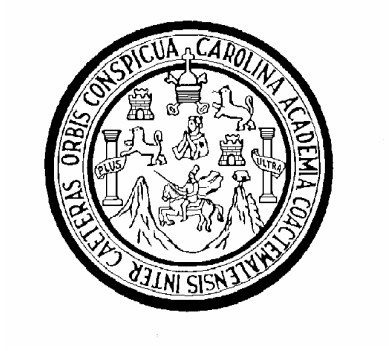
Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

COMPUTACIÓN FORENSE: UNA FORMA DE OBTENER EVIDENCIAS PARA COMBATIR Y PREVENIR DELITOS INFORMÁTICOS

Yuri Vladimir López Manrique
Asesorado por el Ing. Rolando Martín Gándara Grijalva

Guatemala, marzo de 2007

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA



FACULTAD DE INGENIERÍA

COMPUTACIÓN FORENSE: UNA FORMA DE OBTENER EVIDENCIAS PARA COMBATIR Y PREVENIR DELITOS INFORMÁTICOS

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA

FACULTAD DE INGENIERÍA

POR

YURI VLADIMIR LÓPEZ MANRIQUE

ASESORADO POR EL INGENIERO ROLANDO MARTÍN GÁNDARA GRIJALVA

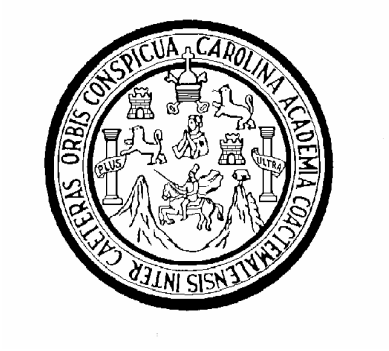
AL CONFERÍRSELE EL TÍTULO DE

INGENIERO EN CIENCIAS Y SISTEMAS

GUATEMALA, MARZO DE 2007

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA



NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Murphy Olympo Paiz Recinos
VOCAL I	Inga. Glenda Patricia García Soria
VOCAL II	Inga. Alba Maritza Guerrero de López
VOCAL III	Ing. Miguel Ángel Dávila Calderón
VOCAL IV	Br. Kenneth Issur Estrada Ruiz
VOCAL V	Br. Elisa Yazminda Vides Leiva
SECRETARIA	Inga. Marcia Ivonne Véliz Vargas

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Sydney Alexander Samuels Milson
EXAMINADOR	Ing. Ligia Maria Pimentel Castañeda
EXAMINADOR	Ing. Virginia Victoria Tala Ayerdi
EXAMINADOR	Ing. Bayron Wosbeli López López
SECRETARIO	Ing. Pedro Antonio Aguilar Polanco

HONORABLE TRIBUNAL EXAMINADOR

Cumpliendo con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

COMPUTACIÓN FORENSE: UNA FORMA DE OBTENER EVIDENCIAS PARA PREVENIR Y EVITAR DELITOS INFORMÁTICOS,

tema que me fuera asignado por la Dirección de la Escuela de Ingeniería en Ciencias y Sistemas, enero de 2006.

_____

Yuri Vladimir López Manrique

ACTO QUE DEDICO A

DIOS	Por ser fuente infinita de sabiduría.
LA VIRGEN MARIA	Por enseñarme a amar a Dios y a nuestros hermanos como ella les amo.
MIS PADRES	Quienes han sido modelo de esfuerzo, trabajo y honradez.
MIS HERMANOS	Gracias por su apoyo incondicional y amor.
MI ESPOSA	Glenda, por su apoyo incondicional.
FACULTAD DE INGENIERÍA	Por haberme brindado la oportunidad de estudiar una carrera universitaria.
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA	Por haberme brindado la oportunidad de estudiar en sus aulas centenarias**.**

AGRADECIMIENTOS A

DIOS	Por que en todo momento me ha guiado.
VIRGEN MARIA	Por colmarme de bendiciones.
MIS PADRES	En todo momento me apoyaron y me dieron el aliento necesario, sin su esfuerzo no hubiera alcanzado esta meta.
MIS HERMANOS	Gracias infinitas.
FAMILIARES	Con cariño sincero, especialmente a la Familia Herrera Manrique y Hector Efraín Veliz López.
MI ESPOSA	Desde el momento que la conocí me apoyo en la faena de alcanzar esta meta.
MIS AMIGOS	Juan Carlos, Edwin, Julio y a todos mis amigos, por su amistad y confianza.
MIS AMIGOS DE LA SUPER	Por sus consejos, amistad, apoyo y cariño.

Y a la Universidad de San Carlos de Guatemala

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

GLOSARIO

Base de datos: Conjunto de archivos interrelacionados que contienen la información de una organización. Interrelacionados implica que están organizados de una manera que contenga la menor redundancia posible.

Caja negra: Se refiere a un sistema cuyo interior no puede ser descubierto, cuyos elementos internos son desconocidos y que sólo puede conocerse "por fuera", a través de manipulaciones externas o de observación externa.

Consultor: Persona con una función independiente de control dentro de la organización para examinar y evaluar actividades de la misma.

Eficacia: La definición más sencilla es hacer las cosas de la manera correcta, ya que en las empresas se pueden llevar a cabo las actividades de una manera rápida pero pueden estar mal hechas.

Eficiencia: Es una parte vital de la administración y ésta se refiere a la relación entre los insumos y la producción. Si se puede obtener más producción con igual cantidad de insumos, habrá incrementado la eficiencia. Con frecuencia en algunas empresas definen la eficiencia como "hacer bien las cosas".

Endógeno: Variables que se forman dentro de un sistema y sirven para interactuar con el ambiente.

Heurística: Arte de inventar.

Informática: Es la parte de los sistemas informáticos que se encarga de organizar todo lo relacionado con el procesamiento, manejo y uso de la información. La función especifica de la informática es ver que la información se guarde de la mejor manera, que se le dé el uso apropiado para el cual se tiene, etc.

Lenguajes de Programación: Conjunto de instrucciones escritas con una sintaxis especial, que la computadora interpreta para lograr solucionar un problema.

Sistema: Conjunto de componentes que interactúan entre sí para lograr un objetivo común. Por su naturaleza pueden ser abiertos o cerrados.

Sistemas abiertos: Sistemas que presentan relaciones de intercambio con el ambiente, a través de entradas y salidas.

Sistemas cerrados: Sistemas que no presentan intercambio con el ambiente que los rodea, éstos son herméticos a cualquier influencia

ambiental. No reciben ninguna influencia del ambiente, pero tampoco influyen al mismo.

Sistema de información: El sistema es un conjunto de elementos organizados que se encuentran en interacción, que buscan de metas comunes, operando para ello sobre datos o información en una referencia temporal para producir como salida información.

OBJETIVOS

General

Definir un plan para implementar políticas de seguridad y las acciones a tomar en caso se presente un delito informático utilizando la computación forense para recabar pruebas, para apoyar la administración de sistemas.

Específicos

1. Definir qué es un delito informático y los potenciales atacantes.

2. Definir los principales métodos de ataque.

3. Definir una metodología para implementar un plan de prevención.

4. Como definir un plan y un equipo de recuperación en caso de un ataque.

5. Establecer cuáles son los Sistemas Detectores de Intrusos y cómo éstos ayudan a minimizar los daños en caso de ataque.

RESUMEN

La viabilidad de los proyectos y negocios sustentados en sistemas de información y telecomunicaciones no está determinada únicamente por las bondades de la tecnología en uso, sino también por la disponibilidad, confidencialidad y seguridad de la infraestructura, servicios, y datos.

La revisión y aseguramiento de estos factores han formado parte de la agenda de los profesionales en informática desde siempre. Sin embargo, la complejidad y evolución continua de los sistemas de comunicación, sumado a la creciente estadística de ataques y sabotajes informáticos, han convertido estos temas en una preocupación central de cualquier administración de sistemas.

Tanto los factores técnicos como aquellos relacionados con la variedad y originalidad de los ataques y sabotajes, aumentan el grado de vulnerabilidad e incertidumbre sobre la seguridad de la instalación.

La computación forense está adquiriendo una gran importancia dentro del área de administración de sistemas, esto debido al aumento del valor de la información y al uso que se le da a ésta, al desarrollo de nuevos espacios donde es utilizada (por Ej. Internet), y al extenso uso de computadores por parte de las compañías de negocios tradicionales (por Ej. Bancos), lo cual nos hace dependientes de los sistemas de información.

Es por esto que cuando se realiza un crimen, muchas veces la información queda almacenada en forma digital. Sin embargo, existe un gran problema, debido a que las computadoras guardan la información de forma tal que no puede ser recolectada o usada como prueba utilizando medios comunes, se deben utilizar mecanismos diferentes a los tradicionales. Es de aquí que surge el estudio de la computación forense como una ciencia relativamente nueva.

La información es considerada un activo muy valioso hoy día y desde esta perspectiva existen tres componentes que configuran la necesidad de protección de la información:

- Organización y Estructura: Referido a los medios y mecanismos que la organización tiene para proteger la información, recursos de personal, recursos técnicos y recursos de operación que debieran estar sujetas a Políticas de Seguridad.

- Rentabilidad y Productividad: Efecto que se relaciona con la continuidad de las operaciones, de manera que se mantengan operativos los procesos de la organización, si es aplicable y que tengan efectos económicos de no estar operativos.

- Ventaja Competitiva: Componente estratégico de la organización que pudiera tener un impacto si la integridad, confidencialidad y disponibilidad de la información se ven comprometidos.

Existe software en el mercado denominado Sistemas Detectores de Intrusos, este permite actuar en dos formas fundamentales; la prevención y la reacción. Con la implementación de estos sistemas se puede asegurar un nivel alto de seguridad en los sistemas, lo cual redundara en la confiabilidad de la integridad de la información y la reducción de pérdidas económicas y de credibilidad.

INTRODUCCIÓN

La acumulación de información ha sido sinónimo de poder. A lo largo del siglo XX los sistemas de información han evolucionado desde la cinta de papel perforado a las redes de computadoras conectadas a Internet. El potencial de cálculo de las computadoras, en el siglo actual, se duplica cada seis meses y la capacidad de almacenamiento de datos aumenta de forma exponencial. Así mismo se anuncia para la presente década la aparición de nuevas tecnologías de computación (cuántica, biológica) que permitirán el proceso simultáneo de miles de operaciones. En este siglo la introducción masiva de los sistemas informáticos en la administración, la defensa, el comercio, la industria, el mundo de los negocios, el ocio, etc. ha significado una revolución en las sociedades más avanzadas.

Pero precisamente ese crecimiento implica paralelamente una gran debilidad: al hacerse más complejos y más interconectados los sistemas aparecen más elementos vulnerables, en lo referente a la seguridad de la información, por dos razones básicas: los medios disponibles y el número de posibles manejadores o atacantes.

La tecnología y los medios para vulnerar un sistema son del mismo nivel de complejidad que los de protección del mismo, ya que tiene un origen tecnológico común.

Por otra parte, la extensión de la formación informática hace que se incremente el número de posibles atacantes con muy diversas motivaciones:

reto personal, ideas políticas o sociales y, como no, la posibilidad del beneficio económico.

Resulta muy difícil hablar de seguridad, ya que la seguridad absoluta no existe. Para poder establecer que un sistema informático es seguro es necesario identificar todas las amenazas a las que puede verse sometido y tomar todas las medidas preventivas y de seguridad correspondientes. Esta tarea se realiza basado en estándares internacionales y la aplicación de la Computación Forense.

El presente trabajo de graduación aborda el tema “Computación Forense: Una forma de obtener evidencias para combatir y prevenir delitos informáticos, definiendo qué es un delito informático, qué es la computación forense y la implementación de las mejores practicas basadas en estándares internacionales.

En el capituló uno se define el delito informático, los tipos de atacantes, tipos de ataques y el riesgo, este ultimo que depende en gran parte de la vulnerabilidad a la cual se encuentra expuesta el sistema de información.

El capítulo dos trata sobre la Computación Forense, definiendo la misma, los términos comúnmente utilizados, la obtención y el manejo de las pruebas.

El siguiente capítulo detalla la Computación Forense y el modelo de Gobernanza de seguridad digital de Cobit, detallando las mejores practicas para identificar, medir, monitorear y controlar los riesgos de seguridad digital.

El capítulo cuatro propone la creación de un equipo de respuesta a un ataque al detallar el porqué de la creación, la metodología para su creación y los pasos a seguir en caso de un ataque.

En el último capítulo se describen los Sistemas Detectores de Intrusos, esto como seguridad pasiva en los sistemas de información.

1 DELITO INFORMÁTICO

El término delito informático se acuñó a finales de los años noventa, a medida que Internet se expandió en todo el mundo. Después de una reunión en Lyón, Francia, se fundó un subgrupo del grupo de naciones que conforman el denominado "G8" con el objetivo de estudiar los nuevos problemas de criminalidad que eran propiciados por Internet o una red de telecomunicaciones. El "Grupo de Lyón" utilizó el término para describir, de forma muy imprecisa, todos los tipos de delitos perpetrados en Internet o en las nuevas redes de telecomunicaciones.

Al mismo tiempo, y guiado por los participantes en el grupo de Lyón, el Consejo Europeo comenzó a diseñar el Tratado sobre Delito Informático. Este tratado, que fuera presentado a la opinión pública por primera vez en el año 2000, incorporó una nueva gama de técnicas de vigilancia que las agencias encargadas de la aplicación de la ley consideraban necesarias para combatir el "delito informático".

Es un término muy amplio referido a los problemas que aumentaron el poder informático, abarataron las comunicaciones y provocaron que haya surgido el fenómeno de Internet para las agencias policiales y de inteligencia.

El tratado detalla los siguientes puntos relacionados:

- Delitos contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos.
- Delitos relacionados con las computadoras [falsificación y fraude].
- Delitos relacionados con el contenido [pornografía].

- Delitos relacionados con la violación del derecho de autor y los derechos asociados.
- Responsabilidades secundarias y sanciones [cooperación delictiva, responsabilidad empresarial].

Podríamos decir que el delito informático es toda acción consciente y voluntaria que provoca un perjuicio a una persona natural o jurídica sin que necesariamente conlleve a un beneficio material para su autor, o que por el contrario produce un beneficio ilícito para su autor aun cuando no perjudique de forma directa o inmediata a la víctima, y en cuya comisión interviene indispensablemente de forma activa dispositivos normalmente utilizados en las actividades informáticas.

En el desarrollo de un delito informático se puede identificar:

- Incidente
- Evento
- Riesgo

1.1 Incidente

Un incidente es cualquier evento relacionado con la seguridad de la información en el cual alguna política de seguridad ha sido violada. Los atributos de un incidente pueden incluir:

- Acceso no autorizado o intento de acceso al sistema de información.
- Interrupción o negación de servicio.
- Alteración o destrucción de los procesos de entrada, almacenamiento o salida de información.

- Cambios o intentos de cambio en hardware, software o firmware sin conocimiento del usuario.

1.1.1 Entendiendo un incidente

Cualquier ocurrencia que es clasificada como un ataque en el sistema, la red o una estación de trabajo es considerada un incidente. La información necesaria para entender un ataque incluye:

- La naturaleza del ataque.
- Por que el atacante escogió ese objetivo (pueda que nunca se sepa si el sujeto nunca es identificado)
- La aplicación de esta información para evaluar:
    - El nivel de riesgo
    - Daño o peligro potencial futuro

1.1.2 Alcance del Incidente

Una vez que la naturaleza del ataque esta completamente entendida, es necesario determinar que afecta. Esto puede incluir:

- Hardware
- Software
- Datos
- Personas
- Documentación física
- Comunicaciones

Esto debe determinarse sin importar si el ataque fue intencional o no.

1.1.3 Motivo del incidente

La naturaleza del motivo o motivos esta identificado y puede incluir:

- Venganza
- Codicia
- Curiosidad
- Envidia
- Necesidad de poder y control
- Conducta compulsiva o adictiva
- Beneficio personal (monetario o notoriedad)
- Actuar en nombre de alguien más
- Accidente o ignorancia

1.2 Evento

El personal involucrado en la administración de un sistema de información puede determinar la presencia de un evento basado en un hecho evidente en el sistema, regularmente este hecho es solo un atributo o una característica del evento.

Ejemplos de atributos de un evento son:

- Colapso del sistema
- Despliegue inusual de graficas
- Algo que no este “correcto”

Sin embargo estos por si mismos pueden ser catalogados como eventos, una exploración mayor de parte de los administradores de sistemas pueden cambiar los parámetros y reclasificar el evento en un incidente. La

reclasificación esta basada en el hecho que la ocurrencia esta basada en la violación de alguna política, un acto malicioso o una infracción externa.

1.3 Riesgo

La vulnerabilidad es una debilidad que expone un activo o bien (cualquier objeto de valor para la organización) a una pérdida o daño físico o lógico. Algunos ejemplos de vulnerabilidades incluyen:

- Fallas en las aplicaciones
- Redes no redundantes
- Seguridad física débil
- Fallas o supresión de los sistemas contra incendios

Un ataque es una persona o alguna condición que tiene alguna probabilidad de explotar una vulnerabilidad. Ejemplos de ataques incluyen:

- Un delincuente
- Un servicio de inteligencia externo
- El clima

El riesgo es descrito como la relación entre la vulnerabilidad y el evento. La formula es Riesgo = Vulnerabilidad * Evento. La vulnerabilidad es determinada por el valor del bien afectado.

El riesgo es la probabilidad que un evento explote la vulnerabilidad dando como resultado el daño a un bien en particular. El impacto o costo del daño a un bien es utilizado para calcular el riesgo. Para calcular el riesgo total de un bien en particular debe considerarse todas las vulnerabilidades y eventos relevantes.

1.4 Clasificación de los delitos

Existen tres tipos de delitos informáticos:

- Fraudes cometidos mediante manipulación de computadoras
- Daños o modificaciones de programas o datos informáticos
- Accesos no autorizados a servicios y sistemas informáticos

1.4.1 Fraudes cometidos mediante manipulación de computadoras

En los fraudes cometidos mediante la manipulación de computadoras se identifica las siguientes modalidades:

- Manipulación de los datos de entrada.
- Manipulación de programas.
- Manipulación de los datos de salida.
- Manipulación informática que aprovecha las repeticiones automáticas de los procesos de cómputo.

Manipulación de los datos de entrada: Este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.

Manipulación de programas: Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos

programas o nuevas rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el denominado “Caballo de Troya”, que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

Manipulación de los datos de salida: Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente estos fraudes se hacían con base en tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente equipos y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

Fraude efectuado por manipulación informática que aprovecha las repeticiones automáticas de los procesos de cómputo: Es una técnica especializada que se denomina "técnica del salchichón o salami" en la que "rodajas muy finas" apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra.

1.4.2 Daños o modificaciones de programas o datos computarizados

Los daños o modificaciones de programas y/o datos computarizados pueden ser ocasionados por:

- Sabotaje informático.
- Virus.

- Gusanos.
- Bomba lógica o cronológica.

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. Las técnicas más comunes que permiten cometer sabotajes informáticos son:

- 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 legítima de soporte lógico que ha quedado infectada.
- 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.
- 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, ya que se activa según una condición. Ahora bien, al contrario 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.

1.4.3 Accesos no autorizados a servicios y sistemas informáticos

Piratas informáticos o *hackers*: El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios que se mencionan a continuación: el delincuente

puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento o que vienen por defecto, que están en el propio sistema.

Reproducción no autorizada de programas informáticos: Esta puede entrañar una pérdida 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.

1.5 Tipos de atacantes

A raíz de la introducción de la informática en los hogares y los avances tecnológicos, ha surgido toda una generación de delincuentes que actúan en la Red y/o cualquier sistema de cómputo.

Todos ellos son catalogados como “piratas informáticos” o “piratas de la Red” la nueva generación de “rebeldes” de la tecnología aportan, sabiduría y enseñanza, y otros, destrucción o delitos informáticos. Hay que saber bien quien es cada uno de ellos y catalogarlos según sus actos de rebeldía en la mayoría de los casos.

Hasta la fecha esta nueva generación, ha sido dividida en una decena de grandes áreas fundamentales en las que reposan con fuerza, la filosofía de cada uno de ellos.

Todos y cada uno de los grupos aporta, en gran medida algo bueno en un mundo dominado por la tecnología, pero esto, no siempre sucede así. Algunos grupos ilícitos toman estas iniciativas como partida de sus actos rebeldes.

1.5.1 Hackers

Los *hackers* son el primer eslabón de una sociedad "delictiva" según los especialistas. Estos personajes son expertos en sistemas avanzados. En la actualidad se centran en los sistemas informáticos y de comunicaciones. Dominan la programación y la electrónica para lograr comprender sistemas tan complejos como la comunicación móvil. Su objetivo principal es comprender los sistemas y el funcionamiento de ellos.

Su objetivo es ingresar en sistemas informáticos, con el fin de decir aquello de "he estado aquí" o "fui yo" pero no modifican ni se llevan nada del computador atacado. Un *hacker* busca, primero el entendimiento del sistema tanto de *Hardware* como de *Software* y sobre todo descubrir el modo de codificación de las órdenes. En segundo lugar, busca el poder modificar esta información para usos propios y de investigación del funcionamiento total del sistema.

El perfil del *hacker* no es el típico charlatán de los computadores que vive solo y para los computadores, aunque si es cierto que pasa largas horas trabajando en él, ya que sin trabajo no hay resultados. Los conocimientos

que adquiere el *hacker* son difundidos por él, para que otros sepan como funciona realmente la tecnología.

Otros datos erróneos sobre la descripción del *hacker*, es aquella que los presenta como personas desadaptadas a la sociedad, pues hoy en día la mayoría son estudiantes de informática. El *hacker* puede ser adolescente o adulto, lo único que los caracteriza a todos por igual, son las ansias de conocimientos.

Los verdaderos *hackers* aprenden y trabajan solos y nunca se forman a partir de las ideas de otros, aunque es cierto que las comparten, si estas son interesantes. Este grupo es el más experto y menos ofensivo, ya que no pretenden serlo, a pesar de que poseen conocimientos de programación, lo que implica el conocimiento de la creación de Virus o *Crack* de un software o sistema informático.

Los buenos *hackers*, no son nunca descubiertos y apenas aparecen en la prensa, a menos que sean descubiertos por una penetración en un sistema demasiado seguro. En otras palabras, un *hacker* es una persona que tiene el conocimiento, habilidad y deseo de explorar completamente un sistema informático. El mero hecho de conseguir el acceso (adivinando la clave de acceso) no es suficiente para conseguir la denominación. Debe haber un deseo de liderar, explotar y usar el sistema después de haber accedido a él. Esta distinción parece lógica, ya que no todos los intrusos mantienen el interés una vez que han logrado acceder al sistema. En el submundo informático, las claves de acceso y las cuentas suelen intercambiarse y ponerse a disposición del uso general. Por tanto, el hecho de conseguir el acceso puede considerarse como la parte "fácil", por lo que aquellos que utilizan y exploran los sistemas son los que tienen un mayor prestigio.

1.5.2 Crackers

Es el siguiente eslabón y por tanto el primero de una familia rebelde. Cracker es aquel *Hacker* fascinado por su capacidad de romper sistemas y Software y que se dedica única y exclusivamente a *Crackear* sistemas.

Un *Crack* es el proceso o la llave necesaria para legalizar un *software* sin limites de tiempo y sin pagar por ello la respectiva licencia. Para los grandes fabricantes de sistemas y los medios de comunicación este grupo es el más peligroso de todos, ya que siempre encuentran el modo de romper una protección.

Pero el problema no radica ahí, sino en que esta rotura es difundida para conocimientos de otros, en esto comparten la idea y la filosofía de los *Hackers*. En la actualidad es habitual ver como se muestran los *Cracks* de la mayoría de *Software* de forma gratuita a través de Internet.

Crack es sinónimo de rotura y por lo tanto cubre buena parte de la programación de *Software* y *Hardware*. Así es fácil comprender que un Cracker debe conocer perfectamente las dos caras de la tecnología, esto es la parte de programación y la parte física de la electrónica.

El *Cracker* diseña y fabrica programas de guerra y hardware para reventar software y comunicaciones como el teléfono, el correo electrónico o el control de otros computadores remotos. Muchos *Crackers* “cuelgan” páginas Web por diversión.

1.5.3 Lamers

Este grupo es quizás el más numeroso que existe y quizás son los que mayor presencia tienen en el Internet. Normalmente son individuos con ganas de hacer *Hacking*, pero que carecen de cualquier conocimiento. Habitualmente son individuos que apenas si saben lo que es un computador, pero el uso de este y las grandes oportunidades que brinda Internet, convierten al nuevo internauta en un obsesivo ser que rebusca y relee toda la información que le fascina y que se puede encontrar en Internet. Normalmente la posibilidad de entrar en otro sistema remoto, le fascinan enormemente.

Este es quizás el grupo que más daño ocasiona ya que ponen en práctica todo el *Software* de *Hackeo* que encuentran en Internet. Así es fácil ver como un Lamer prueba a diestro y siniestro un "bombeador de correo electrónico" esto es, un programa que bombardea el correo electrónico ajeno con miles de mensajes repetidos hasta colapsar el sistema y después se ríe auto denominándose *Hacker*.

También emplean de forma habitual programas como los *Sniffers* (Programa que escucha el trafico de una Red) para controlar la Red, interceptan las contraseñas de las cuentas del sistema y después envían varios mensajes, con dirección falsa amenazando el sistema, pero en realidad no pueden hacer nada mas que cometer el error de que poseen el control completo de el disco duro, aun cuando el computador esta por fuera de una red.

Este tipo de personajes es quien emplea las terminales de trabajo, conocidas también como *Back Office, Netbus* o virus con el fin de generar miedo, sin tener conocimientos de lo que esta haciendo realmente.

1.5.4 Copyhackers

Son conocidos sólo en el terreno del *crackeo* de *Hardware*, mayoritariamente del sector de tarjetas inteligentes empleadas en sistemas de telefonía celular. La principal motivación de estos nuevos personajes, es el dinero.

1.5.5 Bucaneros

Son peores que los *Lamers*, ya que no aprenden nada ni conocen la tecnología. Comparados con los piratas informáticos, los bucaneros sólo buscan el comercio negro de los productos entregados por los *Copyhackers*. Los bucaneros sólo tienen cabida fuera de la red, ya que dentro de ella, los que ofrecen productos "*Crackeados*" pasan a denominarse "piratas informáticos", el bucanero es simplemente un comerciante, el cual no tienen escrúpulos a la hora de explotar un producto de *Cracking* a un nivel masivo.

1.5.6 Phreaker

Este grupo es bien conocido en la Red por sus conocimientos en telefonía. Se convirtió en una actividad de uso común cuando se publicaron las aventuras de John Draper, en un artículo de la Revista Esquire, en 1971. Se trata de una forma de evitar los mecanismos de facturación de las compañías telefónicas. Permite llamar de cualquier parte del mundo sin costo prácticamente. En muchos casos, también evita, o al menos inhibe, la posibilidad de que se pueda trazar el camino de la llamada hasta su origen, evitando así la posibilidad de ser atrapado. Para la mayor parte de los miembros del submundo informático, esta es simplemente una herramienta

para poder realizar llamadas de larga distancia sin tener que pagar enormes facturas. La cantidad de personas que se consideran *Phreakers*, contrariamente a lo que sucede con los *Hackers*, es relativamente pequeña. Pero aquellos que si se consideran *Phreakers* lo hacen para explorar el sistema telefónico. La mayoría de la gente, aunque usa el teléfono, sabe muy poco acerca de este grupo.

Un *Phreaker* posee conocimientos profundos de los sistemas de telefonía, tanto terrestres como móviles. En la actualidad también poseen conocimientos de tarjetas prepago, ya que la telefonía celular las emplea habitualmente.

Sin embargo, en estos últimos tiempos, cuando un buen *Phreaker* debe tener amplios conocimientos sobre informática, ya que la telefonía celular o el control de centrales es la parte primordial a tener en cuenta y/o emplean la informática para su procesado de datos.

1.5.7 Newbie

Es un novato o más particularmente es aquel que navega por Internet, tropieza con una página de Hacking y descubre que existe un área de descarga de buenos programas de *Hackeo*. Después se baja todo lo que puede y empieza a trabajar con los programas. Al contrario que los *Lamers*, los *Newbies* aprenden el *Hacking* siguiendo todos los cautos pasos para lograrlo y no se mofa de su logro, sino que aprende.

1.5.8 Cript Kiddie

Denominados también "*Skid kiddie*", son el último eslabón de los clanes de la red. Se trata de simples usuarios de Internet, sin conocimientos sobre *Hack* o *Crack* en su estado puro. En realidad son devotos de estos temas, pero no los comprenden. Simplemente son ínternautas que se limitan a recopilar información. En realidad se dedican a buscar programas de *Hacking* y después los ejecutan, sin tener idea de sus consecuencias y muchas veces sus mismas computadoras se ven afectadas. Esta forma de actuar, es la de total desconocimiento del tema, lo que le lleva a probar y probar aplicaciones de *Hacking*.

1.6 Tipos de Ataques

Existen diferentes técnicas y procedimientos al realizar un ataque, podemos identificar los siguientes:

- Ingeniería social
- Ingeniería social inversa
- *Shoulder surfing*
- Ataques de autenticación
- Diccionarios
- Negación de servicio
- Modificación daño
- Errores de diseño, implementación y operación

En los ataques se puede identificar claramente dos elementos el sujeto activo y el sujeto pasivo, este último sin saber que esta interactuando.

1.6.1 Sujeto Activo

Se llama así a las personas que cometen los delitos informáticos. Son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, pues, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas, aún cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

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 delitos cometidos. De esta 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.

El nivel típico de aptitudes del delincuente informático es tema de controversia, ya que para algunos 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, teniendo 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 criminólogo norteamericano Edwin Sutherland en el año de 1943.

La "cifra negra" es muy alta; no es fácil descubrirlos ni sancionarlos, 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. A los sujetos que cometen este tipo de delitos no se considera delincuentes, no se los segrega, no se los desprecia, ni se los desvaloriza; por el contrario, es considerado y se considera a sí mismo "respetable". Estos tipos de delitos, generalmente, son objeto de medidas o sanciones de carácter administrativo y no privativos de la libertad.

1.6.2 Sujeto Pasivo

Este, la víctima del delito, es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo. Las víctimas pueden ser individuos, instituciones crediticias, instituciones militares, gobiernos, etc. 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 a estos podemos conocer los diferentes ilícitos que cometen los delincuentes informáticos.

Es imposible conocer la verdadera magnitud de los delitos informáticos, ya que la mayor parte no son descubiertos 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 aplicar el tratamiento jurídico adecuado; 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, trae como consecuencia que las estadísticas sobre este tipo de conductas se mantenga bajo la llamada "cifra negra".

En los primeros tiempos, los ataques involucraban poca sofisticación técnica. Los atacantes internos (operadores, programadores, usuarios internos) utilizaban sus permisos para alterar archivos o registros. Los atacantes externos ingresaban a la red simplemente averiguando una clave válida. A través de los años se han desarrollado formas cada vez más sofisticadas de ataque para explotar "agujeros" en el diseño, configuración y operación de los sistemas.

Son muchos los autores que describen con detalle las técnicas y las clasifican de acuerdo a diferentes características de los mismos. Ante la diversificación de clasificaciones de amenazas y la inminente aparición de nuevas técnicas, para la realización del presente trabajo se darán las clasificaciones de los ataques más comunes.

Cada uno de los ataques abajo descritos será ejecutado en forma remota. Se define Ataque Remoto como "un ataque iniciado contra una máquina sobre la cual el atacante no tiene control (físico)". Esta máquina es distinta a la usada por el atacante y será llamada Víctima.

1.6.3 Ingeniería social

Es la manipulación de las personas para convencerlas de que ejecuten acciones o actos que normalmente no realizan para que revele todo lo necesario para superar las barreras de seguridad. Si el atacante tiene la experiencia suficiente -generalmente es así-, puede engañar fácilmente a un usuario -que desconoce las mínimas medidas de seguridad- en beneficio propio. Esta técnica es una de las más usadas y efectivas a la hora de averiguar nombres de usuarios y claves.

Por ejemplo, suele llamarse a un usuario haciéndose pasar por Administrador del sistema y requerirle la clave con alguna excusa convincente. O bien, podría enviarse un correo electrónico (falsificando la dirección origen a nombre del Administrador) pidiendo al usuario que modifique su clave a una palabra que el atacante suministra. Desde aquí se tendrá el control total de esa estación de trabajo.

Para evitar situaciones de ingeniería social es conveniente tener en cuenta estas recomendaciones:

- Tener servicio técnico propio o de confianza.
- Instruir a los usuarios para que no respondan ninguna pregunta sobre cualquier característica del sistema y deriven la inquietud a los responsables que tenga competencia para dar esa información.
- Asegurarse que las personas que llaman por teléfono son quien dicen ser. Por ejemplo, si la persona que llama se identifica como proveedor de Internet lo mejor es cortar y devolver la llamada a forma de confirmación.

1.6.4 Ingeniería social inversa

Este tipo de ataque se realiza para observar a la victima y su sistema, con el objetivo de establecer sus vulnerabilidades y posibles formas de acceso futuro. También es llamado Ataque de monitorización.

1.6.5 *Shoulder Surfing*

Llamado también Señuelos (Decoy), Búsqueda, TCP *Connect Scanning* o *TCP SYN Scanning*. Cuando dos procesos establecen una comunicación usan el modelo Cliente/Servidor para establecer la conexión. La aplicación del Servidor "escucha" todo lo que ingresa por los puertos.

La identificación del Servidor se efectúa a través de la dirección IP del sistema en el que se ejecuta y del número de puerto del que depende para la conexión. El Cliente establece la conexión con el Servidor a través del puerto disponible para luego intercambiar datos.

La información de control llamada *HandShake* (saludo) se intercambia entre el Cliente y el Servidor para establecer un dialogo antes de transmitir datos. Los "paquetes" o segmentos TCP tienen banderas que indican el estado del mismo.

El protocolo TCP de Internet, sobre el que se basa la mayoría de los servicios (incluyendo el correo electrónico, el web y el IRC) implica esta conexión entre dos máquinas. El establecimiento de dicha conexión se realiza mediante lo que se llama *Three-Way Handshake* (“conexión en tres pasos”), ya que intercambian tres segmentos.

La técnica TCP SYN Scanning, se implementa un escaneo de "media-apertura", dado que nunca se abre una sesión TCP completa. Se envía un paquete SYN (como si se fuera a usar una conexión real) y se espera por la respuesta. Al recibir un SYN/ACK se envía, inmediatamente, un RST para terminar la conexión y se registra este puerto como abierto.

La principal ventaja de esta técnica de escaneo es que pocos sitios están preparados para registrarlos. La desventaja es que en algunos sistemas Unix, se necesitan privilegios de Administrador para construir estos paquetes SYN.

1.6.6 Ataques de autenticación

Este tipo de ataque tiene como objetivo engañar al sistema de la víctima para ingresar al mismo. Generalmente este engaño se realiza tomando las sesiones ya establecidas por la víctima u obteniendo su nombre de usuario y clave. También se le denomina *TCP FIN Scanning-Stealth Port Scanning, Fragmentation Scanning y Eavesdropping-Packet Sniffing*.

1.6.7 Diccionarios

Los Diccionarios son archivos con millones de palabras, las cuales pueden ser claves utilizadas por los usuarios. Este archivo es utilizado para descubrir dicha clave en pruebas de fuerza bruta.

El programa encargado de probar cada una de las palabras encripta cada una de ellas (mediante el algoritmo utilizado por el sistema atacado) y compara la palabra encriptada contra el archivo de clave del sistema atacado

(previamente obtenido). Si coinciden se ha encontrado la clave de acceso al sistema mediante el usuario correspondiente a la clave hallada.

A esta técnica se le conoce también como:

- Spoofing-Looping
- Spoofing
- IP Spoofing
- DN2S Spoofing
- Web Spoofing
- IP Splicing-Hijacking
- Utilización de BackDoors
- Utilización de Exploits
- Obtención de Passwords

1.6.8 Negación de Servicio (*DENIAL OF SERVICE, DoS*)

Los protocolos existentes actualmente fueron diseñados para ser empleados en una comunidad abierta y con una relación de confianza mutua. La realidad indica que es más fácil desorganizar el funcionamiento de un sistema que acceder al mismo; así los ataques de Negación de Servicio tienen como objetivo saturar los recursos de la víctima de forma tal que se inhabilita los servicios brindados por la misma.

1.6.9 Ataques de modificación-daño

Esta categoría se refiere a la modificación desautorizada de los datos o el software instalado en el sistema víctima (incluyendo borrado de archivos). Son particularmente serios cuando el que lo realiza ha obtenido

derechos de Administrador o Supervisor, con la capacidad de ejecutar cualquier comando y por ende alterar o borrar cualquier información que puede incluso terminar en la baja total del sistema. Aún así, si no hubo intenciones de “bajar” el sistema por parte del atacante; el Administrador posiblemente necesite darlo de baja por horas o días hasta chequear y tratar de recuperar aquella información que ha sido alterada o borrada.

Se le puede encontrar bajo los siguientes nombres:

- Jamming o Flooding
- Syn Flood
- Connection Flood
- Net Flood
- Land Attack
- Smurf o Broadcast Storm
- OOB, Supernuke o Winnuke
- Teardrop I y II-Newtear-Bonk-Boink
- E-Mail Bombing-Spamming

1.6.10 Errores de diseño, implementación y operación

Muchos sistemas están expuestos a "agujeros" de seguridad que son explotados para acceder a archivos, obtener privilegios o realizar sabotaje. Estas vulnerabilidades ocurren por variadas razones, y miles de “puertas invisibles” son descubiertas (cada día) en sistemas operativos, aplicaciones de software, protocolos de red, *browsers* de Internet, correo electrónico y todas clase de servicios informático disponible.

2 COMPUTACIÓN FORENSE

2.1 Introducción

La computación forense está adquiriendo una gran importancia dentro del área de la información electrónica, esto debido a:

- Al aumento del valor de la información y/o al uso que se le da a ésta.
- Al desarrollo de nuevos espacios donde es usada (por Ej. El Internet).
- Al extenso uso de computadores por parte de las compañías de negocios tradicionales (por Ej. bancos).

Es por esto que cuando se realiza un delito informático, muchas veces la información del mismo queda almacenada en forma digital. Sin embargo, existe un gran problema, debido a que las computadores guardan la información de forma tal que no puede ser recolectada o usada como prueba utilizando medios comunes, se deben utilizar mecanismos diferentes a los tradicionales. Es de aquí que surge el estudio de la computación forense como una ciencia relativamente nueva.

Resaltando su carácter científico, tiene sus fundamentos en las leyes de la física, de la electricidad y el magnetismo. Es gracias a fenómenos electromagnéticos que la información se puede almacenar, leer e incluso recuperar cuando se creía eliminada.

La computación forense, aplicando procedimientos estrictos y rigurosos, puede ayudar a resolver grandes crímenes apoyándose en el

método científico, aplicado a la recolección, análisis y validación de todo tipo de pruebas digitales.

2.2 Definición

La computación forense es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional.

También se define como el proceso de identificar, preservar, analizar y presentar evidencia digital de tal forma que puede ser aceptada en la solución de un caso donde esta involucrada la tecnología digital para investigar un crimen tecnológico.

La computación forense no es utilizada solo para investigar crímenes tecnológicos, como lo son el ingreso no autorizado a una red o la distribución de material ilegal, también es utilizada para investigar cualquier crimen donde una computadora puede tener alguna evidencia almacenada (por ejemplo, correo electrónico entre una victima de violación y el violador).

2.3 Objetivos de la computación forense

La computación forense tiene 3 objetivos primordiales:

- La compensación de los daños causados por los criminales o intrusos.
- La persecución y procesamiento judicial de los criminales.
- 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.

2.4 Usos de la Computación Forense

Existen varios usos de la computación forense, muchos de estos usos provienen de la vida diaria, y no tienen que estar directamente relacionados con la computación forense:

- Prosecución Criminal: Evidencia incriminatoria que puede ser usada para procesar una variedad de crímenes, incluyendo homicidios, fraude financiero, tráfico y venta de drogas, evasión de impuestos o pornografía infantil.
- Litigación Civil: Casos que tratan con fraude, discriminación, acoso, divorcio, pueden ser ayudados por la computación forense.
- Investigación de Seguros: La evidencia encontrada en computadores, puede ayudar a las compañías de seguros a disminuir los costos de los reclamos por accidentes y compensaciones.
- Temas corporativos: Puede ser recolectada información en casos que tratan sobre acoso sexual, robo, mal uso o apropiación de información confidencial o propietaria, o aún de espionaje industrial.
- Mantenimiento de la ley: La computación forense puede ser usada en la búsqueda inicial de órdenes judiciales, así como en la búsqueda de información una vez se tiene la orden judicial para hacer la búsqueda exhaustiva.

2.5 Importancia de la computación forense

A primera vista pareciera que la computación forense no es importante hasta que se examinan los eventos que conllevan al uso de esta.

Existen visitantes no autorizados en las redes de las organizaciones, estos pueden ser internos o externos. Estos visitantes pueden tener conocimientos técnicos muy altos y esto los hará destructivos y los daños serán de muy alto costo, en algunas ocasiones en forma monetaria y otras en imagen. Para detectar la técnica que fue utilizada y el daño que causaron debe de hacerse uso de la computación forense.

Los delitos informáticos son perpetrados en una variedad de formas. Las computadoras son el objetivo o son utilizadas para ejecutar el crimen, las huellas y pistas de estos delitos son almacenadas en forma digital. Para obtener la evidencia dejada es necesario hacer uso de la computación forense.

Los fraudes ejecutados por medios tecnológicos merecen atención especial por el alto costo que estos representan para las organizaciones. Casi todos los fraudes utilizan una computadora y es en esta en donde queda almacenada la evidencia, por lo que personal entrenado será necesario para llevar a cabo la investigación. Este personal debe tener conocimiento de computación forense.

Otras instancias que requerirán de la computación forense incluyen el uso de Internet en forma inapropiada, el uso de correo electrónico en una forma no correcta, el uso del equipo en una red para un fin que no fue especificado u orientado, violación de políticas o procedimientos de seguridad, violaciones a los derechos de propiedad intelectual y alteraciones

de los medios tecnológicos. Cualquier pista o evidencia será obtenida por medio de la computación forense.

Si no se esta preparado para alguno de los casos antes expuestos al momento de darse alguno se estará sujeto a presiones de tiempo y costos muy altos.

2.6 Valores agregados de la Computación Forense

Si bien se menciona que la computación forense es una ciencia que se encarga de analizar sistemas informáticos en busca de evidencia que colabore a llevar adelante una causa judicial o una negociación extrajudicial, el resultado de una investigación forense también puede determinar oportunidades de mejoramiento en los controles de los procesos de la organización, ya que el caso investigado pudo haberse facilitado por algunas debilidades de control.

Las siguientes serían algunas medidas de control que se podrían implementar:

- Revisar, evaluar y reducir al mínimo necesario el número de funcionarios con acceso a transacciones que alteren la información.
- Implementar la doble intervención (supervisión) en la realización de las transacciones de cancelación.
- Segregación de funciones entre los funcionarios que realizan los ajustes al sistema y los que realizan cuadres.
- Monitoreo periódico de las transacciones de cancelación.
- Clarificar y detallar las funciones de las personas que laboran en el centro operativo.
- Reiterar a los funcionarios las normas sobre el manejo de las claves de acceso al sistema.

2.7 Dificultades que se le podrían presentar al investigador forense

El profesional de la computación forense enfrentara en sus labores algunas dificultades, las cuales podrán relacionarse con el personal, los procesos, escasa o ninguna documentación de los sistemas, etc.

A continuación se enumeran algunas de las dificultades a las cuales podrá enfrentarse:

- No contar con los registros de auditoría. Esto puede suceder, porque el aplicativo no los tiene implementados o si los tiene, están desactivados (la entidad podría justificar que los *logs* están degradando la máquina).
- Registros incompletos o no claros de las pistas de auditoría. Esto ocurre porque solo se graban algunos campos para no cargar el sistema o no existen descripciones detalladas de los *logs*.
- No se realiza un buen levantamiento de información de la arquitectura del sistema y se dificulta determinar la forma y quién realizó la transacción fraudulenta.
- Poca habilidad en el manejo de las herramientas.
- Resistencia por parte de los funcionarios para suministrar información porque no les agrada ser investigados o porque podrían estar relacionados con el ilícito.
- Restricción de acceso a la información de la entidad. Si se cuenta con el conocimiento y las herramientas necesarias, los funcionarios de seguridad informática y/o auditoría de sistemas de la entidad podrían adelantar la investigación forense y no habría mayor dificultad en el acceso a la información; pero si se requiere que por la especialización del tema lo realice un tercero, éste investigador deberá trabajar de manera estrecha con las áreas de seguridad bancaria, jurídica y la auditoría de sistemas.

2.8 Evidencia

Para la obtención de evidencia hay que estar relacionado con los diferentes medios de almacenamiento y su funcionamiento. Si se dio un delito o hay la sospecha del mismo, existen muchos medios por los cuales el delincuente informático pueda esconder o mover los datos y las pistas, desde un medio de almacenamiento como puede ser su computadora a un medio portátil de almacenamiento.

La lista incluye memorias flash que son tan pequeñas que pueden ser llevadas en la bolsa de una prenda de vestir o la palma de la mano, también pueden ser disfrazadas como plumas, relojes digitales, cámaras digitales, chips de memoria para cámaras digitales y estos pueden ser escondidos en un sobre, PDA's y teléfonos celulares, estos últimos pueden almacenar una variedad de información tal como mensajes de voz, mensajes de texto, notas en archivos almacenados, números telefónicos y direcciones, así como bitácoras de llamadas perdidas, recibidas y hechas.

La razón de esta lista es para recordar que, cuando se realiza una investigación, se debe de pensar en todos los medios posibles de almacenamiento de información, deben de buscarse estos y ponerlos en custodia para su posterior análisis.

Debe tenerse especial cuidado en el manejo y custodia de la evidencia, la evidencia puede verse corrupta debido a un mal manejo. Dependiendo del tipo de delincuente informático puede darse que este tenga configurado su equipo para borrarse o corromperse al momento de

reinicializar o conectarlo, lo cual eliminara la evidencia, razón por la cual un experto debe de estar a cargo de la manipulación.

2.9 Pasos para la Recolección de Evidencia

El procedimiento para la recolección de evidencia varía de un caso a otro. Sin embargo, existen unas guías básicas que pueden ayudar a cualquier investigador forense:

2.9.1 Lineamientos Generales para la Recolección de Evidencias

El aspecto más importante a la hora de recolectar evidencia, es la preservación de la integridad de ésta; en el caso particular de la información almacenada en medios magnéticos, la naturaleza volátil de ésta hace que dicha labor sea particularmente difícil.

La primera gran decisión que se debe tomar a la hora de colectar evidencias, es la cantidad de ésta que se debe tomar. Un investigador podría estar tentado a llevarse todo el equipo que encuentre, para no arriesgarse a dejar piezas de información potencialmente importantes. Sin embargo, esta alternativa tiene sus inconvenientes, ya que el investigador podría terminar siendo demandado por dañar o alterar la vida de una persona o de un negocio más de lo absolutamente necesario. Desde este punto de vista, quizás lo indicado sería incautar sólo lo mínimo necesario para efectuar una investigación. Aunque en últimas, es la severidad y la categoría del crimen las que determinan cuánta evidencia digital se debe recolectar.

El *hardware* es uno de los elementos que se deben tener en cuenta a la hora de la recolección de evidencia, debido a que puede ser usado como

instrumento, como objetivo del crimen, o como producto del crimen (por Ej. contrabando o robo), es por esto que se deben tener consideraciones especiales. Lo primero que se debe preguntar el investigador es qué partes se deben buscar o investigar. Generalmente, es necesario recolectar computadores y, de ser necesario, elementos de almacenamiento (CDs, cintas magnéticas, *diskettes*, etc.) que puedan contener evidencia.

En este punto se debe tomar otra decisión crítica: ¿los equipos involucrados en una investigación deben ser apagados, o deben permanecer encendidos? Muchas agencias de cumplimiento de la ley recomiendan apagar los equipos en todas las situaciones, y los expertos insisten en que es la mejor alternativa debido a la posibilidad de que la evidencia sea destruida mientras el computador permanece encendido. Aún así, hay casos en que apagar un equipo puede causar más daños que beneficios, por ejemplo, si se trata de un servidor que presta servicios a muchas personas que no necesariamente están involucradas en una investigación. Como siempre, la mejor opción para el investigador es utilizar su buen juicio y sentido común para determinar las acciones a seguir.

Cuando se presenta el caso en que la evidencia está en formato digital el objetivo de la investigación debe ser el contenido del computador, no el *hardware* de éste. Hay dos opciones cuando se recolecta evidencia digital: copiar todo, o sólo copiar la información necesaria. Si se dispone de mucho tiempo y no se sabe a ciencia cierta qué se está buscando, lo ideal es copiar todo el contenido del computador y examinar todo detenidamente. Por otra parte, si lo que se necesita es una pista rápida, como pasa en la mayoría de casos, o sólo se necesita una porción de la evidencia digital, es más práctico buscar en el computador y tomar sólo lo que se necesite.

Cuando se recolecta todo el contenido de un computador, en general los pasos a seguir son los mismos:

- Toda la evidencia importante debe ser leída de la memoria RAM.
- El computador debe ser apagado.
- El computador debe ser reiniciado usando otro sistema operativo que desvíe el existente y no cambie el contenido de el (los) disco(s) duro(s).
- Debería sacarse una copia de la evidencia digital encontrada en el (los) disco(s) duro(s).

Debe tenerse en cuenta que cuando se habla de hacer una "copia" de un disco duro, ésta debería ser una copia bit-a-bit de todo el contenido de éste; muchísima información está "escondida" en sitios no-convencionales de un disco.

Hay otra gran categoría de evidencia que puede ser recolectada en el caso de los crímenes informáticos, y es la evidencia presente en las redes. Todo el flujo de información que corre a través de una red, sea interna o externa a una organización, o aún en Internet, podría contener evidencia potencialmente útil a la hora de investigar un crimen. Adicionalmente, hay ciertos tipos de crímenes, como la falsificación de correos electrónicos, intercambio de información ilegal a través de Usenet (por ej., pornografía infantil) o uso del IRC para concertar crímenes –práctica común entre la comunidad *hacker*-, que no podrían cometerse sin la utilización de redes.

En este caso, la evidencia digital difiere de aquella que está almacenada en un solo computador. Por lo general, se encuentra almacenada en computadores remotos o, aún peor, no está almacenada en ninguna parte, a no ser que se haga un esfuerzo explícito para capturarla (por ej., mediante el uso de *sniffers*). Los investigadores deberán hacer esfuerzos adicionales para poder demostrar que la evidencia en Internet es

auténtica y no ha sido modificada mientras estaba siendo transmitida o recolectada.

La evidencia presente en redes debe ser buscada de manera activa, y su recolección puede ser bastante dispendiosa puesto que la información podría estar almacenada en muchos sitios diferentes.

2.9.2 Cuidados en la Recolección de Evidencia

La recolección de evidencia informática es un aspecto frágil de la computación forense, especialmente porque requiere de prácticas y cuidados adicionales que no se tienen en la recolección de evidencia convencional. Es por esto que:

- Se debe proteger los equipos del daño.
- Se debe proteger la información contenida dentro de los sistemas de almacenamiento de información (muchas veces, estos pueden ser alterados fácilmente por causas ambientales, o por un simple campo magnético).
- Algunas veces, será imposible reconstruir la evidencia (o el equipo que la contiene), si no se tiene cuidado de recolectar todas las piezas que se necesiten.

2.9.3 Análisis de Evidencias

Una vez que se cuenta con todas las posibles evidencias de un delito informático, entra en juego el análisis de éstas. Esto involucra tareas como lo son:

- Análisis de *logs*

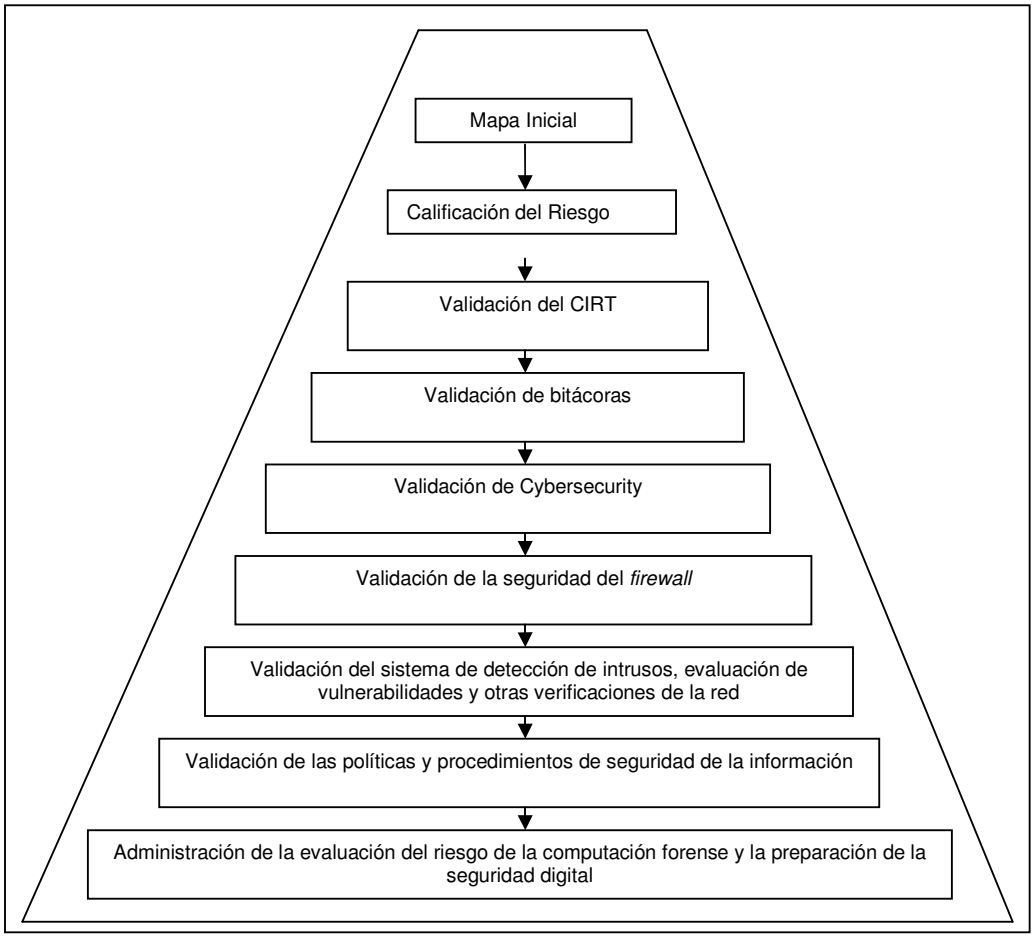
- Reconstrucción de información destruida
- Recuperación de información oculta

El punto que vale la pena recalcar, es que el análisis se debe llevar a cabo siguiendo una metodología rigurosa y científica, que permita la posterior reconstrucción de los pasos seguidos y que siempre conduzca al mismo resultado. También es imperativo preservar la integridad de la información que se está analizando, preferiblemente trabajando sobre una copia de ésta y no sobre el original para evitar alteraciones que podría invalidar la evidencia como una prueba aceptable.

3 COMPUTACIÓN FORENSE Y EL MODELO DE GOBERNANZA DE SEGURIDAD DIGITAL

La computación Forense y el Modelo de Gobernanza de Seguridad (figura 1), proveen un enfoque lógico para evaluar el riesgo. Específicamente, el aseguramiento de los procedimientos de tecnología es desarrollado como un componente mayor de la computación forense y la metodología de verificación de la seguridad digital para proveer la estructura del proceso de enfoque en riesgo.

Figura 1. **La Computación Forense y el Modelo de Gobernanza de Seguridad Digital**[1]



[1] Fuente www.isaca.org

El gobierno corporativo sobre la computación forense y la seguridad digital es un aliado entre los empleados, administradores, el comité de auditoria, los directores y consultores. Establecer una relación con cada individuo dentro de la organización es crucial para el éxito del establecimiento y mantenimiento de un modelo de gobernanza funcional.

La ejecución y la autoridad del modelo de gobernanza son regularmente implementadas por un profesional de aseguramiento tecnológico. La cadena de comunicación inicia desde el campo del auditor o evaluador, quien reporta al supervisor, luego al jefe del departamento tecnológico y por último al gerente de la organización.

Las conclusiones alcanzadas y las recomendaciones finales del equipo de aseguramiento tecnológico son comunicadas al comité de auditoria y finalmente al grupo de directores. Cualquier material de tareas de alto riesgo es reportado al personal de seguridad como garantía.

3.1 El modelo de proceso de Gobernanza

Tres pasos son necesarios para el uso efectivo del modelo de gobernanza y para entender si existe o no una intersección entre la seguridad de la información (infosec) y la computación forense. El plan primario utilizado para llevar a cabo la evaluación de riesgo es la evaluación del proceso del modelo contenido dentro de esta sección para cada uno de los siguientes pasos:

1. Evaluación del aseguramiento del riesgo de la seguridad de la información (prevención). Entender el único perfil de riesgo de la información en una organización depende de su infraestructura (sistema operativo, red, etc.) y las aplicaciones. La administración de la organización necesita entender los riesgos específicos de la información asegurando que una evaluación continua es realizada

en la infraestructura y las aplicaciones para conocer los de mayor riesgo en el apoyo. Al finalizar la verificación de los procedimientos del modelo, se elabora una tabla de evaluación del riesgo identificada con colores, basado en la administración de riesgo de la información que fue percibido (ver figuras 2 y 3).

2. Evaluar la computación forense (detección): El modelo funciona con una capacidad dual, ambas para el aseguramiento del riesgo de la información (prevención) y para la realización de una análisis forense postmorten (detección) al sospecharse un ingreso no autorizado. Al realizar este paso se provee a la gerencia de un entendimiento claro de las debilidades y vulnerabilidades en la seguridad de la información no identificadas en el paso 1. Al completar este paso de la verificación del proceso del modelo, una tabla de evaluación con colores es preparado para mostrar la administración actual de los riesgos de la información (Ver figuras 2 y 3).
3. Análisis de la intersección entre la seguridad de la información y la computación forense: Las tablas de evaluación obtenidas en la seguridad de la información (prevención) y la computación forense (detección), completados en el paso 1 y 2, pueden ahora ser analizados. Específicamente, el análisis de seguridad de la información necesita ser comparado con los hallazgos de las dos tablas para identificar semejanzas y desigualdades entre las dos tablas de evaluación.

Una intersección existe cuando las calificaciones de prevención y detección son iguales en las tablas de evaluación, lo cual demuestra la validez original de la administración del riesgo (prevención), basado en el análisis de la computación forense efectuado en el paso 2. Una intersección no existe cuando hay disparidad en las calificaciones asignadas a los procesos de la evaluación del riesgo (prevención) y la Computación Forense (detección).

Figura 2. **Metodología de verificación de la Computación Forense y la Seguridad Digital**

Responsabilidad : Auto evaluación de la Administración superior	Responsabilidad : Aseguramiento de la seguridad de la información y las autoridades	Responsabilidad : Aseguramiento de la seguridad de la información y las autoridades	Responsabilidad : Aseguramiento de la seguridad de la información y las autoridades	Responsabilidad : Aseguramiento de la seguridad de la información y las autoridades	Responsabilidad : Aseguramiento de la seguridad de la información y las autoridades
Computación forense / Evaluación de la administración del riesgo ejecutado por la administración como un riesgo de auto aseguramiento (Revisión del proceso)	Computación Forense / Evaluación del riesgo de la seguridad digital; "evaluación del proceso" ejecutado por las autoridades	Computación Forense / Evaluación del riesgo de la seguridad digital; "evaluación del proceso" ejecutado por las autoridades	Computación Forense / Evaluación del riesgo de la seguridad digital; "revisión de la practica" ejecutada por aseguramiento y las autoridades.	Computación Forense / Evaluación del riesgo de la seguridad digital; "la tabla de calificación final" ajustada por aseguramiento y las autoridades luego de una verificación forense.	Computación Forense / Evaluación del riesgo de la seguridad digital; "proceso de reporte" ejecutado por aseguramiento y las autoridades.
Paso 1 Realizar los procedimientos de verificación del modelo de Gobernanza de la Computación Forense y Seguridad Digital. Paso 2 Llenar las tablas de calificación de procesos y prácticas de riesgo. Paso 3 Desarrollar el mapa final (Una consolidación de las tablas de calificación en colores)	Paso 4 Evaluar la tabla de calificación del proceso de riesgo para completar y precisión contra la computación forense, las políticas de seguridad digital y procesos (políticas y procedimientos). Paso 5: Verificar los procesos de verificación de Computación Forense y aseguramiento del Riesgo de seguridad digital (verificación de procesos, políticas y procedimientos	Paso 6 Desarrollar un documento de conclusión del proceso que describa las fortalezas y debilidades del proceso de la computación forense y la seguridad digital (políticas y procedimientos)	Paso 7 Realizar la verificación de las prácticas y procedimientos de la Computación Forense y la Seguridad Digital. Paso 8 Evaluar la tabla de evaluación de la administración del riesgo contra las resultados obtenidos en el paso 7 Paso 9 Desarrollar un documento describiendo las fortalezas y debilidades de la Comp. Forense y la Seguridad Digital.	Paso 10 Realizar una revisión de las tablas de evaluación de los procesos y las prácticas de riesgo y el mapa final basado en una completa revisión de los procedimientos de la Computación Forense y la Seguridad Digital.	Paso 11 Desarrollar un reporte Ejecutivo que contenga la conclusión final de los riesgos de la Computación Forense y la Seguridad Digital.

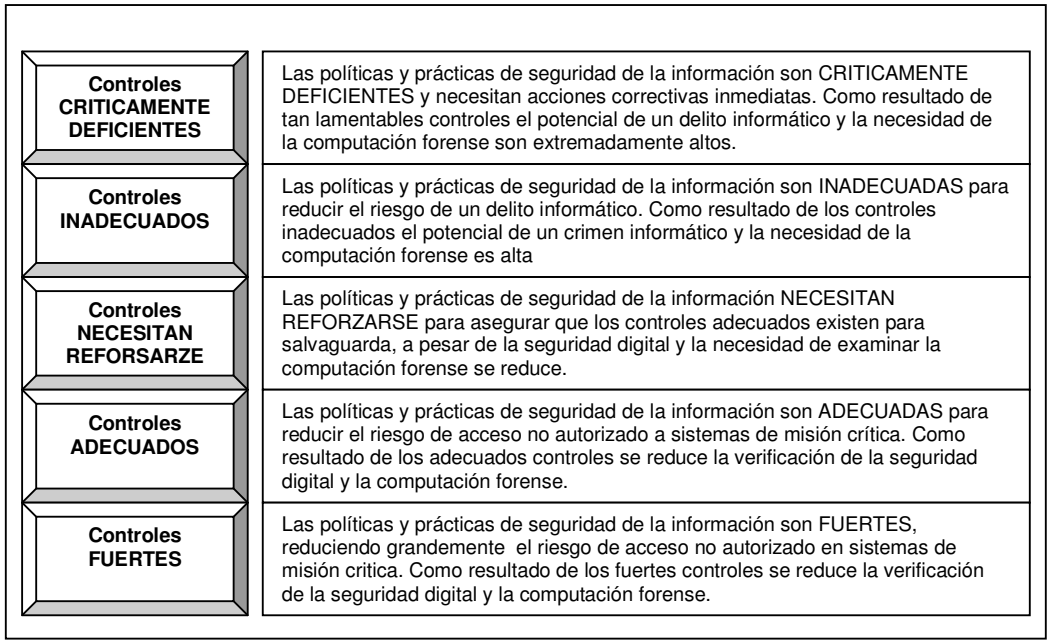
Figura 3 **La Computación Forense y la Gobernanza de la Seguridad Digital Modelo: Criterio de evaluación del riesgo**

A	B	C	D	E
Confidencialidad	**Confidencialidad**	**Confidencialidad**	**Confidencialidad**	**Confidencialidad**
Las políticas y procedimientos de seguridad proveen fuertes controles documentados para proteger la confidencialidad de la información.	Las políticas y procedimientos de seguridad proveen adecuados controles documentados para proteger la confidencialidad de la información.	Las políticas y procedimientos de seguridad necesitan reforzarse para asegurar fuertes controles documentados para proteger la confidencialidad de la información.	Las políticas y procedimientos de seguridad son inadecuados para asegurar la existencia de fuertes controles documentados para proteger la confidencialidad de la información.	Las políticas y procedimientos de seguridad son muy deficientes para proveer fuertes controles documentados para proteger la confidencialidad de la información.
Integridad	**Integridad**	**Integridad**	**Integridad**	**Integridad**
Las políticas y procedimientos de seguridad digital protegen fuertemente la integridad de los datos por medio de altos niveles de autenticidad y responsabilidad.	Las políticas y procedimientos de seguridad digital protegen adecuadamente la integridad de los datos por medio de altos niveles de autenticidad y responsabilidad.	Las políticas y procedimientos de seguridad digital necesitan reforzarse para asegurar que existe un nivel alto de integridad de los datos por medio de altos niveles de autenticidad y responsabilidad.	Las políticas y procedimientos de seguridad digital son inadecuados para asegurar un que existe un nivel alto de integridad por medio de altos niveles de autenticidad y responsabilidad.	Las políticas y procedimientos de seguridad digital son críticamente deficientes para asegurar que existe un nivel alto de integridad de los datos por medio de altos niveles de autenticidad y responsabilidad
Disponibilidad	**Disponibilidad**	**Disponibilidad**	**Disponibilidad**	**Disponibilidad**
Las políticas y procedimientos de seguridad proveen un alto estándar de control interno para proteger la disponibilidad en el tiempo de los recursos de IT.	Las políticas y procedimientos de seguridad digital proveen estándares razonables de control interno para proteger la disponibilidad de la los recursos de IT.	Las políticas y procedimientos de seguridad necesitan ser mejoradas para proteger la disponibilidad de los recursos de IT.	Las políticas y procedimientos de seguridad son inadecuados para proteger la disponibilidad de los recursos de IT en el tiempo.	Las políticas y procedimientos de seguridad son críticamente deficientes y requieren mejoras de fondo para proteger la disponibilidad de los recursos de IT en el tiempo.

Como un resultado de la disparidad de las calificaciones de riesgo, será necesaria mayor investigación, un análisis de la raíz de la causa y los problemas resueltos para prevenir futuras ocurrencias de las vulnerabilidades de la seguridad digital.

En la figura 5 están incluidos los procedimientos que deben de ser ejecutados por los profesionales de aseguramiento y reguladores cuando se este implementando el Modelo de Gobernanza de Seguridad Digital y de Computación Forense.

Figura 4. **Referencia de preparación para Computación Forense y Seguridad Digital**[2]



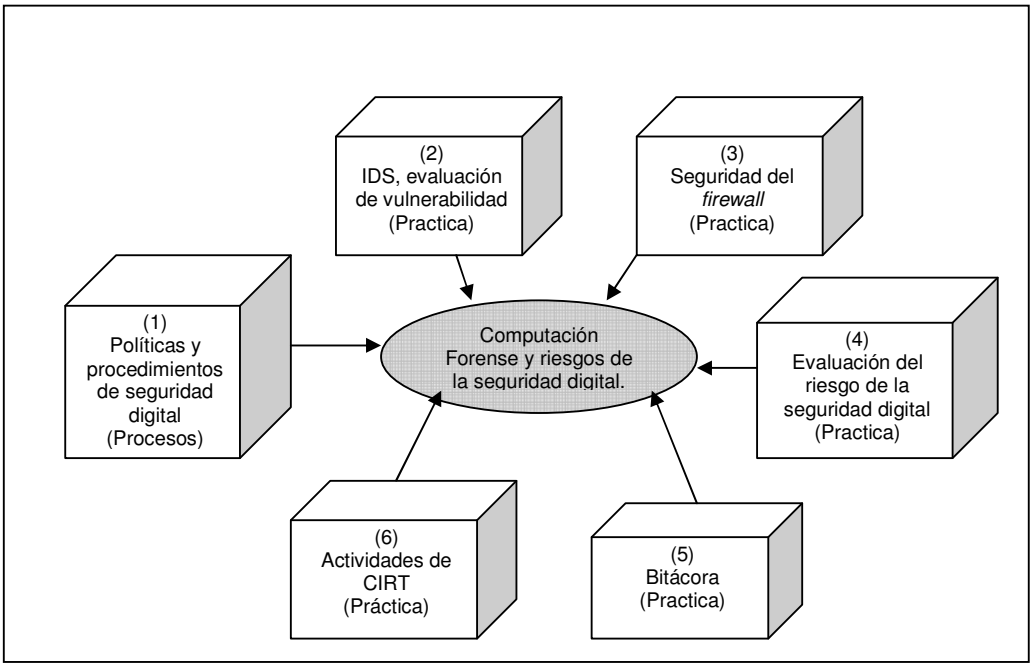
La figura 6 es una referencia cruzada para la figura 5, la figura 4 es referencia cruzada para la figura 7.

[2] Fuente www.isaca.org

Figura 5. **Modelo de Gobernanza de la Computación Forense y la Seguridad Digital**

Modelo de Gobernanza de la Computación Forense y Seguridad Digital				**Homeland de Seguridad**
Paso 1 (Administración)	**Paso 2** (Personal de aseguramiento, regulación y seguridad digital.	**Paso 3** (Personal de aseguramiento, regulación y seguridad digital)	**Paso 4** (Personal de aseguramiento, regulación y seguridad digital)	**Paso 5** (Personal de aseguramiento, regulación y seguridad digital)
Aseguramiento del riesgo y calificación preliminar.	Validación.	Mejoras en la calificación del riesgo.	Mapa critico.	Calificación final
La administración realiza un auto evaluación del riesgo de la seguridad digital y la computación forense y una calificación preliminar del modelo de gobernanza.	La suficiencia de los siguientes procesos y practicas es evaluada y validada: ▪ Políticas, estándares y procedimientos. ▪ Evaluación de vulnerabilidades en la red. ▪ Seguridad digital ▪ Seguridad del firewall.	Mejoras a la calificación inicial de la administración del riesgo son efectuadas, al examinar los procedimientos del modelo de gobernanza.	Todos los procesos y prácticas listadas en el paso 2 son consolidadas para concluir en la asignación de una calificación de la evaluación final del riesgo basada en el criterio dentro del modelo de gobernanza de la Calificación del Riesgo.	Utilizando las calificaciones del mapa crítico se desarrolla una estimación de acuerdo con los criterios dentro de la figura 3.4.

Figura 6. **Metodología de los proceso de la Computación Forense y la Seguridad Digital**[3]



El principal objetivo de la Computación Forense y el Modelo de Gobernanza de seguridad digital es establecer el marco de referencia inicial de Gobernanza que intentara clarificar el rol del aseguramiento de la tecnología al entender el riesgo y los controles que gobiernan la computación forense y la seguridad preventiva de la información.

Al elevar el sentimiento y conocimiento de los riesgos y los controles que gobiernan la computación forense y sus relaciones en las defensas preventivas en la seguridad de la información es crítica para desarrollar controles adecuados necesarios para la salvaguarda de los sistemas de información contra los delitos informáticos y prevenir la necesidad de la computación forense.

Al finar el riesgo existe debido a la carencia general de un claro entendimiento de la computación forense y la seguridad digital alrededor de los profesionales de aseguramiento a personal de seguridad de IT.

[3] Fuente www.isaca.org

4 PROGRAMA DE PREVENCIÓN Y RESPUESTA ANTE UN DELITO INFORMÁTICO

Las organizaciones que reconocen las ventajas de instituir un programa fuerte de respuesta a incidentes, tienen muchas opciones de cómo debe ser la mejor forma de implementarlo. Desde la perspectiva de la administración, una de las consideraciones primarias alrededor de las capacidades de respuesta es el financiamiento: ¿El presupuesto de quien respaldara los servicios de respuesta? Desde la perspectiva operacional, sin embargo, las consideraciones primarias son responsabilidad y servicios, ¿a quién o a qué el equipo de respuesta responderá? ¿Y qué servicios ofrecerá? En este capitulo se proveerán algunas respuestas a estas preguntas.

4.1 ¿Por qué crear un programa?

El código abierto es una forma de vida para quienes realizan delitos informáticos en su conquista para obtener información crítica. Esta información se relaciona con aplicaciones de software, hardware y su objetivo, en este caso información interna que ayudara a romper las defensas de alguna organización.

Con la gran cantidad de software disponible viene la necesidad de proveer “parches”, reparaciones urgentes y actualizaciones de protección contra virus. En la mayoría de los casos, los atacantes informáticos se actualizan en los sitios *web* con noticias acerca de qué empresas han emitido parches o actualizaciones para una aplicación específica.

Un ejemplo lo podemos ilustrar con el siguiente caso de una compañía de software, como se describe a continuación. Una compañía de

software, Soluciones Integrales, comercializa un procesador de palabras. Soluciones Integrales descubre una deficiencia de seguridad en su versión mas reciente y desarrolla un parche para su corrección. Acto seguido, Soluciones Integrales publica la deficiencia de seguridad encontrada y solicita a sus usuarios que accedan el sitio *web*, descarguen el parche y lo instalen conforme a las instrucciones. Es obvio ahora que un atacante informático esta en posesión de la misma información que los usuarios del software.

La siguiente fuente de información con respecto al hardware es ilustrada en el siguiente ejemplo. Quisco Hardware fabricante de servidores, *routers*, *gateways* y algunas otras piezas necesarias para el funcionamiento de una red descubre una deficiencia de seguridad en uno de sus productos de hardware. También realiza el anuncio a sus clientes de la deficiencia, estos deben acceder su sitio *web* y descargar el parche respectivo para su instalación conforme a las instrucciones. De nuevo es obvio que los atacantes informáticos están posesión de la misma información que los usuarios del hardware en cuestión.

La tercera pieza de fuente de información es el usuario final corporativo, las empresas que utilizan el software y hardware para realizar sus tareas diarias. Con la disponibilidad de la tecnología, una corporación típica tiene un sitio *web* para publicar sus mercancías, servicios y sus logros. Estos sitios son una fuente de publicidad, los clientes potenciales son alentados a visitarlos.

Parte de lo que las organizaciones publican por medio de sus sitios *web* son las oportunidades de empleo disponibles, en muchos casos para IT. En ciertas ocasiones en medio de estas se encuentra información de la tecnología. Para que la organización contrate a la persona correcta deberá publicar requisitos tales como: experiencia en sistemas operativos *UNIX*,

Windows y *Linux*, o algún conocimiento específico de la arquitectura de hardware y/o software.

Habiendo dicho lo anterior, es obvio que la información publicada en la sección de oportunidades no esta restringida a personas que buscan empleo o personas que visiten el sitio por curiosidad, esta disponible para el mundo entero. Y por supuesto esta sección será visitada por atacantes informáticos. Los atacantes informáticos aprenden en este sitio el tipo de hardware, las aplicaciones y el tipo de red que están siendo utilizadas.

De lo descrito anteriormente se puede concluir lo siguiente de la empresa:

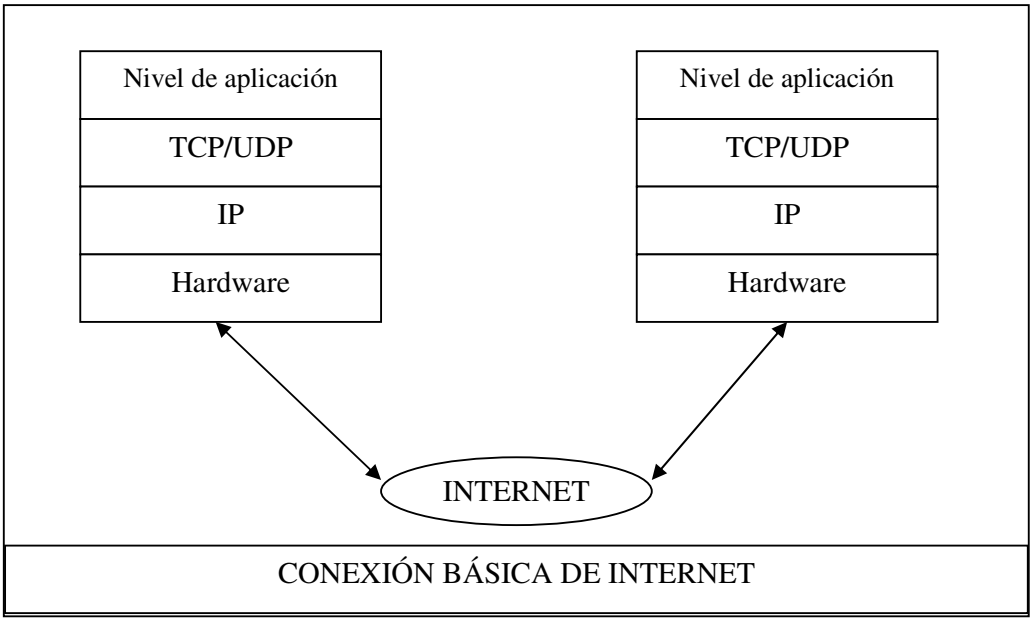
- Vulnerabilidades y debilidades del software
- El parche de software que debe descargarse y como implementarlo
- El hardware con debilidades
- El parche de hardware que debe descargarse y como implementarlo
- Los requisitos para el personal de IT, el tipo de hardware, software y la red implementada en la organización

Los delincuentes informáticos navegan en el Internet hasta que se encuentran con una organización que utiliza el software o hardware identificado con alguna vulnerabilidad. Una vez que se identifica la organización, el delincuente verifica la vulnerabilidad e intenta identificar si el parche ya fue implementado. Es por esto que es necesario tener implementado un programa de prevención y respuesta.

4.2 Metodologías de ataque

Internet es una fuente de ataques utilizada por los delincuentes informáticos, en el siguiente diagrama se ilustra como funciona:

Figura 7. Conexión básica de Internet.



En el nivel de aplicación los usuarios conversan con un servidor con el mismo tipo de protocolo. El protocolo de control de transmisión (TCP) provee una conexión confiable. Cualquier persona puede desarrollar un nuevo protocolo entre dos servidores.

TCP establece un circuito entre el cliente y el servidor. Este convierte una secuencia de datos en paquetes los son ensamblados de nuevo utilizando Servicios 1-655535. UDP (Procolo Usuario de Datagrama) es mensajeria sin conexión no ofrece corrección de error. Es útil para algunos servicios de red que no deben de ser confiables, tales como voz.

Al nivel de IP, los paquetes tienen tamaños limitados. Son eliminados en tránsito si existe congestión y pueden arribar en forma desordenada o duplicados. El direccionamiento es por el número IP.

Al nivel de hardware, tal como *Ethernet*, los mensajes pueden ser observados si están en la misma red. Existen ataques que su objetivo es en este nivel.

Los enlaces mas débiles son las mayores amenazas. Las vulnerabilidades son comunes en los servicios de red. Una intrusión compromete el resto de los servidores y la red en general. La seguridad requiere disciplina que no se encuentra en los líderes del mercado.

Los perfiles de los atacantes incluyen:

- Network mapping
  - Consultas InterNIC
  - Transferencia de zonas DNS
  - Escaneo de ping
  - Escaneo de puertos
- Servios de información
  - SNMP
  - Finger
  - Rusers
  - Rstat
- Explotación de BUGS
  - TFTP
  - FTP
  - SMTP
  - NIS
  - NFS
  - DNS
  - Kerberos
  - POP
  - http

4.3 Preparación

La primera fase en el ciclo de respuesta es la preparación. La formación de un Equipo de Respuesta a un Ataque (ERA) es crítica para mitigar un incidente rápida y efectivamente. El equipo de respuesta a un ataque de una organización incluye administración, seguridad corporativa, profesionales especializados para análisis y redacción técnica, relaciones públicas, recursos humanos y representantes de consejero legal y de auditoria. Un asistente administrativo es asignado al ERA. Cada miembro del ERA esta familiarizado con la organización y tiene profundos conocimientos de las políticas y procedimientos definidos por la organización.

Las organizaciones pueden crear varios tipos de equipos de repuesta, entre los que se encuentran:

- Equipo de respuesta a emergencias Informáticas: Usualmente encargado del análisis y respuesta a ataques e intentos de violación de la seguridad. Regularmente estos equipos son formados por entidades gubernamentales.
- Punto de alarma, asesoramiento y reporte: Un grupo de ayuda mutua que puede estar conformado en una región o una ciudad.
- Proveedores de administración de seguridad: Firmas privadas que ofrecen varios tipos de servicios entre los que se incluyen monitoreo de sistemas de las organizaciones al realizar el pago de una cuota.

Para que el ERA encaje en la organización apropiadamente, algunos factores son tomados en consideración. Para iniciar, todas las secciones de la organización deben estar identificadas y sus requerimientos del negocio deben de ser entendidos. Una vez que las secciones o divisiones han sido identificadas, los administradores y personal selecto son seleccionados y

entrevistados. Este proceso genera información de cómo cada sección funciona en el día a día, que procedimientos son ejecutados y con que documentación cuentan. Las recomendaciones pertinentes son normalmente hechas en base a la información obtenida luego que se han entrevistas las entrevistas.

4.3.1 Selección del equipo

¿Quién esta incluido en el ERA? Este equipo debe incluir representantes de todas las divisiones afectadas. Esto incluye como mínimo el área de seguridad informática, relaciones publicas, legal, auditoría, recuperación de desastres y recursos humanos. Un administrador y personal técnico son miembros de tiempo completo del equipo. Los miembros de recursos humanos, seguridad física, relaciones publicas, auditoria, recuperación de desastres y legal pueden ser de medio tiempo o personal disponible al momento de una llamada para que se incorporen durante un incidente. Sin embargo es posible que basado en las necesidades y requerimientos de la organización este personal este de tiempo completo. El ERA contiene un núcleo de de técnicos expertos, otros son alertados si existe un incidente y ellos deciden que deben mantenerse en el equipo si sus conocimientos son requeridos. Por lo menos un asistente administrativo debe ser asignado a tiempo completo en el equipo.

El ERA debe tener un número apropiado de miembros. La organización evalúa sus necesidades y determina cuantos miembros son necesarios, así como cuantos miembros existirán en cada área geográfica en los cuales se tenga una representación. Miembros de respaldo pueden ser necesarios en caso que alguno de los miembros no este disponible cuando se le requiera en caso de un incidente. El número apropiado de miembros depende de:

- Numero de usuarios en la organización
- Necesidades y metas
- Propagación geográfica
- Infraestructura tecnológica

En la mayoría de las organizaciones los miembros del núcleo del ERA tienen responsabilidades diarias dentro de la organización. Estos miembros realizan tareas fuertes de informes administrativos. Durante un incidente, sin embargo, los miembros del equipo reportan al director del equipo. La razón de esto es para mantener la confidencialidad y la integridad del incidente.

ERA es un equipo virtual dentro de la organización. Sus miembros son seleccionados basados en su conocimiento y su experiencia. Organizaciones pequeñas o medianas puede que no tengan este tipo de personal o su presupuesto no lo permite, en este caso puede ser necesario la contratación de terceros para que actúen en el momento de un incidente.

4.3.1.1 Conocimientos, habilidades y destrezas de los miembros de ERA

En el medio ambiente de hoy día y con el numero de incidentes identificados en los cuales ciertas organizaciones han tenido resultados devastadores, es imperativo que las organizaciones cuenten con equipo que puedan evitar un desastre. Los técnicos de equipo deben ser visualizados como los primeros en responder. Cada miembro de estos equipos tienen conocimientos altamente especializados, sin embargo cuando son conformados como un equipo, es una unidad especializada altamente funcional. El ERA debe ser diseñado con ese concepto en mente.

Definiremos el conjunto fundamental de conocimientos, experiencias y habilidades que un individuo requiere para ser efectivo y competente al momento de manejar un incidente. Estos son divididos en aspectos técnicos y personales. No existe una prioridad o importancia en la forma en que se van mencionando. La meta es seleccionar a los miembros técnicos que tengan múltiples conocimientos. Por ejemplo si un candidato tiene un fuerte conocimiento de UNIX y desarrollo en ambiente *web* y un buen entendimiento de *firewalls*, los otros candidatos deberán tener conocimientos complementarios (*Windows*, *Mac*, etc.). Sin embargo debe existir un traslape en las habilidades técnicas entre los miembros, el equipo debe de ser tan diverso como sea posible. Las deficiencias pueden ser cubiertas con capacitación o entrenamiento.

En los ambientes actuales y con el número de incidentes identificados que han sido devastadores para algunas organizaciones, es imperativo para las organizaciones que cuenten con equipo que pueda ser puesto en acción en forma inmediata. El equipo técnico debe ser visualizado como el primero en responder. Cada miembro debe tener un conocimiento especializado, sin embargo, cuando trabajan en equipo, es una unidad altamente especializada.

4.3.1.2 Habilidad de comunicación

En general todos los miembros del ERA necesitan:

- Excelente habilidad de comunicación escrita y oral.
- Un conocimiento sólido de la cultura y políticas internas.
- Habilidad demostrada para seguir políticas y procedimientos internos.
- Habilidad de ser parte de un equipo multidisciplinario
- Sentido de integridad

- Habilidad para manejar stress
- Habilidades de administración del tiempo y resolución de problemas.

Las personas que manejan los incidentes necesitan excelentes habilidades de comunicación para asegurar que pueden obtener y suplir la información necesaria para hacer su trabajo en forma efectiva. Estos individuos deben mantener el control de las interacciones entre el personal para obtener información especifica del incidente y determinar que está sucediendo, que hechos son importantes y que asistencia puede ser necesaria. Este miembro necesita adaptarse para asegurar la comunicación más efectiva con personal de diferentes niveles de conocimiento. Así también necesita ajustarse al nivel apropiado de discusión sin ser condescendiente o hablar arriba del nivel del cliente o usuario.

La habilidad para comunicarse en forma escrita de manera efectiva es necesaria para asegurar que la persona podrá realizar tareas como:

- Documentar reportes de incidentes.
- Desarrollo de documentación en aspectos técnicos
- Documentación de políticas y procedimientos internos
- Revisión y actualización de políticas y procedimientos

La habilidad para comunicarse en forma oral de manera efectiva es necesaria para asegurar que la persona que maneja un incidente puede hablar con individuos o grupos. Estos grupos pueden incluir:

- Otros miembros del grupo
- Miembros de equipos de respuesta
- Expertos
- Administradores
- Medios de comunicación

Independientemente de la forma de comunicación, la naturaleza del lenguaje y el tono utilizado debe de ser profesional, relajado y convincente.

4.3.1.3 Diplomacia

Quien maneja un incidente regularmente se encuentran con que los individuos que necesitan entrevistar se encuentran en pánico, ansiosos o molestos en diferentes niveles. A pesar de esto quien este manejando el incidente debe mantener la diplomacia y el profesionalismo para asegurar que ellos intercambian la información necesaria para el control de la situación. Aún dentro de la organización existirán diferencias en las prioridades y percepciones del evento. Barreras entre los departamentos y requerimientos operacionales conducirán a los miembros del ERA a realizar un balance en las competencias. Este balance incluye decir no a las personas con fundamentos validos cuando lo mejor para la organización se encuentra en juego. La diplomacia y la buena comunicación son herramientas vitales para el ERA.

4.3.1.4 Habilidad para seguir políticas y procedimientos

Para asegurar un servicio de respuesta a un incidente en forma consistente y confiable, el personal debe seguir políticas y procedimientos establecidos de la organización. Algunas veces los individuos deben decidir en modificar las policitas y procedimientos existentes para ajustar sus necesidades o para reflejar que lo que ellos piensan es lo apropiado. Como resultado, quienes manejan el incidente necesitan aceptar y seguir las políticas y procedimientos de la organización independientemente de que ellos se encuentren de acuerdo con estas. Necesitan entender como y por que existen estas políticas y procedimientos y justificar cualquier sugerencia

de actualización que crean pueda ser apropiada para ser tomada en consideración.

4.3.1.5 Habilidad de trabajo en equipo

Es imperativo para la persona que maneja un incidente tener la habilidad de trabajo en equipo y ser productivo y cordial con los demás miembros. Regularmente trabajara con otros miembros para intercambiar experiencias, información y cargas de trabajo. Además necesita la habilidad de comunicarse con otras personas, tales como miembros de otro equipo de respuesta. Si la persona no esta dispuesta a involucrarse en el trabajo en equipo afectara la moral de los otros miembros o causara resentimiento, esto derivara en una baja de la productividad.

4.3.1.6 Integridad

La persona que maneja un incidente se encuentra constantemente tratando con información sensible. De forma regular tienen acceso a información nueva y valiosa. Se pueden encontrar en situaciones muy tentadores, no deben de comentar la información con la que cuentan de ninguna manera con personal que no este relacionado con el trabajo, el no observar esta regla puede ocasionar la publicación de información sensible. El exponer información confidencial de parte de cualquier miembro del equipo puede ocasionar la pérdida de la integridad de todo el equipo. Todos deben de ser muy confiables y capaces de manejar información en forma confidencial de acuerdo a las políticas y procedimientos de la organización. Quien maneja el incidente mantiene la confidencialidad de la información del mismo y publica esta solo en la medida que es permitido por las políticas y procedimientos del equipo.

4.3.1.7 Manejo de presiones

Quienes manejan un incidente regularmente se encuentran en situaciones apremiantes. Necesitan saber cuando están en un nivel alto de presión y poder hacerlo saber a los otros miembros del equipo para poder tomar las acciones para controlar y mantener la compostura. Se necesita la habilidad para mantener la calma en situaciones tensas, las cuales pueden darse debido a cargas altas de trabajo, una llamada pesada o un incidente donde la vida de una persona se encuentre en riesgo. La reputación del equipo y cada uno de sus miembros se ve influenciada en como se manejan las presiones. Aunque una solución rápida de un incidente es lo deseable, los miembros del ERA no pueden verse presionados para actuar en forma mas rápida de lo que cualquier situación dicta.

4.3.1.8 Resolución de problemas

Quien maneja un incidente tendrá que trabajar con grandes volúmenes de información, debido a esto es esencial identificar que esta información es:

- Relevante
- Importante
- Perdida
- Incorrecta

Sin la habilidad de resolución de problemas, el personal puede encontrarse perdido en los grandes volúmenes de información y puede que no tenga la habilidad para ordenar la información y así determinar la que es necesaria para cada paso del trabajo que se realiza.

4.3.1.9 Administración del tiempo

Los miembros del ERA se verán cargados con muchas tareas que van desde enfrentar un incidente a las tareas diarias, tales como completar informes y prepararse para entrevistas. Aun cuando se les provea el criterio de priorizar, los individuos necesitan priorizar y administrar múltiples responsabilidades a las cuales ellos son asignados de acuerdo con estos criterios. Para asegurar su productividad, necesitan balancear su esfuerzo entre completar las tareas diarias con el constante cambio en prioridades de las tareas de nuevas cargas de trabajo.

4.3.1.10 Conocimientos técnicos

Un conjunto fundamental de habilidades técnicas es requerido para asegurar que un individuo es competente y eficiente al manejar un incidente. Estas habilidades se pueden agrupar en dos categorías: Fundamentos Técnicos y Manejos Específicos de incidentes. En cualquiera de los dos casos se recomienda que además de las cualidades de comunicación, los miembros técnicos del ERA tengan entre dos y cinco años de experiencia. Esta experiencia debe de haber sido aplicada a manejo de incidentes.

4.3.1.11 Fundamentos técnicos

Un entendimiento básico de la tecnología es necesario. La naturaleza de estos conocimientos es similar, independiente del software y el hardware en uso, ejemplos de estos conocimientos son:

- Principios de seguridad: Conocimiento de principios básicos de seguridad, en los que se incluye:

    - Autenticación
    - Integridad
    - Control de accesos
    - Privacidad
    - Negación de servicio
- Debilidades de seguridad: Para entender como un ataque en específico se manifiesta en un software o hardware, primero debe entenderse que tipos de ataques existen. Es necesario reconocer y categorizar cada tipo de ataque como:
    - Seguridad física
    - Debilidades de configuración
    - Errores de usuarios
    - Código malicioso
- Internet: Es importante que se tenga un buen conocimiento de el Internet. Sin la información básica no se entenderán los aspectos técnicos, tales como debilidades en la seguridad en los protocolos y servicios utilizados para el acceso a Internet o los peligros pueden ser anticipados en el futuro. El material cubierto de Internet debe incluir:
    - Historia
    - Filosofía
    - Estructura
    - Componentes
    - Protocolos
    - Aplicaciones
- Protocoles de red: Se requiere un conocimiento básico de los protocolos con los cuales se trabajara, el conocimiento de estos protocolos incluye:
    - Propósito
    - Especificación
    - Forma de operación

4.3.2 Políticas y procedimientos del equipo

Es necesario que el personal involucrado en el ERA sea capacitado profundamente en las políticas y procedimientos que regirán las operaciones al momento de existir un incidente. Sin este conocimiento los miembros del equipo no podrán entender el marco de trabajo y los limites en los cuales ellos pueden aplicar sus conocimientos.

4.3.3 Entendimiento e identificación de las técnicas de ataques

El personal deberá tener la habilidad de reconocer las técnicas de ataque más conocidas, para esto es básico poder detectar las huellas dejadas. Así también es necesario tener conocimiento de los diferentes métodos para protegerse de un ataque y el riesgo asociado con cada uno de los ataques. El reconocimiento de las huellas se basa en la habilidad para interpretar la documentación de los análisis y los métodos de protección utilizados. Al detectar información no común el equipo podrá identificar la posibilidad de una nueva forma de ataque o una potencial vulnerabilidad.

4.4 Respuesta a un ataque

El ERA será el encargado de responder a un ataque, esta respuesta debe de ser coordinada, independiente de la naturaleza del ataque la metodología es la misma:

- Preparación: Organizar el equipo de respuesta.
- Identificación: Identificar lo que se encuentra contaminado.
- Mitigación y aislamiento: Prevenir que el ataque tenga mayores consecuencias.
- Investigación: Encontrar el problema y quien es el responsable.

- Erradicación: Eliminar el problema.
- Recuperación: Descontaminar los sistemas afectados.
- Seguimiento y tomar medidas preventivas: Aplicar medidas de seguridad para prevenir o reducir el impacto de futuros ataques.

Mantener registros detallados es parte de la metodología y también evidencia vital en caso de seguirse un caso por la ley.

Enfocarse en la organización cuando múltiples sistemas se encuentran fuera de servicio y la red esta saturada puede ser contra producente. Sin embargo un plan de respuesta no coordinado puede resultar en una perdida de tiempo, desperdicio de recurso humano. Lo primero a realizarse será:

- Identificar el ataque.
- Unir al grupo de respuesta
- Coordinar y configurar los mecanismos de comunicación
- Recolectar herramientas de trabajo
- Desarrollar una metodología especifica de respuesta

4.4.1 Organización de la evidencia digital

Recolectar información y seguir los procedimientos adecuados puede convertirse en una tarea ardua. Un cuestionario para recolectar información es una guía estructurada y ordenada (Ver apéndices A y B). Este cuestionario incluye aspectos como evaluar el ataque, estrategias de respuesta y métodos para el manejo de evidencias. Este cuestionario permitirá guiar al equipo en aspectos no técnicos para luego ser distribuido al

personal involucrado en la administración y operación de la información de sistemas y así apoyar el funcionamiento de los sistemas.

4.4.2 Seguimiento del incidente

Una vez que el evento ha sido identificado y validado como un evento valido, deberá asignársele un identificador único, el cual puede ser por medio de un número, el cual será utilizado para formar un expediente con toda la información recabada.

4.4.3 Documentación

Los miembros del equipo deben documentar todos los hallazgos y eventos del incidente. Esto incluye conversaciones con clientes, empleados, administración y terceros que den soporte a la organización. La información recaba es distribuida a todos los miembros del equipo utilizando medios seguros en caso de información confidencial.

En las primeras etapas el distribuir la información a todos los miembros es importante debido a que puede existir algún miembro que tenga experiencia en el tipo de incidente que se esta presentando y con esto podrían tomar el liderazgo para mitigar en forma rápida y efectiva el incidente. Un expediente con toda la información es necesario para centralizar toda la información y para referencia de parte de cualquiera de los miembros del equipo, este deberá permanecer en un área segura y con los controles de acceso respectivos.

Documentar y mantener los registros de un incidente es importante por muchas razones, podemos mencionar:

- Eventualmente será necesario presentar un informe a las autoridades de la organización
- El incidente puede conducir a un hecho criminal el cual deberá ser resuelto por la vía civil.
- Toda información puede ser considerada evidencia, la cual puede influir en la solución del incidente.

4.4.4 Prioridades en respuesta a un incidente

Las prioridades en las acciones a tomar en el manejo de un incidente son definidas y deben de ser mantenidas en mente. Las prioridades son definidas en base a las políticas de la organización.

Las cuatro prioridades organizacionales incluyen:

- Pérdidas financieras
- Seguridad
- Empleados
- Publicidad

La importancia de asignar una prioridad a estas tareas esta basado en la experiencia de que los incidentes típicamente afectan más de un área.

4.4.4.1 Pérdidas financieras

Pueden ser definidas y clasificadas por las diferentes áreas de la organización. Entre estas pérdidas podemos mencionar:

- Bienes perdidos o robados
- Demandas en la recuperación de estos bienes

- Pagos por juicios
- Perdida de reputación
- Costos operacionales
- Propiedad intelectual

4.4.4.2 Seguridad

La seguridad incluye la seguridad física y bienestar de los empleados y el medio ambiente físico en el cual desarrollan sus labores. Muebles, equipos y facilidades (luz, componentes de seguridad) son ejemplos de prioridades en la seguridad. Aunque el ataque solo sea a nivel digital este puede repercutir afectando la seguridad de los empleados.

4.4.4.3 Empleados

Los empleados pueden sufrir efectos y consecuencias luego de un incidente, estas pueden ser:

- La necesidad de contar con recurso humano para mitigar la reacción de los empleados.
- Horarios adecuados a las exigencias para los miembros del equipo.
- La demanda del estatus de la investigación de parte de personal no involucrado en el manejo del incidente.

4.4.4.4 Publicidad

Publicidad negativa o no deseada puede dañar o destruir la reputación de cualquier organización. Esta puede surgir de varias fuentes, incluyendo empleados de la organización. Deben de existir políticas claras en que

información puede ser revelada y quien podrá hacerlo ya sea a los empleados o los medios de comunicación si fuera el caso.

4.4.5 Mitigación y aislamiento

El fin de esta fase es determinar el alcance y la magnitud del incidente y prevenir que este se extienda, con esto se puede determinar el curso de acción para la solución, una vez que el problema ha sido claramente definido el equipo determinara como descontaminar los sistemas afectados y su restauración o aislar el sistema, buscar la fuente del ataque y encontrar el responsable.

La decisión de restaurar o investigar debe ser tomada en conjunto por la administración y el ERA.

En la mayoría de los casos la protección del personal y los bienes son la prioridad. El aislar y descontaminar los equipos y/o sistemas rápidamente impedirá a los miembros del equipo determinar la naturaleza y el motivo del ataque. Aunque se haya realizado un respaldo de los equipos no será posible determinar el método que el atacante utilizo, que vulnerabilidades fueron explotadas, o si el atacante estuvo dentro o fuera de la organización. Esta información es esencial para prevenir futuros ataques.

En el caso de tomar la decisión de aislar el sistema, debe determinarse cuales serán aislados, a que nivel deberán aislarse. Entre otras debe considerarse lo siguiente:

- ¿Fue un ataque local, regional o nacional?
- ¿Se destruyeron los archivos?
- ¿El intruso sólo esta visualizando la información?

- ¿El intruso esta utilizando la información para su beneficio?
- ¿Están siendo utilizadas las instalaciones para lanzar un ataque a otros sistemas?
- ¿Es prudente seguir la pista a las actividades del intruso o deben de ser paradas lo más rápidamente posible?
- ¿Están siendo violadas las leyes de propiedad intelectual?
- ¿El ataque esta siendo perpetrado dentro o fuera de las instalaciones?

4.4.5.1 Preservación de información

Las actividades de investigación incluye el examinar datos relacionados con el incidente para poder obtener la identidad del atacante. Esta información debe de ser obtenida y manejada en forma cuidadosa ya que puede convertirse en evidencia al convertirse en un caso legal.

4.4.5.2 Implementación de computación forense

Al momento de encontrarse en medio de un ataque es importante determinar el curso de acción a tomar. La computación forense es la recolección, preservación, análisis y presentación de evidencia digital de manera que sea entendible por cualquier miembro en la organización, útil al aplicar políticas internas y ser utiliza como evidencia al convertirse en un caso legal. La Computación Forense también permitirá evidenciar las debilidades y vulnerabilidades que incrementan el riesgo de un ataque. En el ERA deben de existir personal capacitado en Computación Forense.

5. SISTEMAS DETECTORES DE INTRUSOS

Las redes de computadoras se han convertido en un recurso indispensable para las instituciones de todo el mundo. Al colocar sus recursos informativos en la red, resulta imprescindible trabajar en la protección de los mismos, por lo que los aspectos de seguridad se convierten en pieza clave dentro de este entorno.

Con el objetivo de proteger las redes, la información que en ellas se almacena, procesa e intercambia, y los servicios que en ellas se ofrecen, se utilizan diferentes herramientas.

Existe una larga relación de programas empleados en estas tareas, destacándose los siguientes por su utilidad y popularidad:

- Antivirus
- Monitores de red y sistemas
- Detectores de vulnerabilidades
- Analizadores de logs
- Proxies
- Cortafuegos (Firewalls).
- IDS (Intruder Detection Systems)

En particular los Sistemas de Detección de Intrusos han constituido un campo de investigación activo desde hace dos décadas. Sin embargo, solo desde hace pocos años existen, al alcance de la comunidad internacional, productos con un grado de efectividad satisfactorio. En todo el mundo se reconoce la utilidad e importancia que tienen estas herramientas. Son relevantes sus facilidades en el accionar proactivo y reactivo a corto plazo en la seguridad de las redes. La cantidad de software y hardware que se comercializa en este sentido ya alcanza niveles asombrosos.

5.1 Formas de trabajo

Los IDS fortalecen la labor de la seguridad en la red siguiendo dos formas de trabajo fundamentales: la prevención y la reacción.

La prevención de las actividades de intrusos se realiza a través de herramientas que escuchan el tráfico en la red o en una computadora. Estos programas identifican el ataque aplicando el reconocimiento de patrones (normas) o técnicas inteligentes. Este trabajo en "caliente" permite notificar el intento de ataque o la actividad sospechosa de manera inmediata. Existe la posibilidad además, de elaborar respuestas defensivas antes de la materialización del ataque.

El método reactivo se garantiza utilizando programas que básicamente realizan el análisis de logs en los sistemas protegidos. En las trazas de los servicios de la red o del comportamiento de los sistemas se trata de detectar patrones que evidencian las actividades de intrusión realizadas por elementos malignos. También son utilizados como "evidencias" la modificación de ficheros comunes, ficheros del sistema y otros.

5.2 ¿Qué puede hacer un IDS?

Debe adelantarse a cualquier comentario que estas herramientas no constituyen la solución a todos los problemas de seguridad de la red. Los IDS introducen novedosos métodos de trabajo permitiendo establecer la llamada defensa en profundidad y complementando el trabajo realizado por soluciones ya establecidas y maduras como los cortafuegos. Abajo se relacionan algunas de sus posibilidades:

- Detección ataques en el momento que están ocurriendo o poco tiempo después de haber ocurrido.
- Automatización de la búsqueda de nuevos patrones de ataque (principalmente, modificaciones de ataques conocidos) gracias a herramientas estadísticas de búsqueda, y al análisis de trafico anómalo.
- Monitorización y análisis de las actividades de los usuarios. De esta forma se pueden conocer los servicios que usan los usuarios, e incluso estudiar el contenido de este tráfico, en busca de elementos anómalos.
- Auditoria de configuraciones y vulnerabilidades de determinados sistemas.

Mediante el análisis de tráfico y de *logs* pueden descubrirse sistemas que tienen servicios habilitados cuando en realidad no deberían tenerlos:

- Análisis de comportamiento anormal. Si se detecta una conexión fuera de hora, reintentos de conexión fallidos y otros, existe la posibilidad que se esté en presencia de una intrusión. Un análisis detallado del trafico y los logs puede revelar una maquina comprometida o un usuario con su contraseña al descubierto.
- Disminución de la complejidad de las tareas de administración de la seguridad en la red. Se automatizan tareas como la actualización de reglas, la obtención y análisis de *logs*, la configuración de cortafuegos y otros.

5.3 Componentes de las herramientas

Las herramientas que implementan la tecnología de detección de intrusos poseen, de forma general, tres componentes fundamentales:

- Los sensores

- Los analizadores
- La interfaz de usuario.

Los sensores tienen la responsabilidad de coleccionar datos de interés y enviar esta información a los analizadores. La información puede ser obtenida de cualquier parte del sistema que contenga evidencia de intrusiones, esto es, paquetes provenientes del análisis de tráfico, secciones de logs, atributos de ficheros y otros.

Los componentes denominados analizadores atienden la información que reciben de los sensores o de otro analizador. Su obligación fundamental consiste en determinar si ha ocurrido o está ocurriendo una intrusión y presentar pruebas de esta afirmación. Como resultado de su trabajo debe indicar el tipo de intrusión detectada de forma clara y, en muchos casos, proponer o ejecutar un grupo de medidas que permitan contrarrestar los efectos de la misma.

La interfaz de usuario tiene un uso trivial pues permite, probablemente el administrador de seguridad, observar las salidas del sistema y controlar su comportamiento.

5.4 Métodos de detección

De manera general puede afirmarse que los sistemas detectores de intrusos (IDS) son herramientas con cierta inteligencia que automatizan la detección de intentos de intrusión en un sistema. Esta identificación puede resultar inmediata o en un plazo de tiempo muy corto. Es por eso que en muchas ocasiones se emplea el término de tiempo real.

Dentro de la gran familia de IDS se presentan dos grandes grupos partiendo de la base informativa de su trabajo: los sistemas basados en normas (trabajan en la detección de uso indebido (MD)) y los sistemas adaptables (trabaja en la detección de anomalías (AD)).

5.4.1 Detección de mal uso

El primer grupo mencionado actúa a partir de bases de datos que contienen todos los patrones de ataques conocidos hasta el momento de salida del producto. Estas bases deben ser actualizadas de manera periódica, para que la herramienta se mantenga cumpliendo sus objetivos. No hacer esto puede traer como consecuencia que cualquier nuevo ataque, por simple que sea, tenga éxito en sus intenciones de penetrar o alterar el funcionamiento de la red. Este esquema se limita a conocer lo anormal para poderlo detectar (conocimiento negativo).

Fortalezas:

- Detección efectiva de ataques sin generar de un número grande de falsas alarmas.
- Diagnóstico rápido del uso de una técnica específica o herramienta de ataque.
- Permiten a los responsables de seguridad, independientemente de su experiencia, dar seguimiento a los problemas de seguridad en su sistema.

Debilidades:

- Sólo pueden detectar los ataques que son conocidos.
- Son incapaces de detectar pequeñas variaciones de ataques conocidos.

5.4.2 Detección de anomalías

En el caso de los sistemas adaptables se trata de incorporar técnicas avanzadas, como la inteligencia artificial, para reconocer y aprender nuevos patrones de ataques. Este grupo de herramientas presupone una mayor complejidad, por lo que su desarrollo se observa, esencialmente, en entornos de investigación. La base del funcionamiento de estos sistemas es suponer que una intrusión se puede ver como una anomalía, para lo cual se hace necesario establecer un perfil del comportamiento habitual de los usuarios y/o sistemas. A partir de ahí pueden detectarse las intrusiones por estudios estadísticos: una desviación excesiva en la media del perfil de comportamiento muy probablemente evidencia una intrusión.

Fortalezas:

- Detectan comportamientos inusuales y poseen la habilidad de detectar síntomas de ataques sin tener un conocimiento detallado del mismo.
- Pueden producir información que luego se emplee para definir patrones de ataques y pueden ser usados para realizar un análisis de tendencias de las amenazas de seguridad.
- No requiere de actualización constante de patrones.

Debilidades:

- Producen una gran cantidad de falsas alarmas debido al comportamiento poco predecible de usuarios y sistemas.
- Frecuentemente se requieren extensas "sesiones de entrenamientos" para el aprendizaje de eventos del sistema con el objetivo de obtener los perfiles de comportamiento “normal”.

5.5 Clasificación

Existen varias formas de agrupar las herramientas IDS de acuerdo a las características que poseen. Es muy común encontrar una división en dos grupos principales: *network based* (trabajan a partir de la información que obtienen de la red) y *host-based* (trabajan a partir de la información que obtienen de una computadora).

5.5.1 IDS basados en red (*Network Intrusion Detection Systems*)

Un IDS de red (NIDS) revisa los paquetes que circulan por la red en busca de elementos que denoten un ataque contra alguno de los sistemas ubicados en ella. El NIDS puede situarse en cualquiera de las computadoras o en un elemento que analice todo el tráfico (como un repetidor). Esté donde esté, protegerá varias computadoras y no una sola: esta es la principal diferencia con los sistemas de detección de intrusos basados en host.

Para funcionar apropiadamente estos IDS deben estar posicionados de forma adecuada en la red. En las redes actuales donde todo el tráfico se segmenta con conmutadores (switchs) la adecuada ubicación de estos IDS puede llegar a ser un problema. Los conmutadores modernos, con capacidad de duplicar puertos para facilidades de monitoreo suplen parcialmente esta limitación.

5.5.2 IDS basados en computadoras

Mientras que los sistemas de detección de intrusos basados en red operan bajo todo un dominio de colisión o ubican sensores en dominios

diferentes, los basados en computadoras realizan su función protegiendo un único servidor.

Dentro de este gran grupo existen subgrupos que utilizan diferentes vías para detectar las intrusiones. Algunas de estos subgrupos son los siguientes:

- *System Integrity Verifiers* (SIV): típicamente monitorizan los sistemas de archivos en busca de modificaciones relevantes.
- *Log File Monitors* (LFM): chequean los archivos *logs* en busca de patrones sugerentes.
- *Deception Systems (A.K.A. decoys, lures, fly-traps, honeypots)*: sistemas que aparentan servidores o computadoras vulnerables para desviar la actividad de los intrusos.

Algunas de las herramientas, como los LFM, son utilizados desde hace mucho tiempo en las labores de aseguramiento de las redes. Sin embargo, el hecho de emplearse como IDS implica una nueva óptica de su aplicación en el problema de la seguridad. Haciendo una búsqueda de los programas disponibles internacionalmente pueden encontrarse soluciones híbridas que combinan dos responsabilidades o más de las descritas arriba. Estas propuestas son válidas y están alcanzando gran popularidad.

5.6 Descripción de las variantes de IDS

A continuación se ofrece una muy breve caracterización de los aspectos distintivos de cada grupo de herramientas IDS.

5.6.1 Sistemas Detectores de Intrusos de Red (NIDS)

Estos programas realizan una comprobación exhaustiva de la composición de cada paquete que circula por la red. En los mismos se verifica la validez de algunos parámetros y el comportamiento de los protocolos de la familia TCP/IP empleados. En su análisis busca patrones que identifiquen ataques ya conocidos, lo que permitiría detectar los mismos en el momento de su ejecución.

Los sensores se posicionan en diferentes segmentos de red para que analicen todos los paquetes que circulan por ellos en busca de patrones de ataques o indicios de intrusiones, generando alarmas en caso positivo. Por su parte, la consola de administración recibe las alertas de los sensores y las visualiza al administrador de seguridad.

Los sensores para lograr su objetivo, deben tener al menos una de las interfaces de red trabajando en modo promiscuo, capturando y analizando todas las tramas que pasan por ella en busca de patrones que indiquen la presencia de un ataque. Estos patrones, pudieran encontrarse en cualquiera de los diferentes campos de un datagrama de red TCP/IP: campos relativos a la fragmentación, direcciones fuente y destino, puertos fuente y destino, banderas TCP y campo de datos.

Estos IDS deben estar preparados no solo para detectar ataques apreciables en un único paquete, sino aquellos que vengan distribuidos en varios de ellos y su efecto solo puede notarse al chequear un grupo de estos. Los sistemas de detección de intrusos basados en red son de los más utilizados.

5.6.1.1 Ubicación en la red

Los NIDS pueden colocarse en diferentes lugares de acuerdo a los intereses de la entidad que los emplea. Incluso, pueden combinarse varios programas en diferentes sitios de la red que se protege. Este aspecto resulta de enorme importancia para el éxito de sus operaciones. Las ubicaciones más comunes son las siguientes:

- Computadora conectada a la red. En este caso se trata de proteger computadoras personales en general. Las herramientas de este tipo, son las más sencillas.
- Zona desmilitarizada. Se protegen los bastiones ubicados de cara a las redes externas. La configuración en este lugar suele ser muy compleja.
- *Backbone* de la LAN o WAN. Estos programas van a manejar una enorme y muy variada cantidad de tráfico.
- Servidores. Esta es una variante que permite proteger cada servidor individualmente.

La colocación de varios NIDS en las ubicaciones señaladas ofrecerá una solución de seguridad mucho más completa. Existen dos soluciones al problema de la ubicación de NIDS en redes conmutadas para proteger determinadas zonas de las mismas: *los puertos espejos* y los *TAPS*.

El puerto espejo es un puerto del conmutador en el que se replican los paquetes de otros puertos definidos, lo que permite monitorizar todo su tráfico con un sensor. En algunos casos, los conmutadores no suelen garantizar que el 100% del tráfico pase a este puerto por lo que existe la posibilidad de perder paquetes y no reconocer un ataque que el IDS es capaz de detectar.

La otra variante son los *TAPS*, que viene a solucionar los inconvenientes anteriores. Básicamente, es un dispositivo de 3 puertos que permite duplicar el tráfico entre 2 puertos a un tercero, de forma unidireccional (el puerto de copia no puede enviar ni recibir tráfico, solo recibir las copias). Así se consigue la revisión del tráfico de red de una de forma segura.

5.6.2 Sistemas Verificadores de Integridad (SIV)

Básicamente estos programas se ocupan de comprobar la integridad de los ficheros del sistema donde se ubican. Ya es tradicional que este trabajo se realice empleando sumas de verificación que son ejecutadas cada cierto intervalo de tiempo y sobre los ficheros seleccionados por el administrador del sistema.

Dichos programas suelen verificar los permisos en archivos y directorios, las cuentas de usuarios, sentencias en el registro de Windows y en el cron de Unix. De manera general no emiten alarmas sino que generan registros (logs) con los resultados del trabajo que realizan. El análisis de estos registros suele ser complejo debido a la cantidad de información que genera esta labor.

5.6.3 Monitores de Ficheros de Auditoria (LFM)

Estas herramientas revisan los ficheros *logs* de cualquier sistema, siempre que el contenido se encuentre en texto claro. En el análisis que realiza busca patrones de ataques reflejados en los registros por los programas servidores del sistema. La labor de revisión de los ficheros se

apoya en marcas (*offset*) para garantizar la reanudación del trabajo de forma eficiente.

Las bases de datos utilizadas son modificables y/o actualizables. Esto permite el "afinamiento" de la herramienta de acuerdo a las características del sistema que se pretende proteger. De manera general envían mensajes de correo para notificar el resultado de su trabajo.

La frecuencia de ejecución de estos programas está directamente relacionada con la rapidez de reacción ante los ataques. Una revisión más frecuente de los *logs* ofrece la garantía de responder más rápidamente ante un ataque. Sin embargo, hay que cuidar la frecuencia de ejecución de estos programas está directamente relacionada con la rapidez de reacción ante los ataques.

Una revisión más frecuente de los *logs* ofrece la garantía de responder más rápidamente ante un ataque. Sin embargo, hay que cuidar la cantidad y el contenido de las notificaciones. Mensajes muy largos y demasiado frecuentes hacen perder importancia a las notificaciones. Por otra parte, mensajes muy espaciados no permitirían efectuar una reacción rápida ante una intrusión detectada.

5.6.4 Sistemas víctimas (potes de miel)

La implementación de esta herramienta puede ser compleja e incluso la comprensión de su necesidad difícil para muchas entidades. De forma general consiste en una computadora que posee un sistema operativo o servicio desactualizado, con un gran número de vulnerabilidades conocidas.

En ocasiones, se emplea una sola herramienta que simula varios sistemas operativos y los servicios que los mismos ofrecen.

El objetivo fundamental es desviar la atención de los intrusos hacia estos sistemas "indefensos". Esto permitirá detectar el momento de inicio, el origen (si no se emplean técnicas de *spoofing*) y la estrategia de los ataques que se realizan contra una red determinada.

Normalmente los programas o computadoras configuradas para estos propósitos generan *logs* detallados acerca de todas las actividades del sistema. Además, envían notificaciones de la actividad de intrusos detectada.

Estos constituyen un tipo de IDS que están recibiendo mucha atención tanto por usuarios como por investigadores. Existen incluso, grupos de investigadores, que trabajan en el desarrollo de redes enteras con estos propósitos (http://project.honeynet.org). En este caso se trata de redes completas trabajando en lugares e incluso redes diferentes y reportando hacia lugares comunes. El objetivo del proyecto es usar estas redes, sometiéndolas a ataques reales, estudiar los procedimientos usados por la "comunidad *hacker*" en Internet. Según sus organizadores son tres los objetivos fundamentales: elevar la atención en la comunidad de usuarios de las amenazas existentes en la red, informar y enseñar sobre los procedimientos mencionados y realizar investigaciones sobre el tema de la seguridad.

5.6.5 Respuestas

Los IDS de manera general crean un registro bastante amplio de todos los protocolos de aplicación utilizados y de los paquetes analizados. Ante la presencia de una intrusión se presentan variedad de reacciones que son configuradas por el administrador en dependencia de sus intereses.

Respuestas pasivas:

- Emisión de un sonido de alerta.
- Emisión de un *trap* SNMP (*Simple Network Management Protocol*).
- Emisión de un evento al *log* del sistema.
- Envío de mensajes de correo.

Respuestas activas

- Almacenamiento de paquetes con evidencias.
- Incremento de la monitorización de un evento.
- Corrección de vulnerabilidades.
- Ejecución de programas.
- Cierre de la conexión TCP.
- Cierre de conexión de usuarios.
- Configuración del *firewall*.

Algunas de estas variantes, como la configuración del *firewall* de la entidad, pueden resultar riesgosas si no se encuentran correctamente configuradas. Otras, como la ejecución de programas, permiten iniciar ataques en respuesta al supuesto sistema intruso, aspecto que debe cuidarse sobremanera.

5.7 Fortalezas y debilidades de los IDS

A continuación se enumeran algunas de las ventajas y desventajas de los dos grupos principales de IDS.

Detectores de intrusos de red (NIDS)

Fortalezas

- Pocos sensores bien posicionados pueden monitorizar redes grandes.
- Los sensores no interfieren en la operación normal de la red.
- Los sensores se pueden proteger contra ataques.
- Un NIDS puede detectar un ataque antes de que este alcance su objetivo.

Debilidades

- En sentido general un NIDS puede colapsar frente a elevados volúmenes de tráfico.
- Un sensor no puede monitorizar más allá de su segmento en una red conmutada.
- Un NIDS no puede analizar tráfico de red cifrado (VPN, *IPSec* u otros).
- Un NIDS no puede determinar cuándo un ataque es exitoso.

Detectores de intrusos de host

Fortalezas

- Revisa eventos locales en una computadora por lo que puede detectar ataques que un NIDS no tiene capacidad de detectar.
- Pueden disminuir la carga asociada con el monitoreo en redes grandes.
- Su funcionamiento no se ve afectado por el tráfico de red cifrado.

Debilidades

- El sensor HIDS es específico del sistema operativo. Tiene que ser instalado, configurado y mantenido en cada computadora que se desee proteger.
- El sensor usa los recursos de la computadora que monitorea, influyendo en su costo de desempeño.
- Un HIDS puede ser atacado y deshabilitado como parte de un ataque a una computadora, por ejemplo con un ataque de DoS (Denegación de servicio).

5.8 Requisitos de un IDS

Los IDS deben poseer algunas características que los conviertan en instrumentos de seguridad aceptables en un entorno de trabajo determinado:

- Ejecución autónoma continúa.
- No introducir cambios en el comportamiento habitual del sistema que protege.
- Adaptación a cambios en el entorno de trabajo.
- Tolerancia a fallos.

En primer lugar, el IDS debe ejecutarse continuamente sin nadie que esté obligado a supervisarlo. Aunque al detectar un problema se informa al administrador o se envía una respuesta automática, el funcionamiento habitual no tiene que implicar interacción con un humano.

Otra necesidad es el grado de aceptación del IDS. Los mecanismos de detección de intrusos han de ser aceptables para las personas que trabajan habitualmente en el entorno. No han de introducir una sobrecarga en el sistema, ni generar una cantidad elevada de falsos positivos o de *logs*.

Una tercera característica de los sistemas de detección de intrusos debe ser la adaptabilidad del mismo a cambios en el entorno de trabajo. Como es conocido, ningún sistema informático puede considerarse estático, todo cambia con una periodicidad más o menos elevada. Si los mecanismos de detección de intrusos no son capaces de adaptarse rápidamente a esos cambios, están condenados al fracaso.

Todo IDS debe además presentar cierta tolerancia a fallos o capacidad de respuesta ante situaciones inesperadas. Algunos de los cambios que se pueden producir en un entorno informático no son graduales sino bruscos, y el IDS debe ser capaz de responder siempre adecuadamente ante los mismos.

5.9 Ventajas y limitaciones del empleo de productos IDS

Como conclusión de lo anterior un breve análisis de los beneficios y limitaciones del empleo de IDS en la protección de las redes de datos.

5.9.1 Ventajas

- El simple conocimiento de su empleo actúa como freno para los intrusos.
- Detecta usos indebidos que otras herramientas de protección no pueden prevenir.
- Detecta el preámbulo de algunos ataques, como puede ser sondeos de la red y sus servicios.
- Permite obtener argumentos de las amenazas existentes para una organización.

- Actúa como control de calidad para el diseño y la administración de la seguridad.
- Ofrece información muy útil sobre las intrusiones que son efectivas.
- Permite monitorizar la actividad alrededor de servicios débiles desde el punto de vista de la seguridad.
- Su empleo facilita el trabajo de defensa en profundidad.
- Ofrece cierta protección ante ataques desconocidos a partir de la detección de comportamientos o eventos anormales.
- Permite detectar, no solo ataques externos sino también, comportamientos malignos provocados por usuarios internos.

5.9.2 Limitaciones

- No constituyen una solución integral o única.
- Las respuestas activas pueden crear problemas de seguridad o generar ataques a otros sistemas.
- En entornos muy tranquilos, los falsos positivos generan descontento y desatención.
- La intervención humana sigue siendo necesaria.

CONCLUSIONES

1. El principio fundamental es que la seguridad absoluta es inviable, ya que ni material ni económicamente es posible eliminar todos los riesgos posibles. Además existen una gran carencia de personas especializadas en estos temas, y de ellas la mayoría trabajan en el lado oscuro de la red. Por consiguiente una prioridad sería la oficialización de esta especialidad.

2. La cantidad de información disponible en Internet ha permitido que los delincuentes informáticos estén siempre un paso adelante en los temas de vulnerabilidad.

3. Un delito informático no necesariamente será realizado por alguien ajeno a la organización.

4. En todo delito informático siempre existirán pistas digitales, las cuales pueden ser obtenidas al utilizar la Computación Forense.

5. La implementación de mejores prácticas basadas en estándares internacionales permiten reducir las vulnerabilidades de los sistemas de información.

RECOMENDACIONES

1. Realizar una evaluación de exposición al riesgo basado en estándares internacionales.

2. Implementar políticas de seguridad basado en estándares internacionales.

3. Conformar un equipo o contratar una empresa para recuperación en caso de un incidente.

4. Capacitar e informar al personal de la organización en los temas de delitos informáticos.

5. Toda evidencia digital es útil para evaluar el daño de un ataque informático.

BIBLIOGRAFÍA

1. FITZGERALD, Jerry, Ardra Fitzgeradl y Warren Stallings. **Fundamentos de Análisis de Sistemas.** México, D.F. Cía. Editorial Continental, S.A. 379-385 pp.

2. KENDALL, Keneth y Julie Kendall. **Análisis y Diseño de Sistemas.** México, D.F.: Editorial McGraw Hill. 483-529 pp.

3. FAYOL, Henry. **Administración Industrial y General.** México, D.F.: Herrero Hermanos. 23 pp.

4. PRESMAN, Roger. **Ingeniería del Software.** México, D.F.: Editorial McGraw Hill. 37-141 pp.

5. SENN, James A. **Análisis y Diseño de Sistemas de Información.** Tr. Edmundo Gerardo Urbina Medal y Oscar Alfredo Palmas Velasco. 2ª. Ed. México, D.F.: Editorial McGraw Hill. 443-458 pp.

6. SHCPERBERG, Robert, Cybercrime: Incident Response and Digital Forensics. Illinois USA. Information Systems Audit and Control Association (ISACA)

7. www.vecam.org/article659.html, junio 2006

8. http://monografias.com marzo 2006

9. http://www.quadernsdigitals.net/index.php?accionMenu=hemeroteca.VisualizaArticuloIU.visualiza&articulo_id=2850 Junio 2006

10. www.diccionarios.com mayo 2006

11. http://www.criminalistaenred.com.ar/Informatica_F.html

12. http://www.canalhosting.com/diccionario mayo 2006

13. http://www.definicion.org octubre 2006

14. http://www.wikipedia.org septiembre 2006

15. http://www.criptored.upm.es/guiateoria/gt_m189d.htm