
- ICMP Spoofing

OpenSSH es una versión libre de los protocolos SSH/SecSH bajo licencia BSD y es totalmente compatible con los protocolos SSH1 y SSH2. La ultima versión de OpenSSH cliente/servidor para Unix es la 2.3.0 P1 (Liberada el 6 de Noviembre del 2000).

Debido a que OpenSSH rompe la barrera de los protocolos que ha causado confusión entre diversos sectores, esta herramienta esta siendo muy usada en la comunidad, tal es el caso de distribuciones como Linux RedHat 7.0 que ya la incluyen dentro de su sistema operativo.

Sin embargo OpenSSH ha demostrado en los últimos meses cierta inestabilidad, por lo que sí se instala dicha versión es altamente recomendable estar actualizando periódicamente el OpenSSH y estar al pendiente de vulnerabilidades presentadas.

VIII. TCP Wrappers

TCP Wrappers es una herramienta simple que sirve para monitorear y controlar el tráfico que llega por la red. Esta herramienta utilizada exitosamente en la protección de sistemas y la detección de actividades ilícitas. Fue desarrollada por

Wietze esta basada en el concepto de Wrapper; es una herramienta de seguridad libre y muy útil.

TCP Wrappers permite controlar y proteger los servicios de red, limitando el acceso como sea posible, y registrado todos para hacer el trabajo de detectar y resolver problemas de forma más fácil.

Un Wrapper es un programa para controlar el acceso a un segundo programa. El Wrapper literalmente cubre la identidad programa, obteniendo con esto un más alto nivel de seguridad.

Los Wrappers son usados dentro de la Seguridad en Sistemas UNIX. Estos programas nacieron de la necesidad de modificar comportamiento del sistema operativo sin tener que modificar su funcionamiento.

Los Wrappers son ampliamente utilizados, y han llegado a formar parte de herramientas de seguridad debido a que:

- La seguridad lógica esta concentrada en un solo programa, los Wrappers son fáciles y simples
- El programa protegido se mantiene como una entidad separada, éste puede ser actualizado cambiando el Wrapper.
- Los Wrappers llaman al programa protegido mediante la llamada al sistema estándar, un solo Wrapper puede controlar el acceso a diversos programas que se necesiten proteger.

Para explicar cómo trabaja el TCP Wrappers, primero necesitamos entender cómo funcionan los servicios de red TCP/UNIX.

Los servicios de red se basan en el modelo Cliente−Servidor. Por ejemplo, cuando alguien usa el comando telnet para servidor, el Daemon[9] del proceso telnet dentro del servidor es ejecutada actuando así, como servidor, dando al usuario permiso para poder tener acceso al sistema.

Lo más común en sistemas Server es correr un Daemon que espera cualquier solicitud de conexión a través de la red. Cuando la solicitud de conexión tiene lugar, este Daemon (Usualmente llamado inetd[10] en Unix) corre el servicio apropiado y regresa latente, en espera de otras solicitudes de conexion, como se ilustra en la figura 6:

[9] Daemon ó dæmon es un proceso de fondo

[10] Inetd es un demonio presente en la mayoría de sistemas tipo Unix, conocido como el "Super Servidor de Internet", ya que gestiona las conexiones de varios demonios. La ejecución de una única instancia de inetd reduce la carga del sistema, en comparación con lo que significaría ejecutar cada uno de los demonios que gestiona, de forma individual.

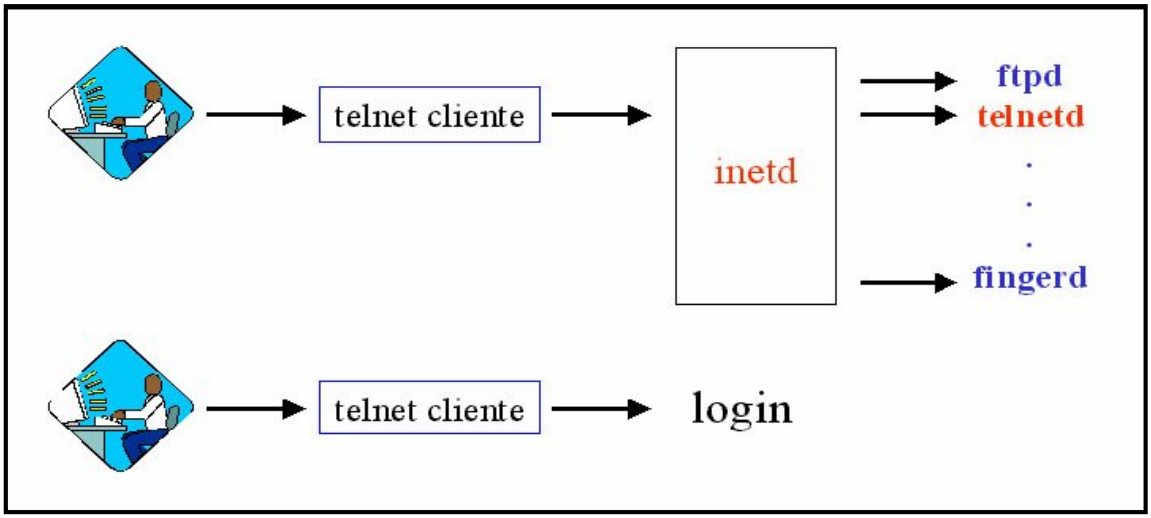


FIGURA 6

Una vez analizado el modo en que los servicios de red son inicializados en TCP/IP, veamos como lo hace TCP Wrappers:

El truco consiste en hacer un intercambio, se mueve el programa servidor de red a otro lugar, y se instala un programa servidor original de red. Siempre que una conexión tiene lugar, este programa registra el nombre del servidor remoto y servicio de red correspondiente como se ilustra en la figura 7:

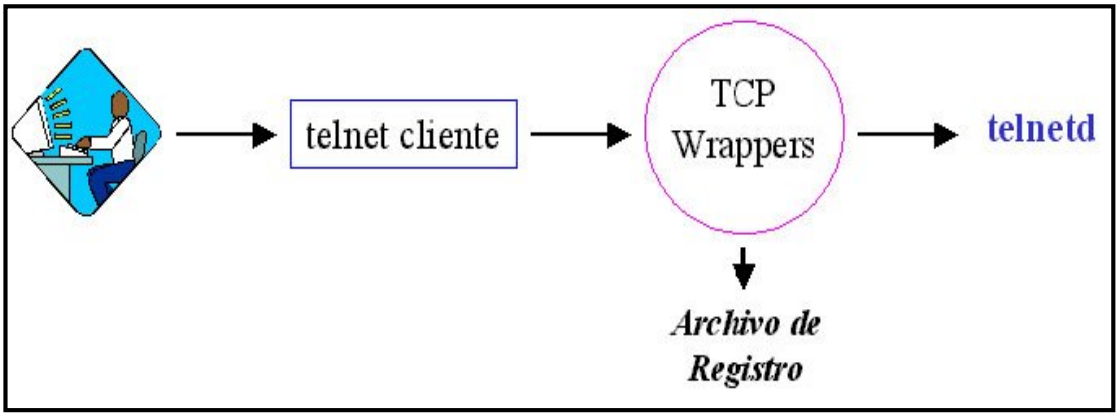


FIGURA 7

TCP−Wrappers se compone de 5 programas:

- tcpd. Es el demonio del TCP−Wrappers.
- tcpdmatch. Predice como el tcpd manejaría una petición en específico.
- tcpdchk. Verifica las reglas de control de acceso contenidas en los archivos /etc/hosts.allow y /etc/hosts.deny.

- safe−finger[11]. Versión de finger para implementar el finger reversivo.
- try−from. Programa que permite probar si el sistema es capaz de reconocer qué máquina la esta contactando.

Existen muchos lugares de donde obtener esta herramienta, pero los más conocidos son los siguientes:

ftp://ftp.asc.unam.mx/pub/tools/tcp−wrappers.tar.gz

ftp://ftp.win.tue.nl/pub/security/tcp_wrappers_7.6.tar.gz

ftp://ftp.cert.org.pub/tools/tcp_wrappers/tcp_wrappers_7.6.tar.gz

ftp://coast.cs.purdue.edu/pub/tools/unix/tcp_wrappers/tcp_wrappers_7.6.tar.gz

IX. SNIFFERS

Un sniffer es un programa de captura de tramas en una red. Generalmente se usa para gestionar la red con una finalidad de detectar accesos no autorizados, aunque también puede ser utilizado con fines maliciosos.

Es algo común que, por topología de red y necesidad material, el medio de transmisión (cable coaxial, UTP, fibra óptica etc.) sea compartido por varias computadoras y dispositivos de red, lo que hace posible que una computadora capture las tramas de información no destinadas a ella.

Para conseguir esto el sniffer pone la tarjeta de red en un estado conocido como "modo promiscuo[12]" en el cual en la capa de enlace de datos no son descartadas las tramas no destinadas a la MAC address de la tarjeta de red; de esta manera se puede obtener todo tipo de información de cualquier aparato conectado a la red como contraseñas, correos electrónicos, conversaciones de chat o cualquier otro tipo de información personal (por lo que son muy usados por hackers, aunque también suelen ser usados para realizar comprobaciones y solucionar problemas en la red de modo legal).

La cantidad de tramas que puede obtener un sniffer depende de la topología de red, del nodo donde esté instalado y del medio de transmisión. Por ejemplo:

- Para redes antiguas con topologías en estrella, el sniffer se podría instalar en cualquier nodo, ya que lo que hace el nodo central es retransmitir todo lo que recibe a todos los nodos. Sin embargo en las

[11]El servicio finger (puerto 79, TCP) ha sido una de las principales fuentes de problemas del sistema operativo Unix. Este protocolo proporciona información - demasiado detallada - de los usuarios de un máquina, estén o no conectados en el momento de acceder al servicio.

[12] el modo promiscuo, es aquel en el que una computadora conectada a una red compartida, tanto la basada en cable de cobre como la basada en tecnología inalámbrica, captura todo el tráfico que circula por ella. Este modo esta muy relacionado con los sniffers que se basan en este modo para realizar su tarea.

redes modernas, en las que solo lo retransmite al nodo destino, el único lugar donde se podría poner el sniffer para que capturara todas las tramas sería el nodo central.

- Para topologías en anillo, doble anillo y en bus, el sniffer se podría instalar en cualquier nodo, ya que todos tienen acceso al medio de transmisión compartido.

- Para las topologías en árbol, el nodo con acceso a más tramas sería el nodo raíz, aunque con los switches más modernos, las tramas entre niveles inferiores de un nodo viajarían directamente y no se propagarían al nodo raíz.

Es importante recordar el hecho de que los sniffers sólo tienen efecto en redes que compartan el medio de transmisión como en redes sobre cable coaxial, cables de par trenzado, o redes WiFi[13].

El uso de un switch en lugar de un hub incrementa la seguridad de la red ya que limita el uso de sniffers al dirigirse las tramas únicamente a sus correspondientes destinatarios.

Los principales usos que se le pueden dar a los sniffers son:

- Captura automática de contraseñas enviadas en claro y nombres de usuario de la red. Esta capacidad es utilizada en muchas ocasiones por hackers para atacar sistemas.

- Conversión del tráfico de red en un formato entendible por los humanos.

- Análisis de fallos para descubrir problemas en la red, tales como problemas de comunicación entre nodos.

- Medición del tráfico, mediante el cual es posible descubrir cuellos de botella en algún lugar de la red.

- Detección de intrusos, con el fin de descubrir hackers. Aunque para ello existen programas específicos llamados IDS (Intrusion Detection System, Sistema de Detección de intrusos), estos son prácticamente sniffers con funcionalidades específicas. Creación de registros de red, de modo que los hackers no puedan detectar que están siendo investigados.

Sniffer Wireshark

Existen sniffers para ethernet/LAN y algunos de ellos son (Wireshark (anteriormente conocido como Ethereal ,WinPcap).

[13] Wi-Fi (o Wi-fi, WiFi, Wifi, wifi) es un conjunto de estándares para redes inalámbricas basados en las especificaciones IEEE 802.11. Creado para ser utilizado en redes locales inalámbricas, es frecuente que en la actualidad también se utilice para acceder a Internet.

Wireshark es un analizador de red que capturará los paquetes que transitan en una red LAN y desplegara datos de éste de la manera mas detallada posible.

Se puede pensar en un analizador de paquetes de red como un dispositivo para examinar qué es lo que transita por la red dentro de un cable de red, como un electricista usa un voltímetro para gestionar que es lo que está pasando dentro de un cable eléctrico (pero a un nivel más alto, claro).

Wireshark es quizás uno de los mejores analizadores de paquetes más popular y disponibles de hoy en día (ver figura 8).

Algunos propósitos de Wireshark son:

- Los administradores de red lo usan para resolver problemas de red.
- Los ingenieros en seguridad informática lo usan para examinar comportamientos de seguridad de la red.
- La gente regular que conoce de redes lo usan para comprender un poco mas los protocolos internos de red

Al lado de estos ejemplos, Wireshark puede ser también útil en muchas otras situaciones.

Algunas de las características de Wireshark son:

- Funciona para UNIX y Windows.
- Captura los paquetes de la red en tiempo real.
- Muestra los paquetes acompañados de información muy detallada de su comportamiento en la red.
- Apertura y almacenaje de los paquetes capturados.
- Filtra paquetes bajo ciertos criterios.
- Busca paquetes bajo ciertos criterios.
- Destaca de manera gráfica los paquetes desplegados que cumplen con ciertos criterios.
- Crea estadísticas de los paquetes estudiados.

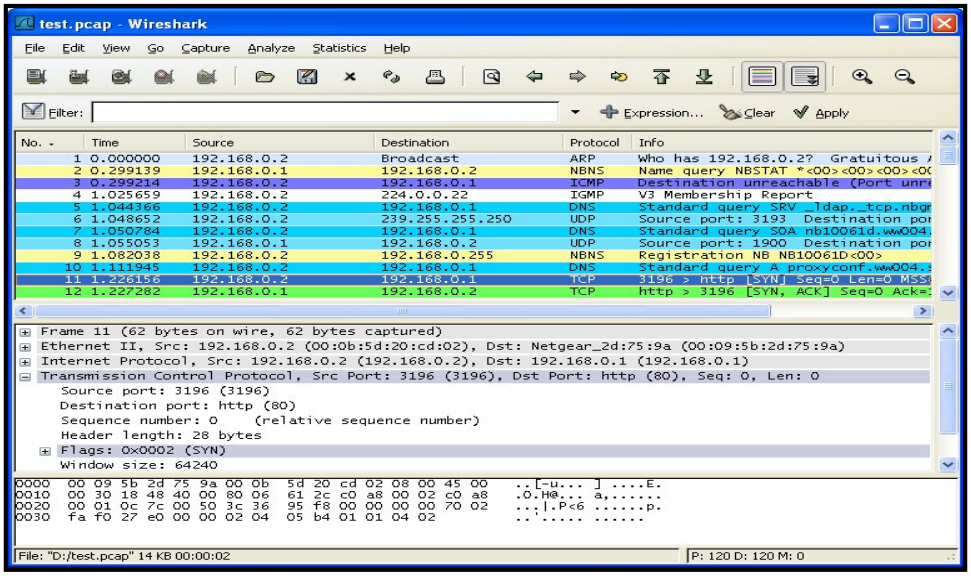


FIGURA 8 WIRESHARK CAPTURA ALGUNOS PAQUETES PARA SER EXAMINADOS.

Aquí son algunas cosas que Wireshark no proporciona:

- Wireshark no es un sistema de detección de intrusos, no advertirá cuando alguien entra a la red de manera ilícita, sin embargo, si advierte de las cosas extrañas que puedan pasar.
- Wireshark puede ayudar a deducir una intrusión.
- Wireshark no manipulará los paquetes de la red, sólo muestra información sobre ellos.

X. NMAP y PORTSENTRY

Nmap (Network Mapper) es un programa que sirve para efectuar rastreo de puertos. Se usa para evaluar la seguridad de sistemas informáticos, así como para descubrir servicios o servidores en una red informática ver figura 9).

```
notwist@notwist:~$ nmap localhost

Starting Nmap 4.20 ( http://insecure.org ) at 2007-04-02 15:50 CEST
Interesting ports on localhost (127.0.0.1):
Not shown: 1691 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
631/tcp  open  ipp
3306/tcp open  mysql

Nmap finished: 1 IP address (1 host up) scanned in 0.213 seconds
notwist@notwist:~$
```

FIGURA 5.9 NMAP MUESTRA LOS PUERTOS Y SU ESTADO DEL HOST INDICADO

Características

- Identifica computadoras en una red, por ejemplo listando aquellas que responden a los comandos ping.
- Identifica puertos abiertos en una computadora objetivo.
- Determina qué servicios está ejecutando la misma.
- Determinar qué sistema operativo y versión utiliza dicha computadora, (esta técnica es también conocida como fingerprinting).
- Obtiene algunas características del hardware de red de la máquina analizada

Nmap ha llegado a ser una de las herramientas imprescindibles para todo administrador de redes, y es usado para pruebas de penetración y tareas de seguridad informática en general.

Como muchas herramientas usadas en el campo de la seguridad informática, Nmap puede ser utilizado tanto por los administradores de sistema como por crackers o cualquier potencial intruso.

Nmap permite hacer el inventario y el mantenimiento del inventario de computadoras de una red. Se puede usar entonces para auditar la seguridad de una red, mediante la identificación de todo nuevo servidor que se conecte a esta.

Es difícilmente detectable, ha sido creado para evadir los sistemas de detección de intrusos (IDS) e interfiere lo menos posible con las operaciones normales de las redes y de las computadoras que son analizadas.

Entornos de trabajo

Nmap puede funcionar en sistemas operativos como Unix, Linux, Solaris, Mac OS X, y BSD, también en Microsoft Windows.

Como la mayoría de herramientas utilizadas en seguridad informática, Nmap puede usarse para el bien o para el mal; los administradores de redes pueden utilizarlo para verificar la presencia de posibles aplicaciones no autorizadas ejecutándose en el servidor, así como los crakers pueden usarlo para descubrir objetivos potenciales.

- Puede usarse solo o para preparar un ataque, con otra herramienta de intrusión
- Los administradores lo utilizan para buscar fallas en sus propias redes, o bien para detectar computadoras que no cumplen con los requisitos mínimos de seguridad de la organización. (Nótese que Nmap por sí solo sólo dará una indicación básica de la vulnerabilidad de una

computadora, y que normalmente es usado en conjunto con otras herramientas)

La manera más común en que un atacante va a intentar obtener información acerca de un sistema es el barrido de puertos, intenta conectarse a cada uno de los puertos que tiene abiertos un servidor, anotando qué es lo que se tiene activo y analizando dicha información.

Detectar un barrido de puertos es muy fácil muchas conexiones casi simultáneas a una gran cantidad de puertos originadas en la misma dirección. Si bien los programas barredores se han vuelto muy sofisticados y cada vez es más difícil detectarlos por diferentes estrategias que emplean, el principio básico es el mismo. Hay un excelente programa dedicado precisamente a encontrar éste patrón y tomar la acción que le indique el administrador del sistema: Portsentry, de Psionic.

Portsentry es un programa muy sencillo. Su misión es sentarse y escuchar a los puertos que le indique el administrador del servidor y que deben permanecer siempre inactivos. En caso de llegar una conexión a uno de ellos puede marcarlo en la bitácora del sistema, bloquear toda la comunicación con la dirección identificada como agresora, o correr un comando externo.

Portsentry es un programa muy portable, y podremos utilizarlo para virtualmente cualquier sistema operativo Unix. En el sitio FTP de Psionic hay un archivo llamado portsentry.COMPAT, donde detalla que los sistemas operativos compatibles con Portsentry son:

- Linux 1.x/2.x
- BSDI 2.x/3.x
- OpenBSD 2.x
- FreeBSD 3.x
- HPUX 10.20
- Solaris 2.6+
- AIX
- SCO
- Digital Unix
- NetBSD

De esta manera podemos observar que si se usa Nmap en conjunto con Portsentry ya que Nmap puede ayudarnos a escanear el estado de los puertos de una computadora y Portsentry nos dirá cuales de esos puertos son vulnerables a algún ataque y tomar medidas al respecto.

XI. TRIP WIRE

No existen los sistemas perfectos e invulnerables que desearíamos, y siempre estaremos expuestos a ataques. Más allá de todas las medidas preventivas que tomemos (firewalls, parches, políticas, etc.) siempre cabe la posibilidad de ser alcanzados por un hacker.

Los ataques exitosos a través de la red regularmente involucran la modificación parcial del sistema mediante la alteración o reemplazo de ciertos archivos, lo cual

suele ser empleado por el atacante para posteriormente tomar el control total del sistema.

Tripwire asume que todos los controles de seguridad han fallado, y que nuestro sistema a ha sido alterado; al menos, parcialmente. Sin embargo, parte del arte de los atacantes consiste en no ser descubiertos, y para esto emplean diversas técnicas relativamente sofisticadas.

Tripwire servirá para alertar al administrador de estos cambios, los cuales de otro modo podrían pasar desapercibidos por semanas o meses, a fin de tomar acciones con rapidez.

Para esto, Tripwire monitorea rutinariamente la integridad de una gran cantidad de información que tienden a ser blanco de los atacantes. Sin embargo, este proceso es pesado, y se suele ejecutar a intervalos; por ejemplo, diarios o interdiarios, aunque no hay ninguna restricción (salvo de recursos) para no lanzarlo cada media hora.

En diversas distribuciones de Linux, incluyendo RedHat 7.2 y superiores, Tripwire ya está instalado.

Tripwire utiliza dos claves (que pueden ser palabras u oraciones) para almacenar su información. Una de ellas, la "site key" o "clave del site", se emplea para encriptar los archivos de configuración y de las políticas. La otra "local key" o "clave local", se usa para encriptar la información referida al estado de los archivos del sistema que se monitorean.

Se necesitan estas dos claves para las tareas de administración de Tripwire. Estas se deben generar tan pronto como se ha instalado Tripwire.

La configuración de los archivos que van a ser monitoreados se mantiene en un gran archivo conocido como "archivo de políticas" (policy file.) Su manipulación es algo tediosa dada su extensión. Tripwire viene con un archivo que sirve de "plantilla" como base de archivo de políticas.

Cuando el archivo de políticas contiene todo lo que pretendemos monitorear, se debe instalar también, en realidad Tripwire usa una versión compilada y encriptada de este archivo.

Una vez configurado e instalado el archivo de políticas, Tripwire necesita recolectar la información actual de los archivos que debe monitorear. Dicha información se almacena en una base de datos especial.

Y que está correctamente configurado con la base de datos de políticas bien instalada, se puede comenzar a verificar la integridad del sistema de archivos propuesto cada vez que se desee saber si un sistema ha sido o no alterado.

Si por algún motivo algunos de los archivos monitoreados son modificados (por ejemplo, por una actualización en el software) entonces se debe reconstruir la

base de datos de políticas a fin de que no aparezcan discrepancias con el estado actual del sistema de archivos para las próximas verificaciones.

Si se desea dejar de monitorear ciertos archivos o iniciar el monitoreo de otros, entonces se debe configurar el archivo de políticas y reinstalarlo. Después, se volverá a generar la base de datos del sistema de archivos para su posterior monitoreo.

Ya que se ha probado la correcta ejecución de Tripwire, se debe programar su ejecución automática. Se aconseja una frecuencia diaria, aunque el administrador es libre de usar otro esquema. En RedHat 7.1, la ejecución diaria de Tripwire se efectúa fácilmente creando un archivo en el directorio /etc/cron.daily (por ejemplo, /etc/cron.daily/tripwire con el siguiente contenido:

/usr/sbin/tripwire -m c | mail root@localhost

Donde se deberá modificar la dirección "root@localhost" por lo el correo electrónico al que serán notificados los resultados del escaneo de Tripwire.

XII. HONEY POTS

Honeypot es el software o conjunto de computadoras cuya intención es atraer a crackers o spammers, simulando ser sistemas vulnerables o débiles a los ataques. Es una herramienta de seguridad informática utilizada para recoger información sobre los atacantes y sus técnicas.

Los Honeypots pueden distraer a los atacantes de las máquinas más importantes del sistema, y advertir rápidamente al administrador del sistema de un ataque, además de permitir un examen en profundidad del atacante, durante y después del ataque.

Algunos honeypots son programas que se limitan a simular sistemas operativos no existentes en la realidad y se les conoce como honeypots de baja interacción y son usados fundamentalmente como medida de seguridad. Otros sin embargo trabajan sobre sistemas operativos reales y son capaces de reunir mucha más información; sus fines suelen ser de investigación y se los conoce como honeypots de alta interacción.

Un tipo especial de honeypot de baja interacción son los sticky honeypots (honeypots pegajosos) cuya misión fundamental es la de reducir la velocidad de los ataques automatizados y los rastreos.

En el grupo de los honeypot de alta interacción nos encontramos también con los honeynet, los cuales son un tipo especial de honeypots de alta interacción que actúan sobre una red entera, diseñada para ser atacada y recobrar así mucha más información sobre posibles atacantes. Se usan equipos reales con sistemas operativos reales y corriendo aplicaciones reales.

Este tipo de honeypots se usan principalmente para la investigación de nuevas técnicas de ataque y para comprobar el modus-operandi de los intrusos.

También se llama honeypot a un website o sala de chat, que se ha creado para descubrir a otro tipo de usuarios con intenciones criminales, (e.j., pedofilia).

Los Honeypots son un concepto increíblemente simple, los cuales ofrecen una fortaleza muy poderosa. Podemos observar sus ventajas en los siguientes puntos:

- Nuevas Herramientas y Tácticas: Son diseñadas para capturar cualquier cosa que interactúa con ellos, incluyendo herramientas o tácticas nunca vistas mejor conocidas como 'zero-days'.

- Mínimos Recursos: Esto significa que los recursos pueden ser mínimos y aún así se puede implementar una plataforma lo suficientemente potente para operar a gran escala. Ejemplo: Una computadora con un procesador Pentium con 128 Mb de RAM puede manejar fácilmente una red de clase B entera.

- Información: Pueden recopilar información de manera detallada a diferencia de otras herramientas de análisis de incidentes de seguridad.

- Simplicidad: Debido a su arquitectura, son conceptualmente simples. No existe razón por la cual se deba desarrollar o mantener nuevos algoritmos, tablas o firmas. Mientras mas simple sea la tecnología, habrá menos posibilidades de error.

Cuando son utilizados con propósitos productivos, los honeypots proveen protección mediante prevención, detección y respuesta a un ataque. Cuando son utilizados con propósitos de investigación, éstos recolectan información que depende del contexto bajo el cual hayan sido implementados. Algunas organizaciones estudian la tendencia de las actividades intrusivas, mientras otras están interesadas en la predicción y prevención anticipada.

Los Honeypots pueden ayudar a prevenir ataques en varias formas:

- Defensa contra ataques automatizados: Estos ataques son basados en herramientas que aleatoriamente rastrean redes enteras buscando sistemas vulnerables. Si un sistema vulnerable es encontrado, estas herramientas automatizadas atacaran y tomaran el sistema. Uno de las métodos para proteger de tales ataques es bajando la velocidad de su rastreo para después detenerlos. Los “Sticky Honeypots”, monitorean el espacio IP no utilizado. Cuando los sistemas son analizados, estos Honeypots interactúan con el y disminuyen la velocidad del ataque. Esto se logra poniendo al atacante en un estado de espera continua.

- Protección contra intrusos humanos: Este concepto se conoce como engaño o disuasión. La idea es confundir al atacante y hacerle perder tiempo y recursos mientras interactúa con el Honeypot. Mientras ese

proceso se lleva a cabo, se puede detectar la actividad del atacante y se tiene tiempo para reaccionar y detenerlo.

- Métodos de Detección Precisa: Los Honeypots son excelentes en el ramo de la detección, solventando muchos de los problemas de la detección clásica: Reducen las falsas alarmas, capturan pequeñas cantidades de datos de gran importancia como ataques desconocidos y nuevos métodos de explotación de vulnerabilidades (zero-days) y trabajan en forma encriptada o en entornos IPv6.

- Labor Ciber-Forense: Los Honeypots son excelentes herramientas de análisis de incidencias que pueden rápida y fácilmente ser sacados de la red para un análisis forense completo, sin causar impacto en las operaciones empresariales diarias. La única actividad que guardan los Honeypots son las relacionadas con el atacante, ya que no son utilizadas por ningún otro usuario, excepto los atacantes. La importancia de los Honeypots, es la rápida entrega de la información, analizada en profundidad previamente, para responder rápida y eficientemente a un incidente.

XIII. KERBEROS

El protocolo kerberos basa toda su tecnología en un servidor central que conoce las contraseñas y las almacena (servidor kerberos) por este hecho es de vital importancia que el servidor Kerberos sea seguro de manera física y lógica.

Hay un usuario autorizado (administrador), un usuario autenticado.

La función principal del servidor kerberos es responder solicitudes y entregar tickets o pases de acceso a los diferentes usuarios, lo que les permitirá tener acceso a la red de manera autenticada.

Las principales características de Kerberos son:

- Provee un servidor de autenticación centralizado, cuya función es autenticar usuarios frente a servidores y al revés servidores frente a usuarios.

- Usa cifrado simétrico.

- Su objetivo principal es la autenticación pero también puede utilizarse para mantener la integridad y el carácter confidencial de los datos.

- Las claves y contraseñas no se transmiten por la red ni se almacenan mucho tiempo en la máquina.

- Se usan timestamps para detectar la retransmisión maliciosa de los mensajes.

- Las claves de autentificación tienen asociados plazos de expiración para dificultar los ataques contra la seguridad.

- Permite operaciones entre dominios (realms) en las que un cliente se autentifica ante el servidor de un dominio remoto. Los servidores de autentificación de ambos dominios comparten claves para validar la operación.

- Una vez que un cliente está autenticado o bien se asume que todos sus mensajes son fiables, o si se desea mayor seguridad se puede elegir trabajar con mensajes seguros (autenticados) o privados (autenticados y cifrados).

Además de todo lo anterior cabe anotar que toda la responsabilidad recae sobre la máquina del cliente en el manejo del Ticket, para poder acceder a todos los sistemas. Esto en otras palabras hace que solo se deba autenticar a un usuario frente al servidor Kerberos una única vez y logra autenticación frente a los demás servidores en su entorno de manera automática.

Un servidor Kerberos se denomina KDC (Kerberos Distribution Center), y provee de dos servicios fundamentales: el de autenticación (AS, Authentication Service) y el de tickets (TGS, Ticket Granting Service).

La arquitectura de Kerberos está basada en tres objetos de seguridad: Clave de Sesión, Ticket y Autenticador.

- La clave de sesión es una clave secreta generada por Kerberos y expedida a un cliente para ser usado con un servidor durante una sesión; no es obligatorio utilizarla en toda la comunicación con el servidor, sólo si el servidor lo requiere (porque los datos son confidenciales) o si el servidor tiene como uso principal ser un servidor de autenticación.

- El ticket es un testigo expedido a un cliente del servicio de tickets de Kerberos para solicitar los servicios de un servidor; garantiza que el cliente ha sido autenticado recientemente.

- Este ticket incluye el nombre del cliente, para evitar su posible uso por impostores, un periodo de validez y una clave de sesión asociada para uso de cliente y servidor.

Funcionamiento de Kerberos (ver figra 10)

1. La estación envía la información de login / password al servidor.

2. El servidor por si mismo descifra la contraseña por usuario, si el usuario existe utiliza la clave para descifrar el mensaje, que a su vez es usado para garantizar que el sistema se encuentra inscrito en la red.

3. Una vez que el servidor logra descifrar el mensaje crea un Ticket el cual es cifrado con la contraseña del usuario y se envía de regreso a la máquina del usuario, la que almacena la información en este Ticket en memoria no en disco duro.

4. Una vez en posesión del Ticket, el usuario puede autenticarse frente a cualquier máquina que pertenezca al entorno del servidor Kerberos, incluyendo máquinas que pertenezcan a otros dominios dentro de la organización.

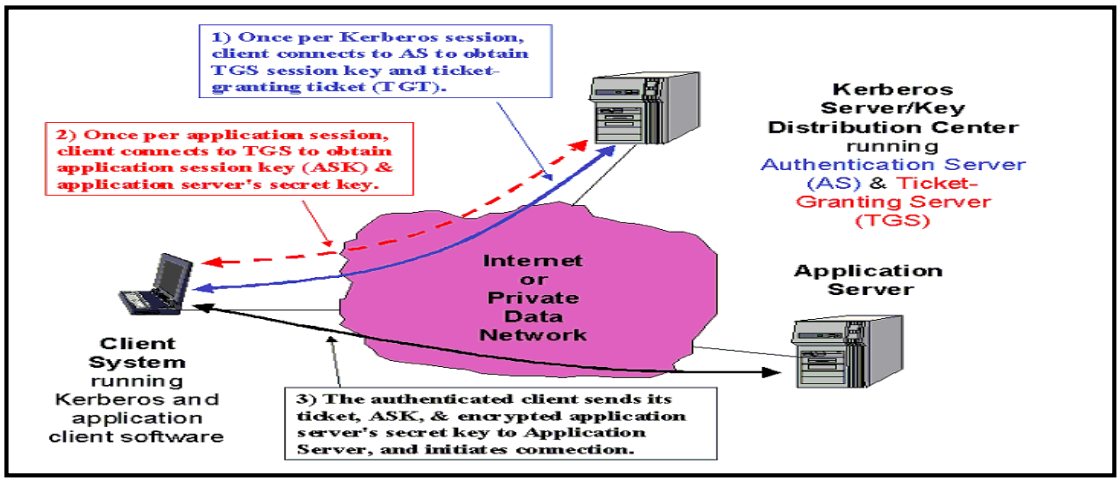


FIGURA 5.10 FUNCIONAMIENTO LOGEO Y OBTENCIÓN CON UN SERVIDOR KERBEROS

LOGIN

Inicialmente el cliente, a través de un programa denominado login, necesita obtener las credenciales necesarias para acceder a otros servicios. Para ello cuando un usuario se conecta a un sistema Unix `kerberizado' teclea su nombre de usuario, de la misma forma que en un sistema habitual; entonces el programa login envía el nombre de usuario al servidor de autenticación (AS) de Kerberos para solicitar un ticket que le permita comunicarse posteriormente con el servidor de tickets (TGS).

Si el usuario es conocido, el servidor de autenticación AS le regresa al cliente un mensaje que contiene una clave para la comunicación con TGS cifrada con la clave secreta del cliente, así como un ticket para la comunicación con TGS cifrado con la clave secreta de este servidor.

El programa de login intentará descifrar la clave que el usuario proporciona, y si ésta es correcta podrá obtener los elementos mencionados y sólo este cliente podrá descifrar el mensaje con su clave secreta (en este caso el password). Una vez obtenida, la clave para comunicar al cliente con el servidor de tickets TGS, el programa passwd la guarda para una posterior comunicación con este servidor y borra la clave del usuario de su memoria, ya que el ticket será suficiente para

establecer la comunicación; este modelo consigue que el password nunca viaje por la red.

OBTENCIÓN DE TICKETS

El cliente ya posee una clave de sesión para comunicarse con el servidor de tickets TGS y el ticket necesario para hacerlo, cifrado con la clave secreta de este servidor (el cliente no puede descifrar este ticket). Cuando el cliente necesita acceder a un determinado servicio es necesario que disponga de un ticket para hacerlo, por lo que lo solicita al TGS enviándole un autenticador que el propio cliente genera, el ticket (*T*) y el nombre del servicio al que desea acceder en el servidor de aplicación (*S*) y un indicador de tiempo.

Cuando TGS recibe el ticket comprueba su validez y si todo es correcto retorna un mensaje que contiene una clave para comunicación con *S* cifrado con la clave de sesión del par *CT*, junto a un ticket para que el cliente *C* y el servidor *S* se puedan comunicar de manera cifrada con la clave secreta del servidor.

PETICION DE SERVICIO

Tras obtener el ticket para comunicarse con *S* el cliente ya está preparado para solicitar el servicio; para ello presenta la credencial autenticada ante el servidor final, que es quien va a prestar el servicio. El cliente se comporta de la misma forma que cuando solicitó un ticket a *T*: envía a *S* el autenticador recién generado, el ticket y una petición que puede ir cifrada si el servidor lo requiere, aunque no es necesario.

El servidor envía entonces al cliente la prueba de actualidad cifrada con la clave secreta de la sesión.

PROBLEMAS CON KERBEROS

- Cualquier aplicación que lo utilice ha de ser modificada para poder funcionar correctamente, siguiendo un proceso denominado “kerberización”.
- La seguridad es la gran centralización que presenta el sistema. Debido a que mantiene la base de datos de claves en un servidor.
- La presencia de Kerberos implica cierto mantenimiento. El administrador debe inicializar la base de datos de Kerberos al instalarlo. En caso de tener la base de datos replicada, será necesario administrarlas para que se mantengan consistentes.
- Esto implica tener que sincronizar las bases de datos replicadas con la base de datos principal cada cierto tiempo

- Se debe tener especial cuidado con la administración de las máquinas que tienen la base de datos Kerberos.
- El sistema podría volverse inseguro si alguien obtiene el control de alguna de estas máquinas.
- El administrador también debe asegurarse de que la fecha y hora de todas máquinas del sistema estén medianamente sincronizadas.
- Si el usuario escoge una contraseña pobre, un atacante que la consiga tratando de adivinarla puede hacerse pasar por él.
- No hay un lugar seguro donde guardar las claves de sesión. De hecho, el lugar donde se guardan puede ser accedido por el root. Así es que un intruso que logre crackear el mecanismo de protección de la computadora local podrá robar las claves de sesión.

XIV. PARCHES

Los parches de seguridad son actualizaciones que se ponen a disposición de los usuarios, y que tienen como función actualizar los programas, solucionar problemas conocidos y/o mejorar la seguridad del software.

Es importante estar al día en cuanto a instalación de estos parches, ya que muchos de los gusanos y troyanos que existen actualmente en Internet utilizan la vulnerabilidad de los programas para hacer daño a los usuarios. Sobretodo hablando del sistema operativo de Windows (95,98,NT,2000 o XP) o del software de correo electrónico Outlook.

La instalación y descarga de estos service packs no tienen costo, solo es necesario ser usuario de Microsoft para descargar estas opciones sin costo alguno. Para lo cual deberá utilizar la página Web de Microsoft http:///microsoft.com y buscar aquella actualización que le haga falta. Recuerde visitar estas páginas con frecuencia, ya que siempre encontrara actualizaciones importantes para su sistema.

Utilice Windows Update para elegir actualizaciones para el sistema operativo que este utilizando. Asimismo si usted actualizó el sistema operativo de su máquina, en la pagina del fabricante de su PC podrá encontrar actualizaciones para instalar correctamente el hardware de su maquina (tarjeta de sonido, módem, teclado, monitor, etc). Se recomienda siempre visitar las paginas tanto del fabricante de su computadora como del software que esta utilizando, ya que en Internet encontrara las ultimas mejoras para que su computadora funcione de la mejor manera posible y lo mas seguro que se pueda.

XV. FIREWALLS

Un firewall es una solución de software o hardware implementada en la infraestructura de red para imponer las políticas de seguridad de una organización mediante el acceso restringido a recursos de red específicos. Un firewall es el equivalente a la cerradura en la puerta exterior de un edificio, o en la puerta de una sala dentro del edificio, ya que sólo los usuarios autorizados puedan entrar. La tecnología de un firewall también está disponible en versiones adecuadas para el uso doméstico.

El firewall crea una capa protectora entre la red y el mundo exterior. De hecho, el firewall copia la red en el puerto de entrada para que pueda recibir y transmitir datos autorizados sin una demora prolongada. No obstante, contiene filtros integrados que pueden impedir el acceso al sistema real de material potencialmente peligroso, o no autorizado. También registra una intrusión frustrada y la reporta a los administradores de red.

El propósito general de un firewall es evitar los accesos no autorizados de redes y proporcionar un único punto de defensa con acceso controlado y auditado a los servicios, desde dentro y fuera de la red privada de una organización. Un firewall basa su funcionamiento en el examen de los paquetes IP que viajan entre el servidor y un cliente.

Las siguientes capacidades caen dentro de los alcances de un firewall

- Define un único punto de entrada y salida que deja fuera de la red protegida a los usuarios no autorizados, prohíbe que los servicios no confiables entren o salgan de la red y proporcionan protección de varios tipos de spoofing y ataques de ruteo.
- Proporciona una ubicación para monitorear los eventos relacionados a seguridad. Auditorias y alarmas se pueden implementar en un firewall.
- Es una plataforma conveniente para varias funciones de Internet no relacionadas a seguridad. Estas incluyen la traducción de direcciones de red, la cual mapea direcciones locales a direcciones de Internet y la administración de red que audita o registra el uso de Internet.

Existen cuatro técnicas que usan los firewalls para controlar el acceso y lograr implementar la política de seguridad de la organización. Inicialmente los firewalls tenían como objetivo principal el control de servicio pero han evolucionado para proporcionar las siguientes técnicas:

- Control de Servicio: Determina los tipos de servicios de Internet que pueden accederse hacia adentro o hacia fuera. El firewall puede filtrar tráfico basándose en la dirección IP y en el número del puerto TCP.

- Control de Detección: Determina la dirección en la cual los servicios pueden iniciarse y se les permite fluir a través del firewall.
- Control de Usuarios: Controla el acceso a los servicios de acuerdo al usuario que intenta el acceso. Este control se aplica a los usuarios internos que se encuentran dentro del perímetro de seguridad.
- Control de conducta: Controla como se utilizan los servicios de red. Por ejemplo, se puede filtrar correo electrónico para eliminar spam, o puede habilitar acceso externo a solo una parte de la información en el servidor web local.

APÉNDICE II.
REGLAMENTO DEL CENTRO DE CÓMPUTO DE LA ENP No.5 "JOSÉ VASCONCELOS"

ÍNDICE

CAPÍTULO X

DE LA SUSPENSIÓN DE SERVICIO Y LAS SANCIONES
REFERENCIAS DOCUMENTALES Y CONSULTAS EN INETERNET

ANEXOS

CAPÍTULO I
DEL OBJETIVO Y PROPÓSITO DEL REGLAMENTO DEL CENTRO DE CÓMPUTO

Artículo 1. Del Propósito del Reglamento

Los siguientes lineamientos tienen como finalidad hacer del conocimiento a los usuarios del centro de cómputo los derechos y las obligaciones que adquieren con el uso de las instalaciones.

El siguiente reglamento se redacta con el propósito de establecer los objetivos, funciones, actividades, estructura y operación de los Laboratorios del Centro de Cómputo de la ENP No. 5 “José Vasconcelos” de la UNAM.

Artículo 2. Del Objetivo del reglamento

Dar a conocer a los usuarios los derechos, las responsabilidades y obligaciones que adquieren con el uso de los servicios del centro de cómputo.

CAPÍTULO II
DE LAS DEFINICIONES DEL CENTRO DE CÓMPUTO

Para los efectos del presente reglamento se entiende por:

Artículo 3. Centro de cómputo:

A la estructura académico-administrativa creada por la ENP No. 5 teniendo como objetivo general proporcionar los servicios de cómputo dentro y fuera de sus instalaciones.

Teniendo como objetivo desarrollar la cultura informática en el estudiante y docente de la ENP No 5 para el ejercicio más competitivo en los diferentes ámbitos de la materia, así como ampliar el acervo académico y científico de los estudiantes y académicos mediante el uso de equipo de cómputo.

Ofreciendo de manera prioritaria a profesores y alumnos las instalaciones necesarias para la realización del aspecto práctico de las asignaturas de Informática e

Informática Aplicada a la Ciencia y a la Industria las cuales son asignaturas teórica-prácticas contempladas oficialmente como curriculares en el plan de estudios y reflejan créditos; buscando favorecer que los anteriores aprovechen estos espacios para fortalecer su trabajo docente y académico, respectivamente; así como tener el contacto con las nuevas tecnologías de computación.

El Centro de Cómputo cuenta con:

- Cuatro laboratorios orientados a la realización de prácticas de las asignaturas de Informática e Informática Aplicada a la Ciencia y a la Industria, estas son las establecidas formalmente como curriculares en el programa de estudios de 4to. y 6to. Año respectivamente y cuentan con créditos en el historial académico de los alumnos. Estos son nombrados como: salón 3, salón 4, salón 5 y salón 6.

- Un laboratorio con servicio de red conocido como salón 2 orientado a la impartición del desarrollo de clases prácticas de las asignaturas antes mencionadas y al préstamo de equipo a alumnos en horarios específicamente asignados.

- Un laboratorio con servicio de red conocido como salón 1 orientado exclusivamente al préstamo de equipo a la planta docente, la realización de actividades vinculadas con el colegio, eventos institucionales, cursos de capacitación y otras actividades previamente solicitadas y aprobadas por las autoridades correspondientes.

- Una oficina asignada para la realización de diversos procesos como: control de insumes, desarrollo de proyectos y tecnologías, mantenimiento de equipo e instalaciones, validación y manejo de información así como cualquier actividad propia del área que realicen los Técnicos Académicos que laboran en el centro de computo.

Artículo 4. Equipo de cómputo:

Se considera como equipo de cómputo toda aquella computadora de escritorio, dispositivo periférico o cualquier objeto relacionado con lo descrito en este reglamento, cómputo.

Artículo 5. Uso académico:

Se considera como uso académico del equipo, a toda acción que ejerza un usuario y que este enfocada al apoyo de la elaboración, solución, investigación de tareas, proyectos o trabajos; así como el uso destinado a la preparación de material de apoyo y a la comunicación electrónica con otros usuarios relacionados directamente con asignaturas impartidas en el plantel.

Artículo 6. Coordinador de Cómputo:

El Coordinador de Cómputo es aquella persona designada por el director del Plantel para gestionar y administrar los servicios de cómputo, (figura Honoraria)

Artículo 7. Para ser coordinador de cómputo del plantel deberá ser Técnico

Académico de tiempo completo adscrito a plantel y asignado al Centro de Cómputo.

Artículo 8. Técnicos Académicos:

Son Técnicos Académicos quienes hayan demostrado tener la experiencia y las aptitudes suficientes en el área de cómputo, para realizar tareas específicas y sistemáticas de los programas académicos y/o servicios técnicos de la dependencia.

Artículo 9. Usuarios:

Son usuarios en el centro de cómputo todas aquellas personas que pertenecen a la Universidad Nacional Autónoma de México y que bajo previa autorización tienen acceso a los laboratorios y al equipo de cómputo.

Tipos de usuario

- Usuarios Internos: Son usuarios internos del centro de cómputo todas aquellas personas que, bajo previa autorización, tienen acceso al centro de cómputo y estos deben pertenecer:

    - Técnicos Académicos, asignados al centro de cómputo.
    - Profesores: Pertenecen a este rubro únicamente los profesores que imparten las asignaturas de Informática e Informática Aplicada a la Ciencia y a la Industria y Opción Técnica en Computación.
    - Alumnos: Pertenecerán a este rubro todos los alumnos inscritos en las asignaturas mencionadas anteriormente.

- Usuarios Externos: Todas aquellas personas que no estén contemplados en el rubro anterior y que soliciten de los servicios del centro de computo.

    - Profesores del plantel, quienes anticipadamente han hecho expresa petición de un laboratorio y ha cumplido con los tramites establecidos por la coordinación, para otorgar el préstamo.
    - Alumnos que no estén contemplados en la clasificación anterior.
    - Personal Administrativo y Funcionarios, que requieran de los servicios de cómputo y que pertenezcan al plantel.

- Usuarios Temporales: Todas aquellas personas que bajo previa autorización hacen usos de los laboratorios y equipo del centro de cómputo, por un periodo de tiempo

no mayor a quince días hábiles o bien en periodos de tiempo especificados. Como pueden ser: Profesores que no pertenecen a la planta docente del plantel y que por alguna causa hacen uso del equipo de cómputo. En el caso de no pertenecer a la Universidad Nacional Autónoma de México, requerirá de un permiso especial de la autoridad correspondiente con la justificación pertinente.

El Centro de Cómputo se reserva el derecho de admisión a los usuarios en condiciones extraordinarias.

Artículo 10. Servicios de Cómputo:

Se traduce en conjunto de acciones académicas, técnicas y administrativas relacionadas con el uso de equipo de cómputo mediante las cuales se apoyan los fines sustantivos del Plantel.

Artículo 11. Sanciones

Se considera como sanciones, a las acciones tomadas para resarcir el daño causado por incumplimiento del presente reglamento.

Artículo 12. Servicio Comunitario

Es una sanción impuesta a un alumno que haya incurrido en una falta al presente reglamento, y consta de proporcionar apoyo en algunas actividades en el Centro de Cómputo en un número específico de horas establecidas según sea la falta.

Artículo 13. Servicio Social y/o Prácticas Escolares

Apoyo en algunas actividades al Centro de Cómputo por parte de alumnos que estén obligados a la prestación del mismo.

CAPÍTULO III
DE LAS FUNCIONES, SERVICIOS Y ESTRUCTURA DEL CENTRO DE CÓMPUTO

Artículo 14. De las Funciones

Para el cumplimiento del objetivo del centro de cómputo se desarrollan las siguientes funciones:

- Poner a disposición de los usuarios el equipo de cómputo para el desarrollo de actividades académicas.

- Ofrecer con excelencia y eficiencia los servicios de cómputo, orientados permanentemente a satisfacer las necesidades académicas de los usuarios.

- Capacitar y/o actualizar a los alumnos y personal académico-administrativo de la Escuela Nacional Preparatoria en el área informática.

Artículo 15. De los Servicios

Para el desarrollo de las funciones se llevaran a cabo las siguientes actividades:

A. Ofrecer préstamo de los Laboratorios del Centro de Cómputo en horarios establecidos.

B. Asesorar a los usuarios en el buen uso y mejor manejo de los sistemas de cómputo.

C. Programar oportunamente las actividades de los laboratorios.

D. Mantener las instalaciones y equipos en óptimas condiciones.

E. Impartir cursos y talleres de capacitación y actualización en materia de cómputo para la planta docente y administrativa de la Escuela Nacional Preparatoria.

F. Brindar soporte y asesoría técnica a los usuarios.

G. Coordinar las acciones generales para la organización de actividades que impliquen la participación de todos los laboratorios de cómputo.

Artículo 16. De la Estructura

El Centro de Cómputo del plantel depende directamente de la coordinación de Centros de Cómputo de la Escuela Nacional Preparatoria.

En plantel, el Centro de Cómputo, se encuentra bajo la supervisión de la Dirección a través de la Secretaría General.

El responsable directo del Centro de Cómputo es el Coordinador de Cómputo. Los servicios en el centro de cómputo se desarrollarán bajo la supervisión y apoyo de los Técnicos Académicos encargadps.

CAPÍTULO IV
DE LA OPERACIÓN
DEL CENTRO DE CÓMPUTO

Artículo 17. De la Operación

Para el desarrollo de actividades, los laboratorios del centro de cómputo operan a través de:

A. El Coordinador de Cómputo, es directamente el responsable del Centro de Cómputo y podrá auxiliarse de los Técnicos Académicos, su función general es la planeación, distribución, aplicación y control de sus recursos y actividades.

B. Técnicos Académicos, personal auxiliar de la coordinación y tendrán de manera general las siguientes tareas:

- Atender solicitudes de préstamo y asignación de equipos.
- Gestionar el servicio de préstamo e impresión.
- Registrar sucesos relevantes en la bitácora del Centro de cómputo.
- Apoyar en el desarrollo de las prácticas docentes.
- Realizar las acciones de mantenimiento preventivo de software permitido y mantenimiento correctivo del mismo.
- Administrar recursos.
- Gestionar la funcionalidad del software instalado, la operatividad de la red, diagnóstico, prevención y eliminación de virus informáticos, orientación técnica a usuarios.
- Notificar de manera oportuna al Coordinador del Centro de Cómputo sobre las necesidades de mantenimiento general, solicitudes de reservaciones, cronogramas y sugerencias, así como problemas en el cumplimiento de las funciones.
- Otras.

C. Vigilantes: trabajador administrativo que tiene como función verificar, monitorear y controlar el acceso al centro de computo, la conducta general de los usuarios dentro y fuera del los salones y áreas comunes.

D. Personal de Intendencia: trabajador administrativo que tiene como función realizar y mantener la limpieza en todas y cada una de las áreas del Centro de Cómputo.

E. Servicio Social y Práctica Escolar: alumno que presta sus servicios de manera NO REMUNERADA para apoyo a las actividades del Centro de Cómputo.

Artículo 18. Del Horario de servicio

El horario de operación y servicio del Centro de Cómputo es de lunes a viernes de las 7:00 a las 21:10 horas, dentro del calendario de días hábiles para la Escuela Nacional Preparatoria.

Artículo 19. De los servicios del centro de cómputo

A. El acceso a las áreas de servicio será permitido solo en el horario y condiciones estipuladas en este reglamento.

B. Toda solicitud de servicio de cómputo deberá hacerse por medio de la entrega de la solicitud correspondiente en tiempo y forma.

C. Los servicios de cómputo dependerán de la prioridad del servicio, así como de la disponibilidad del personal y de los recursos con que se cuentan.

D. Las solicitudes de servicio en áreas fuera del Centro de Cómputo, deberán ser solicitadas en forma personal mediante una llamada telefónica o una visita del interesado al centro de cómputo; el usuario está obligado a firmar de conformidad por la recepción del servicio.

E. Después de la evaluación correspondiente, el personal del Centro de Cómputo podrá canalizar peticiones de servicio a proveedores externos mediante la petición al departamento encargado de los bienes y suministros, siempre que se considere conveniente.

F. El personal del Centro de Cómputo estará encargado de instalar únicamente los programas que sean de uso estrictamente justificado para la impartición de las materias de Informática, Informática Aplicada a la Ciencia y a la Industria y Opción Técnica en Computación, según lo establecido en el programa temático de las asignaturas.

G. La prioridad de los servicios se dará conforme a las asignaturas establecidas expresamente de forma curricular y que registren créditos para el historial académico.

H. El personal del Centro de Cómputo se reserva el derecho de desconectar equipos de la red por mal uso de este recurso.

I. A peticiones de servicio que dan pauta al mal uso del equipo con programas inseguros de música, videos o juegos, entrada repetitiva de virus a través de correo no filtrado, antivirus no actualizados o con sistemas operativos sin los parches de actualización, programas de charla en línea, etc. el personal del Centro de Cómputo está autorizado a rechazar dicha solicitud.

J. El centro de cómputo cuenta con un estructura de red con acceso a Internet, el uso de este servicio se hará con base al capítulo IX de este reglamento.

K. La solicitud de préstamo de equipo expresamente PARA AUDITORIOS se regirá sobre los mismos lineamientos para la reservación y préstamo de un laboratorio dentro del Centro de Cómputo.

L. Nota: Cualquier inconformidad en los servicios que presta el centro de cómputo dentro de sus instalaciones relacionada directamente con los colegios de Informática y Opciones Técnicas, deberá ser notificada por los coordinadores de colegio directamente al coordinador del centro de cómputo.

Artículo 20. De la orientación Técnica y préstamo de equipo

A. El usuario podrá solicitar orientación técnica a los técnicos académicos del Centro de Cómputo sobre aspectos generales del manejo de los equipos.

B. La orientación consistirá en dar respuestas a preguntas concretas.

C. El usuario debe hacer solicitud expresa para el préstamo del equipo a la persona correspondiente en tiempo y forma, este asignará un solo equipo por usuario.

D. El usuario deberá registrarse en la libreta de ingreso con las referencias siguientes: nombre, fecha, situación (alumno/profesor), número de cuenta en el caso de alumnos, paquetería a utilizar, número de equipo asignado, número de impresiones si fuera el caso, hora de entrada y hora de salida.

E. Para poder acceder como alumno al servicio de préstamo de equipo, es requisito indispensable presentar la credencial interna de plantel.

F. El usuario debe tener claro el manejo de la PC, paquetería a utilizar, y saber el manejo básico de los diferentes dispositivos periféricos del equipo de cómputo.

G. En el caso de solicitar el servicio de impresión se deberá regir por el o los artículos referentes al servicio de impresión.

Artículo 21. Del servicio de impresión

A. Para solicitar el servicio de impresión, el usuario debe tener establecido el formato final del documento y sus dispositivos de almacenamiento protegidos contra escritura.
B. Hacer solicitud expresa del servicio en tiempo y forma.

C. La autorización del servicio de impresión dependerá de que el centro de cómputo cuente con la existencia suficiente de suministros y equipo disponible.

D. El servicio de impresión se limita a 10 páginas como máximo por usuario y éste debe traer sus hojas.

E. Se considera que el usuario hace mal uso de la impresora cuando:

- no haga solicitud expresa de uso de manera previa.
- envíe impresiones con contenido no académico.
- envíe impresión de "basura" haciendo que la impresora se "bloquee" o cambie su configuración.
- modifique su configuración a través del sistema operativo o de la misma impresora.
- no utilice el tipo adecuado de papel.
- manipule los cables de impresión y/o sustraiga algún componente.
- habilite un equipo que no tiene acceso a este recurso.

F. Si el usuario se retira del área y deja trabajando la impresora, el proceso de impresión será cancelado.

G. La impresión de documento deberá ser en su mayoría, texto.

H. No se podrán realizar impresiones a color ya que no se cuenta con el equipo para este fin.

I. Solo se realizan impresiones en papel bond tamaño carta y oficio.

J. No se imprimirán documentos si se detecta la existencia de virus en el dispositivo.

Artículo 22. Del Monitoreo del Centro de Cómputo

El monitoreo del centro de cómputo son todas aquellas acciones que realizan conjuntamente todos los usuarios, con el fin de garantizar y prever el óptimo funcionamiento del centro de cómputo.

A. Es obligación de todos y cada uno de los usuarios, monitorear el buen uso y desarrollo de las actividades propias de su área establecidas dentro de sus funciones.
B. El personal del Centro de Cómputo se reserva el derecho de monitorear el uso de los servicios con el fin de detectar el posible mal uso de los mismos.

C. Durante el monitoreo se tomarán todas las medidas necesarias para garantizar la privacidad del usuario.

D. Por ningún motivo se examinará el contenido de comunicaciones individuales de correo electrónico.

E. En el caso de abuso por parte de un usuario en alguno de los servicios se le pedirá una explicación sobre la actividad detectada, lo cual se hará en estricta confidencialidad y por consecuencia cualquier acto de abuso comprobado acarreará una sanción.

F. En caso de abusos reiterados por parte de algún usuario, queda a discreción de la Coordinación del Centro de Cómputo la suspensión del servicio dentro de los laboratorios.

G. Es obligación de los Técnicos Académicos y la coordinación, agendar campañas de detección de códigos maliciosos y actualización de antivirus.

H. Es obligación de los Técnicos Académicos informar a los usuarios de manera oportuna la disponibilidad del uso de instalaciones.

I. Es obligación del profesor, vigilar que sus alumnos hagan buen uso del equipo y las instalaciones del centro de cómputo en desarrollo de su cátedra.

J. Durante el desarrollo de la cátedra, es responsabilidad del profesor verificar que sus alumnos se apeguen a las actividades del programa de la asignatura.

K. Para complementar el monitoreo diario del equipo en los laboratorios, el profesor tiene la obligación de reportar y notificar de manera escrita mediante el FORMATO DE REPORTES, las fallas o anormalidades encontradas en los laboratorios y equipos si fuera el caso.

Artículo 23. De la reservación y préstamo de los Laboratorios.

La reservación de laboratorios para el uso de equipo está orientada principalmente a los usuarios externos y/o temporales, quienes requieren del uso de las instalaciones.

A. Los laboratorios sólo podrán ser reservados para cursos o prácticas como apoyo a algún área académica o para eventos extraordinarios e institucionales que requieran las autoridades correspondientes.

B. La reservación de los laboratorios será a través de la entrega del formato llamado SOLICITUD DE LABORATORIO que le será proporcionado en el centro de cómputo, deberá anexar copia de su credencial de académico y el documento que justifique y la realización del evento con la autorización correspondiente.

C. Una vez autorizado y agendado un evento, se considerará una tolerancia de 15 minutos para dar inicio, después de este tiempo queda a discreción de la Coordinación la cancelación. El servicio regular del laboratorio se reanudará inmediatamente.

D. El organizador de evento deberá cumplir con el trámite correspondiente a la reservación y préstamo de equipo y entregar a la Coordinación de cómputo, una relación de los asistentes inscritos.

E. En los casos específicos de las asignaturas de Informática e Informática Aplicada a al Ciencia y la Industria en sus unidades del temario que contemplen el uso Internet y/o red; se hará a la coordinación la solicitud correspondiente a la reservación de laboratorios con la idea de agendar el laboratorio en cuestión, siempre dando prioridad a estas dos asignaturas.

CAPITULO V DE LAS OBLIGACIONES Y PROHIBICIONES

Artículo 24. De las Obligaciones

A. Generales:

- Cumplir con los lineamientos generales que en materia de cómputo se dicten en la UNAM y en el reglamento interno para el Centro de Cómputo.

- El equipo de Cómputo es para uso exclusivo del personal o usuarios autorizados.

- Responsabilizarse del uso adecuado del equipo que le sea asignado, respetando el horario establecido es obligación de todo usuario.

- Tener conocimientos mínimos para la adecuada operación del equipo y software que utilice.

- Contribuir en la preservación del equipo y mobiliario del Centro de Cómputo, sujetándose a los mecanismos de control, higiene, seguridad y vigilancia que se establezcan.

- Guardar respeto y consideración a otros usuarios y al personal del Centro de Cómputo.

- Utilizar únicamente el equipo asignado y en caso de mal funcionamiento, reportarlo al personal técnico encargado.

- Apagar el equipo al término de la sesión y acomodarlo.

- La información que se almacene en cualquier equipo del centro de cómputo, residirá de manera provisional durante su sesión de trabajo, por lo que no es responsabilidad del personal la conservación de la misma.

- Permanecer dentro del laboratorio asignado y en el horario estipulado.

- El centro de cómputo NO proveerá material para almacenar información de los usuarios, por lo que cada uno de ellos deberá traer sus propios dispositivos de almacenamiento externo,

- Los equipos de los laboratorios del centro de cómputo NO cuentan con quemadores, por lo que en relación a este servicio se deberá solicitar con anticipación a la coordinación, Toda persona ajena al centro de cómputo deberá solicitar de manera expresa la autorización para el ingreso y uso del equipo y efectuar su registro en bitácora

- Es obligación del usuario vacunar sus dispositivos de almacenamiento externo,

- Sólo se permite un máximo de dos usuarios por equipo, salvo exista la necesidad justificada y la autorización del coordinador de cómputo o el técnico Académico.

B. De los profesores

- Es obligación de los profesores mantener el orden, monitorear el buen uso y estado del equipo del laboratorio asignado para su clase, pues es considerado autoridad durante su cátedra.

C. De los Alumnos

- Los alumnos deberán guardar silencio y orden, evitando correr y/o jugar en las áreas comunes y dentro de los laboratorios, recordando en todo momento que hay clase en otros salones.

D. Del personal

- Durante la clase ningún elemento del personal del Centro de Cómputo, deberá interferir de manera directa con los alumnos dentro del laboratorio, salvo la violación o incumplimiento del presente reglamento o si se consideran situaciones que ponen en riesgo la integridad o seguridad de usuarios, equipo o información y sus excepciones.

- Es responsabilidad del personal asegurar el orden, buen uso y conservación del equipo y las instalaciones de los laboratorios, pasillos, escaleras, entrada, oficina y área de estantes; por lo que solo estos deberán tomar las medidas pertinentes para el mejor desempeño de las actividades del área.

Artículo 25. PROHIBICIONES

A. Generales

- El acceso a toda persona con fines ajenos a las actividades académicas que se realicen en el centro de cómputo.
- Utilizar las instalaciones con propósitos diferentes a los de tipo académico.
- Introducir equipo de cómputo externo a plantel sin importar el motivo, salvo autorización escrita de la autoridad correspondiente.
- Comportarse indebidamente dentro de las instalaciones del Centro de Cómputo.
- El uso lúdico y con fines de lucro de los equipos.
- El ingreso al centro de cómputo a usuarios que se encuentren bajo los efectos de alguna bebida alcohólica o de alguna sustancia tóxica.
- Faltar al respeto a los usuarios y al personal del Centro de Cómputo.
- Maltratar, romper y/o rayar cualquiera de los letreros o avisos publicados en las áreas comunes.
- Pegar cualquier tipo de propaganda y/o publicidad ajena a las actividades propias del Centro de Cómputo.
- Sustraer de manera ilícita material o equipo del Laboratorio.
- Extraer equipo de cómputo, sus partes o consumibles de las áreas de servicio.
- Alterar o dañar etiquetas de identificación del mobiliario y equipo.
- Utilizar los equipos para desplegar material obsceno o que atente contra los valores que promueve la Universidad Nacional Autónoma de México,
- Quebrantar las medidas de seguridad de los sistemas establecidos.
- Tirar basura en el lugar de trabajo y áreas comunes.
- Recibir visitas en horario de labores.

- Llevar a cabo actividades que conduzcan al uso no autorizado de información y de recursos ajenos a la institución.

- Realizar cualquier acción o tipo de comercio.

B. De los Profesores

- No podrán autorizar a los alumnos que se encuentren tomando clase a realizar actividades fuera del contexto de la cátedra.

- Quedan restringidas las salidas del salón durante la hora de clase.

- El consumo de alimentos, bebidas, golosinas, cigarros dentro del Centro de Cómputo.

- Mover o maltratar el mobiliario, conectar y desconectar periféricos y el equipo de cómputo. Cualquier modificación o cambio se deberá solicitar a la coordinación y pedir apoyo a los técnicos académicos del centro de cómputo.
- Ausentarse más de 10 minutos dejando a los alumnos sin supervisión en el salón de clase.

- Ausentarse más de 15 minutos dejando el equipo encendido.

- Recibir visitas de carácter comercial (vendedores, cobradores, aboneros, agentes bancarios, etc.) durante el desarrollo de su clase.

- Abrir el equipo de cómputo, sin previa autorización.

- Dejar basura y sucio el pizarrón de los laboratorios.

- Permitir el acceso de alumnos una vez que la tolerancia ha transcurrido.

C. De los Alumnos

- El consumo de alimentos, bebidas, golosinas, cigarros, etc.

- Mover o maltratar el mobiliario, conectar y desconectar periféricos y equipo de cómputo. Cualquier modificación o cambio se deberá solicitar a la coordinación a través del profesor y pedir apoyo a los técnicos académicos del centro de cómputo.

- Ausentarse más de 15 minutos dejando los equipos encendidos.

- Correr, gritar y/o jugar en los salones de clase y en las áreas comunes del centro de cómputo.

- Enviar cualquier objeto a través de las ventanas de los laboratorios.

- Hacer un llamado al profesor a través de las ventanas (gritarle) desde el exterior del Centro de Cómputo, para solicitar su acceso al laboratorio.

- Utilizar el barandal de la escalera como resbaladilla.

D. Del Personal

- Permitir el acceso a personas ajenas al centro de cómputo.

- Maltratar físicamente a los alumnos y/o profesores.

- Interferir de manera directa en el desarrollo de la cátedra de los profesores, sin ninguna justificación.
- No reportar irregularidades a las autoridades correspondientes.

- Negar servicios sin una justificación válida.

- Quitar credenciales a los alumnos.

- Jugar, catear y realizar cualquier otra actividad no relacionada con los servicios del Centro de Cómputo.

- Abusar de su autoridad con los alumnos.

CAPITULO VI DEL ACCESO AL CENTRO DE CÓMPUTO

El acceso al Centro de Cómputo para el uso de los servicios deberá observar lo siguiente:

Artículo 26

El acceso será en los horarios de clase establecidos y cada 50 minutos.

Artículo 27.

Se establece una tolerancia de 10 minutos para el acceso entre cada clase. En caso de no haber entrado en el tiempo de tolerancia, habrá de esperarse hasta el siguiente cambio de hora (esto incluye a los grupos con horario continuo de clase).

Artículo 28.

Si el profesor llega retrasado a su clase, sólo tendrán acceso los alumnos que se encuentren en ese momento esperándolo, ya que la tolerancia se considera a partir del horario establecido cada 50 minutos y no a partir de la llegada del profesor.

Artículo 29.

La tolerancia del profesor es la establecida por la Legislación Universitaria.

Artículo 30.

El profesor deberá supervisar la entrada de sus alumnos en los horarios establecidos, apoyado por el vigilante o responsable para evitar cualquier tipo de incidente.

Artículo 31.

Una vez terminada la tolerancia el profesor deberá incorporarse inmediatamente a su salón de clase evitando así cualquier incidente con los alumnos que ya se encuentran en el laboratorio.

Artículo 32.

El alumno portará en mano únicamente las cosas necesarias para trabajar durante su práctica o sesión, solo así tendrá acceso a los laboratorios.

Artículo 33.

Los alumnos dejarán sus mochilas en el estante que corresponde a su salón de clase, estos están marcados e identificados con colores y nombres.

Artículo 34.

Por propia conveniencia, el alumno tiene la obligación de dejar su mochila bien cerrada sin objetos de valor a la vista como: monederos, teléfonos celulares, carteras, calculadoras o cualquier otro artículo llamativo.

Artículo 35.

En caso de no traer nada o traer bolsas, mochilas, paquetes, guitarras, maquetas, etc., adicionales, éstas se deberán acomodar en el área de estantes; es necesario notificar y dejar la credencial al responsable de la puerta.

Artículo 36.

Una vez que el alumno haya entrado al Centro de Cómputo no podrá guardar y/o sacar cosas de su mochila. Esta medida se implementa con la finalidad de agilizar el acceso y la salida de los alumnos, así como la seguridad de los objetos que se encuentran en los estantes.

NOTA: El personal del Centro de Cómputo, **NO** se hará responsable de la pérdida de mochilas u objetos extraviados.

Artículo 37.

No se permitirá tomar la mochila de otro compañero, bajo ninguna circunstancia.

Se sugiere educación ante todo, recordando que en la forma de pedir está el otorgar. Solicite su acceso adecuadamente.

CAPITULO VIl
DEL DESARROLLO DE LA PRÁCTICA Y SU PERMANENCIA EN EL CENTRO DE CÓMPUTO

Artículo 38.

Los trabajos, tareas, proyectos, investigaciones, etc. Que sean realizados por los usuarios en todos los equipos, deben ser de carácter estrictamente académico.

Artículo 39.

En cada laboratorio o lugar del centro de cómputo, es una obligación que el comportamiento de todo usuario este regido por las normas de la moral y las buenas costumbres.

Artículo 40.

El uso adecuado del equipo de cómputo será responsabilidad del usuario.

Artículo 41.

No se podrá permanecer en los pasillos ni escaleras del centro de cómputo.

Artículo 42.

No deberán permanecer alumnos solos en los laboratorios sin la presencia de un profesor, tutor, o técnico encargado.

Artículo 43.

El usuario trabajará en la cuenta de invitado en el caso de los equipos que cuentan con Windows XP; para evitar en lo más posible infecciones de virus y cambios de configuración al sistema.

Artículo 44.

El uso de las sesiones de Administrador de sistema en los equipos (Windows XP) están restringidas para profesores y alumnos.

El uso de equipo

Consiste en facilitar equipo de cómputo a los usuarios para que puedan trabajar dentro de los laboratorios.

Artículo 45.

Se le dará prioridad a las materias de Informática e Informática Aplicada al Ciencia y la Industria ya que estas son asignaturas las establecidas formalmente en el plan de estudios de la Escuela Nacional Preparatoria; así como a los eventos agendados por la Dirección de Plantel, Dirección General o Consejo Técnico.

Artículo 46.

En segundo lugar se dará atención a los colegios de Opción Técnica.

Artículo 47.

Por último, pero no menos importantes, a los colegios restantes y usuarios externos; a todos sin afectar a los primeros ya que son los que dieron cabida a la existencia del Centro de Cómputo.

Artículo 48.

Los usuarios podrán utilizar el equipo de manera extemporánea o extraordinaria solo con la autorización del coordinador del centro de Cómputo y/o los Técnicos Académicos encargados.

Artículo 49.

Los usuarios que soliciten el servicio de préstamo de quipo podrán disponer de el hasta por 2 horas continuas, pudiendo refrendar si no hay demanda por parte de otros usuarios.

Artículo 50.

Sólo se permite un máximo de dos usuarios por equipo, salvo exista la necesidad justificada y autorización correspondiente de la coordinación de cómputo.

Artículo 51.

Solo los Técnicos Académicos están autorizados a instalar el software especificado, autorizado y justificado.

Artículo 52.

Los profesores y alumnos tienen prohibido modificar la configuración propia del equipo y establecer cuentas de usuarios, contraseñas e instalar cualquier tipo de software.

Si existe el interés en la instalación de algún software en específico, se deberá realizar el trámite correspondiente a la Coordinación, justificando la necesidad de éste y se anexará una copia del software con un mínimo dos semanas de anticipación y una vez instalado el profesor solicitante deberá realizar las pruebas pertinentes.

Artículo 53.

Todos los usuarios deben hacer una exploración visual del equipo asignado así como realizar una revisión general del funcionamiento del sistema pues será responsabilidad de él reportar cualquier irregularidad.

Artículo 54.

Es obligación del usuario conservar el equipo en el mejor estado posible.

Artículo 55.

Es responsabilidad de los usuarios darle al equipo asignado el uso adecuado conforme al fin para el que fue destinado.

Artículo 56.

Los usuarios deberán hablar en voz baja para no perturbar las clases y otras actividades que se realicen en el momento.

Artículo 57.

No se podrá realizar ninguna otra actividad que no este relacionada directamente con el tema que se imparte en cada clase.

Artículo 58.

Esta restringido almacenar cualquier tipo de información en los discos duros de los equipos. O extraer la información que pertenezca a otros usuarios.

Artículo 59.

No se podrá conectar a los equipos ni hacer uso de audífonos, teléfonos celulares, radio localizadores, reproductores de audio y video externos o cualquier tipo de dispositivo electrónico no permitido.

Por norma básica de orden se prohíbe escuchar música dentro de los salones.

Artículo 60.

A toda persona que se le sorprenda rayando, maltratando, introduciendo objetos en las unidades de disco, quitando o cambiando piezas, o dañando de cualquier forma algún equipo, será severamente sancionada.

Artículo 61.

Esta estrictamente prohibido abrir el equipo de cómputo.

Artículo 62.

Los usuarios tienen la obligación de mantener limpia el área de trabajo

Artículo 63.

No se deberán sobrecargar los contactos

CAPÍTULO VIII DE LA SALIDA DEL CENTRO DE CÓMPUTO

Artículo 64.

Una vez finalizado el horario de su clase, el profesor debe otorgar la salida a sus alumnos y dejar libre el laboratorio que le fue asignado, en un lapso no mayor a 10 minutos.

Artículo 65.

Es responsabilidad del usuario, una vez terminada la clase, cerrar las sesiones de usuario y apagar los equipos inmediatamente sobre todo aquellos dispositivos periféricos que presentan un nivel mas delicado de sobrecalentamiento como son: monitores, impresoras y escáner

Artículo 66.

Dejar el área utilizada tan ordenada y limpia como la encontró.

Artículo 67.

El alumno colocará sobre el monitor el teclado y el Mouse y la silla en su lugar. El alumno se formará para recoger sus cosas y procurará seguir el resto de los lineamientos ya mencionados.

Artículo 68.

No olvidar ningún objeto personal en los laboratorios ya que el personal no se hace responsable de objetos olvidados.

Artículo 69.

La salida del laboratorio se efectuará después de que el profesor brinde autorización y una vez que el equipo utilizado haya sido entregado en el estado en que se encontró. Esta salida será en forma estrictamente ordenada y en silencio para no importunar a otros grupos en clase.

Artículo 70.

El alumno deberá recoger del estante correspondiente los objetos que haya depositado a la entrada. Y deberá guardar sus cosas una vez que ha abandonado el Centro de Cómputo.

En el caso de haber dejado en prenda la credencial deberá recogerla de igual manera antes de retirarse.

CAPITULO IX DEL USO DE LA RED Y ACCESO A INTERNET

La información que consulte el usuario no deberá ser ofensiva y esta estrictamente prohibido el acceso a páginas con contenido ofensivo, sexual, violento o ilegal.

Artículo 71.

El acceso de los usuarios a Internet debe ser utilizado únicamente para visitar sitios relacionados con actividades académicas. Se permitirá el uso personal de la red en la consulta de correos electrónicos, siempre y cuando sea razonable y no comprometa de ninguna forma la seguridad de los servicios de cómputo de este Laboratorio.

Artículo 72.

El acceso a Internet contará con restricciones para sitios inseguros, y será particularmente importante que los usuarios tengan un comportamiento responsable en aquellos sitios que

no queden restringidos, ya que un uso inadecuado puede comprometer seriamente la seguridad de los servicios de cómputo.

Artículo 73.

Está estrictamente prohibido acceder a páginas sin ningún interés académico, esto es, páginas visitadas por los alumnos en alguna distracción del responsable del grupo para buscar información no concerniente a actividades académicas dentro del tiempo de práctica. Está a discreción del personal del Centro de Cómputo el suspender temporalmente el servicio de red si el responsable del grupo no pone estricta atención a lo que los alumnos visitan en Internet en su hora de práctica.

Artículo 74.

Queda estrictamente prohibido el uso de programas para descargar o copiar desde Internet archivos de procedencia no segura o ilegal, tales como archivos de música, video, juegos, DVD y similares. Por estos motivos queda también prohibido instalar y ejecutar programas que permitan el intercambio de archivos tales como Ares, Kazaa, Morpheus, y similares. Queda también prohibido utilizar los recursos de cómputo para actividades no académicas o de trabajo, como el uso de pláticas en línea o "chats".

Artículo 75.

Esta prohibida la práctica de descargar e instalar programas gratuitos de Internet, tales como salva pantallas, programas de modificación de punteros y similares, pues estos frecuentemente instalan programas indeseables como espías, virus y códigos maliciosos.

Artículo 76.

Queda prohibida la instalación de servidores Web o páginas Web en las computadoras de los Laboratorios de Cómputo así como utilizar los servicios de cómputo de la Red de Cómputo para realizar cualquier tipo de actividades comerciales.

Artículo 77.

Todas las conexiones a Internet tendrán que estar dentro del Firewall para seguridad del sistema de red este puede ser el Firewall del sistema operativo, a excepción de aquellas expresamente autorizadas por la Coordinación de Cómputo. Toda máquina en la red que se le detecte algún incidente de seguridad podrá ser desconectada físicamente de la misma en tanto se corrija el problema, y deberá ser nuevamente autorizada por la Coordinación de Cómputo para poder operar fuera del Firewall.

Artículo 78.

El personal del Centro de Cómputo deberá configurar y certificar los equipos para que se puedan conectar a la red, las direcciones IP fijas serán asignadas por la coordinación de

Cómputo. Todo equipo que se vaya a conectar deberá contar con un antivirus vigente y con las actualizaciones del sistema operativo que permitan asegurar la no existencia de vulnerabilidades que pongan en entredicho la integridad y seguridad de la red.

Artículo 79.

Queda estrictamente prohibido cambiar la dirección IP asignada o usar una dirección IP que no haya sido previamente autorizada por la Coordinación de Cómputo. También está prohibido configurar equipos y conectarlos a la red sin haber sido revisados y certificados por el personal de Cómputo. Lo anterior incluye la prohibición de instalar y configurar concentradores inalámbricos. En caso de existir la necesidad de instalar puntos de acceso inalámbrico a la red, se deberá emitir una solicitud por escrito a la Coordinación de Cómputo, para que el personal de éste lleve a cabo las acciones necesarias para garantizar la seguridad de la red.

Artículo 80.

Las máquinas que estén dispersando virus o códigos maliciosos deberán ser desconectadas de la red hasta que se resuelva el problema y los virus sean eliminados. Los usuarios que detecten virus en sus equipos deberán apagarlos y dar aviso al personal de Cómputo, quien deberá darle máxima prioridad a la valoración de la gravedad del problema y su consecuente solución.

Artículo 81.

El personal del Centro de Cómputo no se hace responsable de problemas de comunicación con servidores externos por problemas de Red UNAM o DGSCA.

Artículo 82.

Es responsabilidad tanto del usuario como del profesor asignado el dar aviso oportuno al personal del Centro de Cómputo, de la existencia y propagación de algún virus, código malicioso y/o petición de actualizaciones de cualquier índole; ya que con esto se acelerará la no proliferación de tales códigos tomado las medidas justas por parte del personal.

Artículo 83.

Cualquier excepción a los puntos anteriores puede ser válida siempre y cuando el usuario proporcione una clara justificación académica, excepto los puntos de prohibición estricta que no deberán ser transgredidos por ningún motivo.

Artículo 84.

El centro de cómputo no se hace responsable por el exceso de tráfico en la red y servidores; de igual forma por fallas en servidores remotos que impliquen la lenta transferencia de información.

Artículo 85.

La sección de computo se reserva el derecho de desconectar equipos de la red y de restringir ordenes de servicio por mal uso de la computadora: equipo con programas inseguros de música o video, entrada repetitiva de virus a través de correo no filtrado, equipos operando sin antivirus actualizados o con sistemas operativos sin los parches de actualización. La Coordinación de Cómputo deberá ser informada de estos casos.

CAPITULO X DE LA SUSPENSIÓN DE SERVICIO Y LAS SANCIONES

Artículo 86 De la Suspensión de Servicios por Evento

Se suspenderán los servicios del Centro de Cómputo bajo las siguientes circunstancias:

A. De manera total cuando:

- Existan causas de fuerza mayor
- Por eventos y sistemas calendarizados como son: Instrumento de Apoyo a la Superación Académica (IASA).
- Cuando la autoridad del plantel así lo designe.

B. De manera parcial (sólo salones 1 y 2) cuando:

- Existan causas de fuerza mayor
- Por eventos y sistemas calendarizados como son: Instrumento de Apoyo a la Superación Académica (IASA); Avances Programáticos, etc.
- En caso de alguna otra actividad o evento con características de prioritario o extraordinario.
- Cuando la autoridad del plantel así lo designe.

Artículo 87.

La Coordinación de Cómputo se reserva el derecho de suspender el servicio a un usuario cuando se sospeche de un abuso o uso indebido del mismo o bien haga caso omiso del presente reglamento.

Artículo 88.

La persona que sea sorprendida destruyendo, modificando, o haciendo mal uso del software, hardware, instalaciones y en general, del material que tiene el centro, así como de no apegarse a los lineamientos establecidos, será objeto de una sanción que irá desde la restitución del daño y cancelación del servicio, hasta la remisión con las autoridades universitarias correspondientes.

Artículo 89.

La reincidencia en alguna de las actividades no licitas originará la suspensión TOTAL o PARCIAL del servicio.

Artículo 90.

Todos los artículos del presente reglamento pueden presentar excepciones las cuales serán expuestas, analizadas y validadas por la Coordinación de Cómputo quien les dará el seguimiento pertinente.

Artículo 91. De las Sanciones

Las sanciones que pueden aplicarse a un alumno son: amonestaciones verbales, suspensión temporal o definitiva del servicio y baja definitiva en los servicios de cómputo.

A. Primera amonestación llamada de atención y/o servicio comunitario (según la gravedad).

B. Segunda amonestación suspensión del servicio en esa sesión y servicio comunitario (según la gravedad)
C. Tercera amonestación suspensión del servicio parcialmente y presentación ante la autoridad competente según cada caso.

NOTA IMPORTANTE:

En caso de que un alumno cometa algún acto de indisciplina grave dentro del centro de cómputo se procederá a reportar el caso ante la Secretaría de Apoyo a la Comunidad y/o a la oficina Jurídica del plantel, a efecto de que se proceda conforme a la Legislación Universitaria aplicándose, en su caso, las sanciones estipuladas en la misma.

APENDICE III.
INSTALACIONES Y SEGURIDAD PARA CENTROS DE TECNOLOGÍA DE INFORMACIÓN

1. Selección del local

- Ha de analizarse:
- Acceso de máquinas.
- Disponibilidad y requerimientos de la fuerza eléctrica adecuada.
- Espacio para el equipo de aire acondicionado.
- Unidad autocontenida (dispositivos de control, compresores, bomba,
- humidificador, deshumidificador).
- Intercambiador de calor.
- Altura del techo, área de paredes exteriores y área de ventanas de cristal.
- Capacidad de carga de piso (loza o piso firme).
- Normas de seguridad.
- Peligro de inundación.
- Protección contra incendios.
- Facilidad de comunicación interior y exterior con los restantes servicios.

2. Necesidades de espacio

- Componentes específicos deseados, tales como: consolas, servidores, nodos, racks de modems, equipo de conectividad de redes (multiplexores, ruteadores, concentradores, ether-switchs, etc., unidades de cinta y cartuchos de cinta magnética, unidades de disco y de CD-ROM, impresoras de impacto o laser (de baja o alta velocidad), etc.
- Relación largo-ancho del local.
- Ubicación de las columnas.
- Previsión para futuras ampliaciones.
- Espacio para archivar en la sala del equipo de cómputo: cartuchos de cinta magnética, discos y discos compactos del día, etc.

- Espacio para sillas, estantería, mesas, etc.
- Integración del área de trabajo del equipo de cómputo con otras áreas.

3. Disposición en planta

- Hablar con el representante de planificación de instalaciones del proveedor.
- Antes de hacer el pedido de cables de comunicaciones, entre el procesador y los diferentes dispositivos electrónicos, el cliente debe aprobar la disposición y conocer:
- Unidades de control asignadas a cada canal.
- Dispositivos en todas las unidades.
- Prioridad de las unidades de control en cada canal.
- Unidades de entrada/salida o dispositivos conectados a cada unidad de control.
- Debe haber acceso visual entre la consola de la unidad central y las unidades de cartucho de cinta magnética y de discos compactos, así como de las unidades de entrada/salida.
- Estudiar los desplazamientos más frecuentes de los operadores.
- Distancia y localización del almacén de paso para los insumos de cómputo, tales como: papel stock, formas especiales, cartuchos de cinta magnética nuevos, CD-ROM, alcohol isopropílico, tela de bramante, etc.
- Ubicación de la bóveda de almacenamiento de dispositivos de protección de información.
- Aislar las unidades productoras de polvo, tales como: impresoras, lectoras de formas de marcas ópticas, y todas aquellas que puedan ser elementos de contaminación en la sala de los equipos de cómputo.
- Zona con unidades exigentes en limpieza de aire (unidades de discos compactos y de cartuchos de cinta magnética).
- Adquirir e instalar previamente los cables exteriores necesarios, el cableado estructurado y los switches para conectar los nodos de la(s) red(es).
- Tramitar con mucha anticipación las líneas telefónicas requeridas con la compañía telefónica. Y contactar con la institución apropiada a fin de realizar los trámites o permisos para las telecomunicaciones.

4. Resistencia del piso

- En las hojas de especificaciones comprobar el peso y dimensiones de las unidades.
- Tener en cuenta la resistencia y nivelación del piso falso.
- Comprobar la resistencia del piso.

5. Puertas de acceso

- Las puertas del local serán de doble hoja y con anchura total de 1.4 a 1.6 m.
- Es necesaria una salida de emergencia.
- Tener en cuenta las dimensiones máximas de los equipos si hay que atravesar puertas y ventanas de otras dependencias.

6. Paredes y techo

- Las paredes irán con pintura plástica lavable para poder limpiarlas fácilmente.
- Deberán pintarse el techo real y las placas del falso plafón.
- La altura libre entre piso falso y falso plafón debe estar entre 2.70 y 3.30 m.

7. Piso falso

- Debe permitir cambios en la ubicación de unidades.
- Debe cubrir los cables de comunicaciones entre la unidad central de proceso y los dispositivos periféricos, cajas de conexiones y cables de alimentación eléctrica.
- Deberá proporcionar seguridad al personal.
- Debe permitir que el espacio entre los dos suelos actúe como una cámara plena de aire, que facilite el reparto de las cargas.
- La altura recomendable será de 30 cm si el área de la sala de cómputo es de 100 m2 o menos, y de 40 a 60 cm si es mayor de 100 m2. La altura mínima podrá ser de 18 cm si la sala es pequeña. Todo lo anterior es con objeto de que el aire acondicionado pueda fluir adecuadamente en la cámara plena.
- Puede ser de acero, aluminio o madera resistente al fuego.
- El mejor piso deberá estar soportado por pedestales o gatos mecánicos de aluminio.
- Tener en cuenta la frecuencia con la que se moverán los equipos.

- Estudiar mínima rotura, apariencia, costo.
- Cuando se utilice como cámara plena para el aire acondicionado, tendrá que cubrirse el piso firme con pintura antipolvo.
- Hay que considerar la resistencia eléctrica transversal del recubrimiento del piso falso para evitar cargas electrostáticas.
- Los valores de esta resistencia estarán por debajo de 2x1010 ohms.

8. Iluminación

- En el área de máquinas debe mantenerse un promedio mínimo de 450 luxes a 70 cm del suelo.
- Debe evitarse la luz solar directa para poder observar la consola y las señales.
- Las reactancias (o conocidas también como balastras) de los equipos de iluminación del tipo slim line estarán fuera de la sala.
- La iluminación no se alimentará de la misma acometida que el equipo de cómputo.
- Del 100% de iluminación, deberá distribuirse el 25% para iluminación de emergencia y se alimentará desde un tablero que esté conectado al sistema de fuerza ininterrumpible.

9. Vibraciones

- Si hay vibraciones superiores a las normales es necesario estudiarlas antes de colocar los equipos y utilizar los dispositivos antivibratorios necesarios (juntas de neopreno).

10. Tratamiento acústico

- Las principales fuentes de ruido son las lectoras de formas, impresoras y ventiladores.
- El suelo debe amortiguar la transmisión de la vibración a otras áreas.
- Las paredes deben evitar que el ruido pase a los locales adyacentes.
- Las puertas deben cerrar bien.
- Se tratará adecuadamente el techo, lo mejor es el techo poroso (tipo acustone) con base en módulos.
- Si existen conductos de aire en la cámara plena del piso falso, debe evitarse que el ruido generado por las máquinas se transmita a otras dependencias.

11. Capacidad del equipo de aire acondicionado

- Se tendrá en cuenta:
- Disipación térmica de las máquinas.
- Disipación térmica de las personas.
- Cargas latentes, aire de renovación.
- Pérdidas por puertas y ventanas.
- Transmisión de paredes, techos y suelos.
- Disipación de otros aparatos.
- Las cargas caloríficas del equipo de cómputo y sus periféricos las proporcionará el proveedor, comúnmente se especifican en BTU/hora o en kcal/hora.
- El proveedor del equipo de cómputo también proporcionará la cantidad de aire que requieren los ventiladores de los diferentes dispositivos de cómputo, por lo regular en pies cúbicos por hora o en metros cúbicos por hora.
- El aire acondicionado para la sala de cómputo deberá ser independiente del general del edificio.
- El calor disipado por los diferentes dispositivos de cómputo, obliga a necesitar aire frío todo el año.
- La alimentación eléctrica, para los equipo de aire acondicionado, deberá ser directamente desde un tablero alimentado desde la subestación; de ninguna manera deberá conectarse a la salida del equipo no-brake, ya que por el encendido y apagado automático de motores y compresores ocasionaría disminución en el voltaje y ruido eléctrico al equipo de cómputo.

12. Condiciones de temperatura y humedad

- Las condiciones de proyecto serán las indicadas por el proveedor del equipo de cómputo.
- Cifras aproximadas pueden ser:
- Rango de temperatura de 18 a 22 grados centígrados.
- Humedad relativa (HR): 50% ± 5%.
- En tiempos cortos podrían alcanzarse de 16 a 24 grados centígrados y de 40 a 70% de HR, con máxima temperatura húmeda de 24 grados centígrados.

- Cuando el aire frío se inyecte directamente a los equipos, su temperatura no será inferior a 17 grados centígrados y su HR no será superior al 80%.

13. Filtros y humidificación

- Se requieren filtros de tipo absoluto con una eficiencia del 99% sobre partículas de 3 micrones.
- Si hay contaminación, elegir los filtros adecuados.
- El aire de renovación o ventilación será tratado antes de ser introducido en la sala, tanto en temperatura y humedad como en filtrado.
- Son recomendables los tipos de humidificadores de vapor.

14. Distribución de aire en la sala

- Los componentes de las máquinas se refrigeran, normalmente, mediante la circulación rápida de aire por ventiladores.
- La entrada de aire se efectúa por debajo de las máquinas a través de rejillas.
- El aire caliente es expulsado por la parte superior de las máquinas.
- Debe considerarse con cuidado el sistema de distribución para eliminar áreas con excesiva velocidad de aire.
- El aire de renovación o ventilación vendrá en función del volumen de la sala. Se proyectará para obtener de 1.5 a 2 renovaciones por hora y para crear una sobrepresión que evitará la entrada de polvo y contaminantes por las puertas, procedentes de las zonas adyacentes.
- El aire de renovación se descontaminará previamente.

14.1.Distribución por techo

Por medio de este sistema:

- Se impulsa el aire frío por el techo.
- Se retorna también por el techo a través de rejillas colocadas encima de las salidas de aire caliente.
- Se tratan menores volúmenes de aire.
- Tiene poca flexibilidad para cambios de posición de unidades.
- Debe estudiarse para no crear corrientes de aire frío.

14.2.Distribución por piso falso

De acuerdo con este sistema:

- El espacio entre el suelo del edificio y el piso falso se utiliza como una cámara plena de aire.
- Todo el aire se descarga en la sala a través de registros en el suelo.
- El aire retorna a la unidad acondicionadora por rejillas en el techo.
- Se necesita una cierta cantidad de recalentamiento para controlar la humedad relativa del aire antes de que entre en la sala.
- El sistema debe tener controles de la temperatura del aire en el piso falso.
- Hay que colocar cuidadosamente las rejillas y los retornos para no crear tiros de aire frío a caliente.

14.3.Dos canalizaciones

Es un sistema muy eficaz en el que:

- Una unidad de controles separados suministra aire y filtrado a las tomas de aire de los dispositivos de cómputo.
- La otra unidad suministra aire directamente a la sala por canalización diferente y absorbe el resto de la carga de calor (iluminación, personas, etc.).

En las tres siguientes páginas se muestran diagramas de flujo de aire acondicionado; en ellos se ejemplifican posibilidades de instalación en una sala de cómputo de gran tamaño. Se recomienda que se utilicen equipos de aire acondicionado de 10 TR con unidades integradas dentro de la sala de cómputo. Las intercambiadoras de calor serán de agua si la distancia a la sala de cómputo es grande, en caso contrario se utilizarán intercambiadoras de calor a base de gas.

15. Ductos

- Serán de material que no desprenda partículas al paso del aire.
- No deberán tener revestimientos internos de fibras.

16. Protección contra incendios

16.1.Situación del área del equipo de cómputo

- El área del equipo de cómputo debe estar en un edificio o habitación que sea resistente al fuego.

- La sala del equipo de cómputo no debe situarse encima, debajo o adyacente a un área donde se procesen, fabriquen o almacenen materiales inflamables o explosivos.

- La sala del equipo de cómputo deberá contar con puertas de emergencia.

16.2.Seguridad de la estructura de la sala de cómputo

- Las paredes del área del equipo de cómputo deben ser de material incombustible. Si el área del equipo de cómputo tiene una o más paredes exteriores adyacentes a un edificio que sea susceptible de incendio, la instalación de ventanas irrompibles mejorará la seguridad del personal y del equipo contra los escombros y el agua.

- El techo falso debe ser de material incombustible o resistente al fuego.

- Todas las canalizaciones y materiales aislantes deben ser de materiales incombustibles y que no desprendan polvo.

- El piso falso instalado sobre el piso real debe ser incombustible.

- El techo de la sala y área de almacenamiento de cartuchos de cinta magnética, discos y discos compactos deben ser impermeables.

- Debe preverse un sistema de drenaje en el piso firme.

16.3.Tipos de equipo contra incendio

- Habrá sistema de detección de humos, por ionización, para aviso anticipado.

- El sistema deberá hacer sonar una alarma e indicar la situación del detector activado.

- El sistema de detección no deberá interrumpir la corriente de energía eléctrica al equipo de cómputo.

- Un dispositivo manual de emergencia para cortar el sistema eléctrico y el aire acondicionado deberá instalarse en cada salida de la sala de cómputo.

- Deben ubicarse suficientes extintores portátiles de CO_2 (recomendados para equipo eléctrico), tanto en la sala de cómputo como en el local del sistema de fuerza ininterrumpible en lugares estratégicos.

- Una instalación de CO_2 automática está compuesta por una red de difusores dispuestos en toda la sala y unidos por medio de tuberías de acero estirado sin soldadura a tanques de CO_2 a 250 kg/cm^2 y está almacenado en estado líquido.

- El CO_2 actúa por choque, enfriamiento y ahogo.

- La descarga debe ser automática con base en señales enviadas por los detectores o puede ser en forma manual, accionando botones o palancas.

- Anteriormente se utilizaba el gas halón en lugar del CO_2; el halón es un gas inodoro, no nocivo para la salud y no afecta a los equipos de cómputo, también crea una atmósfera inerte y se dispersa muy rápidamente. Actualmente se estudia por situaciones de posible contaminación ambiental y efectos sobre la capa de ozono, por ello se prefiere el uso del CO2.

- Los detectores de ionización del aire se colocan tanto en el techo falso como abajo del piso falso, repartidos de una manera uniforme y todos ellos estarán conectados al tablero de control del equipo contra incendio, en este tablero se localiza un reloj que puede calibrarse de 0 a 60 segundos para provocar el disparo del CO2 a través de boquillas de aspersión estratégicamente distribuidas en el techo y bajo el piso falso de la sala del equipo de cómputo. También puede activarse manualmente a través de botones o palancas. Los cilindros de CO2 deben colocarse en la propia sala, o en un lugar inmediato a ella. Se precisan tuberías desde los cilindros hasta las boquillas.

16.4.Puntos que se verificarán para realizar pruebas de concentración de gas para un sistema contra incendios

La planeación es la única clave para una prueba exitosa de un sistema de gas CO2. Existe un número importante de aspectos por considerar antes de hacer la prueba. Para ayudarnos a que la prueba sea exitosa, debemos tener en cuenta los siguientes puntos que nos permitirán hacer los preparativos y que deberán verificarse antes de llevar a cabo la prueba de concentración.

1. Disponibilidad del área donde se hará la prueba, el día y la hora programadas.

2. Retirar del área de prueba, papeles o materiales que puedan volar durante la prueba de descarga.

3. Si también se va a probar la descarga bajo el piso falso, éste deberá ser aspirado o limpiado de polvo, escombros o papel que pudieran introducirse en el equipo de cómputo.

4. Comparar el volumen del riesgo que se probará con el volumen original de la memoria de cálculo; los dos volúmenes deben ser iguales.

5. Verificar el local, así como el piso falso en busca de orificios o huecos por los cuales pudiera fugarse el agente, originando una baja en el porcentaje de concentración. Estos orificios o huecos se sellarán o se dejarán abiertos.

6. Verificar que la tubería, boquillas de descarga y equipo operacional sean los correctos.

7. Limpiar o sopletear la tubería para evitar que los residuos de aceite ensucien el local o las rebabas bloqueen los orificios de las boquillas de descarga.

8. Que las conexiones y soportes de las tuberías estén lo suficientemente apretados o fijos para evitar fugas y movimientos peligrosos de la tubería durante la descarga.

9. Asegurar los módulos del falso plafón alrededor de las boquillas de descarga para que soporten la descarga de alta velocidad del gas.

10. Verificar que no exista alguna fuga de agente a otra área con protección, la cual pudiera ser activada con la descarga del agente.

11. Verificar el funcionamiento de todos los elementos del sistema, incluyendo el sistema de detección de incendios, antes de la prueba de descarga.

12. Los puntos seleccionados para las mediciones de concentración deben ser discutidos y aprobados por el personal responsable de la prueba.

13. Los cilindros que contienen el gas para la prueba deben pesarse y estar etiquetados con su peso y tipo de agente.

14. Si la prueba se hace con gas CO2, se deberá poner la cantidad adecuada (82% del peso del CO2). Los contenedores del CO2 deben ser presurizados con nitrógeno a la presión que funciona el sistema.

15. El sistema de aire acondicionado que sirva a esta área ¿estará operando durante la prueba?; si el sistema de aire acondicionado se apaga, ¿cuál es el tiempo en que el extractor se para completamente?; o si tiene compuertas automáticas, ¿en cuánto tiempo cierran?

16. Es recomendable que si existe un sistema de alarma adicional, éste sea silenciado durante la prueba. Verificar que el sistema de aire acondicionado no sea puesto en marcha nuevamente.

17. Hacer las preparaciones adecuadas para la ventilación del local después de terminada la prueba. Verificar si se requieren ventiladores o extractores adicionales; si es así, ¿se tienen disponibles?

18. Si el sistema está conectado a un servicio externo de seguridad se debe notificar a éste, el día, hora y duración de la prueba.

19. ¿Es necesario o deseable que haya gente en el interior del local durante la prueba?, si es así, se requieren equipos de respiración autónomos si la prueba es con CO_2 y el tiempo excede al tiempo de exposición recomendado.

20. Es necesaria una plática previa para el personal relacionado con la prueba de descarga.

16.5. Instrucciones de manejo del panel de control de un sistema contra incendios

NORMAL	En condiciones normales, todos los indicadores rojos y ámbar deberán estar apagados. Solamente el indicador de color verde permanecerá encendido.
PROBLEMA	Cualquier problema en el sistema, deberá ser anunciado por indicador ámbar (problema) en el panel de control y con un sonido interno agudo.
ALARMA	El estado de alarma será anunciado por indicador rojo (alarma) en el panel de control.
DESCARGA	La descarga de CO_2 se efectuará transcurridos 30 segundos (aprox.), después de sonar el sistema de alarmas audiovisuales y sonoras.
ABORTO	Este interruptor de color rojo, colocado a la derecha del panel de control, sólo operará antes del disparo de CO_2 (30 segundos de alarma).
RESTABLECIMIENTO	Existe un interruptor integrado al panel de control, el cual sirve para restablecer el sistema en caso de alarma (verificar que las estaciones manuales de alarma estén en posición normal).
SILENCIADOR	Este interruptor integrado al panel de control opera: a) Silencia las alarmas y mantiene intermitentemente encendidos los indicadores de alarma, b) Silencia la alarma interna del problema, aun cuando los indicadores de problema ámbar permanecen encendidos.

Este instructivo será enmarcado a un lado del panel de control e indicará los teléfonos del proveedor para llamarle en caso de algún problema.

17. Almacenamiento de información

- Los cartuchos de cintas magnéticas, discos magnéticos y CD-ROM se deberán almacenar en una sala aparte, con acceso por la sala de equipo de cómputo, y deberá estar equipada con todos los dispositivos de seguridad posibles, tanto de condiciones ambientales como de extinción de incendios, con garantía de 10 horas, ya que la información almacenada tiene más valor que el mismo equipo de cómputo.

- Estos cartuchos de cintas magnéticas, discos magnéticos y CD-ROM se deberán almacenar en armarios fabricados exprofeso.

- Materiales adecuados para proteger estructuras metálicas.

- Los espesores que se indican proporcionan suficiente defensa ante un fuego tipo de 3 horas de duración:
  - Mortero o cemento sobre malla metálica o perfiles sin pintar 6 cm.
  - Mortero bastardo sobre malla metálica o perfiles sin pintar 6 cm.
  - Mortero o cemento y vermiculita o perlita sobre malla metálica o perfiles sin pintar 4.75 cm.
  - Placas de hormigón ligero 6 cm.
  - Placas de fibra amianto 6 cm.
  - Ladrillos fabricados con mortero o cemento: macizos, huecos, hormigón sin finos sobre perfiles sin pintar 8 cm.

18. Instalación eléctrica

- Se comprobarán, con el proveedor del equipo de cómputo, los voltajes de trabajo del mismo equipo.
- La tolerancia en tensión no deberá ser mayor de 10% ni menor de 8% de la tensión nominal que especifique el fabricante del equipo de cómputo.
- La tolerancia en frecuencia será de un máximo de ½ Hz.
- La variación de voltaje entre fases no tendrá que ser mayor del 2.5% de la media aritmética de las tres fases.
- Respecto al contenido de armónicas el máximo será inferior al 5% con el equipo desconectado.
- La acometida de energía eléctrica que alimente al equipo de cómputo deberá ser completamente independiente y a ella no se conectará ninguna otra carga, a fin de evitar interferencias. El proveedor del equipo de cómputo deberá dar su visto bueno por escrito.
- La sección de los conductores eléctricos de la acometida deberá calcularse para la potencia consumida por el equipo de cómputo, señalada en las hojas de especificaciones, y deberá considerarse un 50% adicional como margen de seguridad y posible crecimiento. Así se evitará todo riesgo de caída de tensión y podrán preverse futuras ampliaciones del equipo de cómputo.
- La acometida independiente llegará desde el equipo de fuerza ininterrumpible y de ahí se alimentará un tablero de distribución, exclusivo para el equipo de cómputo, que quedará situado en un lugar visible y accesible dentro de la sala del equipo de cómputo.
- Este tablero constará, fundamentalmente, de un interruptor general, voltímetro para tres

fases, indicadores luminosos e interruptores termomagnéticos para cada uno de los circuitos derivados, que corresponderán a los dispositivos que necesiten alimentación directa.

- Cada interruptor termomagnético irá rotulado con el nombre de la máquina que le corresponda.

- En los tableros deberán considerarse espacios libres para, al menos, un 30% adicional de posiciones, a fin de cubrir futuras ampliaciones.

- El interruptor general de este tablero puede ir en serie con uno o varios botones de emergencia distribuidos estratégicamente por la sala. Los circuitos derivados saldrán del tablero general y terminarán, cada uno de ellos, abajo del piso falso, en una caja de conexiones situada en las proximidades de la máquina a la que van a alimentar, es necesario que los conductores eléctricos vayan dentro de tubería del tipo “licuatai”, a fin de evitar los campos electromagnéticos que se producen por el paso de la corriente eléctrica, y que puede generar ruidos o interferencias en los cables de comunicaciones que van del procesador central a los dispositivos periféricos.

- Estos circuitos derivados irán protegidos en mangueras flexibles o bajo tubo traqueal (tubo licuatai).

- Para el cálculo de secciones de estos circuitos se tendrán presentes los consumos parciales indicados en la hoja de especificaciones, que proporciona el proveedor, aunque es aconsejable no colocar nunca conductores de sección inferior a 10 mm^2.

- Las cajas de conexiones bajo el piso falso serán ancladas y aisladas o plastificadas exteriormente por razones de seguridad.

- Cada caja contendrá las demás de tamaño apropiado para las tres fases, neutro (si la alimentación es a 220 volts) y tierra física. Las cajas irán también rotuladas con el número de la máquina a la que alimentan.

- La toma de tierra física será también independiente, con una resistencia total de 3 ohms, que incluirá conductor más electrodo.

- La sección del conductor de la tierra física será igual a una de las fases e irá aislado en todo su recorrido.

- El electrodo estará situado a más de 15 metros de otra toma de tierra física.

- Habrá una red de enchufes o contactos auxiliares monofásicos a 117 volts por toda la sala, sacados de otra alimentación de energía eléctrica no regulada, diferente de la del equipo de cómputo, con objeto de conesctar aspiradoras, pulidoras, etc.

- Es necesario que las terminales, microcomputadoras e impresoras remotas, que se localizan dentro del edificio, fuera de la sala de cómputo, o fuera de él, estén alimentadas por energía eléctrica regulada y cuenten con una alimentación de tierra física, a fin de mantenerlas en operación cuando se presenta una interrupción de energía

eléctrica por la compañía suministradora.

- Es indispensable que la alimentación a los equipos de cómputo sea mediante energía eléctrica regulada; para ello, y dependiendo de las condiciones, deberá considerarse:

  - *Primero:* A través de un sistema de energía ininterrumpible (equipo no-brake con regulador de voltaje), respaldado por un tablero de transferencia y una planta de generación de energía eléctrica para emergencia (PGEEE), que aunque resulta de alto costo nos proporciona continuidad en el servicio.
  - *Segundo:* A través de un regulador de voltaje, el cual puede tener dispositivos que eliminen ciertas armónicas perjudiciales al equipo de cómputo.
  - *Tercero:* Para equipos de cómputo pequeños del tipo PC a través de un multicontacto que permita eliminar armónicas y conectado a un regulador de voltaje individual o de mayor capacidad o conectado a un equipo no-brake con regulador de voltaje.

19. Cálculo de la capacidad de equipos

En esta sección se dan una serie de elementos que permiten calcular, de manera sencilla y práctica, la capacidad de los siguientes equipos:

- Aire acondicionado
- Sistema de fuerza ininterrumpible (SFI o NO-BREAKE o UPS)
- Planta generadora de energía eléctrica para emergencia (PGEEE)

Para el cálculo de la capacidad del equipo de aire acondicionado debemos considerar que la disipación de calor de los equipos de cómputo (BTU/HRA) la proporciona el proveedor; deberá considerarse que 12,000 BTU/hora = 1 TR (TR = Tonelada de refrigeración) para equipos grandes existen en el mercado unidades de 10, 15 y 20 TR.

Para fines prácticos (en la zona metropolitana de la ciudad de México) la disipación de calor generada por personas, iluminación, paredes, techos, pisos, puertas y ventanas, se considera que debe ser de 500 BTU/hora por metro cuadrado de la sala de cómputo, con una altura de 2.70 m (piso falso a falso plafón).

Supongamos que el proveedor nos presenta la siguiente tabla:

Capacidades de dispositivos de cómputo						
Tipo de dispositivo	Número de fases	Número de conductores	Calibre del conductor	Capacidad interruptor en amperes	Consumo en KVA	Disipación BTU/hora
Disposit. 1	1	3	12	15	8	7,000
Disposit. 2	1	3	10	30	11	12,000
Disposit. 3	2	3	12	15	8	22,000
Disposit. 4	1	3	6	30	17	35,000
Disposit. 5	1	3	4	30	23	13,000
Disposit. 6	3	4	12	15	12	9,000
Disposit. 7	2	3	10	30	9	4,000
Disposit. 8	1	3	12	15	8	7,000
Disposit. 9	1	3	14	15	5	9,000
				TOTALES:	**101**	**118,000**

Con los elementos anteriores, considerando también los diagramas unifilares de alimentación eléctrica de páginas anteriores, se deberá calcular:

1)	Capacidad del equipo de aire acondicionado, si la sala de cómputo tiene una superficie de:					
	a) 30 m^2			c) 75 m^2		
	b) 50 m^2			d) 100 m^2		
2)	Calcular la capacidad del sistema de fuerza ininterrumpible (SFI o UPS o no-brake), si:					
	a)	La iluminación total de la sala de cómputo consume:	b)	El equipo contra incendio consume:		
		- Si es de 30 m^2	-- 4 KVA	- Si es de 30 m^2	-- 2 KVA	
		- Si es de 50 m^2	-- 6 KVA	- Si es de 50 m^2	-- 4 KVA	
		- Si es de 75 m^2	-- 8 KVA	- Si es de 75 m^2	-- 5 KVA	
		- Si es de 100 m^2	-- 10 KVA	- Si es de 100 m^2	-- 6 KVA	

3)	Calcular la capacidad de la planta generadora de energía eléctrica de emergencia (PGEEE), si:				
	c)	Contactos, pueden consumir:		d)	Cada Unidad de aire acondicionado
		- Si es de 30 m^2	-- 3 KVA		de 10 TR consume 25 KVA
		- Si es de 50 m^2	-- 5 KVA		considerando todos sus componentes
		- Si es de 100 m^2	-- 7 KVA		eléctricos (compresores,
		- Si es de 150 m^2	-- 9 KVA		bombas, resistencias, etc.)

BIBLIOGRAFÍA

LIBROS

- Maiwald, Eric, ***Fundamentos de Seguridad de Redes***, Segunda Edición, McGraw-Hill, México 2005.
- Map, **Magerit, *Metodología de análisis y Gestión de Riesgos de los Sistemas de Información*.** BOE, 1997.
- Molina, J. M. ***Seguridad, información y poder*.** Incipit, 1994
- Morant, J. L. y otros. ***Seguridad y Protección de la Información*.** Cera, 2001.
- Ribagorda, A. ***Glosario de términos de Seguridad de las T.I.*** Coda, 1997.
- Olguín Romo Heriberto, ***Dirección, organización y administración de centros de Tecnología de Información,*** México, UNAM, Facultad de Ingeniería, 2005.
- López Barrientos, Ma. Jaquelina. ***Fundamentos de Seguridad***, México, UNAM, Facultad de Ingeniería, 2006.

TESIS

- López Nava, Leticia, ***Sistemas de seguridad en computo***, México 1998
- Mendoza Gayosso, Ignacio Ramses, ***Centro de Tecnología de Información de la Facultad de Ingeniería***, México 2006
- Hidalgo Caballero, Juan Carlos, ***Una metodología para la formulación de políticas en seguridad informática***, México 1994
- Camarillo Sandoval, Lourdes Alejandra, ***Servicios de autenticación y control de acceso para un sistema informático***, México 2006
- González Trujillo, Luis Mauricio, ***Elementos de seguridad en informática***, México 2005

ARTÍCULOS

- SARZANA, Carlo. ***Criminalità e tecnologia en Computers Crime***. Rassagna Penitenziaria e Criminologia. Nos. 1-2 Año 1. Roma, Italia. P.53.
- ARTEGA S., Alberto. ***El delito informático: algunas consideraciones jurídicas penales*** Revista de la Facultad de Ciencias Jurídicas y Políticas**.** No. 68 Año 33. Universidad Central de Venezuela.. 1987. Caracas, Venezuela. P. 125-133.

ARTÍCULOS DE INTERNET

- Facultad de Ingeniería, ***Plan Institucional de Desarrollo Informático***, Pagina de la Facultad de Ingeniería, http://www.ingenieria.unam.mx/~pidi/
- Federico García Crespí.,Marco A. Marhuenda García, ***Seguridad en Sistemas de Información,*** Universidad Miguel Hernández de Elche, fecha de ultima actualización: 30 Mayo 2004, http://ulises.umh.es/cc/personal/marco/ssi/default.html
- Patrick O'Callaghan, ***Criptografía y Seguridad de Datos, Control de Acceso***, Universidad Simón Bolivar, fecha de ultima actualización: 12 Junio 2002, http://www.ldc.usb.ve/~poc/Seguridad/acceso.pdf#search='control%20de%20acceso
- Asociación Latinoamericana de Profesionales en Seguridad Informática, A.C, ***Memorias del Foro de Consulta Sobre Derecho e Informática***, Poder Legislativo Federal, fecha de última actualización : Septiembre de 1996, http://www.cddhcu.gob.mx/camdip/foro/jalisco/tipi_del.htm
- Web Hosting, ***Servicios de Seguridad Informática***, Grupo Inter. México, fecha de ultima actualización: Octubre 2007, http://www.inter.org.mx/web_hosting/servicios_seguridad.htm
- Oscar Pérez Cano, ***Seguridad Informática y Seguridad en Redes***, Universidad Iberoamericana, Departamento de Ingeniería Electrónica y de Comunicaciones, fecha de ultima actualización: otoño 2003, http://www.iec.uia.mx/proy/titulacion/proy14/seguridad.htm
- Gunnar Wolf, ***Implementación de seguridad con sistemas operativos y herramientas libres***, Departamento de Seguridad en Cómputo, DGSCA, UNAM FES Iztacala, UNAM, fecha de ultima actualización: 15 de octubre 2003 http://www.gwolf.org/seguridad/impl/impl.html

- Núñez Sandoval Alejandro, ***Estándares de seguridad en la información***, DGSCA, UNAM, fecha de ultima actualización: febrero 2005 http://www.enterate.unam.mx/Articulos/2005/febrero/seguridad.htm

- Yagüe y Maña, ***Un modelo de control de acceso basado en la Semántica***, RedIRIS, fecha de última actualización: enero 2005 http://www.rediris.es/rediris/boletin/66-67/ponencia15.pdf#search='modelos%20de%20control%20de%20acceso'

- Ramos Suarez, Fernando ***Eficacia Jurídica de una Transacción Electrónica. La Figura del No Repudio***, Revista de Derecho Informático No. 012, fecha de ultima actualización, Julio del 1999 http://www.alfa-redi.org/rdi-articulo.shtml?x=300

- Celorio Suárez Mariana, ***UNAM-CERT organismo especializado en seguridad en cómputo***, Departamento de Seguridad en Cómputo, DGSCA UNAM, fecha de ultima actualización, Noviembre del 2002, http://www.enterate.unam.mx/Articulos/dos/noviembre/unamcert.htm

- Cao Avellaneda Javier, ***Traducción libre, con fines didácticos, de ISO 27001 e ISO 27002 al español***, ISO 27001, fecha de ultima actualización, 05 de septiembre del 2007, http://www.iso27000.es

- Cancelado González Alberto, ***Sistema de Administración de Riesgos en Tecnología Informática***, Gestiopolis, fecha de última actualización, Noviembre 2003. http://www.gestiopolis1.com/recursos/documentos/archivodocs/degerencia1/sisrisinfo.zip

- ***Know Your Enemy: Honeynets*****,** Honeynet.org, fecha de última actualización 31 May, 2006, http://www.honeynet.org/papers/honeynet/index.html

- ***Seguridad Informática*****,** Sección de Estudios de Posgrado e Investigación Maestría en Informática UPIICSA, IPN**,** http://www.upiicsa.ipn.mx/maestrias/Seguridad Informatica/