Enfoque forense de la seguridad informática en la empresa privada

Autor: Rafael David García Zamora

Tesina presentada para obtener el título de:
Lic. En Sistemas computarizados [sic]

Nombre del asesor:
Sergio Francisco Barraza Ibarra

UNIVERSIDAD VASCO DE QUIROGA

FACULTAD DE SISTEMAS COMPUTARIZADOS

ENFOQUE FORENSE DE LA SEGURIDAD INFORMÁTICA EN LA EMPRESA PRIVADA

TESINA

QUE PARA OBTENER EL TÍTULO DE:

LICENCIADO EN SISTEMAS COMPUTARIZADOS

PRESENTA

Lic. RAFAEL DAVID GARCIA ZAMORA

ASESORES DE TESINA:

ING. Y M.A. SERGIO FRANCISCO BARRAZA IBARRA

ING. VICTOR MANUEL PINEDA ALMANZA

MORELIA, MICH., MARZO 2004.

AGRADECIMIENTOS

A todas aquellas personas que han estado en esta tesina

A mis profesores que fueron los que me brindaron de sus conocimientos en el ámbito profesional, también gracias a ellos se realizo todo lo que debía hacerlo bien.
Todas sus enseñanzas.
Mis conocimientos asi como la forma de ver la vida ha hecho posible la terminación de esta tesina.

A los Ing. Sergio Francisco Barraza Ibarra, al Ing. Víctor Pineda Almanza y al Ing. Miguel Ángel Álvarez Martínez. con los cuales pude consultar todas mis dudas y aclaraciones.
Así como mis ideas que iban saliendo para formar parte de esta tesina.

A mis padres que gracias a ellos estoy concluyendo mi tesina. Que han estado conmigo para brindarme todo tipo de apoyo y respetando mis decisiones confiando en mi.

Gracias a todos ustedes por confiar en mi.

INDICE

JUSTIFICACIÓN

Con el pasar de los años la información se ha visto comprometida los datos de los sistemas informáticos están en constante peligro por varias causas: errores de los usuarios o ataques intencionados o fortuitos. Pueden producirse accidentes y ciertas personas con intención de atacar el sistema pueden obtener acceso al mismo e interrumpir los servicios, inutilizar los sistemas, alterar, suprimir o robar información.

Objetivo General

El Presente trabajo de investigación tiene como la finalidad auxilar a los profesionales de la seguridad Informática a desarrollar las estrategias para proteger la disponibilidad, integridad y confidencialidad de los datos de los sistemas informáticos de las organizaciones.

Objetivos Particulares

- Crear conciencia en los usuarios y administradores informáticos sobre como se debe de asegurar la información que hoy en dia es considerada un activo valioso de las empresas.
- Tomar las medidas necesarias para evitar que la información de acuerdo a su contenido confidencial sea utilizada por una o varias personas ajenas a la organización.
- Considerar la analogía al momento de establecer políticas de seguridad que sea como crear un contrato laboral que implique un contrato de resguardo de la información.
- Establecer los lineamientos para de esta manera tener seguridad plena de quien este manipulado la información sea una persona competente, de igual forma se pretende saber lo que los empleados hacen con el equipo en sus horas laborales así asegurar que el personal esta realizando la labor por la cual fue contratado.

INTRODUCCIÓN

"Ser lo que soy, no es nada sin la Seguridad"'. Sin duda W. Shakespeare (1564-1616) tenía un concepto más evolucionado de la seguridad que sus contemporáneos del siglo XV y quizás también que algunos de los nuestros.

La meta es ambiciosa. La seguridad como materia académica no existe, y es considerada por los "estudiosos" como una herramienta dentro del ámbito en que se la estudia: relaciones internacionales-nacionales, estudios de riesgo, prevención de crímenes y pérdidas, etc. Muchos sostienen que es una teoría tan amplia, compleja y abstracta como la pobreza, la belleza o el amor; y ni siquiera arriesgan su definición.

El amplio desarrollo de las nuevas tecnologías informáticas está ofreciendo un nuevo campo de acción a conductas antisociales y delictivas manifestadas en formas antes imposibles de imaginar, ofreciendo la posibilidad de cometer delitos tradicionales en formas no tradicionales.

El motivo del presente es desarrollar un estudio completo del estado actual y futuro posible de Seguridad Informática, que continuamente se pone sobre el tapete y en realidad se conoce muy poco; se suele manejar con el amarillismo de los medios no especializados, dificultando esto su accionar y colocando en tela de juicio el arduo trabajo de los especialistas. También intentaré brindar un completo plan de estrategias y metodologías, que sin bien no brindan la solución total (como muchos prometen), podrá cubrir parte del "'agujero" que hoy se presenta al hablar de Seguridad Informática.

La mayoría del mundo informático desconoce la magnitud del problema con el que se enfrenta y, generalmente no se invierte ni el capital humano ni económico necesario para prevenir, principalmente, el daño y/o pérdida de la información que, en última instancia es el Conocimiento con que se cuenta

Paradójicamente, en el mundo informático, existe una demanda constante y muy importante que está esperando a que alguien los atienda.

1.1 EVOLUCIÓN DEL TERMINO SEGURIDAD

"La seguridad es una necesidad básica estando interesada en la prevención de la vida y las posesiones es tan antigua como ella"

Se sabe que los primitivos, para evitar amenazas, reaccionaban con los mismos métodos defensivos de los animales: luchando o huyendo, para eliminar o evitar la causa. Así la pugna por la vida se convertía en una parte esencial y los conceptos de alertar, evitar, detectar, alarmar y reaccionar ya eran manejados por ellos.

Como todo concepto, la Seguridad se ha desarrollado y ha seguido una evolución dentro de las organizaciones sociales. La sociedad se conformó en familias, y esto se convirtió en un elemento limitante par huir. Se tuvieron que concebir nuevas estrategias de intimidación y disuasión para convencer al atacante que las pérdidas eran inaceptables contra las posibles ganancias.

La primera evidencia de una cultura y organización en seguridad "'madura" aparece en los documentos de la antigua Roma Imperial y Republicana.

El próximo paso de la Seguridad fue la especialización. Así nace la Seguridad Externa (aquella que se preocupa por la amenaza de entes externos hacia la organización); y la seguridad interna (aquella preocupada por las amenazas de nuestra organización con la organización misma). De estas dos se pueden desprender la seguridad privada y la publica al aparecer el estado y depositar su confianza en las fuerzas armadas.

La seguridad moderna se origino con la revolución industrial para combatir delitos y movimientos laborales, tan comunes en aquella época. Finalmente, un teórico y pionero del Management, Henry Fayol en 1919 identifica la seguridad como una de las funciones empresariales, luego de la técnica, comercial, financiera, contable y directiva.

Al definir el objetivo de la seguridad Fayol dice "salvaguardar propiedades y personas contra el robo, fuego o inundación contrarrestar huelgas y felonías, y de esta forma ampliada todos los disturbios sociales que puedan poner en peligro el progreso e incluso la vida del negocio. Es generalmente hablando, todas las medidas para conferir la requerida paz y tranquilad al personal.

Las medidas de seguridad a las que se refería Farol, solo se refería a los medios físicos de la instalación, ya que el mayor activo era justamente ese: los equipos, ni siquiera el empleado. Con la aparición de los "cerebros electrónico" esta mentalidad se mantuvo, por que ¿Quién seria capaz de entender estos complicados aparatos como para poner en peligro la integridad de los datos por ellos utilizados?

Hoy, la seguridad, desde el punto de vista legislativo, esta en manos de los políticos, a quienes les toca decidir sobre su importancia, los delitos en que se pueden incurrir, y el respectivo castigo, se correspondiera. Este proceso ha conseguido importantes logros en las áreas de prevención del crimen, terrorismo y riesgo más que en el pensamiento general sobre la seguridad.

En cambio desde el punto de vista empresarial, la seguridad esta en manos de la dirección de las organizaciones y, en última instancia, en cada uno de nosotros y en nuestro grado de concientización respecto a la importancia de la información y el conocimiento en este nuevo milenio.

1.2 De que estamos hablando

Conceptos como Seguridad son borrosos o su definición en el área empresarial se maneja con cierto grado de incertidumbre teniendo distinto significado para distintas empresas y personas. Esto tiene la peligrosa consecuencia de que la función de seguridad empresarial puede ser frecuentemente etiquetada como inadecuada o negligente, haciendo imposible a los responsables justificar sus técnicas ante reclamos basados en ambigüedades de conceptos y definiciones.

Para dar una respuesta satisfactoria es necesario eliminar la incertidumbre y distinguir entre la seguridad filosófica y la operacional o práctica.

Como se sabe los problemas nunca se resuelven: la energía del problema no desaparece, sólo se transforma y la "solución" estará dada por su transformación en problemas diferentes, más pequeños y aceptables. Por ejemplo: la implementación de un sistema informático puede solucionar el problema de velocidad de procesamiento pero abrirá problemas como el de personal sobrante o reciclable. Estos, a su ves, descontentos pueden generar un problema de seguridad interno.

En el problema planteado pueden apreciarse tres figuras:

1. El poseedor del valor: **Protector.**
2. Un aspirante a poseedor: **Competidor-Agresor**
3. Un elemento a proteger: **Valor**

Luego, la Seguridad se definirá como:
"La interrelación dinámica (competencia) entre el agresor y el protector para obtener (o conservar) el valor tratado, enmarcada por la situación global."

Algunas aclaraciones:

1. El protector no siempre es el poseedor de valor.
2. El agresor no siempre es el aspirante a poseedor.
3. Ambas figuras pueden ser delegadas a terceros por el cambio de otro valor, generalmente dinero.
4. El valor puede no ser algo concreto. Por ejemplo se podría querer cuidar el honor, la intimidad, el conocimiento, etc.
5. La situación global indica que no será lo mismo el robo de un comercio en Argentina que en Andorra en donde sus habitantes se ven obligados a robar para subsistir.

Los competidores se pueden subdividir en:

• Competidor Interno: es aquel que piensa que el interés de la organización está por encima de sus intereses y, por lo tanto, actúa para sobreponer su interés personal, provocando daños a la organización.

• Competidor Externo: es aquel que actúa para arrebatar al poseedor lo que para él significa un valor empresarial o personal (clientes, mercado, información, etc.).

La seguridad en un problema de antagonismo y competencia Si no existe un competidor – amenaza el problema no es de seguridad.

En el plano social, comercial e industrial hemos evolucionado técnica y científicamente desde una era primitiva agrícola a una era postmoderna tecnológica, pero utilizando los mismos principios (e inclusos inferiores) a la época de las cavernas en el ambiente virtual:

No es mi interés en el presente texto iniciar mis argumentaciones explicando la evolución y cambios que ha causado la última de las tres grandes revoluciones de la humanidad, la revolución de la era de la información, ('Tercera Ola"); que sigue a las anteriores revoluciones agrícola e industrial. Pero sí está en mi interés demostrar en que se nos crea un nuevo problema, el de la Seguridad Informática. Y también es mi interés demostrar que ella, como tal, para las organizaciones y empresas, todavía no existe.

Este problema será solucionado satisfaciendo las necesidades de comprensión del concepto "'Seguridad" y "'Sistema Informático" en torno de alguien (organización o particular) que gestiona información. Para esto es necesario acoplar los principios de Seguridad expuestos en un contexto informático y viceversa. En definitiva los expertos en seguridad y los expertos en informática deben interactuar ínter disciplinariamente para que exista Seguridad Informática.

En la presente, cada vez que se mencione Información se estará haciendo referencia a la Información que es procesada por un Sistema Informático; definiendo este último como el "conjunto formado por las personas, computadoras (hardware y software), papeles, medios de almacenamiento digital, el entorno donde actúan y sus interacciones."

Contrario a lo que se piensa, este concepto no es nuevo y nació con los grandes centros de cómputos. Con el pasar de los años, y como se sabe, las computadoras pasaron de ser grandes monstruos, que ocupaban cuartos enteros, a pequeños elementos de trabajos perfectamente ubicables sobre un escritorio de oficina. En este proceso de digitalización y miniaturización llamado "'downsizing" la característica más importante que se perdió fue la seguridad.

Los especialistas de Seguridad Informática de hoy se basan en principios de aquellos antiguos MainFrames (grandes computadoras). Seguridad que aun no existe en México.

1.2.1 análisis del objetivo de la seguridad Informática

Para comenzar el análisis de la Seguridad Informática se deberá conocer las características de lo que se pretende proteger: **la Información.**

Así, definimos Dato como "'la unidad mínima con la que compone cierta información. Datum es una palabra latina, que significa "'lo que se da"
La Información es una agregación de datos que tiene un significado específico más allá de cada uno de éstos", y tendrá un sentido particular según como y quien la procese.
Establecer el valor de la información es algo totalmente relativo, pues constituye un recurso que, en muchos casos, no se valora adecuadamente debido a su intangibilidad, cosa que no ocurre con los equipos, las aplicaciones y la documentación.
Existe Información que debe o puede ser pública: puede ser visualizada por cualquier persona (por ejemplo índice de analfabetismo en un país); y aquella que debe ser privada: sólo puede ser visualizada por un grupo selecto de personas que trabaja con ella (por ejemplo antecedentes médicos). En esta última debemos maximizar nuestros esfuerzos para preservarla de ese modo reconociendo las siguientes características en la Información:

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

La Integridad de la Información es la característica que hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada para posteriores controles o auditorias. Una falla de integridad puede estar dada por anomalías en el hardware, software, virus informáticos y/o modificación por personas que se infiltran en el sistema.

La Disponibilidad u Operatividad de la Información es su capacidad de estar siempre disponible para ser procesada por las personas autorizadas. Esto requiere que la misma se mantenga correctamente almacenada con el hardware y el software funcionando perfectamente y que se respeten los formatos para su recuperación en forma satisfactoria.

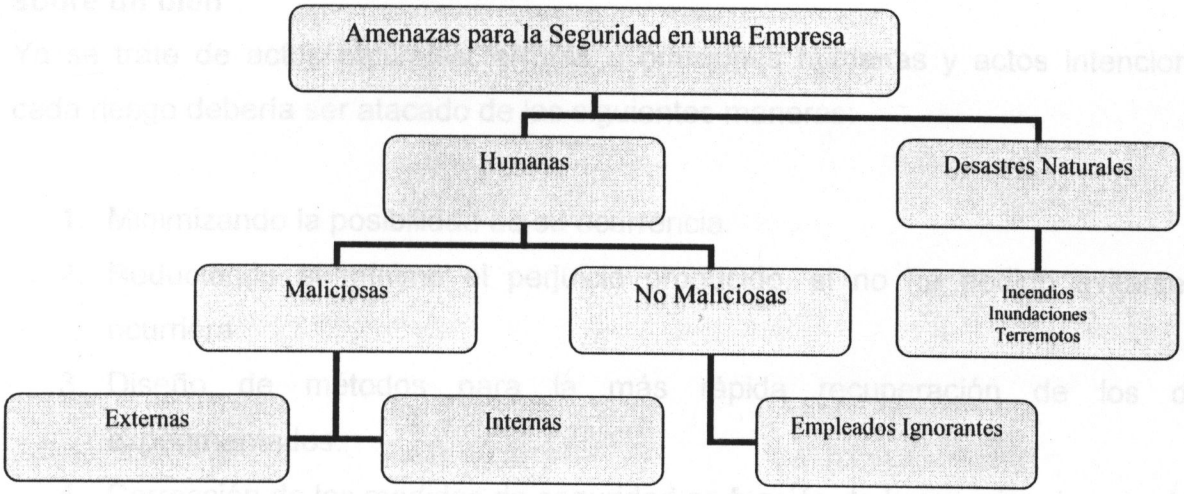
La Privacidad o Confidencialidad de la Información es la necesidad de que la misma sólo sea conocida por personas autorizadas. En casos de falta de confidencialidad, la Información puede provocar severos daños a su dueño (por ejemplo conocer antecedentes médicos de una persona) o volverse obsoleta (por ejemplo: los planes de desarrollo de un producto que se "filtran" a una empresa competidora, facilitarán a esta última desarrollar un producto de características semejantes).

El Control sobre la información permite asegurar que sólo los usuarios autorizados pueden decidir cuando y como permitir el acceso a la misma.

La Autenticidad permite definir que la información requerida es válida y utilizable en tiempo, forma y distribución. Esta propiedad también permite asegurar el origen de la información, validando el emisor de la misma, para evitar suplantación de identidades.
Adicionalmente pueden considerarse algunos aspectos adicionales, relacionados con los anteriores, pero que incorporan algunos aspectos particulares:

- **Protección a la Réplica:** mediante la cual se asegura que una transacción sólo puede realizarse una vez, a menos que se especifique lo contrario. No se deberá poder grabar una transacción para luego reproducirla, con el propósito de copiar la transacción para que parezca que se recibieron múltiples peticiones del mismo remitente original.
- **No Repudio:** mediante la cual se evita que cualquier entidad que envió o recibió información alegue, ante terceros, que no la envió o recibió.
- **Consistencia:** se debe poder asegurar que el sistema se comporte como se supone que debe hacerlo ante los usuarios que corresponda.
- **Aislamiento:** este aspecto, íntimamente relacionado con la Confidencialidad, permite regular el acceso al sistema, impidiendo que personas no autorizadas hagan uso del mismo.
- **Auditoria:** es la capacidad de determinar qué acciones o procesos se están llevando a cabo en el sistema, así como quién y cuando las realiza.

Cabe definir **Amenaza**, en el entorno informático, como cualquier elemento que comprometa al sistema.



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

- La Prevención (antes): mecanismos que aumentan la seguridad (o fiabilidad) de un sistema durante su funcionamiento normal. Por ejemplo el cifrado de información para su posterior transmisión.
- La Detección (durante): mecanismos orientados a revelar violaciones a la seguridad. Generalmente son programas de auditoria..
- La Recuperación (después): mecanismos que se aplican, cuando la violación del sistema ya se ha detectado, para retomar éste a su funcionamiento normal. Por ejemplo recuperación desde las copias de seguridad (backup) realizadas..

Las preguntas que se hace un técnico en sistemas de información ante un problema de seguridad, normalmente, están relacionadas con medidas defensivas que no solucionan un problema dado, sólo lo transforma o retrasa. La amenaza o riesgo sigue allí y las preguntas que este técnico debería hacerse son:

- ¿Cuánto tardará la amenaza en superar la "solución" planteada?
- ¿Cómo se hace para detectarla e identificarla a tiempo?
- ¿Cómo se hace para neutralizarla'7

Para responderlas definiremos **Riesgo** como **"la proximidad o posibilidad de daño sobre un bien".**

Ya se trate de actos naturales, errores u omisiones humanas y actos intencionales, cada riesgo debería ser atacado de las siguientes maneras:

1. Minimizando la posibilidad de su ocurrencia.
2. Reduciendo al mínimo el perjuicio producido, si no ha podido evitarse que ocurriera.
3. Diseño de métodos para la más rápida recuperación de los daños experimentados.
4. Corrección de las medidas de seguridad en función de la experiencia recogida.

Luego, el **Daño** es el resultado de la amenaza; aunque esto es sólo la mitad del axioma. El daño también es el resultado de la no – acción, o acción defectuosa, del protector. El daño puede producirse porque el protector no supo identificar adecuadamente la amenaza y, si lo hizo, se impusieron criterios comerciales por encima de los de seguridad. De allí que se deriven responsabilidades para la amenaza (por supuesto) pero también para la figura del protector.

Luego, el protector será el encargado de detectar cada una de las Vulnerabilidades (debilidades) del sistema que pueden ser explotadas y empleadas, por la amenaza, para comprometerlo. También será el encargado de aplicar las Contramedidas (técnicas de protección) adecuadas.

La Seguridad indicara el índice en que un Sistema Informático está libre de todo peligro, daño o riesgo. Esta característica es muy difícil de conseguir (según los especialistas imposible) en un 100% por lo que sólo se habla de Fiabilidad y se la define como "la probabilidad de que un sistema se comporte tal y como se espera de él", y se habla de Sistema Fiable en vez de sistema seguro.

Luego para garantizar que un sistema sea fiable se deberá garantizar las características ya mencionadas de Integridad, Operatividad, Privacidad, Control y Autenticidad. Se deberá conocer "'qué es lo que queremos proteger", "de quién lo queremos proteger", "cómo se puede lograr esto legislativa y técnicamente"; para luego concluir con la

formulación de estrategias adecuadas de seguridad tendientes a la disminución de los riesgos.

Comprender y conocer de seguridad ayudará a llevar a cabo análisis sobre los Riesgos, las Vulnerabilidades, Amenazas y Contramedidas; evaluar las ventajas o desventajas de la situación; a decidir medidas técnicas y tácticas metodológicas, físicas, e informáticas, en base de las necesidades de seguridad.

Es importante remarcar que cada unas de estas técnicas parten de la premisa de que no existe el 100% de seguridad esperado o deseable en estas circunstancias (Por ejemplo: al cruzar la calle ¿estamos 100% seguros que nada nos pasará).

1.2.2 sistema de seguridad

En los siguientes capítulos se estudiarán las distintas funciones que se deben asegurar en un sistema informático.

1. **Reconocimiento:** cada usuario deberá identificarse al usar el sistema y cada operación del mismo será registrada con esta identificación. En este proceso se quiere conseguir que no se produzca un acceso y/o manipulación indebida de los datos o que en su defecto, esta quede registrada.
2. **Integridad:** un sistema integro es aquel en el que todas las partes que lo constituyen funcionan en forma correcta y en su totalidad.
3. **Aislamiento:** Los datos utilizados por un usuario deben ser independientes de los de otro física y lógicamente (usando técnicas de ocultación y/o compartimiento). También se debe lograr independencia entre los datos accesibles y los considerados críticos.
4. **Auditabilidad:** procedimiento utilizado en la elaboración de exámenes, demostraciones, verificaciones o comprobaciones del sistema. Estas comprobaciones deben ser periódicas y tales que brinden datos precisos y aporten confianza a la dirección. Deben apuntar a contestar preguntas como:

   - ¿El uso del sistema es adecuado?
   - ¿El sistema se ajusta a las normas internas y externas vigentes?
   - ¿Los datos arrojados por el sistema se ajustan a las expectativas creadas?

- ¿Las transacciones realizadas por el sistema pueden ser registradas adecuadamente?
- ¿Contienen información referente al entorno: tiempo, lugar, autoridad, recurso, empleado, etc.?

5. **Controlabilidad:** todos los sistemas y subsistemas deben estar bajo control permanente.
6. **Recuperabilidad:** en caso de emergencia, debe existir la posibilidad de recuperar los recursos perdidos o dañados.
7. **Administración y Custodia:** la vigilancia nos permitirá conocer, en todo momento, cualquier suceso, para luego realizar un seguimiento de los hechos y permitir una realimentación del sistema de seguridad, de forma tal de mantenerlo actualizado contra nuevas amenazas.

1.2.3 De quien debemos protegernos

Se llama Intruso o Atacante a la persona que accede (o intenta acceder) sin autorización a un sistema ajeno, ya sea en forma intencional o no.

Los tipos de Intrusos podríamos caracterizarlos desde el punto de vista del nivel de conocimiento, formando una pirámide.

1. Clase A: el 80% en la base son los nuevos intrusos que bajan programas de Internet y prueban, están jugando , son pequeños grupos que se juntan y dicen vamos a probar o ver que pasa si ... .

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

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

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

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

1.2.4 Qué debemos proteger

En cualquier sistema informático existen tres elementos básicos a proteger: el **hardware, el software y los datos.**

Por hardware entendemos el conjunto de todos los sistemas físicos del sistema informático: CPU, cableado, impresoras, CD-ROM, cintas, componentes de comunicación.

El software son todos los elementos lógicos que hacen funcional al hardware: sistema operativo, aplicaciones, utilidades.

Entendemos por datos al conjunto de información lógica que maneja el software y el hardware: bases de datos, documentos, archivos.

Además, generalmente se habla de un cuarto elemento llamado los consumibles; que son los aquellos que se gastan o desgastan con el uso continuo: papel, toner, tinta, cintas magnéticas, disquetes.

De los cuatro, los datos que maneja el sistema serán los más importantes ya que son el resultado del trabajo realizado. Si existiera daño del hardware, software o de los elementos fungibles, estos pueden adquirirse nuevamente desde su medio original; pero los datos obtenidos en el transcurso del tiempo por el sistema son imposibles de recuperar: hemos de pasar obligatoriamente por un sistema de copias de seguridad, y aún así es difícil de devolver los datos a su forma anterior al daño.

Para cualquiera de los elementos descriptos existen multitud de amenazas y ataques que se los puede clasificar en:

Ataques Pasivos: el atacante no altera la comunicación, sino que únicamente la "escucha" o monitoriza, para obtener información que está siendo transmitida. Sus objetivos son la intercepción de datos y el análisis de tráfico. Generalmente se emplean para:

- Obtención del origen y destinatario de la comunicación, a través de la lectura de 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.

Ataques Activos: estos ataques implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos. Generalmente son realizados por Hackers, piratas informáticos o intrusos remunerados y se los puede subdividir en cuatro categorías:

Interrupción: si hace que un objeto del sistema se pierda, quede inutilizable o no disponible.

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

Con demasiada frecuencia se cree que los piratas son lo únicos que amenazan nuestro sistema, siendo pocos los administradores que consideran todos los demás riesgos analizados en el presente.

1.2.5 Objetivos de la Seguridad Informática

Un sistema de información con una base de seguridad débil llegará a verse comprometido. Algunos ejemplos de esta situación son la pérdida, daño o revelación de datos, la pérdida de disponibilidad de los sistemas, etcétera. En función del sistema de información y de la gravedad del daño, los resultados pueden variar desde el desconcierto, a la pérdida de beneficios o, incluso, a riesgos graves para la salud.

Los objetivos principales de la seguridad son garantizar:

- La confidencialidad de los datos. Sólo las personas autorizadas deben poder ver la información.

- La integridad de los datos. Todos los usuarios autorizados deben estar seguros de que los datos que obtienen son precisos y de que no fueron modificados de forma inadecuada.
- La disponibilidad de los datos. Los usuarios autorizados deben poder tener acceso a la información que necesiten, en cualquier momento.

La seguridad se puede dividir en cinco requisitos o principios. Todos estos principios son igualmente importantes para garantizar la confidencialidad, integridad y disponibilidad de los datos. Los principios son los siguientes:

- Identificación. La identificación está relacionada con los nombres de los usuarios y con la forma en que éstos se identifican en un sistema informático.
- Autenticación. La autenticación es todo aquello que tiene que ver con contraseñas, tarjetas inteligentes, biometría, etcétera. Es el método que utilizan los usuarios para demostrar al sistema que realmente son quienes pretenden.
- Control de acceso (también llamado autorización). El control de acceso se ocupa del acceso y los privilegios concedidos a los usuarios para que puedan realizar determinadas funciones en un sistema informático.
- Confidencialidad. La confidencialidad está relacionada con el cifrado. Los mecanismos de confidencialidad garantizan que sólo las personas autorizadas puedan ver los datos almacenados o que recorren la red.
- Integridad. La integridad tiene que ver con las sumas de comprobación y las firmas digitales. Los mecanismos de integridad garantizan que los datos no se pierden, dañan o cambian mientras se transmiten a través de la red.

2. CONCEPTOS BÁSICOS

2.1 Que es la Informática Forense

Los investigadores forenses en informática, profesionales que contando con un conocimiento de los fenómenos técnicos en informática, son personas preparadas para aplicar procedimientos legales y técnicamente válidos para establecer evidencia en situaciones donde se vulneran o comprometen sistemas, utilizando métodos y procedimiento científicamente probados y claros que permitan establecer posibles hipótesis sobre el hecho y contar con la evidencia requerida que sustente dichas hipótesis.

Esta se ocupa de investigar los intentos de intrusión a un sistema una ves que estos ya se han producido, para tratar de averiguar las causas o los autores y los daños que han conllevado.

La idea principal en este tipo de análisis es contar completamente con todo el apoyo del cliente y depende exclusivamente del manejo inmediato que el cliente le haya dado al incidente, ya que al ingresar al sistema o apagar el servidor se puede perder información valiosa para análisis posteriores.

2.2 Objetivos de la Informática Forense

La informática forense tiene 3 objetivos, a saber:

1. La compensación de los daños causados por los criminales o intrusos.
2. La persecución y procesamiento judicial de los criminales.
3. La creación y aplicación de medidas para prevenir casos similares.

Estos objetivos son logrados de varias formas, entre ellas, la principal es la Recolección de evidencia.

2.3 Sabotaje informático

Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema.

2.4 Virus

Es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Un virus puede ingresar en un sistema por conducto de una pieza legitima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya.

2.5 Gusanos

Se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus: por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco pare que transfiera continuamente dinero a una cuenta ilícita.

2.6 Bomba lógica o cronológica

Exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro. Ahora bien, al revés de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño. Su detonación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde se halla la bomba.

2.7 Acceso no autorizado a Sistemas o Servicios

Por motivos diversos: desde la simple curiosidad, como en el caso de muchos piratas informáticos (Hacker) hasta el sabotaje o espionaje informático.

2.8 Piratas informáticos o Hackers

Persona Que tiene un conocimiento profundo acerca del funcionamiento de redes y que puede advertir los errores y fallas de seguridad del mismo. Al igual que un craker busca acceder por diversas vías a los sistemas informáticos pero con fines de protagonismo.

2.9 Reproducción no autorizada de programas informáticos

Esta puede entrañar una perdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas. Al respecto, consideramos, que la reproducción no autorizada de programas informáticos no es un delito informático debido a que el bien jurídico a tutelar es la propiedad intelectual.

2.10 Gurus

Son considerados los maestros y los encargados de "formar" a los futuros Hacker generalmente no están activos pero son identificados y reconocidos por la importancia de sus hackeos, de los cuales solo enseñaban las técnicas básicas.

2.11 Lamer O SCRIPT - KIDDERS

Son aficionados Jactosos, prueban todos los programas (con el titulo "como ser un hacker en 21 días" que llegan a sus manos. Generalmente son los responsables de soltar virus y bombas lógicas en la red solo con fines de molestar y que otros se enteren que usa tal o cual programa. Son aprendices que presumen de lo que no son aprovechando los conocimientos hacker y lo penen en practica sin saber.

2.12 CopyHacker

Literalmente son falsificadores sin escrúpulos que comercializan todo lo copiado (robado)

2.13 Newbie

Son novatos del hacker. Se introducen en sistemas de fácil acceso y fracasan en muchos intentos, solo con el objetivo de aprender las técnicas que pueden hacer de el, un hacker reconocido

2.14 Wannaber

Es aquella persona que desea se un hacker pero estos consideran que su coeficiente no da para tal fin. A pesar de su actitud positiva difícilmente consigue avanzar en sus propósitos.

3. AMENAZAS HUMANAS.

Existen muchos estudios que hablan sobre por que un buen empleado llega a traicionar a la empresa y que llevan a una persona a cometer un delito informático pero sean cuales sean, estos motivos existen y deben de prevenirse y evitarse. Suele decirse que todos tenemos un precio dinero, chantaje, extorsión, factores psicológicos, entre otros motivos que nos pueden hacer que un buen empleado que tenga contacto con información de carácter confidencial sea capas de vender o robar esta información o simplemente proporcionarla a terceros.

Es realmente preocupante que una persona que trabaje con el administrador, el programador o el encargado de una maquina conoce perfectamente el sistema, sus puntos fuertes y débiles; de manera que un ataque realizado por esta persona podrá ser mas directo y difícil de detectar y mas efectivo que el que un atacante externo pueda realizar.

Las personas que cometen los "Delitos informáticos" son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, 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 sistema Informatizados, aún cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

3.1.1 Personal Interno

Las amenazas a la seguridad de un sistema, provenientes del personal del propio sistema informático, rara vez es tomada en cuenta porque se supone que todo el personal que labora en esta área es personal de confianza muchas veces inexistente. Generalmente estos ataques son accidentes por desconocimiento o inexistencia de las normas básicas de seguridad; pero también pueden ser del tipo intencional.

Es de destacar que un simple electricista puede ser mas dañino que el mas peligrosos de los Hacker, ya que un corte de energía no esperado puede causar en desastre en los datos del sistemas. Al evaluar la situación, se vera que aquí el daño no es

intencionado pero ello no esta en discusión; el daño existió y esto es lo que comprende a esta tesina sobre seguridad informática.

3.1.2 El Ex – Empleado

Esta persona esta especialmente interesado en violar la seguridad de nuestra empresa, sobre todo aquellos que han sido despedidos y no han quedado conformes; o bien aquellos que han renunciado por pasar a trabajar en la competencia. Generalmente se trata de personas descontentas con la organización que conocen a la perfección la estructura del sistema y tienen los conocimientos necesarios como para causar cualquier tipo de daño también han existido casos donde el Ex - Empleado deja Bombas Lógicas que "EXPLOTAN" tiempo después de marcharse en la investigación hay muchos caso como este.

3.1.3 Los Curiosos

Suelen los atacantes mas habituales de los sistemas son los típicos que te tumban la red a cada rato o que por querer bajar su música saturan la red. Estas personas tienen un alto interés en las nuevas tecnologías, pero a un no tienen los conocimientos ni la experiencia básica para considerarlos hacker o crakers (podrían ser NewBies). En la mayoría de los casos son estudiantes intentando penetrar servidores de su facultad o empleados consiguiendo privilegios para obtener información de carácter personal. Generalmente no se trata de ataques de daño pero afectan el entorno de fiabilidad hay que estar observando a este tipo empleados ya que su conducta puede no ser peligrosa pero si de cuidado.

3.1.4 El Terrorista

Bajo esta definición se engloba a cualquier persona que ataca a nuestro sistema para causar un daño de cualquier índole en el; y no solo a la persona que coloca bombas o quema automóviles. Son ejemplos concretos de este tipo, tales como ataques de modificación en los cuales el intruso no roba la información solo la modifica a su conveniencia o para esto se puede tipificar como terrorismo informático o espionaje industrial.

3.1.5 Intrusos remunerados

Este es, sin duda uno de los ataques de mas peligrosos, a un que también el menos habitual en otros países pero en México creo que es uno de los mas comunes. Se trata de Crakers o piratas con grandes conocimientos y experiencia, pagados por una tercera parte para robar "secretos" ya saben códigos fuentes, bases de datos, clientes, información confidencial, diseños entre otros.

3.2. Maliciosas

Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que lo que los diferencia entre sí es la naturaleza de los cometidos. De este forma, la persona que "entra" en un sistema informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que desvía fondos de las cuentas de sus clientes.

3.2.1 Sujeto Activo

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 aducen 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.

Sin embargo, tendiendo en cuenta las características ya mencionadas de las personas que cometen los "delitos informáticos", estudiosos en la materia los han catalogado como "delitos de cuello blanco" término introducido por primera vez por el criminológico norteamericano Edwin Sutherland en el año de 1943.

Efectivamente, este conocido criminólogo señala un sin número de conductas que considera como "delitos de cuello blanco", aún cuando muchas de estas conductas no están tipificadas en los ordenamientos jurídicos como delitos, y dentro de las cuales cabe destacar las "violaciones a las leyes de patentes y fábrica de derechos, el mercado negro, el contrabando en las empresas, la evasión de impuestos, las quiebras fraudulentas, corrupción de altos funcionarios entre otros".

Asimismo, este criminológico estadounidense dice que tanto la definición de los "delitos informáticos" como las de los "delitos de cuello blanco" no es de acuerdo al interés protegido, como sucede en los delitos convencionales sino de acuerdo al sujeto activo que los comete. Entre las características en común que poseen ambos delitos tenemos que: el sujeto activo del delito es una persona de cierto status socioeconómico, su comisión no puede explicarse por pobreza ni por mala habitación, ni por carencia de recreación, ni por baja educación, ni por poca inteligencia, ni por inestabilidad emocional.

Hay dificultad para elaborar estadísticas sobre ambos tipos de delitos. La "cifra negra" es muy alta; hay dificultades para descubrirlo y sancionarlo, en razón del poder económico de quienes lo cometen, pero los daños económicos son altísimos; existe una gran indiferencia de la opinión pública sobre los daños ocasionados a la sociedad; la sociedad no considera delincuentes a los sujetos que cometen este tipo de delitos, no los segrega, no los desprecia, ni los desvaloriza, por el contrario, el autor o autores de este tipo de delitos se considera a sí mismos "respetables" otra coincidencia que tiene estos tipos de delitos es que, generalmente, son objeto de medidas o sanciones de carácter administrativo y no privativos de la libertad.

Por nuestra parte, consideramos que a pesar de que los "delitos informáticos" no poseen todas las características de los "delitos de cuello blanco", si coinciden en un número importante de ellas, aunque es necesario señalar que estas aseveraciones pueden y deben ser objeto de un estudio más profundo, que dada la naturaleza de nuestro objeto de estudio nos vemos en la necesidad de limitar.

3.2.2 Sujeto Pasivo

En primer término tenemos que distinguir que sujeto pasivo o víctima del delito es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, y en el caso de los "Delitos Informáticos" las víctimas pueden ser individuos, instituciones crediticias, gobiernos, entre otros que usan sistemas automatizados de información, generalmente conectados a otros.

El sujeto pasivo del delito que nos ocupa, es sumamente importante para el estudio de los "Delitos Informáticos", ya que mediante él podemos conocer los diferentes ilícitos que cometen los delincuentes informáticos, con objeto de prever las acciones antes mencionadas debido a que muchos de los delitos son descubiertos curiosamente por el desconocimiento del modus operandi de los sujetos activos.

Dado lo anterior, "Ha sido imposible conocer la verdadera magnitud de los "Delitos Informáticos", ya que la mayor parte de los delitos no son descubierto o no son denunciados a las autoridades responsables" y si a esto se suma la falta de leyes que protejan a las víctimas de estos delitos; la falta de preparación por parte de las autoridades para comprender, investigar y dar tratamiento jurídico adecuado a esta problemática; el temor por parte de las empresas de denunciar este tipo de ilícitos por el desprestigio que esto pudiera ocasionar a su empresa y las consecuentes pérdidas económicas, entre otros más, trae como consecuencia que las estadísticas sobre este tipo de conductas se mantenga bajo la llamada "cifra oculta" o "cifra negra".

Por lo anterior, se reconoce que para conseguir una prevención efectiva de la criminalidad informática se requiere, en primer lugar, un análisis objetivo de las necesidades de protección y de las fuentes de peligro. Una protección eficaz contra la criminalidad informática presupone ante todo que las víctimas potenciales conozcan las correspondientes técnicas de manipulación, así como sus formas de encubrimiento".

En el mismo sentido, podemos decir que mediante la divulgación de las posibles conductas ilícitas derivadas del uso de las computadoras, y alertando a las potenciales víctimas para que tomen las medidas pertinentes a fin de prevenir la delincuencia informática, y si a esto se suma la creación de una adecuada legislación que proteja los intereses de las víctimas y una eficiente preparación por parte del personal encargado de la procuración, administración y la impartición de justicia para atender e investigar estas conductas ilícitas, se estaría avanzando mucho en el camino de la lucha contra la delincuencia informática, que cada día tiende a expandirse más.

Además, debemos destacar que los organismos internacionales han adoptado resoluciones similares en el sentido de que "educando a la comunidad de víctimas y estimulando la denuncia de los delitos se promovería la confianza pública en la capacidad de los encargados de hacer cumplir la ley y de las autoridades judiciales para detectar, investigar y prevenir los delitos informáticos".

3.3 No Maliciosas

3.3.1 Empleado falto de conocimiento

Amenazas como empleados ignorantes o descuidados, y los desastres naturales no implican motivos u objetivos; por lo tanto, no se utilizan métodos, herramientas o técnicas predeterminadas para iniciar los ataques. Casi todos estos ataques o infiltraciones en la seguridad se generan internamente; raras veces los va a iniciar alguien ajeno a la organización.

Para estos tipos de amenazas, el personal de seguridad necesita implementar estrategias preactivas o reactivas.

3.4 Recomendaciones

Una norma básica, seria verificar a cada aspirante a ser nuevo empleado; aunque tampoco debemos de olvidar que el echo de que alguien entre limpio a la empresa no implica que vaya seguir así durante todo el tiempo que trabaje en la misma, y mucho menos cuado abandone su trabajo.

Para minimizar el daño que un atacante interno pueda causar se pueden seguir estos principios fundamentales.

Necesidad de Conocimiento

Comúnmente llamado mínimo privilegio. Cada usuario debe tener el mínimo privilegio que necesite para desempeñar correctamente su función, es decir, que solo se le debe de permitir que sepa lo necesario para realizar su trabajo.

- Conocimiento parcial

  Las actividades más delicadas dentro de la organización deben ser realizadas por dos personas competentes, de forma que si uno comete un error en las políticas de seguridad el otra pueda subsanarlo. Esto también es aplicable al caso de que si uno

abandona la organización el otro pueda seguir operando el sistema mientras se realiza el reemplazo de la persona que se retiro.

- Rotación de Funciones

La mayor amenaza del conocimiento parcial de tareas es la complicidad de dos responsables, de forma tal, que se pueda ocultar sendas violaciones a la seguridad. Para evitar el problema, una norma común es rotar (dentro de ciertos límites) a las personas a lo largo de diferentes responsabilidades para establecer una vigilancia mutua.

- Separación de funciones

Es necesario que definan y separen correctamente las funciones de cada persona, de forma que alguien cuya tarea es velar por la seguridad de los sistemas no posea la capacidad para violarla sin que nadie se percate de ello.

- Cancelación inmediata de su cuenta

Cuando un empleado abandona la empresa se debe cancelar inmediatamente todos sus privilegios y accesos a sus antiguos recursos y cambiar las claves que el mismo conocía. Quizás este punto sea el mas difícil de implementar debido a la gran cantidad de usuarios que se deben de informar de los nuevos accesos y de la movilidad de ellos ahora también es recomendable que le comente a responsable del área de sistemas que no deje entrar personal que no este laborando para la empresa en el caso de ser información confidencial ya que esta persona puede ingresar al equipo con la clave de alguno de sus antiguos compañeros.

4. Factores involucrados en la seguridad informática

4.1 Agujeros de Seguridad

Llamaremos agujeros a todos aquellos huecos por los cuales un empleado mal intencionado tratara de penetrar nuestro sistema en la empresa de esta manera podremos detectar con tiempo problemas de seguridad.

Los agujeros de seguridad en la empresa se manifiestan (en general) de cuatro modos:

- Agujeros de Seguridad Físicos
- Agujeros de Seguridad en el Software
- Agujeros de Seguridad por Incompatibilidades
- Elección y Mantenimiento de Filosofía de Seguridad

4.1.1 Agujeros de Seguridad Físicos

Cuando el problema potencial, es debido al hecho de dar a personas, sin autorización, acceso físico a la máquina, siempre que esto les permita realizar cosas que no deberían ser capaces de hacer.

Un buen ejemplo podría ser una sala pública, con estaciones de trabajo, donde sería facilísimo reinicializar una máquina en modo mono-usuario y sustraer información de los archivos de la estación de trabajo, si no se hubieran tomado precauciones.

Otro ejemplo sería la necesidad de restringir el acceso a las bases de batos confidenciales, así como a los sitios destinados para el resguardo de información valiosa para la empresa que de otro modo podrían ser leídas o sustraídas por cualquier usuario no autorizado.

4.1.2 Agujeros de Seguridad en el Software

La gran mayoría de estos problemas se da cuando el personal del área de sistemas instala un programa que en su interior tiene un virus troyano estos programas pueden ser dados al personal con la firme intención de que sean instalados en el departamento. los virus troyanos en su código de programa pueden traer instrucciones sobre lo que deben de hacer una ves instalados y la forma en la cual se deben de ocultar para que el administrador no los detecte. estos virus pueden enviar información a terceras

personas, pueden dar acceso, enviar claves o incluso darle el control completo del sistema.

4.1.3 Agujeros de Seguridad por Incompatibilidades

Se da cuando, por falta de experiencia, o por descuido, el administrador del sistema hace funcionar software sobre un hardware para el que no está optimizado, dando lugar a posibles resultados inesperado y fallos que pueden dañar seriamente la seguridad del sistema. Es la incompatibilidad entre software y hardware la que crea agujeros de seguridad.

Problemas como este son muy difíciles de encontrar una vez que el sistema está montado y funcionando, de manera que es muy conveniente el leer atentamente la documentación del software y del hardware que se va a montar (o que pretendemos atacar) y estar muy atento a cualquier noticia o actualización.

4.1.4 Percepción y Entendimiento de Filosofía de Seguridad

El cuarto problema de seguridad es el de la percepción y el entendimiento. Software perfecto, hardware protegido, y componentes compatibles no funcionan a menos que se la política de seguridad en la empresa sea la correcta y que se hayan puesto en marcha las partes del sistema que la refuerzan.

Tener el mejor mecanismo de password (contraseñas) del mundo es inútil si los usuarios creen que la última parte del nombre de su login es un buen PassWord?

La seguridad está relacionada con una política (o conjunto de políticas / normas) y el funcionamiento del sistema conforme a dicha política.

5. DETECCIÓN DE INTRUSOS DESDE UN ENFOQUE FORENSE

5.1 Análisis Forense

El primer paso de cualquier análisis forense consiste en la captura de la evidencia. De tal forma se entiende por análisis forense que nos veremos forzados a hacer un estudio detallado de el para así capturar la evidencia. Por evidencia se entiende todo aquella información que pueda ser procesada en un análisis detallado. El fin de este análisis es la interpretación lo más exacta posible del suceso ocurrido. El objetivo fundamental es que en el proceso de la captura no se altere, o que sea en la menor medida posible, el escenario a analizar.

- Evidencia Volátil
  - Memoria del sistema
  - Servicios – Procesos – Device drivers
  - Puertos abiertos
  - Conexiones establecidas
  - Cuentas de usuarios y grupos
  - Información de red
- Discos
  - Herramientas de Duplicación de discos

5.2 Análisis de la Evidencia Volátil

Como todos sabemos los que estamos familiarizados con el manejo de información tenemos presente siempre la información guardada en el CACHE del sistema esta información es de carácter volátil lo que seria la memoria ROM esta memoria suele ser diferente cada vez que el sistema es reiniciado si nos topamos con un caso donde el intruso uso el equipo y este no se toma como evidencia después de varias reiniciadas esta evidencia desaparecería borrando con ello los accesos o borrando las rutas que el intruso uso para su intrusión al sistema. Estos serian los puntos a revisar en una posible intrusión a nuestro sistema.

- Memoria del sistema
- Servicios – Procesos – Device drivers
- Puertos abiertos
- Conexiones establecidas
- Cuentas de usuarios y grupos
- Red

5.3. Análisis de la Información de Disco

La parte más importante de cualquier análisis forense es analizar la información que se nos suministra de los posibles registros que tengamos. Si esa información no esta disponible o es insuficiente será necesario realizar un análisis forense exhaustivo del sistema. Para ello se deberán realizar búsquedas de información relativa al caso en las evidencias obtenidas, que básicamente serán, volátil e imagen de disco.

Como se verá en la propia descripción de estos sistemas de archivos la metodología es aplicable a cualquier otro sistema de archivos que se encuentre.

- Ficheros especiales
- Archivos comprimidos
- Archivos cifrados
- Memoria en disco: Pagefile.sys, Swap Partition
- Sistemas de archivos
  - FAT16/FAT32
  - NTFS
  - Ext2/Ext3
- Análisis de la imagen capturada
  - Clasificación de ficheros por fechas
  - Borrado de archivos – Parcial y Total
  - Espacio libre y espacio de relleno (slack space)
  - Ocultación de archivos
  - Búsqueda de patrones en disco
  - Búsqueda de programas maliciosos

5.4. Análisis forense de sistemas cliente

Mucho más abundantes que las intrusiones en servidores son las intrusiones en sistemas cliente. En muchos casos estas intrusiones se realizan teniendo como objetivo el acceso a servidores a los que el usuario víctima tiene derecho. Esto es debido a que normalmente los puestos de los usuarios son el eslabón más débil de la cadena de seguridad de un sistema.

- Interacción con Internet
  - Detectores de intrusos en sistemas clientes
  - Correo electrónico – Outlook
  - Navegación Web – Internet Explorer
- Técnicas de ocultación de código móvil
- Análisis de documentos
  - Microsoft

5.5. Análisis de programas sospechosos

Cuando el conjunto de evidencias encontradas no nos da toda la información requerida o cuando se ha identificado un programa como sospechosos, será necesario realizar un análisis más profundo del citado fichero.

- Estructura de los ficheros ejecutables
- DLLs y librerías
- Análisis en ejecución
  - Entorno seguro de pruebas
  - Interacción con el sistema

6. INTRODUCCIÓN A LA COMPILACIÓN DE UNA ESTRATEGIA DE SEGURIDAD EN UNA EMPRESA

Los administradores de seguridad tienen que decidir el tiempo, dinero y esfuerzo que hay que invertir para desarrollar las directivas y controles de seguridad apropiados. Cada empresa debe analizar sus necesidades específicas y determinar sus requisitos y limitaciones en cuanto a recursos y programación. Cada sistema informático, entorno y directiva organizativa es distinta, lo que hace que cada servicio y cada estrategia de seguridad sean únicos. Sin embargo, los fundamentos de una buena seguridad siguen siendo los mismos y esta tesina se centra en dichos principios.

Aunque una estrategia de seguridad puede ahorrar mucho tiempo a la organización y proporcionar importantes recomendaciones de lo que se debe hacer, la seguridad no es una actividad puntual. Es una parte integrante del ciclo vital de los sistemas. Las actividades que se describen en esta suelen requerir actualizaciones periódicas o las revisiones correspondientes. Estos cambios se realizan cuando las configuraciones y otras condiciones y circunstancias cambian considerablemente o cuando hay que modificar las leyes y normas organizativas. Éste es un proceso iterativo. Nunca termina y debe revisarse y probarse con periodicidad.

6.1.1 Revisar las directivas actuales

La siguiente propuesta de Seguridad Informática está pensada para ayudar y apoyar a los profesionales de la seguridad y a los administradores de centros de computo en empresas a desarrollar una estrategia para proteger la disponibilidad, integridad y confidencialidad de los datos de los sistemas informáticos en la empresa donde se decida aplicar o en las organizaciones que se considere necesario. Es de interés para los administradores de recursos de información, los directores de seguridad informática y los administradores, y tiene un valor especial para todos aquellos que intentan establecer directivas de seguridad. La propuesta ofrece un acercamiento sistemático a esta importante tarea y, como precaución final, también implica el establecimiento de planes de contingencia en caso de desastre.

Los datos de los sistemas informáticos están en constante peligro por varias causas: errores de los usuarios o ataques intencionados o fortuitos. Pueden producirse

accidentes y ciertas personas con intención de atacar el sistema pueden obtener acceso al mismo e interrumpir los servicios, inutilizar los sistemas o alterar, suprimir o robar información.

Los sistemas informáticos pueden necesitar protección en algunos de los siguientes aspectos de la información:

- Confidencialidad. El sistema contiene información que requiere protección contra la divulgación no autorizada. Por ejemplo, datos que se van a difundir en un momento determinado (como, información parcial de informes), información personal e información comercial patentada.
- Integridad. El sistema contiene información que debe protegerse de modificaciones no autorizadas, imprevistas o accidentales. Por ejemplo, información de censos, indicadores económicos o sistemas de transacciones financieras.
- Disponibilidad. El sistema contiene información o proporciona servicios que deben estar disponibles puntualmente para satisfacer requisitos o evitar pérdidas importantes. Por ejemplo, sistemas esenciales de seguridad, protección de la vida y predicción de huracanes.

6.1.2 Identificar métodos, herramientas y técnicas de ataque probables

Las listas de amenazas, de las que disponen la mayor de las organizaciones, ayudan a los administradores de seguridad a identificar los distintos métodos, herramientas y técnicas de ataque que se pueden utilizar en los ataques. Los métodos pueden abarcar desde virus y gusanos a la adivinación de contraseñas y la interceptación del correo electrónico. Es importante que los administradores actualicen constantemente sus conocimientos en esta área, ya que los nuevos métodos, herramientas y técnicas para sortear las medidas de seguridad evolucionan de forma continua.

6.1.3 Establecer estrategias preactivas y reactivas

En cada método, el plan de seguridad debe incluir una estrategia preactiva y otra reactiva.

La estrategia preactiva o de previsión de ataques es un conjunto de pasos que ayuda a reducir al mínimo la cantidad de puntos vulnerables existentes en las directivas de

seguridad y a desarrollar planes de contingencia. La determinación del daño que un ataque va a provocar en un sistema y las debilidades y puntos vulnerables explotados durante este ataque ayudará a desarrollar la estrategia preactiva.

La estrategia reactiva o estrategia posterior al ataque ayuda al personal de seguridad a evaluar el daño que ha causado el ataque, a repararlo o a implementar el plan de contingencia desarrollado en la estrategia proactiva, a documentar y aprender de la experiencia, y a conseguir que las funciones comerciales se normalicen lo antes posible.

6.1.4 Pruebas

El último elemento de las estrategias de seguridad, las pruebas y el estudio de sus resultados, se lleva a cabo después de que se han puesto en marcha las estrategias reactiva y proactiva. La realización de ataques simulados en sistemas de pruebas o en laboratorios permiten evaluar los lugares en los que hay puntos vulnerables y ajustar las directivas y los controles de seguridad en consecuencia.

Estas pruebas no se deben llevar a cabo en los sistemas de producción real, ya que el resultado puede ser desastroso. La carencia de laboratorios y equipos de pruebas a causa de restricciones presupuestarias puede imposibilitar la realización de ataques simulados. Para asegurar los fondos necesarios para las pruebas, es importante que los directivos sean conscientes de los riesgos y consecuencias de los ataques, así como de las medidas de seguridad que se pueden adoptar para proteger al sistema, incluidos los procedimientos de las pruebas. Si es posible, se deben probar físicamente y documentar todos los casos de ataque para determinar las mejores directivas y controles de seguridad posibles que se van a implementar.

Determinados ataques, por ejemplo desastres naturales como inundaciones y rayos, no se pueden probar, aunque una simulación servirá de gran ayuda. Por ejemplo, se puede simular un incendio en la sala de servidores en el que todos los servidores hayan resultado dañados y hayan quedado inutilizables. Este caso puede ser útil para probar la respuesta de los administradores y del personal de seguridad, y para determinar el tiempo que se tardará en volver a poner la organización en funcionamiento.

La realización de pruebas y de ajustes en las directivas y controles de seguridad en función de los resultados de las pruebas es un proceso iterativo. Nunca termina, ya que debe evaluarse y revisarse de forma periódica para poder implementar mejoras.

6.1.5 Equipos de respuesta a incidentes

Es aconsejable formar un equipo de respuesta a incidentes. Este equipo debe estar implicado en los trabajos preactivos del profesional de la seguridad. Entre éstos se incluyen:

El desarrollo de instrucciones para controlar incidentes.

La identificación de las herramientas de software para responder a incidentes y eventos.

La investigación y desarrollo de otras herramientas de seguridad informática.

La realización de actividades formativas y de motivación.

La realización de investigaciones acerca de virus.

La ejecución de estudios relativos a ataques al sistema.

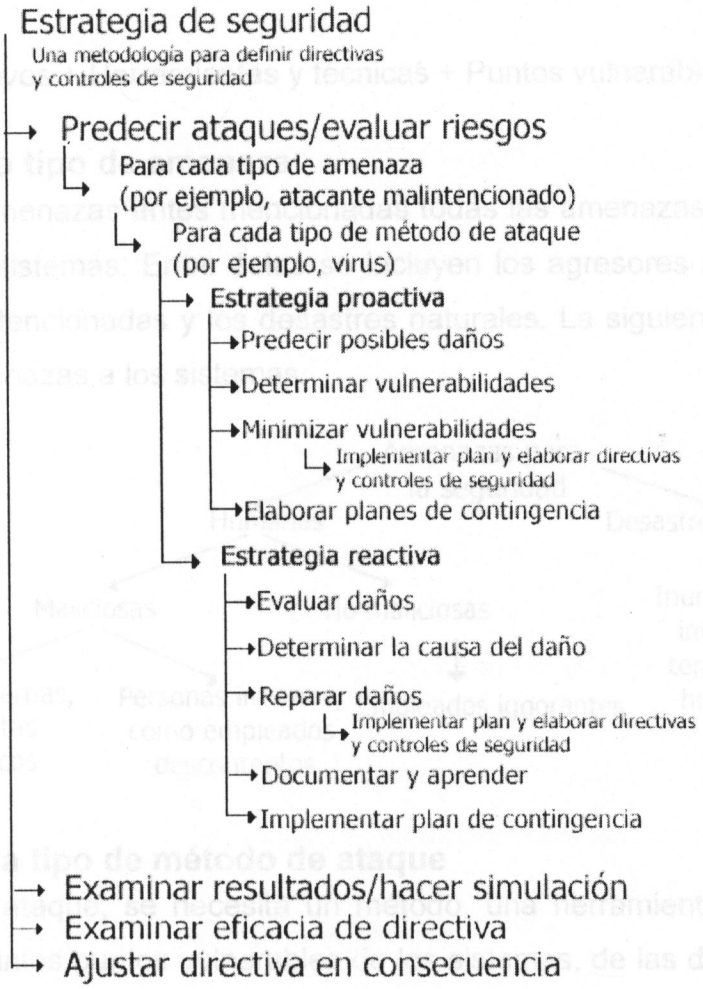
Estos trabajos proporcionarán los conocimientos que la organización puede utilizar y la información que hay que distribuir antes y durante los incidentes.

Una vez que el administrador de seguridad y el equipo de respuesta a incidentes han realizado estas funciones preactivas, el administrador debe delegar la responsabilidad del control de incidentes al equipo de respuesta a incidentes. Esto no significa que el administrador no deba seguir implicado o formar parte del equipo, sino que no tenga que estar siempre disponible, necesariamente, y que el equipo debe ser capaz de controlar los incidentes por sí mismo. El equipo será el responsable de responder a incidentes como virus, gusanos o cualquier otro código dañino; invasión; engaños; desastres naturales y ataques del personal interno. El equipo también debe participar en el análisis de cualquier evento inusual que pueda estar implicado en la seguridad de los equipos o de la red.

6.2 Metodología para la definición de estrategias de seguridad

La estrategia de seguridad informática se puede utilizar para implementar directivas y controles de seguridad con el objeto de aminorar los posibles ataques y amenazas. Los métodos se pueden utilizar en todos los tipos de ataques a sistemas,

independientemente de que sean intencionados, no intencionados o desastres naturales, y, por consiguiente, se puedan volver a utilizar en distintos casos de ataque. La metodología se basa en los distintos tipos de amenazas, métodos de ataque y puntos vulnerables explicados en el capitulo 3. El siguiente diagrama de flujo describe la metodología.



6.2.1 Predecir posibles ataques y analizar riesgos

La primera fase de la metodología esquematizada en el diagrama de flujo es determinar los ataques que se pueden esperar y las formas de defenderse contra ellos. Es imposible estar preparado contra todos los ataques; por lo tanto, hay que prepararse para los que tiene más probabilidad de sufrir la organización. Siempre es mejor prevenir o aminorar los ataques que reparar el daño que han causado.

Para mitigar los ataques es necesario conocer las distintas amenazas que ponen en peligro los sistemas, las técnicas correspondientes que se pueden utilizar para

comprometer los controles de seguridad y los puntos vulnerables que existen en las directivas de seguridad. El conocimiento de estos tres elementos de los ataques ayuda a predecir su aparición e, incluso, su duración o ubicación. La predicción de los ataques trata de pronosticar su probabilidad, lo que depende del conocimiento de sus distintos aspectos. Los diferentes aspectos de un ataque se pueden mostrar en la siguiente ecuación:

Amenazas+ Motivos + Herramientas y técnicas + Puntos vulnerables = Ataque

6.2.2 Para cada tipo de amenaza

Considere las amenazas antes mencionadas todas las amenazas posibles que causan ataques en los sistemas. Entre éstas se incluyen los agresores malintencionados, las amenazas no intencionadas y los desastres naturales. La siguiente ilustración clasifica las distintas amenazas a los sistemas.

6.2.3 Para cada tipo de método de ataque

Para iniciar un ataque, se necesita un método, una herramienta o una técnica para explotar los distintos puntos vulnerables de los sistemas, de las directivas de seguridad y de los controles. Los agresores pueden utilizar varios métodos para iniciar el mismo ataque. Por lo tanto, la estrategia defensiva debe personalizarse para cada tipo de método utilizado en cada tipo de amenaza. De nuevo, es importante que los profesionales de la seguridad estén al día en los diferentes métodos, herramientas y técnicas que utilizan los agresores.

La siguiente es una lista breve de estas técnicas:

- Ataques de denegación de servicio
- Ataques de invasión
- Ingeniería social
- Virus
- Gusanos
- Caballos de Troya
- Modificación de paquetes
- Repetición de paquetes
- Adivinación de contraseñas
- Interceptación de correo electrónico

6.2.4 Estrategia Proactiva

La estrategia proactiva es un conjunto de pasos predefinidos que deben seguirse para evitar ataques antes de que ocurran. Entre estos pasos se incluye observar cómo podría afectar o dañar el sistema, y los puntos vulnerables que explota (pasos 1 y 2). Los conocimientos adquiridos en estas evaluaciones pueden ayudar a implementar las directivas de seguridad que controlarán o aminorarán los ataques. Éstos son los tres pasos de la estrategia proactiva:

1. Determinar el daño que causará el ataque.
2. Establecer los puntos vulnerables y las debilidades que explotará el ataque.
3. Reducir los puntos vulnerables y las debilidades que se ha determinado en el sistema para ese tipo de ataque específico.

El seguimiento de estos pasos para analizar los distintos tipos de ataques tiene una ventaja adicional: comenzará a emerger un modelo, ya que en los diferentes factores se superponen para diferentes ataques. Este modelo puede ser útil al determinar las áreas de vulnerabilidad que plantean el mayor riesgo para la empresa. También es necesario tomar nota del costo que supone la pérdida de los datos frente al de la implementación de controles de seguridad. La ponderación de los riesgos y los costos forma parte de un análisis de riesgos del sistema que se explica en el documento técnico acerca del diseño de la seguridad.

Las directivas y controles de seguridad no serán, en ningún caso, totalmente eficaces al eliminar los ataques. Éste es el motivo por el que es necesario desarrollar planes de recuperación y de contingencia en caso de que se quebranten los controles de seguridad.

6.3 Determinar el daño posible que puede causar un ataque

Los daños posibles pueden oscilar entre pequeños fallos del equipo y la pérdida, catastrófica, de los datos. El daño causado al sistema dependerá del tipo de ataque. Si es posible, utilice un entorno de prueba o de laboratorio para clarificar los daños que provocan los diferentes tipos de ataques. Ello permitirá al personal de seguridad ver el daño físico que causan los ataques experimentales. No todos los ataques causan el mismo daño. Éstos son algunos ejemplos de las pruebas que hay que ejecutar:

Simular un ataque con virus a través de correo electrónico en el sistema del laboratorio y ver el daño que ha provocado y cómo recuperarse de la situación.

Utilizar la ingeniería social para adquirir un nombre de usuario y una contraseña de algún empleado ingenuo y observar cómo se comporta.

Simular lo que ocurriría ante un incendio en la sala de servidores. Mida el tiempo de producción perdido y el tiempo necesario para la recuperación.

Simular un ataque de virus dañino. Anote el tiempo necesario para recuperar un equipo y multiplique ese tiempo por el número de equipos del sistema infectados para averiguar el tiempo de inactividad y la pérdida de productividad.

También es aconsejable implicar al equipo de respuesta a incidentes ya mencionado, ya que es más probable que un equipo, en lugar de una sola persona, consiga localizar todos los tipos distintos de daños que se han producido.

6.4 Determinar los puntos vulnerables o las debilidades que pueden explotar los ataques

Si se pueden descubrir los puntos vulnerables que explota un ataque específico, se pueden modificar las directivas y los controles de seguridad actuales o implementar otras nuevas para reducir estos puntos vulnerables. La determinación del tipo de ataque, amenaza y método facilita el descubrimiento de los puntos vulnerables existentes. Esto se puede reconocer por medio de una prueba real.

A continuación encontrará una lista de los posibles puntos vulnerables. Éstos representan solamente unos pocos de los muchos que existen e incluyen ejemplos en las áreas de seguridad física, de datos y de red.

6.4.1 Seguridad física:

- ¿Hay bloqueos y procedimientos de entrada para obtener acceso a los servidores?
- ¿Es suficiente el aire acondicionado y se limpian regularmente los filtros? ¿Están protegidos los conductos de aire acondicionado contra robos?
- ¿Hay sistemas de alimentación ininterrumpida y generadores, y se comprueban en los procedimientos de mantenimiento?
- ¿Hay equipo para la extinción de incendios y procedimientos de mantenimiento apropiados para el equipo?
- ¿Hay protección contra el robo de hardware y software? ¿Se guardan los paquetes y licencias de software y las copias de seguridad en lugares seguros?
- ¿Hay procedimientos para almacenar los datos, copias de seguridad y software con licencia en las instalaciones y fuera de ellas?

6.4.2 Seguridad de datos:

- ¿Qué controles de acceso, controles de integridad y procedimientos de copias de seguridad existen para limitar los ataques?
- ¿Hay directivas de privacidad y procedimientos que deban cumplir los usuarios?
- ¿Qué controles de acceso a los datos (autorización, autenticación e implementación) hay?
- ¿Qué responsabilidades tienen los usuarios en la administración de los datos y las aplicaciones?
- ¿Se han definido técnicas de administración de los dispositivos de almacenamiento con acceso directo? ¿Cuál es su efecto en la integridad de los archivos de los usuarios?
- ¿Hay procedimientos para controlar los datos importantes?

6.4.3 Seguridad de la red:

- ¿Qué tipos de controles de acceso (Internet, conexiones de la red de área extensa, etc.) existen?
- ¿Hay procedimientos de autenticación?
- ¿Qué protocolos de autenticación se utilizan en las redes de área local, redes de área extensa y servidores de acceso telefónico?
- ¿Quién tiene la responsabilidad de la administración de la seguridad?
- ¿Qué tipo de medios de red, por ejemplo, cables, conmutadores y en ruteadores, se utilizan?
- ¿Qué tipo de seguridad tienen?
- ¿Se ha implementado la seguridad en los servidores de archivos y de impresoras?
- ¿Hace uso la organización del cifrado y la criptografía en Internet, redes privadas virtuales (VPN), sistemas de correo electrónico y acceso remoto?
- ¿Se ajusta la organización a las normas de redes?

6.4.4 Reducir los puntos vulnerables y debilidades que puede explotar un posible ataque

La reducción de los puntos vulnerables y las debilidades del sistema de seguridad que se determinaron en la evaluación anterior es el primer paso para desarrollar directivas y controles de seguridad eficaces. Ésta es la compensación de la estrategia proactiva. Mediante la reducción de los puntos vulnerables, el personal de seguridad puede hacer disminuir tanto la probabilidad de un ataque como su eficacia, si se produce alguno. Tenga cuidado de no implementar controles demasiado estrictos, ya que la disponibilidad de la información se convertiría en un problema. Debe haber un cuidado equilibrio entre los controles de seguridad y el acceso a la información. Los usuarios deben tener la mayor libertad posible para tener acceso a la información.

6.4.5 Elaborar planes de contingencia

Un plan de contingencia es un plan alternativo que debe desarrollarse en caso de que algún ataque penetre en el sistema y dañe los datos o cualquier otro activo, detenga las operaciones comerciales habituales y reste productividad. El plan se sigue si el sistema

no se puede restaurar a tiempo. Su objetivo final es mantener la disponibilidad, integridad y confidencialidad de los datos lo que comúnmente se llama el "Plan B".

Debe haber un plan para cada tipo de ataque y tipo de amenaza. Cada plan consta de un conjunto de pasos que se han de emprender en el caso de que un ataque logre pasar las directivas de seguridad. El plan de contingencia debe:

- Determinar quién debe hacer qué, en qué momento y en qué lugar para que la organización siga funcionando.
- Ensayarse periódicamente para mantener al personal informado de los pasos de la contingencia actual.
- Abarcar la restauración de las copias de seguridad.
- Explicar la actualización del software antivirus.
- Abarcar el traspaso de la producción a otra ubicación o sitio.

Los siguientes puntos resaltan las distintas tareas que deben evaluarse para desarrollar un plan de contingencia:

- Evaluar las directivas y controles de seguridad de la organización para utilizar todas las oportunidades destinadas a reducir los puntos vulnerables. La evaluación debe tratar el plan y los procedimientos de emergencia actuales de la organización y su integración en el plan de contingencia.
- Evaluar los procedimientos actuales de respuesta ante emergencias y su efecto en el funcionamiento continuo de la organización.
- Desarrollar respuestas planeadas a ataques, integrarlas en el plan de contingencia y anotar hasta qué punto son adecuadas para limitar el daño y reducir el impacto del ataque en las operaciones de procesamiento.
- Evaluar procedimientos de copia de seguridad, que incluyan la documentación más reciente y pruebas de recuperación de desastres, para evaluar su adecuación e integrarlos en el plan de contingencia.
- Evaluar planes de recuperación de desastres para determinar su adecuación con el fin de proporcionar un entorno operativo temporal o a largo plazo. Los planes de recuperación de desastres deben incluir la prueba de los niveles de seguridad necesarios, con el fin de que el personal de seguridad pueda ver si siguen exigiendo la seguridad en todo el proceso de recuperación o en operaciones

temporales y el traspaso de la organización otra vez a su sitio de procesamiento original o a un sitio nuevo.

Redactar un documento detallado que describa los distintos descubrimientos en las tareas anteriores. El documento debe mostrar:

- Todos los casos para probar el plan de contingencia.
- El impacto de las dependencias y de la ayuda planeada de fuera de la organización, y las dificultades que la obtención de los recursos esenciales tendrán en el plan.
- Una lista de prioridades observadas en las operaciones de recuperación y el fundamento para establecerlas.

6.4.6 Estrategia reactiva

La estrategia reactiva se implementa cuando ha fallado la estrategia proactiva y define los pasos que deben adoptarse después o durante un ataque. Ayuda a identificar el daño causado y los puntos vulnerables que se explotaron en el ataque, a determinar por qué tuvo lugar, a reparar el daño que causó y a implementar un plan de contingencia, si existe. Tanto la estrategia reactiva como la proactiva funcionan conjuntamente para desarrollar directivas y controles de seguridad con el fin de reducir los ataques y el daño que causan.

El equipo de respuesta a incidentes debe incluirse en los pasos adoptados durante o después del ataque para ayudar a evaluarlo, a documentar el evento y a aprender de él.

6.4.7 Evaluar el daño

Determine el daño causado durante el ataque. Esto debe hacerse lo antes posible para que puedan comenzar las operaciones de restauración. Si no se puede evaluar el daño a tiempo, debe implementarse un plan de contingencia para que puedan proseguir las operaciones comerciales y la productividad normales.

6.4.8 Determinar la causa del daño

Para determinar la causa del daño, es necesario saber a qué recursos iba dirigido el ataque y qué puntos vulnerables se explotaron para obtener acceso o perturbar los servicios.

Revise los registros del sistema, los registros de auditoria y las pistas de auditoria. Estas revisiones suelen ayudar a descubrir el lugar del sistema en el que se originó el ataque y qué otros recursos resultaron afectados.

6.4.9 Reparar el daño

Es muy importante que el daño se repare lo antes posible para restaurar las operaciones comerciales normales y todos los datos perdidos durante el ataque. Los planes y procedimientos para la recuperación de desastres de la organización (que se tratan en el documento acerca del diseño de la seguridad) deben cubrir la estrategia de restauración. El equipo de respuesta a incidentes también debe poder controlar el proceso de restauración y recuperación, y ayudar en este último.

6.4.10 Documentar y aprender

Es importante documentar el ataque una vez que se ha producido. La documentación debe abarcar todos los aspectos que se conozcan del mismo, entre los que se incluyen el daño que ha causado (en hardware y software, pérdida de datos o pérdida de productividad), los puntos vulnerables y las debilidades que se explotaron durante el ataque, la cantidad de tiempo de producción perdido y los procedimientos tomados para reparar el daño. La documentación ayudará a modificar las estrategias proactivas para evitar ataques futuros o mermar los daños.

6.4.11 Implementar un plan de contingencia

Si ya existe algún plan de contingencia, se puede implementar para ahorrar tiempo y mantener el buen funcionamiento de las operaciones comerciales. Si no hay ningún plan de contingencia, desarrolle un plan apropiado basado en la documentación del paso anterior.

7. LOS 10 MANDAMIENTOS DE LA RED

Cualquier usuario o administrador de cualquier red computacional que siga los siguientes mandamientos propuestos esta procurando un nivel de seguridad alto para la información en la empresa y por tanto también para la información de sus compañeros de trabajo.

7.1 Los 10 mandamientos del usuario de la red

Debemos ser completamente fieles a estos mandamientos, si en algún momento pecamos en no cumplirlos entonces debemos atenernos a las consecuencias del bajo nivel de seguridad que le brindamos a nuestra información y a nuestros compañeros usuarios de la red.

1. La contraseña es personal, no debe ser prestada bajo ninguna circunstancia, si por algún motivo se sospecha de su posible uso sin sus autorización, debe cambiarla de inmediato y reportar el hecho al administrador de la red. Recuerde que las contraseñas deben cambiarse periódicamente. No es recomendable utilizar contraseñas cortas, mínimo 8 caracteres y mucho menos palabras que se puedan encontrar en algún diccionario o que tengan alguna relación con el dueño de la misma. Se sugiere que sean palabras sin sentido usando los caracteres especiales.

2. La utilización de los antivirus es importante, se debe ejecutar por lo menos una vez al día a todo el disco duro de su equipo, se recomienda ejecutarlo inmediatamente al llegar a su sitio de trabajo, esto es fácil debido a que existen algunos que se pueden configurar para que se ejecuten al iniciar el equipo, además debe vacunar todo disquete que utilice en su equipo, así sea de su propiedad o de algún origen confiable. Recuerde que si ya ha sido vacunado el disquete y fue utilizado en otro equipo debe vacunarlo nuevamente.

Recuerde vacunar todos los archivos adjuntos a sus correos y aquellos que descargue de la red. No olvide que la actualización de los antivirus es una labor del administrador, pero es su deber como usuario final estar atento a esto.

3. En caso que su equipo quede desatendido por alguna razón, debe colocar el protector de pantalla protegió por contraseña, esta debe ser colocada en el mismo instante que coloco el protector de pantalla y no debe ser igual a las anteriormente utilizadas, debido a que existen programas que logran descifrar la contraseña de los protectores de pantalla y además la de acceso a la red. No sobra colocar una contraseña en el boot de arranque al equipo, esto no permitirá el acceso aunque se apague el equipo. No esta de mas que el equipo tenga una llave física o hardkey, la cual no permita que cualquier persona pueda destapar el equipo, quitar la pila del CMOS o el jumper de la BIOS (Basic Input Output System) y modificar la contraseña.

4. Si maneja información secreta para su empresa, lo mejor es mantenerla encriptada en su disco duro local con una copia respectiva en su servidor. Esto mismo aplica para el correo electrónico. Uno de estos productos es el PGP (Pret Good Princacy). No olvide asegurar su llave privada, si la pierde es probable que su información pueda ser descifrada.

5. Si por alguna razón usted debe compartir información en la red, asegúrese de colocar los permisos estrictamente necesarios a los usuarios adecuados y por el mínimo tiempo posible. Recuerde que al compartir su información con todos los permisos habilitados corre el riesgo de perder toda la información compartida. Además existen programas especializados en descifrar las claves de directorios compartidos por contraseñas para luego colocar programas que se auto ejecuten desde allí y realizar alguna labor especifica.

6. Absténgase de instalar programas no autorizados por su administrador de la red, usted puede convertirse en el responsable del caos en materia de seguridad para toda la red de la empresa.

Estos programas pueden ser troyanos (Son aquellos programas que prometen ser algo y realmente realizan otra cosa que compromete la seguridad del usuario) o puertas traseras (Programas que le permite al vándalo informático entrar al sistema que ya ha vulnerado de manera mas sencilla y reiterativa) que le dan acceso a los vándalos informáticos para realizar alguna labor concreta.

7. Procure que su equipo se encuentre en optimas condiciones, es decir que tenga buena ventilación mantenimiento de hardware y software por personal autorizado de la empresa: No desinstale ni instale ningún tipo de hardware sin autorización del administrador, recuerde que la desinstalación o instalación de este provocara cambios en la configuración de su equipo y esto debe ser manejado por personal especializado, además que su información corre riesgo de perderse.

8. No basta mantener copia de la información encriptada en el servidor. Recuerde realizar copias de respaldo actualizadas de la información vital que maneje en su disco duro y colocarla en un lugar seguro bajo llave y encriptada, el usuario puede realizar esta labor. En el caso que la información se guarde en un lugar fuera de la empresa bajo medidas extremas de seguridad, el administrador de la información de los usuarios debe ser el encargado de esta labor.

9. Mantener la información de la empresa en la misma y no transportarla a otro sitio diferente de esta: Corremos el riesgo de no tener las mismas precauciones de seguridad en otro sitio y por ende estaremos atentando contra la seguridad de nuestra información y de nuestra empresa.

10. Asegúrese de seguir cada uno de los 9 mandamientos anteriores y le garantizo la máxima calidad y nivel de seguridad en el manejo de la información de su empresa. Recuerde que si hace extensiva esta información o distribuirla a través de cualquier medio estará colaborando con la debida educación en el manejo de la información.

7.2 Los 10 Mandamientos del Administrador de la Red

1. Siga, respalde y audite cada uno de los 10 mandamientos del usuario de la red.

Responsabilidades a nivel individual: El acceso a los datos únicamente debe concederse tras la identificación del usuario. Un mismo empleado no debe ser el responsable de autorizar y realizar cambios en el Software de la empresa. Establecer un sistema seguro de contraseñas. Auditar las redes cada dos años ya que los niveles de seguridad establecidos en su momento tienden a deteriorarse con el transcurso del tiempo. Clasificar la información según sus grados de sensibilidad e importancia dentro de la organización. Controlar el procesamiento. La información puede estar en tres estados: proceso, almacenamiento y Transmisión. La confidencialidad y la integridad de la transmisión. La Confidencialidad y la integridad en la transmisión y el almacenamiento las alcanzamos con la encriptación.

2. Establezca políticas de seguridad apropiadas para la red computacional de la empresa, creación de usuarios, manejo de contraseñas, instalación de hardware y software, perfiles de usuario estándar y minimice la cantidad de cuentas de administradores de la red . Estrategias de contingencia en caso de perdida de información de los usuarios o suspensión de los servidores de la empresa por alguna razón.

3. Implemente sistemas de seguridad para la red en cada uno de los servidores de la empresa utilizando firewalls, proxy o filtros. Mantenga un servidor de prueba en donde pueda instalar y desinstalar los programas que tiene en su red para realzar pruebas de seguridad a los programas que usa. Identificar que servidores deben pertenecer a la red militarizada y cuales a la red desmilitarizada, esto se debe realizar para identificar los anillos de seguridad de la red.

4. Responda inmediatamente ante cualquier sugerencia o queja de un usuario con respecto a la seguridad de su información. Probablemente sea un fallo de seguridad importante contra la empresa y su usuario lo ha detectado por usted, ahorrándole tiempo y dinero a la empresa en solucionarlo.

5. Procure no sobrecargar los servidores asignándoles muchos servicios, recuerde que esto baja el rendimiento y atenta contra la seguridad y la constancia de los servicios en los mismos. Ante cualquier tipo de falla de hardware o software acuda inmediatamente al proveedor o recurra de inmediato al servidor BDC (Backup Domain Control) de la empresa.

6. El manejo de los puertos es fundamental a la hora de auditar posibles huecos de seguridad, recuerde que debe tener la menor cantidad de puertos abiertos en los servidores.
Estos pueden ser en cualquier momento puertas de acceso a los vándalos de la red. Existen programas que le avisan en línea si algún puerto ha sido abierto de forma anormal o si alguien esta conectado a alguno de ellos de forma fraudulenta. Recuerde que si tiene instalado algún programa que ofrece un servicio innecesario esta dejando un puerto abierto el cual puede ser violentado.

7. Implementar estrategias para la creación de las copias de respaldo, recuerde que debe mantener copias diarias, semanales, mensuales y anuales; además estas deben ser encriptadas y deben guardarse en lugares seguros como bancos o cajas de seguridad contra incendios en lugares fuera de la empresa y de extrema seguridad.

8. Debe leer diariamente los logs (Archivos de texto que muestran el funcionamiento y la utilización del equipo en momentos específicos) que arroja el servidor, estos muchas veces nos informan de accesos no permitidos en horas no acostumbradas. Recuerde restringir el acceso al máximo de los usuarios de la red, eso incluye días a la semana, horas, directorios y sitios de trabajo.

4. Responda inmediatamente ante cualquier sugerencia o queja de un usuario con respecto a la seguridad de su información. Probablemente sea un fallo de seguridad importante contra la empresa y su usuario lo ha detectado por usted, ahorrándole tiempo y dinero a la empresa en solucionarlo.

5. Procure no sobrecargar los servidores asignándoles muchos servicios, recuerde que esto baja el rendimiento y atenta contra la seguridad y la constancia de los servicios en los mismos. Ante cualquier tipo de falla de hardware o software acuda inmediatamente al proveedor o recurra de inmediato al servidor BDC (Backup Domain Control) de la empresa.

6. El manejo de los puertos es fundamental a la hora de auditar posibles huecos de seguridad, recuerde que debe tener la menor cantidad de puertos abiertos en los servidores.
Estos pueden ser en cualquier momento puertas de acceso a los vándalos de la red. Existen programas que le avisan en línea si algún puerto ha sido abierto de forma anormal o si alguien esta conectado a alguno de ellos de forma fraudulenta. Recuerde que si tiene instalado algún programa que ofrece un servicio innecesario esta dejando un puerto abierto el cual puede ser violentado.

7. Implementar estrategias para la creación de las copias de respaldo, recuerde que debe mantener copias diarias, semanales, mensuales y anuales; además estas deben ser encriptadas y deben guardarse en lugares seguros como bancos o cajas de seguridad contra incendios en lugares fuera de la empresa y de extrema seguridad.

8. Debe leer diariamente los logs (Archivos de texto que muestran el funcionamiento y la utilización del equipo en momentos específicos) que arroja el servidor, estos muchas veces nos informan de accesos no permitidos en horas no acostumbradas. Recuerde restringir el acceso al máximo de los usuarios de la red, eso incluye días a la semana, horas, directorios y sitios de trabajo.

9. El acceso al centro de computo donde se encuentran los servidores de la empresa, debe se completamente restringido y auditado cada instante. Se recomienda utilizar sistemas electrónicos (Biométricos) para verificar el acceso al centro de computo.

10. No olvide que la mejor auditoria de seguridad para la red de la empresa es el intento de violación de la seguridad de la misma, conviértase en el hacker de su empresa, ingrese a los grupos de discusión de hackers, inscríbase a las listas de correos de estos y aprenda de ellos.

8. CONCLUSIONES Y RECOMENDACIONES

Con el pasar de los años el avance la tecnología nos a vuelto dependientes de la computadora, lo que antes era un articulo de lujo hoy es un aparato que nos ayuda a crear, desarrollar e incluso a socializarnos si nos vamos un poco mas allá. Miles de kilobites pueden ser nuestro estado de cuenta o aquel informe donde presentamos el nuevo proyecto de la empresa. La información como tal puede ser solo un CD-ROM o un Diskette o tal ves miles de kilobytes en un disco duro pero en realidad esa información puede ser el trabajo de una vida o la próxima realidad virtual de un mundo que un no imaginamos y alguien fue el creador de dicha información y para el esos simples miles de kilobytes que tienen un valor para alguien o incluso puede ser información invaluable.

En base a esto se trata la siguiente tesina, en comprender que la seguridad en nuestra empresa es un conjunto de recursos destinados a lograr que la información y los activos sean confidenciales, íntegros y disponibles, de resguardar la información, de saber que esos miles de kilobytes están seguros en algún lugar y que podemos tener la certeza que la información es solo para los ojos del personal del autorizado para tal fin. en caso de que la información sea de carácter confidencial.

Las personas que comenten los delitos informáticos pueden clasificarse de varias maneras, desde el personal interno hasta el ex empleado que descontento por su despido busca la manera de tener acceso al sistema a través de sus mismos compañeros que faltos de conocimientos le prestan sus claves de accesos al sistemas. puede a ver un sin numero de excusas por la cual un buen empleado llega a traicionar a la empresa. Y es realmente preocupante que una persona que trabaje con el administrador, el programador o tenga asignada un equipo en la empresa sea capaz de cometer un delito informático para obtener un beneficio propio.

Considero que una vez que un empleado es dado de baja de la institución el administrador del área de sistemas debe de estar enterado de la baja para que este de inmediato realice la baja de acceso al sistema, además de advertir al personal que dicha persona ya no es empleado de la empresa y que su clave es personal e intransferible. Estas medidas pueden sonar algo desconcertantes si solo era un simple

capturista pero nunca sabremos si ese simple capturista pueda ser la persona que atacara a la empresa obteniendo los planes de crecimiento, la nomina o la lista de nuestros mejores clientes, entre otros. No existe enemigo pequeño.

A lo largo de este trabajo me he dado cuenta que contiene todos los elementos metodológicos para que un profesional en sistemas de información comprenda y lleve a la practica las medidas necesarias para implementar políticas y lineamientos de seguridad que tienen como objetivo preservar la integridad, confiabilidad, privacidad, control y autenticidad de la información evitar que personal interno o externo no autorizado tenga acceso a información confidencial.

La informática forense se ocupa de investigar los intentos de intrusión a un sistema una vez que estos ya se han producido, así una vez que un intruso entra en el sistema para obtener información confidencial tener la certeza de que tipo de información tomo o saber con tiempo cual empleado esta amenazando con una posible intrusión al sistema, pienso que el problema mayor en una empresa es siempre el empleado interno no quiero decir que el externo no sea problema pero el empleado interno tiene acceso a toda nuestra empresa, a toda. Ahora nunca vamos a sospechar de un buen empleado que este descontento por su sueldo o que la competencia le ofreció una remuneración por develar los planos del nuevo proyecto. Nunca estaremos preparados para eso para la ingeniera social.

Ahora no falta el empleado con conocimientos estos suelen ser pocos pero los hay, estos pueden crear agujeros en la seguridad de la empresa en una empresa, como administrador de un área de sistemas se tiene la responsabilidad de estar siempre alerta ya que los usuarios con conocimientos o faltos de ellos siempre nos van a tener ocupados para el buen desempeño de la red.

Se tiene que decidir el tiempo, dinero y esfuerzo conjunto con el gerente de la empresa si se plantea crear un área de sistemas segura, ya que hay que desarrollar directivas y controles de seguridad apropiados. De acuerdo al giro de la empresa y sus necesidades de seguridad. Se trata de predecir un posible ataque no de esperar a que este suceda y que las perdidas sean cuantiosas. Simular ataques con virus o perdidas del servidor, hacer que la red en algún departamento sea cortada para estimar el tiempo de reacción las perdidas y el tiempo de respuesta. Reducir los puntos

vulnerables y débiles de un sistema. También debemos tener en cuenta que controles muy estritos pueden causar problemas de disponibilidad de la información no se trata de crear algo que nadie pueda entender, si no de crear políticas con las que todos puedan trabajar.

Recomendaciones

Por muy buena que sea la seguridad en la empresa esta debe de ser flexible que tanto los que saben como los que no sepan las políticas, esto no es una tarea fácil pero se puede lograr y lo mas importante, implementar un plan de contingencia ante desastres naturales.

La información como decía con anterioridad pueden ser solo miles de kilobytes o el trabajo de una vida para alguien y esa información debe ser resguardada y protegida.

ANEXO I

CUESTIONARIOS

En el presente anexo se adjuntan algunos cuestionarios que pueden ser utilizados para la comprobar la seguridad en la empresa estos cuestionarios son explicativos no necesariamente tiene que ser así.

HARDWARE

- Topología y protocolos de red

- Protocolos
- Conexión al exterior con sucursales y fábrica

- Características del servidor:

- tipo o marca de servidor,
- capacidad de procesamiento,
- cantidad de memoria,
- capacidad de disco,
- placas de red,
- dispositivos varios (CD's, cintas, scanner, switch, hub, etc.),
- UPS o sistemas de alimentación alternativa del servidor,
- servidor alternativo, espejo o de contingencia,
- servidor de datos o de impresión,

Impresoras y Gestión de impresión

- PC´s

- Cantidad
- Características particulares

_ Terminales o PC´s

_ Clones o de marcas

_ Características generales

➢ Web

- Tipo de conexión
- Permisos o acceso de las PC´s
- Firewall y virus wall
- Página dinámica o estática
- Servidor propio o web hosting.

➢ Back up

- Disco espejo
- Tercerización
- Dispositivos de back up (CD's, cintas magnéticas, HD, disquete, etc.)

SOFTWARE

Software del servidor

- OS
- Aplicaciones
- Motor de bases de datos

➢ OS y software de las PC´s

➢ Aplicaciones bases en cada sector de la empresa (administración, ventas, cómputos, etc.)

➢ Gestión de virus.

Licencias.

USUARIOS

Organigrama.

Responsabilidades en área de informática

- Responsables de Redes
- Responsables de Bases de datos
- Responsables de Aplicaciones
- Responsables de Servicio técnico

➢ Tipo de perfiles de usuarios según sectores

- Clasificación del perfil
- Accesos del perfil a aplicaciones o datos.

2. SEGURIDAD LÓGICA

2.1 IDENTIFICACIÓN DE USUARIOS

2.1.1 Altas

- ¿Qué datos hay en el perfil del usuario cuando se hace un alta?

¿Se guardan los siguientes datos?

- ID de usuario,
- Nombre y apellido completo,
- Puesto de trabajo y departamento de la empresa,
- Jefe inmediato,
- Descripción de tareas,
- Consentimiento a que auditen sus actividades en el sistema, y de que conoce las normas de "buen uso" del sistema,
- Explicaciones breves y claras de cómo elegir su password,
- Tipo de cuenta o grupo al que pertenece (empleado, gerente, etc.),
- Fecha de expiración de la cuenta,
- Datos de los permisos de acceso y excepciones,
- Restricciones horarias para el uso de recursos,

- ¿Que otros datos del usuario son necesarios en el ID?

¿Que datos guardan en la planilla de Personal?

- ¿El ID de usuario puede repetirse?

¿Y si una cuenta fue borrada o eliminada, puede utilizarse un ID ya usado y eliminado para un usuario nuevo?

2.1.2 Bajas

- ¿Cómo se relacionan con el departamento de recursos humanos?

¿El departamento de recursos humanos se encarga de comunicar las modificaciones en el personal?

¿Qué se hace al respecto?

¿Cómo se actualiza la lista?

- ¿Cómo se administran los despidos (o desvinculación del personal)?

¿Se tiene en cuenta una política de despidos para evitar actos de vandalismo por posibles disgustos de los empleados desvinculados de la empresa?

- ¿Hay algún histórico de las cuentas que se dan de baja?
- ¿Se guardan los archivos y datos de las cuentas eliminadas?

¿Por cuánto tiempo?

¿Qué datos se guardan?

¿Con qué motivo?

2.1.3 Mantenimiento

- ¿Hay procedimientos para asignar los usuarios a un grupo de acuerdo a ciertas características?
- ¿Hay procedimientos para dar de alta, baja, modificar, suspender, etc. Una cuenta de usuario?
- ¿Se hacen revisiones de las cuentas de usuarios?

¿Se revisan sus permisos?

- ¿Hay procedimientos para determinar los nuevos requerimientos relacionados con cambios en funciones del empleado?

¿Cómo se mantienen actualizadas las cuentas cuando esto pasa?

- ¿Se documentan las modificaciones que se hacen en las cuentas?

¿Se lleva un histórico de los cambios?

2.1.4 Acciones correlativas a usuarios

- ¿Los usuarios se identifican en forma única o existen usuarios genéricos que todas las personas usan?

¿Todos los usuarios tienen un perfil o pertenecen a algún grupo?

- ¿El sistema genera históricos o logs de las actividades de los usuarios en el sistema, para poder seguirles el rastro?
- ¿Tienen forma de asignar responsabilidades individualmente a cada usuario, identificándolo a través de su ID?

2.1.5 Grupos – Roles

- ¿Existen grupos de usuarios?

¿Cómo se forman los grupos?

¿Según el departamento de la empresa donde trabajen, según el rol que desempeñen? ¿Por qué esa clasificación?

- ¿El acceso puede controlarse con el tipo de trabajo o la función (rol) del que pide acceso?
- ¿Los ID hacen referencia a una persona, o son anónimos? ¿Hacen referencia a un grupo?
- ¿Se eliminan los que vienen por default en el sistema operativo? (Cuentas Guest, por ejemplo)

2.1.6 Súper usuario

¿Que tipos de perfil de administrador hay?

- ¿Cuántas personas y quiénes son administradores?
- ¿Desde qué Terminal puede logearse un administrador?
- Además de la cuenta de administrador, ¿tienen otra cuenta para las funciones comunes?

3. AUTENTICACIÓN

3.1 Datos de autenticación

- ¿Cómo se protegen los datos de autenticación cuando están siendo ingresados por el usuario? ¿Qué se muestra en pantalla cuando se tipea el password? ¿Espacios, asteriscos, no se mueve el cursor?
- ¿Cómo se guardan los datos de autenticación en disco? ¿Encriptados? ¿Bajo password? ¿De que forma se los asegura?
- ¿Cómo se restringe el acceso a estos datos? ¿Hay un control de acceso más severo con estos datos? ¿Se los clasifica como confidenciales?
- ¿Quién tiene acceso a estos datos?
- ¿Cómo se transfieren los datos de autenticación desde la terminal que se logea hasta el servidor encargado de autenticar? ¿Encriptados, o solo en texto plano?

3.2 Firmas digitales

. ¿Se usan firmas digitales para autenticar a los usuarios dentro de la organización, cuando mandan mensajes internos? ¿Y para mensajes externos?

. ¿Serían necesarias para algún documento?

3.3 PASSWORDS

3.3.1 Generación

. ¿Las passwords son generadas con procesos automáticos (programas de generación de passwords) o son creadas por los usuarios? ¿Se usan estos programas en alguna máquina, por ejemplo en los servidores? ¿Qué características deben tener estas passwords?

- ¿Cuál es el conjunto de caracteres permitidos (alfa, numéricos y caracteres especiales)?
- ¿Cuál es el largo mínimo y máximo del password (seis a ocho, preferentemente nueve)?
- ¿La password se inicializa como expirada para obligar al cambio?
- ¿De qué forma se hace cumplir este requerimiento? ¿Se pone una fecha de expiración? ¿No se permite al usuario logearse ya que su password ha expirado? ¿Se chequean contra un diccionario on line para verificar que no sean palabras que existan?

. ¿Se permite que contengan el nombre de la empresa, o el nombre del usuario?

. ¿Dos cuentas pueden tener las mismas passwords?

. Sexiste más de una cuenta de administrador, ¿algunas de estas (o todas) tienen las mismas passwords?

4. VIRUS – ANTIVIRUS

4.1 Herramientas

. ¿Cuáles de éstas medidas o herramientas poseen para evitar los virus?

- Paquetes de software antivirus
- Firewalls
- Sistemas de detección de intrusos
- Monitorización para evaluar el tráfico de red y detectar anomalías, como la acción de troyanos.

- Creación de un disco de rescate o de emergencia
- Procedimientos para cuando ocurra una infección con virus.
- Hardware de seguridad de red dedicado
- Back up de datos

. ¿Está habilitada alguna herramienta antivirus mientras se envían y reciben mails? ¿Cuál? ¿Por qué se usa esa?

. ¿Están seguros que detecta los virus y los elimina correctamente?

. ¿Han probado con otra herramienta?

. ¿Qué precio tiene el antivirus que compran? ¿Y las actualizaciones?

¿Hay un antivirus instalado en cada PC (incluyendo los servidores) o hay un solo antivirus en toda la red?

. ¿Que significa que el antivirus sea corporativo? ¿Uno para los servidores y otra versión para los clientes? ¿En qué se diferencian?

4.2 Mensajes infectados – Procedimientos

. ¿Se han detectado mensajes infectados? ¿Que problemas trajo? ¿Era de Windows o de Linux? ¿Cómo lo solucionaron?

. Sse encuentra un mail con virus, ¿qué se hace para que no lleguen más de esa misma persona? ¿Se identifica la fuente del mail, para bloquearla desde el router o desde el servidor de correo? ¿Se avisa al ISP para que no deje entrar más mails de esa dirección? ¿Se observan los headers de los mails para identificar su origen verdadero?

. Slas disqueteras están activadas en las PC's de los usuarios, ¿cómo se aseguran que los usuarios analicen los disquetes antes de abrir archivos?

. ¿Se generan disco de rescate con el antivirus? ¿Para todas las máquinas o solo para los servidores? ¿Quién es el encargado de esto? ¿Alguna vez han sido necesarios?

. ¿Cómo es la protección contra el mail-bombing? ¿Que medidas se toman?

. ¿Suspenden la recepción de mail cuando el servidor está ocupado en un determinado porcentaje de su capacidad (80% por ejemplo)?

. ¿Qué procedimiento siguen en el caso de una infección con un virus?

. ¿Cada cuanto se hace un escaneo total de virus en los servidores? ¿Quién se encarga? ¿Se hace automáticamente cada vez que hay una actualización o periódicamente?

- ¿El escaneo de las maquinas se realiza por cuenta de cada usuario o lo realiza el encargado de sistemas? ¿No seria más seguro que el encargado lo haga a intervalos regulares de tiempo?
- ¿Qué prioridad tiene el SendMail?
- ¿El firewall tiene algo que ver con el análisis de los virus, o solo se encarga de los servicios de la red? ¿El antivirus y el firewall están relacionados de alguna forma, son compatibles entre sí? Ej. Firewall y antivirus de Norton se complementan para generar un nivel de seguridad superior.
- ¿Cómo se realiza el download de los mails desde el servidor hasta las PC's?

¿Cada PC se identifica según el usuario que se logea? ¿O es según el número de terminal de la PC en la red? ¿Se puede configurar una cuenta (Ej.: la de algún Gerente) en otra máquina (que no sea la del Gerente) y bajar los mails desde ahí?

4.3 Actualización de antivirus

¿Cómo se actualizan las definiciones de virus? ¿Quién las baja de Internet?

¿Quién ejecuta las actualizaciones en la PC's? ¿Cómo se enteran de las nuevas actualizaciones de virus?

¿Cuánto tiempo lleva diseminar y actualizar el antivirus en toda la organización?

¿Se hacen chequeos ocasionales para ver si se han actualizado los antivirus?

5. SEGURIDAD DE BASES DE DATOS

¿Los archivos de la base de datos tienen control de acceso?

¿O solo se hacen controles en las aplicaciones?

¿Se controlan las siguientes ocurrencias?

- tiempo y duración de los usuarios en el sistema,
- número de conexiones a bases de datos,
- número de intentos fallidos de conexiones a bases de datos,
- ocurrencias de deadlock con la base de datos,
- estadísticas de entrada-salida para cada usuario,
- generación de nuevos objetos de bases de datos,
- modificación de datos.

¿Se hace algún chequeo regular de la seguridad de la base de datos?

¿Se documentan los chequeos incluyendo lo siguiente?

- ¿Se hacen y son efectivos los backups y los mecanismos de seguridad?
- ¿Hay algún usuario de la base de datos que no tenga asignado un password?
- ¿Hay algún usuario que no ha usado la base de datos por un período largo de tiempo?
- Además del administrador de datos, ¿quién tiene acceso a los archivos del software de base de datos, a los del sistema operativo y a las tablas del sistema (FAT)?
- ¿Quién puede ejecutar un editor SQL?
- ¿Quién tiene acceso de lectura – escritura a los archivos de programa?
- ¿Qué usuarios tienen los mismos permisos que el administrador?
- ¿La base de datos tiene suficientes recursos libres para trabajar?

¿Se borran físicamente los registros de las bases de datos cuando un usuario los elimina, o se marcan como "borrados"?

6. SISTEMAS MÓVILES

¿Si se usan laptops o PC's portátiles, se tienen en cuenta los diferentes riesgos a los que se someten los datos de la empresa?

¿Los dueños de las laptops son conscientes de la inseguridad que generan al tener datos sensibles en ellas? ¿Tienen en cuenta estos puntos?

- ¿Se encriptan los datos en un sistema móvil?
- ¿Se almacenan en lugares seguros los equipos móviles?
- ¿Las laptop tienen password de acceso?
- ¿Cómo se maneja el trabajo desde la casa?
- ¿Se hacen backups de los datos de los sistemas móviles? ¿Cómo y en qué medio?

7. PLAN DE RECUPERACIÓN DE DESASTRES

- ¿Cuánto cuesta un plan de recuperación de desastres? ¿Tiene relación con la información a recuperar? ¿O a cualquier costo se salva la información crítica?
- ¿En el caso de que haya un plan, cada miembro del equipo tiene una responsabilidad asignada? ¿O la responsabilidad es del Departamento de Sistemas?
- ¿Se dividen las acciones correctivas en equipos de trabajo? ¿Cómo forman esos equipos? ¿Dependen del desastre ocurrido?

- ¿Luego del desastre existe un equipo de evaluación para corregir y documentar los errores cometidos en tal circunstancia, para luego generar un plan de contingencia de mayor efectividad y eficiencia?

7.1 Antes del desastre

- Identificación de las funciones críticas.

- ¿Cuáles serían los datos críticos a proteger en la organización, en el momento de un desastre? (Agregar lista de datos).

- ¿Cuáles serían los elementos de hardware y de software críticos a proteger en la organización, en el momento de un desastre? (Agregar lista de elementos).

- ¿Cómo se ordenarían según la importancia?

- Constitución del grupo de desarrollo del plan.

- ¿Quién sería le responsable del plan de emergencias, de su implementación y puesta en práctica? ¿El Jefe de Sistemas?

- En cada área que cubrirá el plan debe haber un líder del plan de contingencia. ¿Quién sugiere, el Jefe de cada área? ¿Alguien de más bajo rango? ¿Por qué?

Sistemas de información:

- ¿Existe un responsable de la información, en cada área de la empresa?

¿Conocen sus responsabilidades?

¿Los responsables que figuran en la documentación, son los que ejercen realmente el papel de responsables de la información?

¿Qué funciones tiene que cumplir?

- ¿Están identificados todos los sistemas de información y sus características (como si fuera un inventario de los sistemas)?

- ¿Qué datos se almacenan de los sistemas?

Se sugiere almacenar:

_ Nombre

_ Lenguaje

_ Departamento de la empresa que genera la información (dueño del sistema)

_ Departamentos de la empresa que usan la información

_ Volumen de archivos con los que trabaja

_ Volumen de transacciones diarias, semanales y mensuales que maneja el sistema

_ Equipamiento necesario para un manejo óptimo del Sistema

_ La(s) fecha(s) en las que la información es necesitada con carácter de urgencia.

_ El nivel de importancia estratégica que tiene la información de este Sistema para la Institución (medido en horas o días que la Institución puede funcionar adecuadamente, sin disponer de la información del Sistema).

_ Equipamiento mínimo necesario para que el Sistema pueda seguir funcionando (considerar su utilización en tres turnos de trabajo, para que el equipamiento sea el mínimo posible).

_ Actividades a realizar para volver a contar con el Sistema de Información (actividades de restauración).

- ¿Se puede dar un orden de importancia a los sistemas de la lista de arriba?

Equipos de cómputos:

- ¿Se mantiene un inventario de los equipos de cómputos? Se debería incluir:

_ Hardware: procesadores, tarjetas, teclados, terminales, estaciones de trabajo, computadoras personales, impresoras, unidades de disco, líneas de comunicación, cableado de la red, servidores de terminal, routers, bridges.

_ Software: programas fuente, programas objeto, utilerías, programas de diagnóstico, sistemas operativos, programas de comunicaciones.

_ Datos (principales archivos que contienen los equipos): durante la ejecución, almacenados en línea, archivados fuera de línea, backup, bases de datos, dueño designado de la información.

_ Configuración de los equipos (y sus archivos de configuración).

_ Ubicación de los equipos y de los datos.

_ Nivel de uso Institucional de los equipos.

- ¿Existen pólizas de seguros para los equipos en el caso de siniestros?

¿Cómo son estos seguros?

- ¿Las PC's o equipos se categorizan según su importancia (señalización no etiquetado de los Computadores de acuerdo a la importancia de su contenido, para ser priorizados en caso de evacuación.)?

- ¿Existe una relación de las PC's requeridas como mínimo para cada Sistema permanente de la Institución? ¿Está actualizada siempre?

. **Backup:**

- ¿Existen procedimientos para realizar backup?
- ¿Están incluidos en el plan de contingencia?

. Definición de los niveles mínimos de servicio.

- ¿Cuáles son las contingencias o problemas que pueden ocurrir?

(agregar lista de las posibles contingencias)

_ ¿Cuáles serían los peores problemas a los que se puede ver sometida la empresa? ¿Cuáles serian las peores contingencias?

_ ¿Cuáles serían las más probables?

_ ¿Cuáles son las que ocurren más a menudo?

_ ¿Cuales son las que no ocurren nunca?

- ¿Se pueden nombrar algunas funciones o servicios que funcionen como los niveles críticos de servicio para cada una de las contingencias nombradas arriba? ¿Qué opinión tiene el jefe de cada área en cuanto a los niveles críticos de su área? Un ejemplo puede ser: el que no se caiga el servidor de aplicaciones, o el router, o la conexión de radio.
- ¿Qué recursos se necesitan para que funcione este servicio?

¿Cuales son las prioridades de procesamiento que tendrán estas funciones o servicios críticos en caso de una emergencia?

. Evaluación de la relación coste / beneficio de cada alternativa.

- ¿Qué costo tendría cada uno de los niveles críticos de servicio que se determinaron arriba? Contar los costos de implementación, de mantenimiento, de entrenamiento de usuarios, y de restauración en caso de una emergencia.

Entrenamiento:

- ¿Entrenan al personal de alguna manera ante un siniestro?
- ¿Simulan siniestros para entrenar al personal?

7.2.Durante el desastre

. ¿Poseen un plan de emergencia (consiste de las acciones a llevar a cabo durante el siniestro)?

. ¿Se tienen en cuenta los distintos escenarios posibles? Ej.: durante el día, la noche.

. ¿Se incluyen los siguientes puntos?:

- ¿Vías de salida?
- ¿Plan de evacuación del personal?
- ¿Plan de puesta a buen recaudo de los activos?
- ¿Ubicación y señalización de los elementos contra el siniestro?
- ¿Existen funciones (encargado de retirar los equipos, encargado de las cintas, etc.) y equipos con funciones claramente definidas a ejecutar durante el siniestro?

7.3 Después del desastre

Después de ocurrido el Siniestro o Desastre es necesario realizar las actividades que se detallan, las cuales deben estar especificadas en el Plan de Acción

Evaluación de Daños:

¿Se realizan las siguientes actividades después de que ha ocurrido algún desastre?

- ¿Evalúan la magnitud del daño que se ha producido?
- ¿Que sistemas se están afectando?
- ¿Que equipos han quedado no operativos?
- ¿Cuales se pueden recuperar?
- ¿En cuanto tiempo?
- ¿Qué más se evalúa o debería evaluarse, según sus experiencias?

Ejecución de Actividades.

- ¿Se determina un coordinador que se encargará de las operaciones necesarias para que el sistema funcione correctamente, después de la emergencia?
- Para cada tipo de emergencia, de las enumeradas arriba, ¿qué acciones se deben tomar para que el sistema vuelva a su funcionamiento normal?

Evaluación de Resultados.

- ¿Se evalúan los desempeños de las personas, y del Plan, luego de ocurrido el desastre?
- ¿Se genera una lista de recomendaciones para minimizar los riesgos?

Retroalimentación del Plan de Acción.

- ¿Se evalúa el desempeño del personal durante el desastre?
- ¿Se tiene en cuenta la información que se obtiene luego de una emergencia para retroalimentar el Plan?

- ¿Vías de salida?
- ¿Plan de evacuación del personal?
- ¿Plan de puesta a buen recaudo de los activos?
- ¿Ubicación y señalización de los elementos contra el siniestro?
- ¿Existen funciones (encargado de retirar los equipos, encargado de las cintas, etc.) y equipos con funciones claramente definidas a ejecutar durante el siniestro?

7.3 Después del desastre

Después de ocurrido el Siniestro o Desastre es necesario realizar las actividades que se detallan, las cuales deben estar especificadas en el Plan de Acción

Evaluación de Daños:

¿Se realizan las siguientes actividades después de que ha ocurrido algún desastre?

- ¿Evalúan la magnitud del daño que se ha producido?
- ¿Que sistemas se están afectando?
- ¿Que equipos han quedado no operativos?
- ¿Cuales se pueden recuperar?
- ¿En cuanto tiempo?
- ¿Qué más se evalúa o debería evaluarse, según sus experiencias?

Ejecución de Actividades.

- ¿Se determina un coordinador que se encargará de las operaciones necesarias para que el sistema funcione correctamente, después de la emergencia?
- Para cada tipo de emergencia, de las enumeradas arriba, ¿qué acciones se deben tomar para que el sistema vuelva a su funcionamiento normal?

Evaluación de Resultados.

- ¿Se evalúan los desempeños de las personas, y del Plan, luego de ocurrido el desastre?
- ¿Se genera una lista de recomendaciones para minimizar los riesgos?

Retroalimentación del Plan de Acción.

- ¿Se evalúa el desempeño del personal durante el desastre?
- ¿Se tiene en cuenta la información que se obtiene luego de una emergencia para retroalimentar el Plan?

_ ¿Se reordena la lista de personal afectado en tareas de emergencia, con esta experiencia obtenida?

_ ¿Se modifican las prioridades? ¿Qué elemento tenía demasiada prioridad?

_ ¿Qué actividades faltaron incluir en el plan de emergencia?

_ ¿Qué se mejoraría?

_ ¿Cuál hubiera sido el costo de no haber tenido el plan de contingencias? ¿Qué se hubiera perdido?

ANEXO II

El Estado mexicano esta obligado a proteger los bienes jurídicos de los sectores que utilizan la informática como instrumento de desarrollo, por ello, requiere de un marco jurídico acorde al avance tecnológico.

Algunos estados de la República, conscientes de la necesidad de legislar en esta materia han adoptado en sus ordenamientos penales normas tendientes a la protección de la información; tal es el caso de Sinaloa, que tipifica al delito informático, o Morelos y Tabasco, que protegen la información mediante la tipificación de la violación a la intimidad personal.

CÓDIGO PENAL DEL ESTADO DE SINALOA

Ante la importancia que tiene que el Congreso Local del Estado de Sinaloa haya legislado sobre la materia de delitos, consideramos pertinente transcribir íntegramente el texto que aparece en el Código Penal Estatal.

Título Décimo

Delitos contra el patrimonio

Capítulo V

Delito Informático.

Artículo 217.- Comete delito informático, la persona que dolosamente y sin derecho:

Use o entre a una base de datos, sistemas de computadores o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio con el fin de defraudar, obtener dinero, bienes o información; o

Intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red.

Al responsable de delito informático se le impondrá una pena de seis meses a dos años de prisión y de noventa a trescientos días multa".

En el caso particular que nos ocupa cabe señalar que en Sinaloa se ha contemplado al delito informático como uno de los delitos contra el patrimonio, siendo este el bien jurídico tutelado.

Es claro que se ubicó al delito informático bajo esta clasificación dada la naturaleza de los derechos que se transgreden con la comisión de estos ilícitos, pero a su vez, cabe destacar que los delitos informáticos van más allá de una simple violación a los derechos patrimoniales de las víctimas, ya que debido a las diferentes formas de comisión de éstos, no solamente se lesionan esos derechos, sino otros como el derecho a la intimidad.

ANEXO III

CODIGO PENAL FEDERAL

LIBRO SEGUNDO

TITULO NOVENO

REVELACION DE SECRETOS Y ACCESO ILICITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA

CAPITULO II

ACCESO ILICITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA

ARTICULO 211 BIS 1.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

ARTICULO 211 BIS 2.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

ARTICULO 211 BIS 3.- Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de

información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.

ARTICULO 211 BIS 4.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

ARTICULO 211 BIS 5.- Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

ARTICULO 211 BIS 6.- Para los efectos de los artículos 211 Bis 4 y 211 Bis 5 anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 Bis de este Código.

ARTICULO 211 BIS 7.- Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.

Glosario

ACCESO: es la recuperación o grabación de datos que han sido almacenados en un sistema de computación. Cuando se consulta a una base de datos, los datos son primeramente recuperados hacia la computadora y luego transmitidos a la pantalla de terminal, desde donde pueden ser vistos, modificados o eliminados.

ACTIVE X: es un lenguaje de programación apoyado en controles OLE, Visual Basic y librerías del entorno Windows (OCX) de Microsoft. Active X permite que interactúen aplicaciones Windows con el World Wide Web (Internet).

ADSL: (Asymmetric Digital Suscribe Line - Línea de Usuario Digital Asimétrica). Usa la infraestructura telefónica actual para proveer servicios de transmisión de datos en alta velocidad.

AMENAZA: cualquier cosa que pueda interferir con el funcionamiento adecuado de una computadora personal o equipo informático, o causar la difusión no autorizada de información confiada a una computadora. Ejemplo: fallas de suministro eléctrico, virus, saboteadores o usuarios descuidados.

ANTIVIRUS: son todos aquellos programas que permiten analizar memoria, archivos y unidades de disco en busca de virus. Una vez que el antivirus ha detectado alguno de ellos, informa al usuario procediendo inmediatamente y de forma automática a desinfectar los ficheros, directorios, o discos que hayan sido víctimas del virus.

ARCHIVO DE PROCESO POR LOTES (.BAT o BATCH): los ficheros de proceso por lotes o ficheros Batch se caracterizan por tener extensión BAT. Son ficheros de texto que contienen comandos, uno por cada línea escrita. Cuando se ejecuta este tipo de ficheros, cada una de las líneas en él escritas se va ejecutando de forma secuencial.

ARCHIVO, DOCUMENTO: estos términos tienen el mismo significado y hacen referencia a la información que se encuentra en un soporte de almacenamiento informático.

Es el trabajo real que realiza cada usuario (textos, imágenes, bases de datos, hojas de cálculo, etc.). Cada uno de ellos se caracteriza por tener un nombre identificativo. El nombre puede estar seguido de un punto y una extensión, compuesta por tres caracteres que identifican el tipo de fichero del que se trata. Algunas extensiones

comunes son: EXE y COM (ficheros ejecutables, programas), TXT y DOC (ficheros de texto), etc.

ATAQUE: término general usado para cualquier acción o evento que intente interferir con el funcionamiento adecuado de un sistema informático, o intento de obtener de modo no autorizado la información confiada a una computadora.

ATAQUE ACTIVO: acción iniciada por una persona que amenaza con interferir el funcionamiento adecuado de una computadora, o hace que se difunda de modo no autorizado información confiada a una computadora personal. Ejemplo: borrado intencional de archivos, la copia no autorizada de datos o la introducción de un virus diseñado para interferir el funcionamiento de la computadora.

ATAQUE PASIVO: intento de obtener información o recursos de una computadora personal sin interferir con su funcionamiento, como espionaje electrónico, telefónico o la intercepción de una red. Todo esto puede dar información importante sobre el sistema, así como permitir la aproximación de los datos que contiene (en forma matricial), imágenes (lista de vectores o cuadros de bits), video (secuencia de tramas), etc.

DEPARTAMENTO DE CÓMPUTO: es la entidad encargada del buen uso de las tecnologías de la computación, organización y optimización de los recursos computacionales de la institución. Es la entidad encargada de desarrollar el plan estratégico que favorezca la prestación de servicios eficientes, eficaces y de utilidad en la transmisión de datos para apoyar efectivamente los requerimientos del usuario. Es la entidad encargada de ofrecer sistemas de información administrativa integral permitiendo en forma oportuna satisfacer necesidades de información, como apoyo en el desarrollo de las actividades propias del centro.

DOMINIO: conjunto de computadoras que comparten una característica común, como el estar en el mismo país, en la misma organización o en el mismo departamento. Cada dominio es administrado un servidor de dominios.

DOS (MS/DOS): estas siglas significan Disk Operating System (DOS). Se refieren a sistema operativo (S.O.) anterior a Windows que, en su momento, creó la empresa Microsoft.

EQUIPO DE CÓMPUTO: dispositivo con la capacidad de aceptar y procesar información en base a programas establecidos o instrucciones previas, teniendo la oportunidad de conectarse a una red de equipos o computadoras para compartir datos y recursos, entregando resultados mediante despliegues visuales, impresos o audibles.

EQUIPO DE TELECOMUNICACIONES: todo dispositivo capaz de transmitir y/o recibir señales digitales o analógicas para comunicación de voz, datos y video, ya sea individualmente o de forma conjunta.

FILTRO DE PAQUETES: programa que intercepta paquetes de datos, los lee y rechaza los que no estén en un formato predefinido.

FINGER: programa que muestra información acerca de un usuario específico, o acerca de todos los usuarios, conectados a un sistema remoto. Habitualmente se muestra el nombre y apellido, hora de la última conexión, tiempo de conexión sin actividad y terminal. Puede también mostrar archivos de planificación y de proyecto del usuario.

FIREWALL: es un sistema diseñado para evitar accesos no autorizados desde o hacia una red privada. Los Firewalls pueden estar implementados en hardware o software, o una combinación de ambos. Los firewalls son frecuentemente utilizados para evitar el acceso no autorizado de usuarios de Internet a redes privadas conectadas a la misma, especialmente intranets. Todos los mensajes que dejan o entran a la red pasan a través del firewall, el cual examina cada mensaje y bloquea aquellos que no cumplan con determinado criterio de seguridad.

FIRMA DIGITAL: valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje, permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación.

FTP: (File Transfer Protocol) protocolo parte de la arquitectura TCP/IP utilizado para la transferencia de archivos.

GUSANO: es programa similar a un virus que se diferencia de éste en su forma de realizar las infecciones. Mientras que los virus intentan infectar a otros programas copiándose dentro de ellos, los gusanos solamente realizan copias de ellos mismos.

HACKER: persona que tiene un conocimiento profundo acerca del funcionamiento de redes y que puede advertir los errores y fallas de seguridad del mismo. Al igual que un cracker busca acceder por diversas vías a los sistemas informáticos pero con fines de protagonismo.

HOST: (sistema central) computador que permite a los usuarios comunicarse con otros sistemas centrales de una red. Los usuarios se comunican utilizando programas de aplicación, tales como el correo electrónico, Telnet y FTP.

HTML: lenguaje de marcado de hipertexto, (Hyper-Text Markup Language) es el lenguaje con que se escriben los documentos en el World Wide Web (Internet).

HTTP: Protocolo de Transferencia de Hipertextos (Hyper-Text Transfer Protocol). Es el protocolo usado por el Word Wide Web para transmitir páginas HTML.

HUB: Un punto común de conexión de dispositivos en una red. Los hubs son usados comúnmente para conectar segmentos de una LAN. Un hub contiene múltiples puertos. Cuando un paquete llega al puerto, es copiado a los otros puertos, de esta manera los otros segmentos de la LAN pueden ver todos los paquetes. Un hub pasivo simplemente sirve de conductor de datos entre los diferentes puertos. Los llamados hubs inteligentes incluyen servicios adicionales como permitir a un administrador monitorear el tráfico y configurar cada puerto del hub. Estos hubs se conocen generalmente como hubs administrables (manageable hubs). Un tercer tipo de hub, llamado switching hub, lee la dirección de destino en cada paquete y lo envía al puerto correcto.

IDENTIFICACIÓN: un subtipo de autenticación, verifica que el emisor de un mensaje sea realmente quien dice ser.

INCIDENTE: cuando se produce un ataque o se materializa una amenaza, tenemos un incidente, como por ejemplo las fallas de suministro eléctrico o un intento de borrado de un archivo protegido

INFECCIÓN: es la acción que realiza un virus al introducirse, empleando cualquier método, en nuestro ordenador (o en dispositivos de almacenamiento) para poder realizar sus acciones dañinas.

INTEGRIDAD: se refiere a que los valores de los datos se mantengan tal como fueron puestos intencionalmente en un sistema. Las técnicas de integridad sirven para prevenir que existan valores errados en los datos provocados por el software de la base de

datos, por fallas de programas, del sistema, hardware o errores humanos. El concepto de integridad abarca la precisión y la fiabilidad de los datos, así como la discreción que se debe tener con ellos.

INGENIERÍA SOCIAL: Es la acción de engañar a un usuario o a un administrador de una red para conseguir su contraseña.

Bibliografía

"Seguridad: una Introducción". Dr MANUNTA, Gíovanni. Consultor y Profesor de Seguridad de Cranfield University. Revista Seguridad Corporativa. http://www.seguridadcorporativa.org

"Seguridad Informatica: sus Implicaciones e Implementacion" Cristian F. Borghello.

Seguridad Informática, ALDEGANI, Gustavo. Miguel.. MP Ediciones. Argentina. 1997. Página 22.

Glosario Básico Inglés-Español para usuarios de Internet CALVO, Rafael Fernández. 1994-2000. http://www.ati.es/novatica/2000/145

"Seguridad en Unix y Redes". HUERTA, Antonio Villalón. Versión 1.2 Digital - Open Publication License v.10. 2 de Octubre de 2000. http://www.kriptopoHs.com

ARDITA, Julio César. Director de Cybsec S.A. Security System y ex-Hacker. Entrevista personal realizada el día 15 de enero de 2001 en instalaciones de Cybsec S.A. http://www.cybsec.com

Delitos Informáticos, Estrada Garavilla Miguel

Plan de Seguridad Informatica
MARIA DOLORES CERINI, PABLO IGNACIO PRÁ, Universidad Catolica de Cordoba, Argentina.

ESTRATEGIAS DE SEGURIDAD, Autor: Christopher Benson, Inobits Consulting (Pty)

Denis Bensch, Dawie Human, Louis De Klerk y Johan Grobler, de Inobits Consulting (Pty) Ltd

Microsoft Solutions Framework

Microsoft es una marca registrada de Microsoft en Estados Unidos y en otros países..

http://www.microsoft.com/security/

http://www.forensics-intl.com/art12.html

http://www.fbi.gov/hq/lab/fsc/backissu/april2000/

http://www.delitosinformaticos.com

http://www.portaley.com

Auditoría Informática: un enfoque práctico. Mario Gerardo Piattini Velthius, Emilio del Peso Navarro. 1998 Alfa-Omega - Ra-ma.

Seguridad Computacional, Libro de Consulta para Administradores y Usuarios, Soler Amador Donado, Miguel Angel Niño Zambrano. Facultad de Ingeniería Eléctrica y Telecomunicaciones

Departamento de Seguridad en Cómputo de la UNAM

http://www.seguridad.unam.mx

La ayuda incondicional del **Ing. Miguel Ángel Alavarez Martínez** que sin experiencia en un tema tan nuevo no hubiera sido posible.