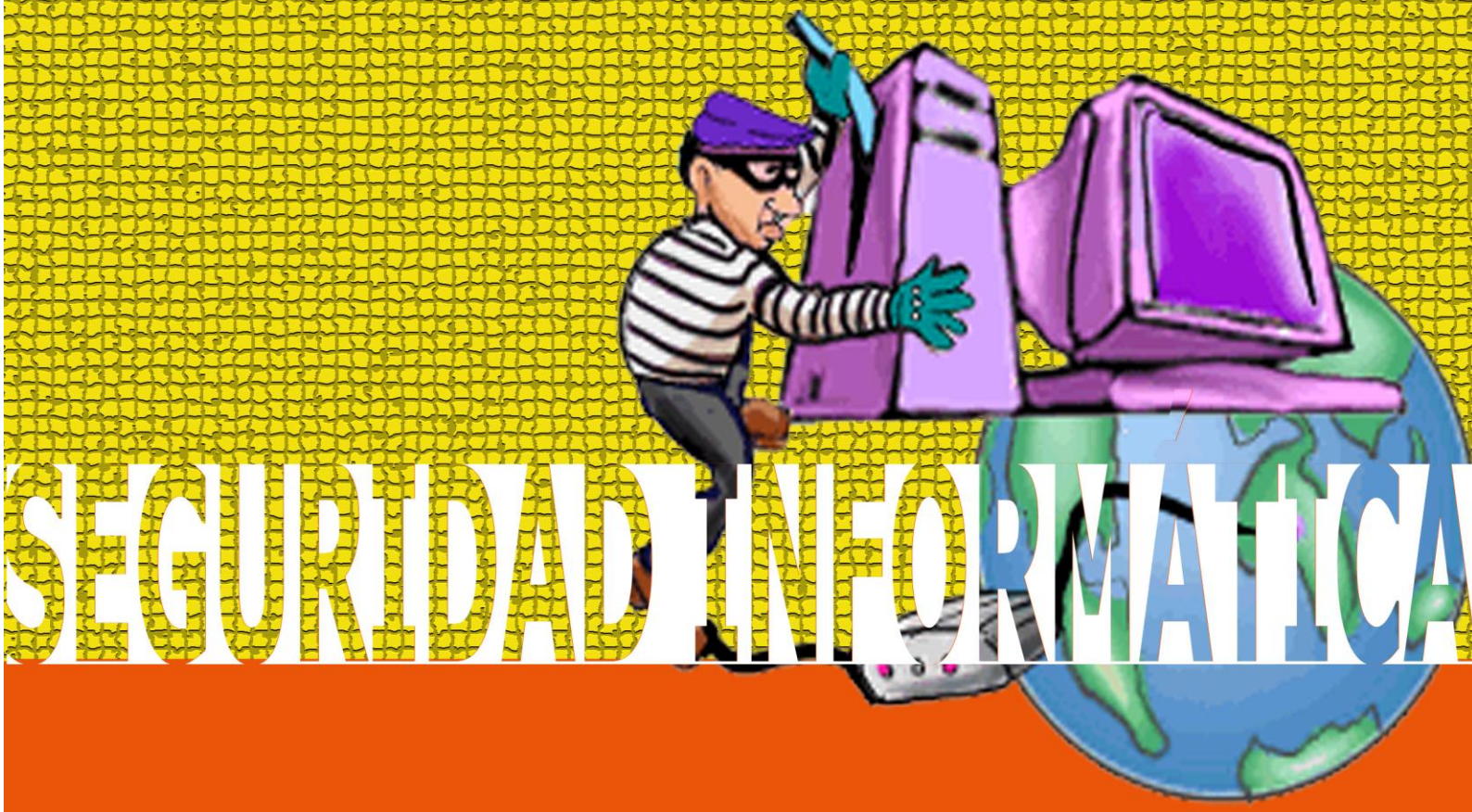
UTPL

La Universidad Católica de Loja

IDENTIFICACIÓN DE VULNERABILIDADES, ANÁLISIS FORENSE Y ATENCIÓN A INCIDENTES DE SEGURIDAD EN LOS SERVIDORES DE LA UTPL



SEGURIDAD INFORMÁTICA

Msc. María Paula Espinoza V.
DIRECTORA

Freddy Bolívar Pinzón Olmedo
AUTOR

INTRODUCCIÓN

Los sistemas de información son esenciales en la mayoría de las organizaciones que cuentan con una tecnología de punta y en constante crecimiento como es el caso de la Universidad, por ello la viabilidad de los proyectos o servicios que están en evolución y desarrollo dependen no solo de las características y ventajas de la tecnología en uso, sino también de la disponibilidad, confidencialidad, integridad, escalabilidad y seguridad de sus equipos, servicios, y datos. Ya que la información ha sido desde siempre un bien invaluable y protegerla ha sido una tarea continua y de vital importancia. A medida que se crean nuevas técnicas para la transmisión de la información.

Actualmente, se puede hacer una infinidad de transacciones a través de Internet y para muchas de ellas, es imprescindible que se garantice un nivel adecuado de seguridad. Esto es posible si se siguen ciertas normas que se pueden definir según la necesidad de la Universidad.

La seguridad no es solo la aplicación de nuevos programas para protegernos, es más bien un cambio de conducta y de pensar. Hay que adueñarse del concepto de seguridad e incluso volverse algo paranoico para que en cada área y servicio que presta la Universidad se piense en seguridad y en cómo incrementarla.

Los intrusos como tal idean formas para acceder a la información sin ser autorizados o detectados, los ataques efectuados son por muchos motivos tales como: curiosidad, sabotaje, beneficio, en fin una gran cantidad de circunstancias que llevan a cometer estos ataques. Por ello se necesario estar preparado a la hora de actuar ante los incidentes que pueden sufrir los equipos ya que esto impediría que los servicios que presta la Universidad se lleven con total normalidad.

En la presente investigación se darán los pasos necesarios para atender de forma rápida y oportuna cualquier incidente de seguridad y enseñará al equipo de seguridad y auditoría a tomar este tema como uno de los puntos claves para el buen funcionamiento de los equipos. En este momento, la seguridad no es un lujo. Es una necesidad.

La identificación de vulnerabilidades de los servidores de la Universidad, son una serie de pasos sin una metodología a seguir, que permite tener una idea del estado de la seguridad informática pero que carece de valides y de resultados aceptados por los administradores, así como del quipo de seguridad y auditoría, por ello se plantea el desarrollo de una metodología hibrida, que en sí es una combinación de varias metodologías, proyectos y estándares, que tiene la ambición de llegar a ser un manual ó un estándar profesional para el testeo e identificación de vulnerabilidades en cualquier entorno desde el exterior al interior ó viceversa, promoviendo la evolución de la seguridad a niveles más aceptados.

Vale la pena preguntar "¿Es importante tener una metodología estandarizada para la identificación de vulnerabilidades de seguridad?" Pues, es difícil evaluar el resultado de un test de seguridad sin una metodología estandarizada. El resultado de un test se ve afectado por muchas variables que intervienen en el proceso como, la experiencia del testeador o analista, conocimiento de los procesos de tecnología, etc. Por la relación de todas estas variables, es importante definir un proceso de testeo, basado en las mejores prácticas y en un consenso a nivel mundial. Si se puede reducir los prejuicios y las parcialidades en el testeo, se reducirá la incidencia de muchos falsos supuestos y también se evitará resultados mediocres. El limitar y guiar suposiciones, convierte a un buen testeador de seguridad en uno excelente y brinda a los novatos la metodología apropiada para llevar a cabo los tests necesarios en las áreas correctas.

Por ello, el objetivo es elaborar una metodología hibrida y que ésta se convierta en un método aceptado para la identificación de vulnerabilidades de cada servidor de la Universidad, sin importar su sistema operativo, bases de datos o aplicativos como software, antivirus o aplicaciones web.

METODOLOGÍA PARA LA IDENTIFICACIÓN DE VULNERABILIDADES

Para que tenga éxito el proceso de identificación de vulnerabilidades en los servidores se deben enmarcar varios aspectos que se relacionan entorno a la seguridad y que son de vital importancia para los administradores de los mismos, de tal forma que se pueda delimitar el problema y nos permita meternos de lleno en la seguridad garantizando el cumplimiento de confidencialidad, integridad, disponibilidad y autentificación. A este proceso se lo ha dividido en tres fases [1] que son:

- ✓ Prevención
- ✓ Identificación
- ✓ Corrección

Vale recalcar que estas fases están íntimamente relacionadas y cada una de ellas se realimenta de las otras en un ciclo repetitivo e iterativo, esto significa que por cada ciclo ejecutado se tendrá en el peor de los casos un listado de vulnerabilidades, con su respectivo identificador y correctivo.

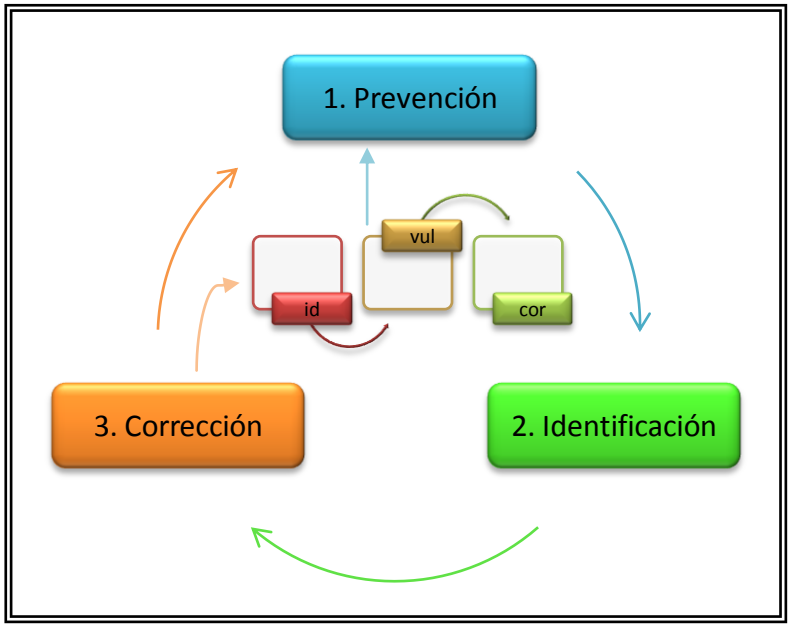


Figura 1: Proceso de identificación de Vulnerabilidades.

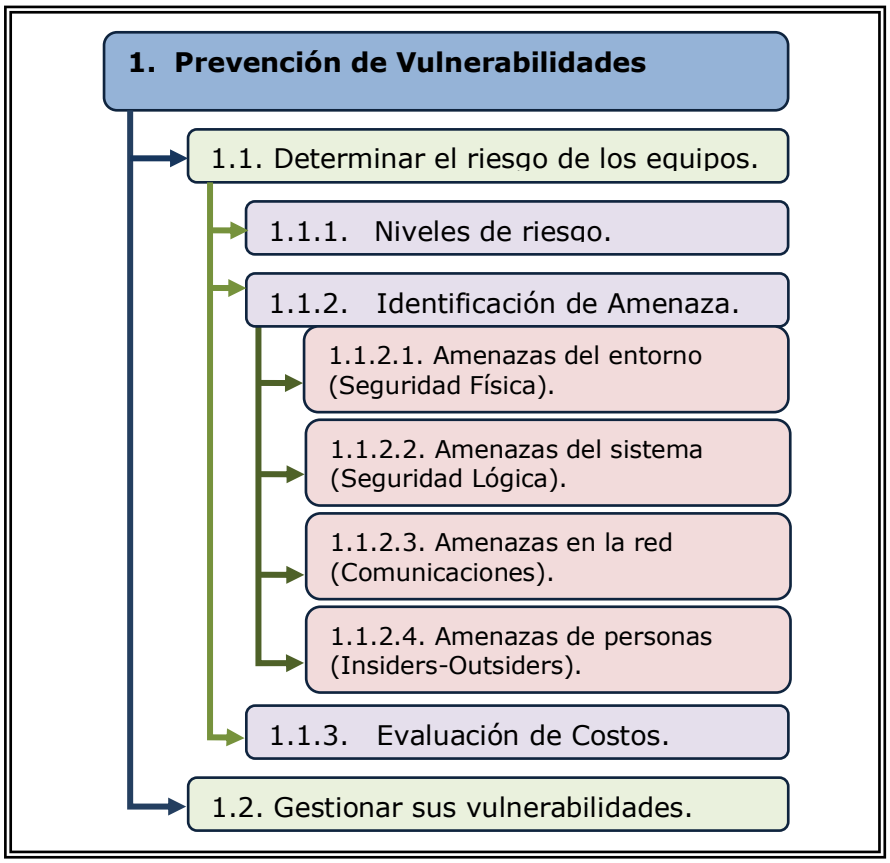


Figura 2: Fase de Prevención de Vulnerabilidades.

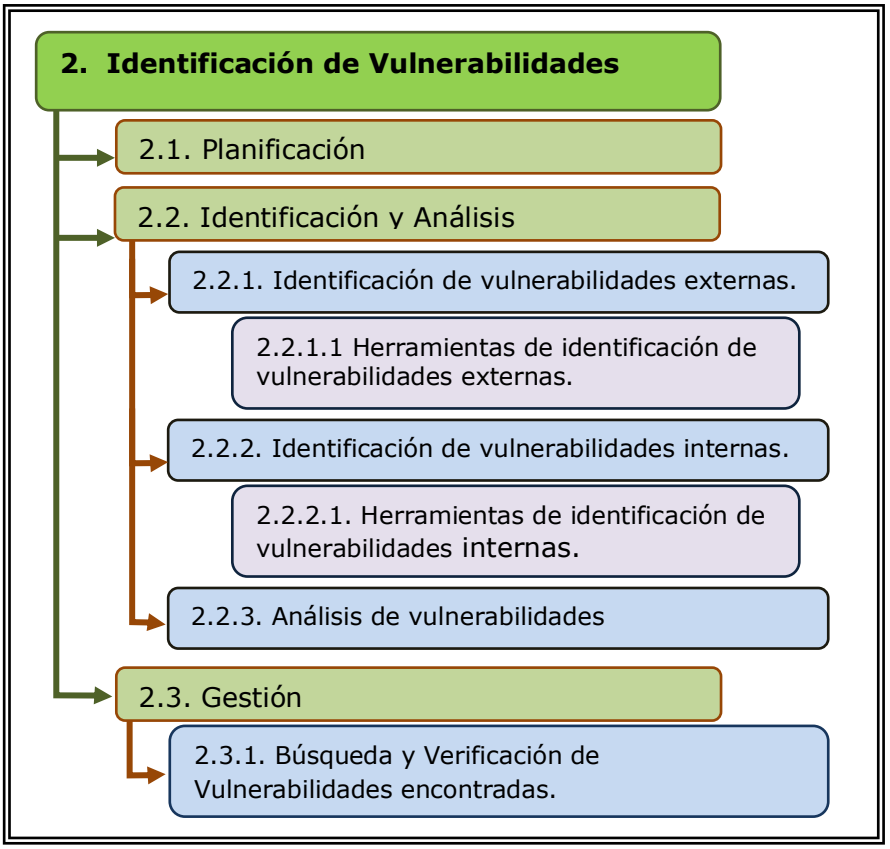


Figura 3: Fase de Identificación de Vulnerabilidades

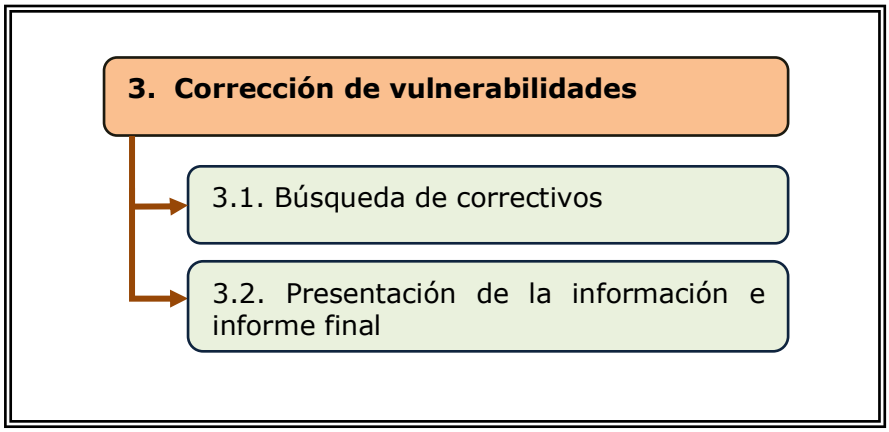


Figura 4: Fase de Corrección de Vulnerabilidades.

1.1. Prevención de vulnerabilidades

Una forma de garantizar la seguridad de los servidores es la prevención, ya que de ésta manera podemos disminuir la aparición de vulnerabilidades así como identificar las amenazas latentes y calcular el riesgo al que se encuentran expuestos los equipos. Para ello es necesario mejorar el proceso de la seguridad de los servidores, incrementando cada día más tareas y procesos[2], tales como:

- ✓ Determinar el riesgo de los equipos.
- ✓ Identificar su exposición.
- ✓ Gestionar sus vulnerabilidades.

1.1. Determinar el riesgo de los equipos

El análisis de riesgos[3] supone más que el hecho de calcular la posibilidad de que ocurran eventos negativos, sino también el de poder predecir y adelantarnos ante cualquier eventualidad que ponga en riesgo el perfecto funcionamiento de los servidores, para ello:

- ✓ Se debe obtener una evaluación económica del impacto de estos sucesos. Este valor se podrá utilizar para contrastar el costo de la protección de la información en análisis versus el costo de volverla a producir (reproducir).
- ✓ Se debe tener en cuenta la probabilidad de que sucedan cada uno de los problemas posibles, de esta forma se pueden priorizar los problemas y su coste potencial desarrollando un plan de acción adecuado.
- ✓ Se debe conocer qué se quiere proteger, dónde y cómo, asegurando que con los costos en los que se incurren se obtengan beneficios efectivos. Para esto se deberá identificar los recursos (hardware, software, información, etc.) con que cuenta cada servidor y las amenazas a las que están expuestos.

Una vez obtenida la lista de cada uno de los riesgos se efectuará un resumen del tipo:

Tipo de Riesgo	Factor
Robo de hardware	Alto
Robo de información	Medio
Vandalismo	Medio
Fallas en los equipos	Medio
Virus Informáticos	Medio
Equivocaciones	Medio
Accesos no autorizados	Medio
Fraude	Bajo
Fuego	Muy Bajo
Terremotos	Muy Bajo

Tabla 1.1. Tipo de Riesgo-Factor

Según esta tabla habrá que tomar las medidas pertinentes de seguridad para cada caso en particular, cuidando incurrir en los costos necesarios según el factor de riesgo representado.

1.1.1. Niveles de riesgo

Como puede apreciarse en la Tabla 1.1., los riesgos se clasifican por su nivel de importancia y por la severidad de su pérdida:

- ✓ Estimación del riesgo de pérdida del recurso (R_i)
- ✓ Estimación de la importancia del recurso (I_i)

Para la cuantificación del riesgo de perder un recurso, es posible asignar un valor numérico de 0 a 10, tanto a la importancia del recurso (10 es el recurso de mayor importancia) como al riesgo de perderlo (10 es el riesgo más alto).

El riesgo de un recurso será el producto de su importancia por el riesgo de perderlo:

$$WR_i = R_i * I_i$$

Luego, con la siguiente fórmula es posible calcular el riesgo general de los recursos de un servidor:

$$W_R = \frac{(WR_1 * I_1 + WR_2 * I_2 + \ldots + WR_n * I_n)}{I_1 + I_2 + \ldots + I_n}$$

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

Ejemplo: el Administrador de un servidor ha estimado los siguientes riesgos y su importancia para los elementos del servidor que administra:

Recurso	Riesgo (R i)	Importancia (I i)	Riesgo Evaluado (R i * I i)
Software	6	7	42
Hardware	6	5	30
Bases de D.	10	10	100
Información	9	2	18

Tabla 1.1.2 - Valuación de Riesgos

Aquí ya puede apreciarse que el recurso que más debe protegerse son las bases de datos. Para la obtención del riesgo total del servidor calculamos:

$$W_R = \frac{42 + 30 + 100 + 18}{7 + 5 + 10 + 2} = 7{,}92$$

Al ver que el riesgo total del servidor es de casi 8 puntos sobre 10 debería pensarse seriamente en buscar las probables causas que pueden provocar problemas a los servicios brindados por los elementos evaluados.

1.1.2. Identificación de Amenaza

Una vez conocidos los riesgos, los recursos que se deben proteger y como su daño o falta pueden influir en el normal funcionamiento de los servidores es necesario identificar cada una de las amenazas y vulnerabilidades que pueden causar estas bajas en los recursos. Como ya se mencionó existe una relación directa entre amenaza y vulnerabilidad a tal punto que si una no existe la otra tampoco.

Amenazas existentes[4] según su ámbito de acción:

- ✓ Amenazas del entorno (Seguridad Física).
- ✓ Amenazas del sistema (Seguridad Lógica).
- ✓ Amenazas en la red (Comunicaciones).
- ✓ Amenazas de personas (Insiders-Outsiders).

1.1.2.1. Amenazas del entorno (Seguridad Física).

Es muy importante tener en cuenta que por más que se tenga un grado aceptable de seguridad desde el punto de vista de ataques externos, Hackers, virus, etc. la seguridad de los servidores será nula si no se ha previsto como atender un incidente de seguridad física.

La seguridad física es uno de los aspectos más olvidados a la hora de implementar políticas de seguridad, puede derivar que para un atacante esa más fácil tomar y copiar una cinta de respaldo del servidor, que intentar acceder vía lógica al mismo.

Así, la Seguridad Física consiste en la "aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial". Se refiere a los controles y mecanismos de seguridad dentro y alrededor de la sala de servidores así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos.

Evaluar y controlar permanentemente la seguridad física de la sala de servidores es la base para comenzar a integrar la seguridad como una función primordial dentro de la Universidad.

Tener controlado el ambiente y acceso físico nos permitirá:

- ✓ disminuir siniestros
- ✓ trabajar mejor manteniendo la sensación de seguridad
- ✓ descartar falsas hipótesis si se produjeran incidentes
- ✓ tener los medios para luchar contra accidentes

1.1.2.1.1. Tipos de Desastres

Las principales amenazas en la seguridad física son:

- ✓ Desastres naturales, incendios accidentales tormentas e inundaciones.

- ✓ Amenazas ocasionadas por el hombre.
- ✓ Disturbios, sabotajes internos y externos deliberados.

1.1.2.1.2. Acciones Hostiles

- ✓ Robo
- ✓ Fraude
- ✓ Sabotaje

1.1.2.1.3. Control de Accesos

El control de acceso no sólo requiere la capacidad de identificación, sino también asociarla a la apertura o cerramiento de puertas, permitir o negar acceso basado en restricciones de tiempo, área o sector dentro de la sala de servidores.

1.1.2.2. Amenazas del sistema (Seguridad Lógica).

Luego de ver como pueden ser afectados los servidores por la falta de Seguridad Física, es importante recalcar que la mayoría de los daños que puede sufrir los mismos no será sobre medios físicos sino contra la información almacenada y procesada.
Así, la Seguridad Física, sólo es una parte del amplio espectro que se debe cubrir para no vivir con una sensación ficticia de seguridad. Como ya se ha mencionado, el activo más importante que se posee es la información, y por lo tanto deben existir técnicas, más allá de la seguridad física, que la aseguren. Estas técnicas las brinda la Seguridad Lógica.

Es decir que la Seguridad Lógica consiste en la "aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo."

Los objetivos que se plantean para atender la seguridad lógica son:

- ✓ Restringir el acceso a los programas y archivos.
- ✓ Asegurar que los usuarios puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
- ✓ Asegurar que se estén utilizados los datos, archivos y programas correctos.
- ✓ Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.
- ✓ Que la información recibida sea la misma que ha sido transmitida.

- ✓ Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
- ✓ Que se disponga de pasos alternativos de emergencia para la transmisión de información.

1.1.2.3. Amenazas en la red (Comunicaciones).

Los protocolos de comunicación utilizados carecen de seguridad, por eso muchas de las veces se implementada en forma de parche tiempo después de su creación, de tal manera que tenemos amenazas como:

- ✓ Agujeros de seguridad en los sistemas operativos.
- ✓ Agujeros de seguridad en las aplicaciones.
- ✓ Errores en las configuraciones de los sistemas.
- ✓ Usuarios que carecen de información respecto al tema.

Esta lista podría seguir extendiéndose a medida que se evalúen mayor cantidad de elementos de un servidor.

Por lo cual los administradores deben tener mayor conciencia respecto de la seguridad de sus servidores y estar en la capacidad de arreglar por sí mismos las deficiencias detectadas. A esto hay que añadir las nuevas herramientas de seguridad disponibles en el mercado.

1.1.2.3.1. Identificación de las Amenazas

La identificación de amenazas requiere conocer los tipos de ataques, el tipo de acceso, la forma operacional y los objetivos del atacante.

Las consecuencias de los ataques se podrían clasificar en:

- ✓ ***Data Corruption*:** Información que contiene defectos
- ✓ ***Denial of Service (DoS):*** Servicios que deberían estar disponibles no lo están
- ✓ ***Leakage:*** Los datos llegan a destinos a los que no deberían llegar

1.1.2.3.2. Tipos de Ataques

Los ataques[5] pueden ser realizados sobre cualquier tipo de red, sistema operativo o servidor usando diferentes protocolos, de tal forma que:

Insiders operadores, programadores y data entrys utilizaban sus permisos para alterar archivos o registros.
Outsiders ingresaban a la red, utilizando herramientas cada vez más sofisticadas para explotar agujeros en el diseño, configuración y operación de los sistemas.

Entre los tipos de ataques tenemos:

- ✓ Ingeniería Social
- ✓ Ingeniería Social Inversa
- ✓ Trashing (Cartoneo)
- ✓ Ataques de Monitorización
- ✓ Ataques de Autenticación
- ✓ Denial of Service (DoS)
- ✓ Ataques de Modificación – Daño

1.1.2.3.3. ¿Cómo defenderse de estos Ataques?

La mayoría de los ataques mencionados se basan en fallos de diseño inherentes a Internet, protocolos y a los sistemas operativos utilizados, por lo que no son solucionables en un plazo breve de tiempo.

La solución inmediata en cada caso es mantenerse informado sobre todos los tipos de ataques existentes y las actualizaciones que permanentemente lanzan las empresas desarrolladoras de software, principalmente de sistemas operativos.

Las siguientes medidas preventivas deben ser ejecutadas por cada administrador de la seguridad y de los servidores:

- ✓ Mantener los servidores actualizados y seguros físicamente
- ✓ Mantener personal especializado en cuestiones de seguridad informática.
- ✓ Aunque un servidor no contenga información valiosa, hay que tener en cuenta que puede resultar útil para un atacante, a la hora de ser empleada en un DoS coordinado o para ocultar su verdadera dirección.
- ✓ No permitir el tráfico broadcast desde fuera de nuestra red. De esta forma evitamos ser empleados como multiplicadores durante un ataque Smurf.
- ✓ Filtrar el tráfico IP Spoof.
- ✓ Auditorias de seguridad y sistemas de detección.
- ✓ Mantenerse informado constantemente sobre cada unas de las vulnerabilidades encontradas y parches lanzados. Para esto es recomendable estar suscripto a listas que brinden este servicio de información.

- ✓ Por último, pero quizás lo más importante, la capacitación continua de los administradores.

1.1.2.4. Amenazas de personas (Insiders-Outsiders).

Hasta aquí hemos presentado al personal como víctima de atacantes externos; sin embargo, de los robos, sabotajes o accidentes relacionados con los servidores, el 70% son causados por el propio personal de las organizaciones ("Inside Factor").

El siguiente gráfico detalla los porcentajes de intrusiones clasificando a los atacantes en internos y externos.

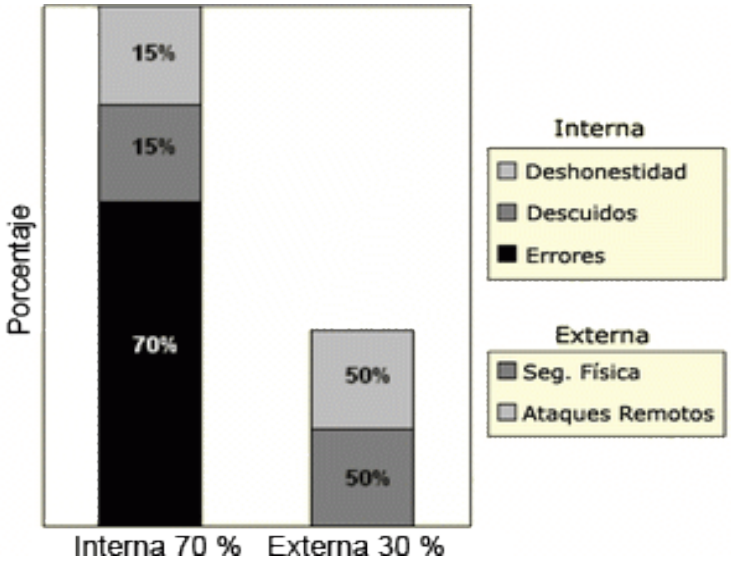


Figura 5: "Tipo de intrusiones"[6]

Esto es realmente preocupante, ya que, una persona que trabaje con el administrador, el programador o el encargado de un servidor conoce perfectamente el sistema, sus puntos fuertes y débiles; de manera que un ataque realizado por esa persona podrá ser más directo, difícil de detectar y más efectivo que el que un atacante externo pueda realizar.

Existen diversos estudios que tratan sobre los motivos que llevan a una persona a cometer delitos informáticos contra su organización, pero sean cuales sean, estos motivos existen y deben prevenirse y evitarse

Como ya se ha mencionado los ataques pueden ser del tipo pasivos o activos, y el personal realiza ambos indistintamente dependiendo de la situación concreta.

Dentro de este espectro podemos encontrar:

- ✓ Personal Interno
- ✓ Ex-Empleado
- ✓ Curiosos
- ✓ Terroristas
- ✓ Intrusos Remunerados

1.1.3. Evaluación de Costo

Responder a la pregunta del valor de la información ha sido siempre difícil, y más difícil aún hacer estos costos justificables.

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

La evaluación de costos más ampliamente aceptada consiste en cuantificar los daños que cada vulnerabilidad puede causar teniendo en cuenta las posibilidades. Un planteamiento para desarrollar esta política es el análisis de lo siguiente:

- ✓ ¿Qué recursos se quieren proteger?
- ✓ ¿De qué personas necesita proteger los recursos?
- ✓ ¿Qué tan reales son las amenazas?
- ✓ ¿Qué tan importante es el recurso?
- ✓ ¿Qué medidas se pueden implantar para proteger los recursos de una manera económica y oportuna?

Con esas sencillas preguntas más la evaluación de riesgo se debería conocer que recursos vale la pena proteger, y entender que algunos son más importantes que otros.

El objetivo que se persigue es lograr que un ataque a los servidores no sea más costoso que su valor. Para esto se define tres costos fundamentales:

CP: Valor de los bienes y recursos protegidos.
CR: Costo de los medios necesarios para romper las medidas de seguridad establecidas.
CS: Costo de las medidas de seguridad.

Para que la política de seguridad sea lógica y consistente se debe cumplir que:

CR > CP: o sea que un ataque para obtener los bienes debe ser más costoso que el valor de los mismos. Los beneficios obtenidos de romper las medidas de seguridad no deben compensar el costo de desarrollo del ataque.

CP > CS: o sea que el costo de los bienes protegidos debe ser mayor que el costo de la protección.

Luego, CR > CP > CS y lo que se busca es:

Minimizar el costo de la protección manteniéndolo por debajo de los bienes protegidos. Si proteger los bienes es más caro de lo que valen (el lápiz dentro de la caja fuerte), entonces resulta más conveniente obtenerlos de nuevo en vez de protegerlo.

Maximizar el costo de los ataques manteniéndolo por encima del de los bienes protegidos. Si atacar el bien es más caro de lo que valen, al atacante le conviene más obtenerlo de otra forma menos costosa.

Se debe tratar de valorar los costos en que se puede incurrir en el peor de los casos contrastando con el costo de las medidas de seguridad adoptadas. Se debe poner especial énfasis en esta etapa para no incurrir en el error de no considerar costos, muchas veces, ocultos y no obvios (costos derivados).

1.1.3.1. Costos Derivados de la Pérdida

Una vez más deben abarcarse todas las posibilidades, intentando descubrir todos los valores derivados de la pérdida de algún componente del sistema. Muchas veces se trata del valor añadido que gana un atacante y la repercusión de esa ganancia para el entorno, además del costo del elemento perdido. Deben considerarse elementos como:

- ✓ Información aparentemente inocua como datos personales, que pueden permitir a alguien suplantar identidades.
- ✓ Datos confidenciales de acuerdos y contratos que un atacante podría usar para su beneficio.
- ✓ Tiempos necesarios para obtener ciertos bienes. Un atacante podría acceder a ellos para ahorrarse el costo y tiempo necesario para su desarrollo.

1.1.3.2. Punto de Equilibrio

Una vez evaluados los riesgos y los costos en los que se está dispuesto a incurrir y decidido el nivel de seguridad a adoptar, podrá obtenerse un punto de equilibrio entres estas magnitudes:

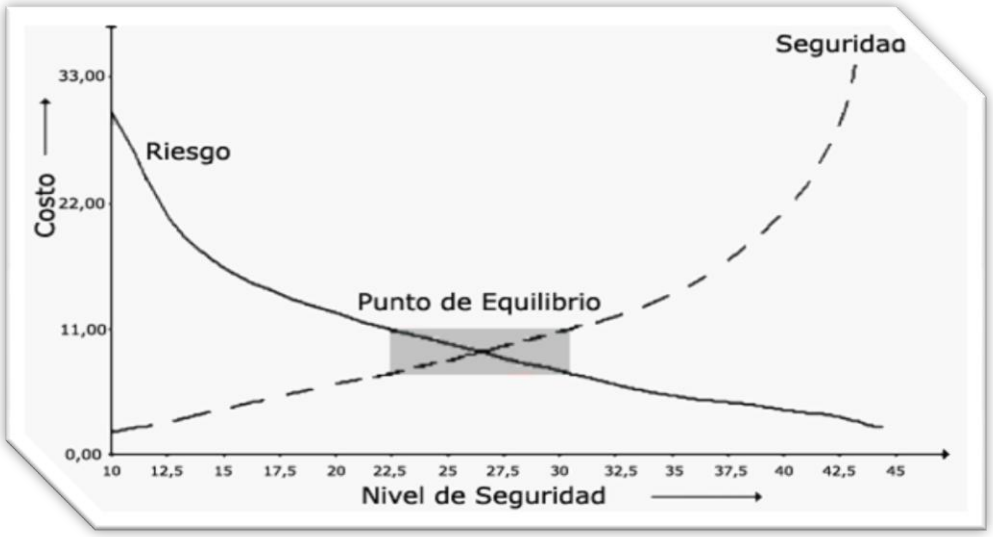


Figura 6: Punto de Equilibrio[7]: Costo/Seguridad/Riesgo

Como puede apreciarse los riesgos disminuyen al aumentar la seguridad, pero como ya se sabe los costos tenderán al infinito sin lograr el 100% de seguridad y por supuesto nunca se logrará no correr algún tipo de riesgo. Lo importante es lograr conocer cuan seguro se estará conociendo los costos y los riesgos que se corren (Punto de Equilibrio).

1.2. Gestionar sus vulnerabilidades.

Una vez analizados los riesgos que rodean a los servidores así como las amenazas latentes y el costo de la pérdida ocasionada por posibles ataques procedemos con la gestión de vulnerabilidades.

La gestión de vulnerabilidades es un proceso que se vale de la ejecución de la metodología con anterioridad esto significa, que por cada ciclo de la metodología aplicada a los servidores tendremos en el peor de los casos un listado, bitácora o base de datos de hallazgos de la cual extraemos las vulnerabilidades que podrían aparecer en un nuevo servidor, esto se debe realizar en pruebas antes de poner un servidor a producción, la creación de éste repositorio o bitácora de vulnerabilidad nos permitirá tener un control de cada servidor, en el que se detalla toda la información necesaria para los administradores de los mismos. Así tendremos un

registro de o historial de los servidores con información tal como se muestra en la figura 5.

Entonces el propósito de esta fase radica, en evitar al máximo la aparición de vulnerabilidades y más si éstas ya son conocidas, para ello podemos aplicar los siguientes correctivos:

- ✓ Parches y Service Packs actualizados para el servidor
- ✓ Una Configuración segura en el servidor
- ✓ Evitar instalaciones de software por defecto
- ✓ Eliminar demos y aplicativos que no se utilicen
- ✓ Controlar y realizar una programación responsable de las aplicaciones web que se ejecutan en cada servidor.
- ✓ El descubrimiento preciso y exhaustivo de todos los activos y recursos de red utilizando tanto agentes de exploración local como de red
- ✓ El correctivo de vulnerabilidades atreves de monitoreos
- ✓ La validación de conformidad con las políticas de seguridad de los servidores.

La aplicación de estos correctivos según sea el caso nos evitará la detección de vulnerabilidades conocidas, que se encuentran dentro del registro o base de datos de los hallazgos encontrados, así no caeremos en el mismo error.
Cada vez que se ejecute un ciclo de la metodología será registrado dentro de la siguiente tabla de hallazgos

Metodología para la identificación de Vulnerabilidades "Tabla de registro de Vulnerabilidades"			
Servidor			
Dirección IP		***Nombre de dominio***	
Sistema O.		***Fecha***	

Puerto	***Protocolo***	***Servicio***	***Detalles del servicio***

Id	***Vulnerabilidad***	***Correctivo***	***Estado***

Figura 7: Tabla de registro de Vulnerabilidades.

1.2. Identificación de vulnerabilidades

Una vez realizada la fase de prevención, en la que se analizó todas las posibles amenazas que podrían afectar el completo funcionamiento de los servidores y el costo que ocasionaría la falta de los servicios que estos prestan, procedemos a identificar las vulnerabilidades que cada servidor posee y que es por donde las amenazas podrían realizar su cometido, para ello, esta fase se divide en tres procesos que son:

- ✓ Planificación
- ✓ Identificación y Análisis
- ✓ Gestión

2.1. Planificación

El objetivo principal de este proceso es establecer el marco general de referencia en el que se debe trabajar, es decir, hay que planificar como se va a desarrollar el proceso de identificación de vulnerabilidades.
Para ello debemos:

- ✓ Identificar la infraestructura de red en la que se encuentra el servidor.- es decir que se debe enmarcar todo lo que rodea al servidor en cuanto a software y hardware de red para tener una idea de la tecnología y de los procesos de seguridad que posee el servidor o los servidores a ser monitoreados; esto se debe obtener del grupo de telecomunicaciones.
- ✓ Obtener un historial del servidor, el cual tendrá como datos:
  - ❖ Software instalado
  - ❖ Servicios que presta
  - ❖ Usuario o usuarios que acceden al servidor, así como las tareas o procesos que realizan.
- ✓ Identificar los puertos que el servidor esta utilizando según cada aplicación o herramienta instalada.
  Esto se lo trabaja directamente con cada administrador de los servidores.

Una vez identificada la estructura de red, los usuarios, los puertos utilizados y que servicios presta el servidor se define el horario para la ejecución de las herramientas de identificación, ya que muchas de estas producen un bloqueo o interrupciones en los servicios y prestaciones de los servidores por lo que no es aconsejable realizarlo en hora de mucha concurrencia.
La información obtenida se debe adjuntar y guardar en el siguiente formato.

Metodología para la identificación de Vulnerabilidades "Tabla de registro de Servidores"							
Servidor							
Dirección IP		**Nombre de dominio**					
Sistema O.		**Administrador**					
Fecha destinada al escaneo de vulnerabilidades			**Horario para el escaneo de Vulnerabilidades**				
Usuario	**Tipo de usuario**	**Funciones**					
Puerto	**Protocolo**	**Servicio**	**Detalles del servicio**				
Software	**Detalle**						

Figura 8: Tabla de registro de historial de los servidores.

La infraestructura de red se debe adjuntar en forma gráfica

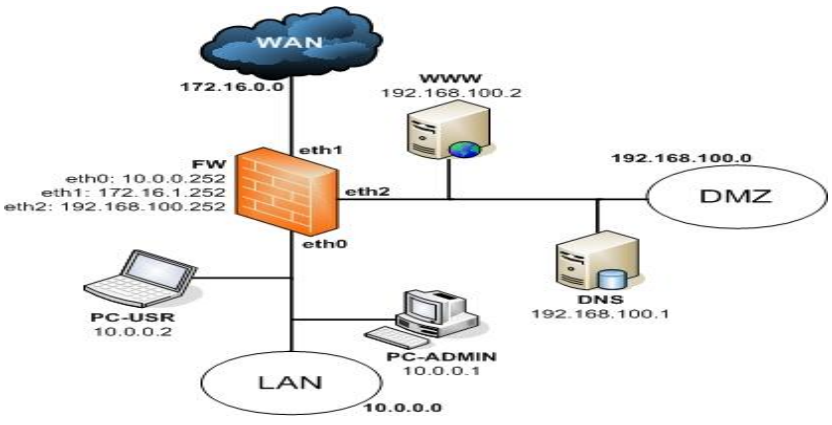
Metodología para la identificación de Vulnerabilidades "Esquema de Red"			
Servidor			
Dirección IP		**Nombre de dominio**	
Sistema O.		**Administrador**	
			

Figura 9: Esquema de Red del servidor o servidores.

Una vez obtenida la información necesaria de cada servidor se procede a la selección de herramientas idóneas, escaners de vulnerabilidades según el sistema operativo y el tipo de información procesada por el servidor así también el fijar un

horario para la ejecución de las herramientas, esto se lo realiza con el administrador y su respectiva aprobación.

2.2. Identificación y análisis

Finalizada la planificación se procede con el proceso de identificación y análisis de vulnerabilidades, para ello se debe comprender que existe dos entornos para la identificación de vulnerabilidades en los servidores, que son:

- ✓ Interno, entorno privilegiado.- El ambiente interno es dentro de la red, o sea que se tiene los permisos necesarios para poder ejecutar las herramientas y que me encuentro dentro de la universidad consumiendo los recursos y servios prestados por los servidores.

- ✓ Externo, entorno no privilegiado.- Esto significa que estoy fuera de la red accediendo a los servicios y recursos de los servidores vía internet, mediante una conexión externa. Por ello se tendrá muchos bloqueos de seguridad como el firewall y todos los equipos de seguridad tanto hardware como software que impiden el acceso libre a los recursos, esto puede impedir la utilización de herramientas ya que no se cuenta con los permisos necesarios.

Es importante comprender que la seguridad total no existe y que seria un error creer que estamos totalmente protegidos contra cualquier incidente sea interno o externo, la tecnología esta en constante evolución y como tal la información cada día es de dominio publico por lo que es muy habitual encontrar en internet noticias e información de cómo romper la seguridad de las organizaciones, es muy fácil encontrar herramientas que permiten romper esta seguridad, por ello no se debe contar con los medios suficientes para hacerles frente.

La única forma existente de estar totalmente seguros es que los servidores estén aislados de cualquier acceso o conexión en un cuarto con llave y que nadie tenga la llave por que esta perdida.

Comprendiendo que existen dos entornos de identificación de vulnerabilidades y que es importante realizar los escaneos tanto dentro de la red como fuera, ya que no sabemos si existen o no agujeros de seguridad, por ello tiene:

- ✓ Identificación de vulnerabilidades externas
- ✓ Identificación de vulnerabilidades internas

2.2.1. Identificación de vulnerabilidades externas

La identificación de vulnerabilidades externas[8], es un proceso en el que busca detectar todas los posibles vulnerabilidades que poseen los servidores y que podrían ser utilizadas por los intrusos (Hackers, virus, crackers, etc.) para explotar la red y ocasionar cualquier daño posible en los recursos y servicios que posen los servidores, este proceso se lo realiza explotando la red desde una conexión externa y utilizando herramientas de detección de vulnerabilidades, para ello se realiza un escaneo de los servidores, el cual nos dará como resultado un listado de vulnerabilidades, que en primera instancia las recogeremos en un tabla previa para su posterior análisis y reporte de hallazgos.

En esta tabla se registra el resultado de un escaneo a determinado servidor, para luego de un profundo análisis registrarlas en la tabla de vulnerabilidades donde constarían las vulnerabilidades y su correctivo, este proceso se debe realizar con cada herramienta utilizada, de manera permita investigar lo obtenido con cada una de los escaneos, ya que este proceso no puede estar sujeto a la utilización de una sola herramienta ni tampoco se puede confiar de su resultado esto se debe verificar para poder clasificar la vulnerabilidad y saber de que se trata.

Metodología para la identificación de Vulnerabilidades "Tabla de registro de Vulnerabilidades Externas"				
Servidor				
Dirección IP		***Nombre de dominio***		
Sistema O.		***Fecha***		
Herramienta				
Vulnerabilidad		***Correctivo***		***Estado***

Figura 10: Tabla de registro de Vulnerabilidades Externas.

2.2.1.1. Herramientas de identificación de vulnerabilidades externas

Las siguientes herramientas[9] permiten realizar un escaneo fuera de la red, para buscar los agujeros por donde se podrían presentar incidentes.

- ✓ ISS Internet Scanner
- ✓ Nessus Security Scanner
- ✓ Retina Netwok Security Scanner

2.2.2. Identificación de vulnerabilidades internas

En este proceso se realizan los escaneos de vulnerabilidades internamente, ósea dentro de la red y con la ayuda de las herramientas automáticas, en la que también se obtendrá una tabla o registro previo de vulnerabilidades según la herramienta utilizada.

La tabla o registro de las vulnerabilidades encontradas según la herramienta utilizada permitirá realizar un análisis minucioso del servidor y su estado actual de manera que se pueda identificar si se trata de una vulnerabilidad o una falsa alarma, la siguiente tabla permitirá realizar el reporte previo a su análisis.

Metodología para la identificación de Vulnerabilidades "Tabla de registro de Vulnerabilidades Internas"				
Servidor				
Dirección IP		***Nombre de dominio***		
Sistema O.		***Fecha***		
Herramienta				
Vulnerabilidad		***Correctivo***		***Estado***

Figura 11: Tabla de registro de Vulnerabilidades Internas.

2.2.2.1. Herramientas de identificación de vulnerabilidades internas

La utilización de herramientas automáticas es una forma eficiente de determinar agujeros de seguridad existentes y niveles de parcheado de los sistemas. Aunque muchos escáneres automáticos están actualmente tanto en el mercado como en el mundo underground. No obstante, es necesaria la verificación manual para eliminar falsos positivos, expandir el ámbito de hacking y descubrir el flujo de datos de entrada y salida del servidor.

- ✓ ISS System Scanner
- ✓ Microsoft Baseline Security Analyzer
- ✓ Tiger Security
- ✓ Sandcat
- ✓ Nessus
- ✓ Nmap

Cada una de las herramientas utiliza su particular método de detección que, por norma general y sobre todo en las herramientas de detección remota, consiste en intentar explotar el problema al que dan pie las vulnerabilidades.

En cuanto al conjunto de vulnerabilidades que cada una puede detectar, cada herramienta suele nutrirse de las colecciones de nuevos problemas que, una vez conocidos, cada producto consigue publicarlo.

2.2.3. Análisis de vulnerabilidades.

Las herramientas de detección de vulnerabilidades tanto externas como internas no tienen mucha diferencia en los servicios y utilidades que prestan, pero si en los resultados que obtienen y por ello no se puede depender ni aceptar un solo resultado, lo que se debe hacer es ejecutar varios escaners para luego evaluar los diferentes resultados obtenidos.

Se debe evaluar de todos los resultados obtenidos las coincidencias, entonces lo que sebe hacer es analizar estos resultados comparándolos con el de todas las herramientas, luego de ello se procede a listar las vulnerabilidades aceptadas y analizadas en la Tabla de registro de Vulnerabilidades (figura 7), para luego dar inicio al proceso de gestión que es donde se comienza a crear una bitácora o base de datos de cada servidor.

2.3. Gestión

De cada escaneo realizado tanto interno como externo se obtiene una tabla de vulnerabilidades las cuales se deben analizar para separar los falsos positivos y los falsos negativos de las vulnerabilidades reales, éste análisis se lo realiza en base a todo el conjunto presentado por las diferentes herramientas utilizadas.

2.3.1. Búsqueda y Verificación de Vulnerabilidades

Lo que se persigue con este proceso es la identificación, comprensión, verificación de vulnerabilidades y errores de configuración en los servidores, reportadas por cada una de las diferentes herramientas y registradas en las tablas tanto de identificación externa como interna.

Una vez realizado los escaneos con las diferentes herramientas para la identificación de vulnerabilidades procedemos con el análisis minucioso de cada reporte, de tal manera que tendremos que seguir los siguientes pasos:

- ✓ Integrar en las pruebas realizadas los escáneres, herramientas de hacking y exploits utilizados actualmente.

- ✓ Determinar y clasificar las vulnerabilidades por tipo de aplicación y sistema operativo.
- ✓ Ajustar las vulnerabilidades a servicios.
- ✓ Determinar el tipo de aplicación y servicio por vulnerabilidad.
- ✓ Realizar la identificación de vulnerabilidades internas como externas con al menos 2 escáneres automáticos de vulnerabilidades.
- ✓ Identificar todas las vulnerabilidades relativas a las aplicaciones.
- ✓ Identificar todas las vulnerabilidades relativas a los sistemas operativos.
- ✓ Identificar todas las vulnerabilidades de sistemas parecidos o semejantes que podrían también afectar a los demás servidores.
- ✓ Verificar todas las vulnerabilidades encontradas durante la fase de búsqueda de exploits con el objetivo de descartar falsos positivos y falsos negativos.
- ✓ Verificar todos los positivos. (vulnerabilidades encontradas).

Una vez haya concluido el proceso de Búsqueda y Verificación de Vulnerabilidades, se deberá contar con un reporte en le que se detallen los datos del servidor y su registro de vulnerabilidades.

Metodología para la identificación de Vulnerabilidades "Tabla de registro de Vulnerabilidades"			
Servidor			
Dirección IP		***Nombre de dominio***	
Sistema O.		***Fecha***	
Puerto	***Protocolo***	***Servicio***	***Detalles del servicio***
Id	***Vulnerabilidad***	***Correctivo***	***Estado***

Figura 12: Tabla de registro de Vulnerabilidades

1.3. Corrección de vulnerabilidades

La investigación concerniente a la búsqueda de vulnerabilidades es necesaria hasta prácticamente el momento de la entrega del informe final de hallazgos. Esta investigación incluye la búsqueda en bases de datos online y listas de correo relativas a los sistemas y servidores que se están escaneando. No se debe limitar la

búsqueda a la web, también se debe considerar la utilización del IRC, grupos de noticias, y sitios underground.

Una vez conocidas las vulnerabilidades que afectan a cada uno de los servidores de la universidad, es decir después del análisis y eliminación de los grupos tanto de falsos positivos como falsos negativos, procedemos a documentar estas vulnerabilidades en el formato presentado en la figura 5, de tal manera que permita a los administradores y al grupo de seguridad y auditoría dar un correcto, ágil y oportuno seguimiento al registro de vulnerabilidades de cada servidor, si mismos nos permitirá tener un registro del estado de la seguridad en el momento actual. De nada sirven los interminables documentos con tablas de vulnerabilidades de de los mismos, si no se les dota de un formato ágil que permita la actualización y seguimiento de cada problema

3.1. Búsqueda de correctivos

Una vez identificadas las vulnerabilidades así como creado el registro de cada servidor según el formato presentado de identificación de vulnerabilidades, procedemos con la búsqueda de correctivos, según lo demande cada vulnerabilidad encontrada, para ello nos valemos del estado de cada vulnerabilidad presentado en el reporte según la herramienta utilizada ya que en este consta el correctivo o también de los sitios que llevan el reporte de vulnerabilidades, tales como:

Vulnerabilidades

- ✓ http://www.seguridad.unam.mx/vulnerabilidadesDB/
- ✓ http://www.vnunet.es/Seguridad/Vulnerabilidades
- ✓ http://www.alerta-antivirus.es/seguridad/busca_vulns.php

Boletines

- ✓ http://www.cert.org.mx/boletin/
- ✓ http://www.vnunet.es/Seguridad/Sistemas_de_protecci%C3%B3n
- ✓ http://www.segu-info.com.ar/boletin/

Organizaciones y empresas colaboradoras:

- ✓ Cybex, http://www.cybex.es
- ✓ Germinus, http://www.germinus.com
- ✓ Guidance Software, http://www.guidancesoftware.com
- ✓ LogiCube, http://www.logicube.com
- ✓ RedIRIS, http://www.rediris.es
- ✓ Revista Red Seguridad , http://www.borrmart.es

- ✓ RNP-CAIS http://www.rnp.br/cais
- ✓ S21Sec, http://www.s21sec.com
- ✓ Sarenet, http://www.sarenet.es
- ✓ SANS, http://www.sans.org
- ✓ UNAM-CERT http://www.seguridad.unam.mx

3.2. Informe final y presentación de la información

Este proceso indica el final del ciclo de la identificación de vulnerabilidades en el que se deben presentar a cada administrador de los servidores el informe final conjuntamente con los registros de vulnerabilidades y los correctivos que se deben aplicar.

3.2.1. Registro de Vulnerabilidades

Metodología para la identificación de Vulnerabilidades "Tabla de registro de Vulnerabilidades"			
Servidor			
Dirección IP		***Nombre de dominio***	
Sistema O.		***Fecha***	
Puerto	***Protocolo***	***Servicio***	***Detalles del servicio***
Id	***Vulnerabilidad***	***Correctivo***	***Estado***

Figura 13: Tabla de registro de Vulnerabilidades

METODOLOGÍA PARA EL ANÁLISIS FORENSE

Cada día que pasa la informática forense adquiere gran importancia dentro de las tecnologías de información, debido al aumento del valor de la misma así como, la proliferación de redes y sistemas informáticos que han diversificado la forma en la que los delincuentes comenten los crímenes.

Es habitual encontrar nuevas amenazas para la seguridad informática, los delitos relacionados con la posesión, distribución, falsificación y fraude de información se realizan tras un escritorio, esto muestra un panorama complejo, en el cual los profesionales de las tecnologías de la información y los profesionales de la defensa de la ley deben cooperar y trabajar juntos en la defensa, detección y procesamiento de las personas que utilizan las nuevas tecnologías para realizar delitos informáticos.

Entre los delitos[10] más habituales tenemos:

- ✓ ***Protección al menor****:* producción, distribución y posesión de pornografía infantil.
- ✓ ***Fraude en las comunicaciones****:* locutorios telefónicos clandestinos
  Dialers: modificación oculta del número de teléfono de destino, Producción y distribución de decodificadoras de televisión privada.
- ✓ ***Fraudes en Internet****:* estafas, subastas ficticias y ventas fraudulentas.
  Carding: uso de tarjetas de crédito ajenas o fraudulentas.
  Phising: redirección mediante correo electrónico a falsas páginas simuladas trucadas (común en las mafias rusas).
- ✓ ***Seguridad lógica****:* virus, ataques de denegación de servicio, sustracción de datos, hacking, descubrimiento y revelación de secretos, suplantación de personalidades, sustracción de cuentas de correo electrónico. Delitos de injurias, calumnias y amenazas a través del e-mail, news, foros, chats o SMS.
- ✓ ***Propiedad intelectual****:* piratería de programas de ordenador, de música y de productos cinematográficos. Robos de código: como en el caso de los juegos Dark Age of Camelot, y Half-Life 2, o de los sistemas Cisco IOS y Enterasys Dragon IDS.

Pero, ¿Por qué se generan más incidentes que antes?

- ✓ **Crecimiento de la dependencia tecnológica.**
- ✓ **Amplia disponibilidad de herramientas para el escaneo de puertos, descifrar contraseñas, sniffers de red, etc.**

- ✓ **No hay leyes globales.**
- ✓ **Internet es un laboratorio.**
- ✓ **Falsa sensación de que todo se puede hacer.**
- ✓ **Gran aumento y auge de las vulnerabilidades.**

Es aquí donde nace la informática forense como una ciencia totalmente nueva, que se encuentra en constante evolución gracias a la iniciativa de la comunidad informática y la empresa privada.

Análisis forense informático

Frecuentemente se publica en internet, noticias y blogs de equipos de seguridad reportes sobre vulnerabilidades, fallas humanas, errores de procedimientos y mala configuración de los equipos y aplicaciones de seguridad que presentan un escenario perfecto para que se lleven a cabo incidentes y delitos informáticos. Los intrusos informáticos que causan cualquier tipo de daño en los equipos poseen diferentes motivaciones, alcances y estrategias que desconciertan a los administradores de los servidores y equipos, pues sus modalidades de ataque y penetración de sistemas varían de un caso a otro.

Definiciones

Existen múltiples definiciones[11] para el análisis forense en informática y por ende varios términos para aproximarnos a este tema, dentro de los cuales se tienen: computación forense, digital forensics (forensia digital), network forensics (forensia en redes), entre otros. Este conjunto de términos puede generar confusión en los diferentes ambientes o escenarios donde se utilice, pues cada uno de ellos trata de manera particular.

"*Computer forensics* (computación forense).- Disciplina de las ciencias forenses, que considerando las tareas propias asociadas con la evidencia, procura descubrir e interpretar la información en los medios informáticos para establecer los hechos y formular las hipótesis relacionadas con el caso. Como la disciplina científica y especializada que entendiendo los elementos propios de las tecnologías de los equipos de computación ofrece un análisis de la información residente en dichos equipos.

Network forensics (forense en redes).- Comprender la manera como los protocolos, configuraciones e infraestructuras de comunicaciones se conjugan para dar como resultado un momento específico en el tiempo y un comportamiento

particular. Esta conjunción de palabras establece un profesional que entendiendo las operaciones de las redes de computadores, es capaz, siguiendo los protocolos y formación criminalística, de establecer los rastros, los movimientos y acciones que un intruso ha desarrollado para concluir su acción.

Digital forensics (forense digital).- semejante a informática forense, al ser una forma de aplicar los conceptos, estrategias y procedimientos de la criminalística tradicional a los medios informáticos especializados, con el fin de apoyar a la administración de justicia en su lucha contra los posibles delincuentes o como una disciplina especializada que procura el esclarecimiento de los hechos (¿quién?, ¿cómo?, ¿dónde?, ¿cuándo?, ¿porqué?) de eventos que podrían catalogarse como incidentes, fraudes o usos indebidos bien sea en el contexto de la justicia especializada o como apoyo a las acciones internas de administración de la inseguridad informática.

Evidencia digital

Cualquier registro generado por o almacenado en un sistema computacional que puede ser utilizado como evidencia en un proceso legal[12].

La evidencia digital puede ser dividida en tres categorías:

1. Registros almacenados en el equipo de tecnología informática (correos electrónicos, archivos de aplicaciones de ofimática, imágenes, etc.)
2. Registros generados por los equipos de tecnología informática (registros de auditoría, registros de transacciones, registros de eventos, etc.).
3. Registros que parcialmente han sido generados y almacenados en los equipos de tecnología informática. (hojas de cálculo financieras, consultas especializadas en bases de datos, vistas parciales de datos, etc.).

Características de la evidencia digital

La evidencia digital posee las siguientes características:

1. Volátil
2. Anónima
3. Duplicable
4. Alterable y modificable
5. Eliminable

Estas características hacen de la evidencia digital un constante desafío para la identificación y el análisis, que exige al grupo de seguridad y auditoria la

capacitación tanto en procedimientos, como en técnicas y herramientas tecnológicas para obtener, custodiar, revisar, analizar y presentar la evidencia en una escena del delito.

Antes de realizar el proceso de análisis forense el equipo de seguridad o auditoría debe considerar los siguientes elementos[13] para mantener la idoneidad del procedimiento forense:

- ✓ ***Esterilidad de los medios informáticos de trabajo***

Los medios informáticos utilizados deben estar libres de variaciones magnéticas, ópticas (láser) o similares, esto significa que los medios deben ser nuevos para evitar que las copias de la evidencia que se ubiquen en ellos puedan estar contaminadas. La esterilidad de los medios es una condición fundamental para el inicio de cualquier procedimiento forense en informática.

- ✓ ***Verificación de las copias en medios informáticos***

Las copias efectuadas en los medios previamente esterilizados, deben ser idénticas al original del cual fueron tomadas, para esto, se debe utilizar algoritmos y técnicas de control basadas en firma digitales que puedan comprobar que la información inicialmente tomada corresponde a la que se ubica en el medio de copia.

- ✓ ***Documentación de los procedimientos, herramientas y resultados sobre los medios informáticos analizados***

El equipo de seguridad debe ser el custodio de su propio proceso, por tanto cada uno de los pasos realizados, las herramientas utilizadas (sus versiones, licencias y limitaciones), los resultados obtenidos del análisis de los datos, deben estar claramente documentados, de tal manera, que cualquier persona del grupo de auditoría pueda validar y revisar los mismos. Ante una confrontación sobre la idoneidad del proceso, el tener documentado y validado cada uno de sus procesos ofrece una importante tranquilidad al equipo, pues siendo rigurosos en la aplicación del método científico es posible que un tercero reproduzca sus resultados utilizando la misma evidencia.

- ✓ ***Mantenimiento de la cadena de custodia de las evidencias digitales***

La custodia de todos los elementos allegados al caso y en poder del equipo de seguridad, debe responder a una diligencia y formalidad especiales para documentar cada uno de los eventos que se han realizado con la evidencia en su poder. Quién la entregó, cuándo, en qué estado, cómo se ha transportado, quién ha tenido acceso a ella, cómo se ha efectuado su custodia, entre otras, son las

preguntas que deben estar claramente resueltas para poder dar cuenta de la adecuada administración de las pruebas a su cargo.

- ✓ ***Informe y presentación de resultados de los análisis de los medios informáticos***

Este elemento es tan importante como los anteriores, pues una inadecuada presentación de los resultados puede llevar a falsas expectativas o interpretación de los hechos que ponga en entredicho la idoneidad del investigador. Por tanto, la claridad, el uso de un lenguaje amable y sin tecnicismos, una redacción impecable sin juicios de valor y una ilustración pedagógica de los hechos y los resultados, son elementos críticos a la hora de defender un informe de las investigaciones. Generalmente existen dos tipos de informes, los técnicos con los detalles de la inspección realizada y el ejecutivo para la gerencia y sus dependencias.

- ✓ ***Administración del caso realizado***

El equipo de seguridad debe prepararse para declarar ante un jurado o juicio, por tanto, es probable que en el curso de la investigación o del caso, un oficial de seguridad[14] sea llamado a declarar en ese instante o mucho tiempo después. Por tanto, el mantener un sistema automatizado de documentación de expedientes de los casos, con una adecuada cuota de seguridad y control, es labor necesaria y suficiente para salvaguardar los resultados de las investigaciones y el debido cuidado, diligencia y previsibilidad del profesional que ha participado en el caso.

- ✓ ***Auditoría de los procedimientos realizados en la investigación***

Finalmente y no menos importante, es recomendable que el grupo de auditoría mantenga un ejercicio de autoevaluación de los procedimientos, para contar con la evidencia de una buena práctica de investigaciones forenses, de tal manera que el ciclo de calidad:

PHVA - Planear, Hacer, Verificar y Actuar, sea una constante que permita incrementar la actual confiabilidad de los procedimientos y cuestionar las prácticas y técnicas actuales para el mejoramiento de un ejercicio profesional y la práctica de la disciplina.

- ✓ ***Herramientas***

Hablar de informática forense sin revisar algunas ideas sobre herramientas[15] es hablar en un contexto teórico de procedimientos y formalidades legales. Las herramientas informáticas, son la base esencial de los análisis de las evidencias digitales en los medios informáticos. Sin embargo, es preciso comentar que éstas requieren de una formalidad adicional que permita validar tanto la confiabilidad de

los resultados de la aplicación de las mismas, como la formación y conocimiento del equipo de seguridad que las utiliza. Estos dos elementos hacen del uso de las herramientas, una constante reflexión y cuestionamiento por parte de la comunidad científica y práctica de la informática forense en el mundo.

Dentro de las herramientas frecuentemente utilizadas en procedimientos forenses en informática detallamos algunas para conocimiento general, que son aplicaciones que tratan de cubrir todo el proceso en la investigación forense en informática:

ENCASE http://www.encase.com/products/ef_index.asp
FORENSIC TOOLKIT http://www.accessdata.com/products/utk/
WINHEX http://www.x-ways.net/forensics/index-m.html

Si bien las herramientas detalladas anteriormente son licenciadas y sus precios oscilan entre los 600 y los 5000 dólares, existen otras que no cuentan con tanto reconocimiento internacional en procesos legales, que generalmente son aplicaciones en software de código abierto:

Sleuth Kit http://www.sleuthkit.org/
Coroner Toolkit http://www.porcupine.org/foren-sics/tct.html

Estás últimas a pesar de que son utilizadas con frecuencia como estrategia de validación en el uso de otras herramientas, vienen haciendo una importante carrera en la práctica de la informática forense, con lo cual no se descarta en un futuro próximo que éstas estén compitiendo mano a mano con las licenciadas mencionadas anteriormente. Para mayor información de otras herramientas forenses en informática se sugiere revisar el enlace:

http://www.e-evidence.info/ven-dors.html

El equipo de seguridad también debe contar con un conjunto de utilitarios que permitan dar una oportuna atención a incidentes que pudieran presentarse, en esta sección se presentan algunas herramientas que serán de gran ayuda y que se las encontrar fácilmente en internet.

La mayor parte de las técnicas se basan en la recuperación de información de discos duros y rígidos. En este entorno de análisis forense de discos tenemos:

- ✓ ***ENCASE***
  http://www.guidancesoftware.com/products/EnCaseForensic/index.shtm

Que puede realizar duplicaciones exactas del contenido de un disco, incluso de forma remota.

- ✓ ***SMART***

  http://www.asrdata.com/SMART/

  Es una utilidad que permite instalar en un disco las imágenes capturadas con Encase.

- ✓ ***Forensic Toolkit***

  http://www.accessdata.com/Product04_Overview.htm?ProductNum=04

  Conjunto de herramientas de análisis forense.

- ✓ ***Disk Doubler II***

  http://www.lec.cz/en/produkty_datove_diskdoubler_II2.html

  Un duplicador hardware de discos.

- ✓ ***Disk Doubler Plus***

  http://www.lec.cz/en/produkty_datove_diskdoublerplus2.html

  Una aplicación de búsqueda de cadenas en los datos adquiridos.

La recuperación de ficheros borrados o no accesibles entra también dentro de este campo y para ello tenemos:

- ✓ ***Foremost***

  http://foremost.sourceforge.net/

  Permite extraer ficheros del interior de una imagen de disco.

- ✓ ***Herramientas de recuperación de ficheros.***

  CIA Unerase - http://www.ciaunerase.com/

  File Recover - http://www.filerecover.com/download.html

  R-Studio - http://www.r-studio.com/

  Ontrack Easy Recovery **-** http://www.ontrack.com/easyrecovery/

  GetDataBack - http://www.runtime.org/

- ✓ ***Sleuth Kit***

  http://www.sleuthkit.org/informer/

  Si se han borrado particiones con fdisk.

- ✓ ***NTFS Reader***

  http://www.ntfs.com/products.htm

  Es un programa Windows que genera una imagen de floppy disk para arrancar en FreeDos y permite leer y copiar ficheros dentro de particiones NTFS.

- ✓ ***Crear imágenes de discos de arranque de sistemas operativos***

  Bootdisk - http://www.bootdisk.com/

  Winimage - http://www.winimage.com/winimage.htm

  PEBuilder - http://www.nu2.nu/pebuilder/

- ✓ ***Wotsit Format***

  http://www.wotsit.org/

  Contiene las especificaciones de múltiples formatos de ficheros.

- ✓ ***Gestión de particiones.***

  Drive Image - http://www.powerquest.com/driveimage/

  Norton Ghost - http://www.symantec.com/ghost/

Por otro lado, el análisis forense también se refiere a determinar las causas del compromiso de seguridad de un sistema, es decir, la alteración de sus datos o la caída o malfuncionamiento del sistema.

- ✓ ***Control de integridad de ficheros***

  Tripwire

  http://www.tripwire.com/downloads/index.cfm

  Osiris

  http://osiris.shmoo.com/

- ✓ ***John the Ripper***

  http://www.openwall.com/john/

  Es el crackeador de contraseñas de fuerza bruta más famoso, probablemente por ser gratuito y uno de los primeros.

- ✓ ***OpenWall***

  http://www.openwall.com/PR/

  Es una recopilación de recuperadores de contraseñas

- ✓ ***Russian Password Crackers***

  http://www.password-crackers.com/

  Incluye crackeadores para compresores, para utilidades de cifrado, BIOS, formatos de ficheros (Office, PDF, etc.), bases de datos, Sistemas Operativos, Aplicaciones, etc. se incluyen además enlaces sobre los algoritmos y sus debilidades

- ✓ ***MDcrack***

  http://membres.lycos.fr/mdcrack/

  Es capaz de romper hashes MD4, MD5 y NTLM1

- ✓ ***Offline NT Password Registry editor***

  http://home.eunet.no/~pnordahl/ntpasswd/

  Permite recuperar o restablecer una contraseña en Windows.

- ✓ ***Recuperar o restablecer una contraseña en Windows 2000***

  Chntpw **-** http://www.cgsecurity.org/index.html?ntfs.html

  pwdump3 **-** http://archives.neohapsis.com/archives/ntbugtraq/2001-q1/0007.html

  Dumpsec **-** http://www.somarsoft.com/

- ✓ ***LC5***

  http://www.atstake.com/research/lc/download.html

  Es la última versión del famoso crackeador de passwords comercial L0phtCrack, antiguo grupo de hacking ahora reconvertido en el empresa @Stake. Se trata de un software de recuperación de passwords por fuerza bruta y por diccionario para Microsoft Windows.

- ✓ ***Cain***

  http://www.oxid.it/cain.html

  Software muy conocido para la recuperación de password Windows.

- ✓ ***Rainbowcrack***

  http://www.antsight.com/zsl/rainbowcrack/

  Permite agilizar el cracking de contraseñas mediante precomputación de hashes.

- ✓ ***Winrtgen***

  http://www.oxid.it/projects.html

  Se puede agilizar la generación de tablas para Rainbowcrack.

- ✓ ***Revelation***

  http://www.snadboy.com/

  Utilidad freeware para revelar las contraseñas ocultas en el GUI de Windows.

Es importante anotar, que estas herramientas se utilizan en los procesos de las tareas propias asociadas con la evidencia en el contexto de la situación bajo inspección.

Por ello se busca identificar todas las actividades realizadas por el o los atacantes de una forma secuencial, desde el inicio de las mismas hasta la culminación del proceso, buscando saber y comprender qué es lo que hizo, cuándo lo hizo y la evidencia que soporta estos datos.

La metodología desarrollada se divide en cinco fases. Estas son:

1. **Identificación**
2. **Preservación**
3. **Análisis**
4. **Documentación y presentación de las pruebas**

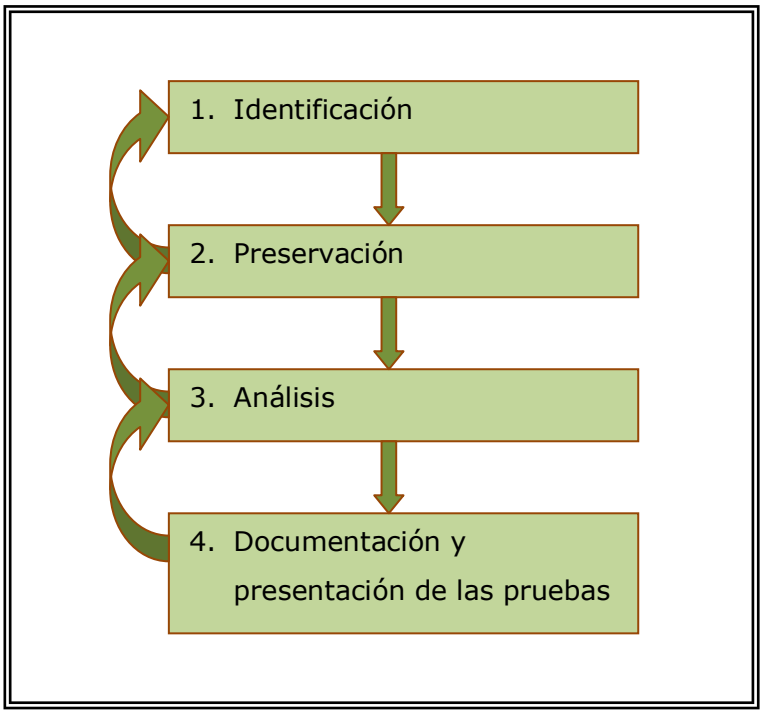


Figura 14: Metodología de Análisis Forense

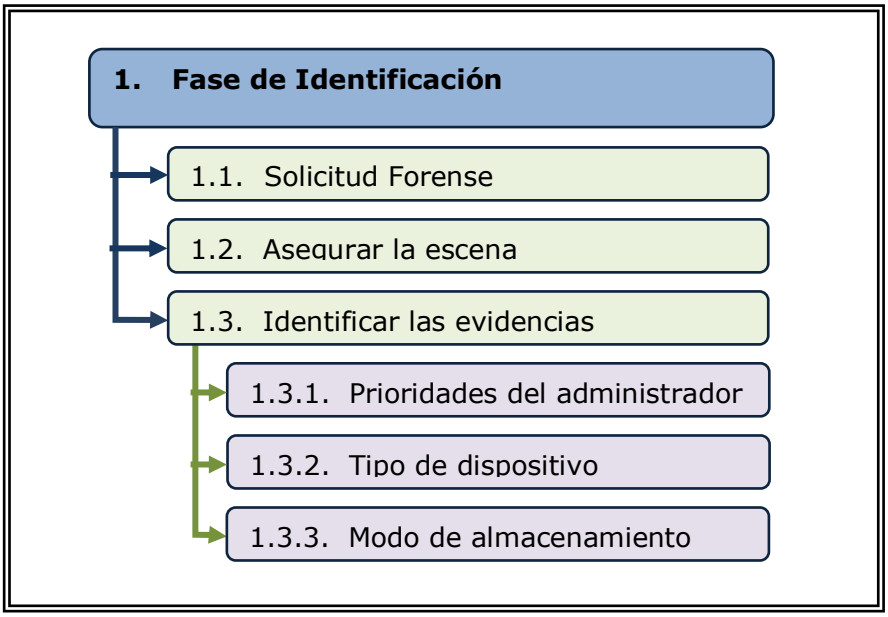


Figura 15: Fase de Identificación

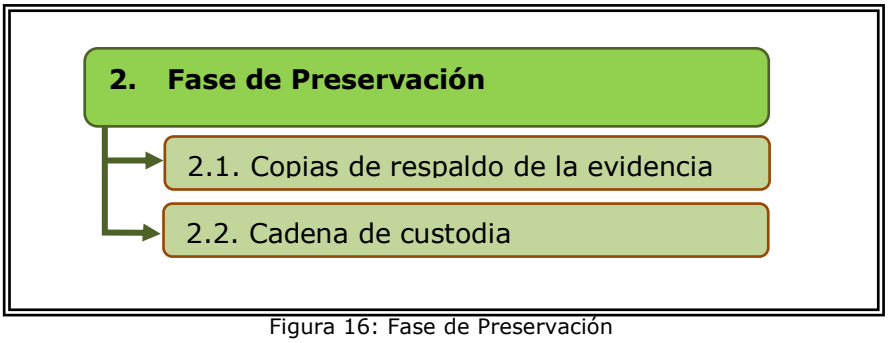


Figura 16: Fase de Preservación

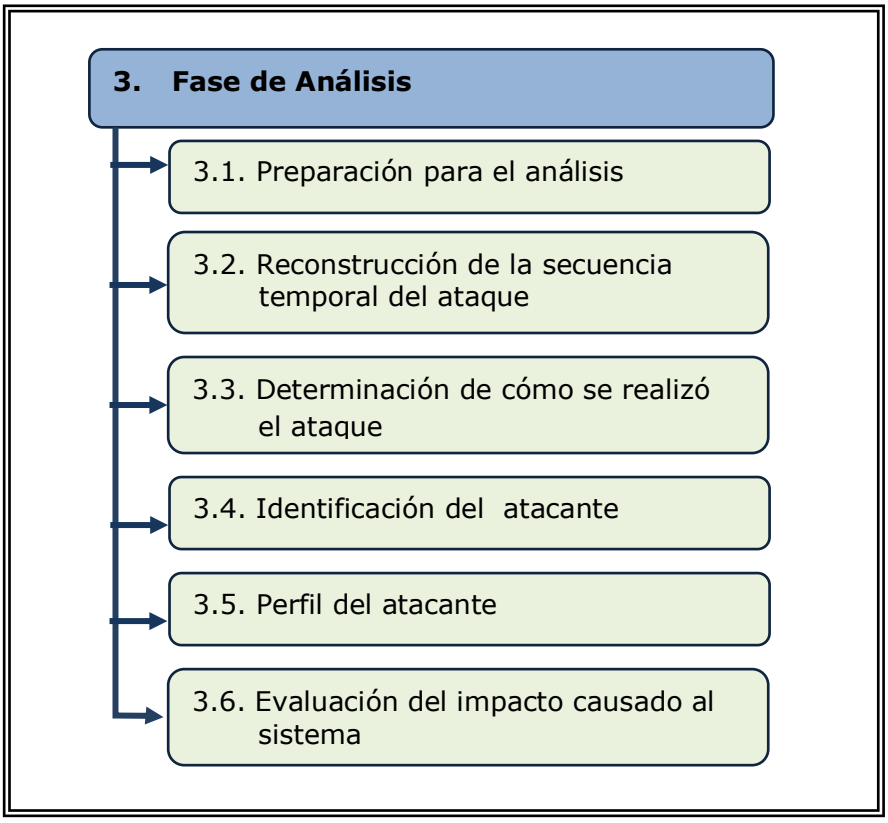


Figura 17: Fase de Análisis

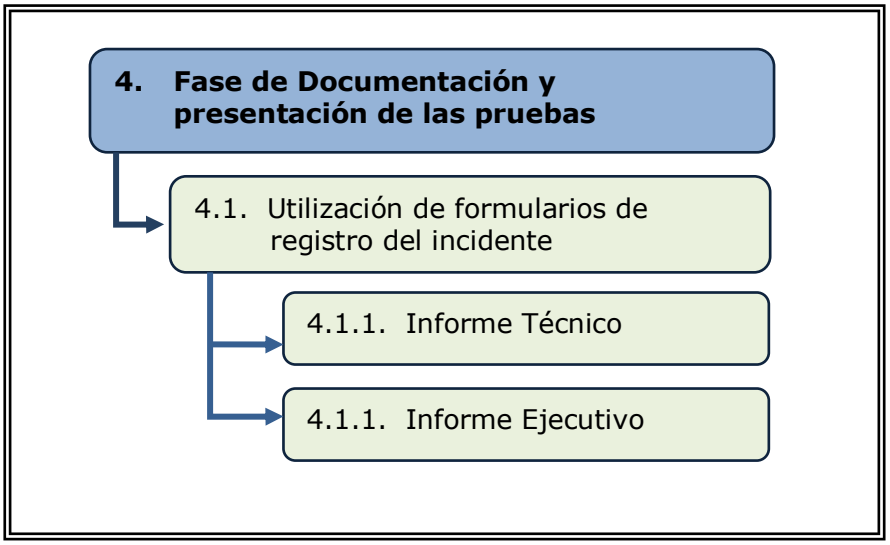


Figura 18: Fase de Documentación y presentación de pruebas

1. Fase de Identificación

La fase de identificación se refiere a la recopilación de información necesaria para trabajar sobre la fuente de datos presentada por el administrador de los servidores (solicitud forense). Aquí se pregunta:

- ✓ ¿Qué información se necesita?
- ✓ ¿Cómo aprovechar la información presentada?
- ✓ ¿En qué orden ubico la información?
- ✓ ¿Acciones necesarias a seguir para el análisis forense?

La identificación debe prever los desafíos que se pasaran durante los procesos de las fases de preservación y extracción. Esta fase culmina con un Plan a seguir.

1.1. Solicitud Forense

La solicitud forense es un documento donde el administrador del equipo afectado notifica de la ejecución de un incidente y para ello solicita al equipo de seguridad la revisión del mismo, donde incluye toda la información necesaria para dar inicio al proceso de análisis. La información incluida en el documento debe ser la siguiente:

- ➢ DESCRIPCIÓN DEL DELITO INFORMÁTICO
  - ➢ Fecha del incidente
  - ➢ Duración del incidente
  - ➢ Detalles del incidente
- ➢ INFORMACIÓN GENERAL

- Área
- Nombre de la dependencia
- Responsable del sistema afectado
  - Nombres y Apellidos
  - Cargo
  - E-mail
  - Teléfono
  - Extensión
  - Celular
  - Fax
- INFORMACIÓN SOBRE EL EQUIPO AFECTADO
  - Dirección IP
  - Nombre del equipo
  - Marca y modelo
  - Capacidad de la RAM
  - Capacidad del disco duro
  - Modelo del procesador
  - Sistema operativo (nombre y versión)
  - Función del equipo
  - Tipo de información procesada por el equipo

- ✓ Toda la información del incidente, la evidencia digital, copias o imágenes de la escena del crimen.

Reconocer un incidente mediante indicadores y determinar su tipo. Esto no esta incluido dentro del análisis forense, pero es significativo en los siguientes pasos.

Esta fase esta dividida en dos procesos iníciales que son:

1.2. Asegurar la escena

Para asegurar que tanto los procesos como las herramientas a utilizar sean las más idóneas se debe contar con un personal competente a quien se le pueda asignar la conducción del proceso forense, para ello el equipo de seguridad debe estar capacitado y entender a fondo la metodología.

1.3. Identificar las evidencias

El siguiente paso y muy importante es la identificación de la evidencia presentada que es nuestra escena del crimen, la misma que estará sujeta a todos los procesos necesarios para la presentación de resultados finales.
La evidencia se clasificara según:

1.3.1. Prioridades del administrador

Las evidencias se pueden clasificar según la prioridad del administrador, las mismas están basadas en la criticidad de los daños producidos por el incidente, una forma de clasificar los daños producidos es saber que tan críticos son y se lo encuentra aplicando la siguiente formula:

$$\text{CRITICIDAD DE LOS DAÑOS} = \text{Extensión de daños producidos} + \text{Criticidad de los recursos afectados}$$

- ✓ La extensión de lo daños producidos es:
  - Graves.- Que el incidente produjo daños muy severos sobre los servicios o información.
  - Moderados.- Que el incidente causo molestias y pérdida de información.
  - Leves.- Que el incidente producido no tiene mayor importancia, no se produjo ningún tipo de perdida pero si un corte o molestia en los servicios.

- ✓ La criticidad de los recursos afectadoses:
  - Alta.- Los recursos afectados son muy importantes dentro de la universidad y como tal comprometen el normal funcionamiento y prestación de servicios.
  - Media.- Los recursos afectados causan molestias a un área de la universidad.
  - Baja.- Los recursos afectados causan ciertas molestias pero se puede seguir con el normal funcionamiento de los equipos.

Un claro ejemplo de como obtener la criticidad de los daños producidos es utilizando las siguientes tablas:

Efectos del incidente y Recursos afectados						
Incidente	**Daños producidos**			**Criticidad de los recursos afectados**		
	Graves	**Moderados**	**Leves**	**Alta**	**Media**	**Baja**
Acceso no autorizado						
✓ Servidor Web	***X***			***X***		

✓ Servidor de archivos		***X***			***X***	
✓ Servidor de aplicaciones	***X***			***X***		
Infección de virus						
✓ Servidor			***X***		***X***	
✓ Estación de trabajo	***X***					***X***
✓ Etc.						

Estado de los recursos				
		Criticidad de los recursos afectados		
		Alta	**Media**	**Baja**
Daños producidos	**Graves**	Muy grave	Grave	Moderado
	Moderados	Grave	Moderado	Leve
	Leves	Moderado	Leve	Leve

Prioridad del administrador	
Estado	**Prioridad**
MUY GRAVE	10
GRAVE	7
MODERADO	4
LEVE	1

1.3.2. Tipo de dispositivo

A las evidencias también se las puede clasificar según el tipo de dispositivo donde se las encuentre como:

- Sistemas informáticos
- Redes
- Redes Inalámbricas
- Dispositivos móviles
- Sistemas embebidos[16]
- Otros dispositivos

1.3.3. Modo de almacenamiento

A las evidencias también se las clasifica según el medio de almacenamiento. Como pueden ser:

- ✓ Volátiles[17] .- Aquellas que se perderán al apagar el equipo como la hora del sistema y desfase de horario, contenido de la memoria, procesos en ejecución, programas en ejecución, usuarios conectados, configuración de red, conexiones activas, puertos abiertos, etc.
- ✓ No volátiles.- medios físicos de almacenamiento como memorias flash, CD, discos duros.

Entonces el primer proceso del análisis forense comprende la identificación, búsqueda y recopilación de evidencias. Se debe identificar qué cosas pueden ser evidencias, dónde y cómo está almacenada, qué sistema operativo se está utilizando. A partir de este paso, el equipo de seguridad puede identificar los procesos para la recuperación de evidencias adecuadas, así como las herramientas a utilizar.

2. Fase de Preservación

Aunque el primer motivo de la recopilación de evidencias sea la resolución del incidente, puede ser que posteriormente se necesite iniciar un proceso legal contra los atacantes y en tal caso se deberá documentar de forma clara cómo ha sido preservada la evidencia tras la recopilación. En esta fase, es imprescindible definir los métodos adecuados para el almacenamiento y etiquetado de las evidencias.

Una vez que se cuenta con todas las evidencias del incidente es necesario conservarlas intactas ya que son las "huellas del crimen", se deben asegurar estas evidencias a toda costa. Para ello se sigue el siguiente proceso:

2.1. Copias de la evidencia

Como primer paso se debe realizar dos copias de las evidencias obtenidas, generar también una suma de comprobación de la integridad de cada copia mediante el empleo de funciones hash tales como MD5 o SHA1. Incluir estas firmas en la etiqueta de cada copia de la evidencia sobre el propio medio de almacenamiento como CD o DVD etiquetado la fecha y hora de creación de la copia, nombre cada copia, por ejemplo "COPIA A", "COPIA B" para distinguirlas claramente del original.

Si además se extrae los discos duros del sistema para utilizarlos como evidencia, se debe seguir el mismo procedimiento, colocando sobre ellos la etiqueta "EVIDENCIA ORIGINAL", incluir además las correspondientes sumas hash, fecha y hora de la extracción del equipo, datos de la persona que realizó la operación, fecha, hora y lugar donde se almacenó, por ejemplo en una caja fuerte.

Tener en cuenta que existen factores externos como cambios bruscos de temperatura o campos electromagnéticos que pueden alterar la evidencia. Toda precaución es poca, incluso si decide enviar esos discos a que sean analizados por empresas especializadas.

2.2. Cadena de custodia

Otro aspecto muy importante es la cadena de custodia, donde se establecen las responsabilidades y controles de cada una de las personas que manipulen la evidencia. Se debe preparar un documento en el que se registren los datos personales de todos los implicados en el proceso de manipulación de las copias, desde que se tomaron hasta su almacenamiento. El documento debe contener la siguiente información:

- ✓ Dónde, cuándo y quién examinó la evidencia, incluyendo su nombre, su cargo, un número identificativo, fechas y horas, etc.
- ✓ Quién estuvo custodiando la evidencia, durante cuanto tiempo y dónde se almacenó.
- ✓ Cuando se cambie la custodia de la evidencia también se deberá documentar cuándo y como se produjo la transferencia y quién la transportó.

Todas estas medidas harán que el acceso a la evidencia sea muy restrictivo quedando claramente documentado, posibilitando detectar y pedir responsabilidades ante manipulaciones incorrectas, intentos de acceso no autorizados o que algún otro dispositivo electromagnético se use dentro de un determinado radio.

3. Fase de Análisis

Antes de iniciar esta fase se deben prepararlas herramientas, técnicas, autorizaciones de monitoreo y soporte administrativo para iniciar el análisis forense sobre las evidencias obtenidas o presentadas por el administrador de los servidores.

Una vez que se dispone de las evidencias digitales recopiladas y almacenadas de forma adecuada, iniciamos la fase más laboriosa, el Análisis Forense propiamente dicho, cuyo objetivo es reconstruir con todos los datos disponibles la línea temporal del ataque, determinando la cadena de acontecimientos que tuvieron lugar desde el inicio del ataque, hasta el momento de su descubrimiento.

Este análisis se dará por concluido cuando se descubra cómo se produjo el ataque, quién o quienes lo llevaron a cabo, bajo qué circunstancias se produjo, cuál era el objetivo del ataque, qué daños causaron, etc.

En el proceso de análisis se emplean las herramientas propias del sistema operativo (anfitrión) y las que se prepararon en la fase de extracción y preparación.

3.1. Preparación para el análisis

Antes de comenzar el análisis de las evidencias se deberá:

1) Acondicionar un entorno de trabajo adecuado al estudio que se desea realizar
2) Trabajar con las imágenes que se recopiló como evidencias, o mejor aún con una copia de éstas, tener en cuenta que es necesario montar las imágenes tal cual estaban en el sistema comprometido.
3) Si dispone de recursos suficientes preparar dos estaciones de trabajo, una de ellas contendrá al menos dos discos duros.
4) Instar un sistema operativo que actuará de anfitrión y que servirá para realizar el estudio de las evidencias. En este mismo ordenador y sobre un segundo disco duro, instalar las imágenes manteniendo la estructura de particiones y del sistema de archivos tal y como estaban en el equipo atacado.
5) En otro equipo instar un sistema operativo configurado exactamente igual que el equipo atacado, además mantener nuevamente la misma estructura de particiones y ficheros en sus discos duros. La idea es utilizar este segundo ordenador como "conejillo de Indias" y realizar sobre él pruebas y verificaciones conforme se vayan surgiendo hipótesis sobre el ataque.

Si no se dispone de estos recursos, se puede utilizar software como VMware, que permitirá crear una plataforma de trabajo con varias máquinas virtuales[18]. También se puede utilizar una versión LIVE de sistemas operativos como Linux, que permitirá interactuar con las imágenes montadas pero sin modificarlas.

Si se está muy seguro de las posibilidades y de lo que va a hacer, se puede conectar los discos duros originales del sistema atacado a una estación de trabajo independiente para intentar hacer un análisis en caliente del sistema, se deberá tomar la precaución de montar los dispositivos en modo sólo lectura, esto se puede hacer con sistemas anfitriones UNIX/Linux, pero no con entornos Windows.

3.2. Reconstrucción de la secuencia temporal del ataque

Si ya se tienen montadas las imágenes del sistema atacado en una estación de trabajo independiente y con un sistema operativo anfitrión de confianza, se procede con la ejecución de los siguientes pasos:

1) Crear una línea temporal o timeline de sucesos, para ello se debe recopilar la siguiente información sobre los ficheros:

- ✓ Marcas de tiempo MACD (fecha y hora de modificación, acceso, creación y borrado).
- ✓ Ruta completa.
- ✓ Tamaño en bytes y tipo de fichero.
- ✓ Usuarios y grupos a quien pertenece.
- ✓ Permisos de acceso.
- ✓ Si fue borrado o no.

Sin duda esta será la información que más tiempo llevará recopilar, pero será el punto de partida para el análisis, podría plantearse aquí el dedicar un poco de tiempo a preparar un script que automatizase el proceso de creación del timeline, empleando los comandos que proporciona el sistema operativo y las herramientas utilizadas.

2) Ordenar los archivos por sus fechas MAC, esta primera comprobación, aunque simple, es muy interesante pues la mayoría de los archivos tendrán la fecha de instalación del sistema operativo, por lo que un sistema que se instaló hace meses y que fue comprometido recientemente presentará en los ficheros nuevos, fechas MAC muy distintas a las de los ficheros más antiguos.

La idea es buscar ficheros y directorios que han sido creados, modificados o borrados recientemente, o instalaciones de programas posteriores a la del sistema operativo y que además se encuentren en rutas poco comunes. Pensar que la mayoría de los atacantes y sus herramientas crearán directorios y descargarán sus "aplicaciones" en lugares donde no se suele mirar, como por ejemplo en los directorios temporales.

A modo de guía centrarse primero en buscar los archivos de sistema modificados tras la instalación del sistema operativo, averiguar después la ubicación de los archivos ocultos, de qué tipo son, identificar también los archivos borrados o

fragmentos de éstos, pues pueden ser restos de logs y registros borrados por los atacantes.

Aquí cabe destacar la importancia de realizar imágenes de los discos pues se puede acceder al espacio residual que hay detrás de cada archivo, (recordar que los ficheros suelen almacenarse por bloques cuyo tamaño de clúster depende del tipo de sistema de archivos que se emplee), y leer en zonas que el sistema operativo no ve.

Pensar que está buscando "una aguja en un pajar", por lo que se deberá ser metódico, ir de lo general a lo particular, por ejemplo partir de los archivos borrados, intentar recuperar su contenido, anotar su fecha de borrado y compararla con la actividad del resto de los archivos, puede que en esos momentos se estuviesen dando los primeros pasos del ataque.

3) Comenzar a examinar con más detalle los ficheros logs y registros que se examinaron durante la búsqueda de indicios del ataque, intentar buscar una correlación temporal entre eventos. Pensar que los archivos log y de registro son generados de forma automática por el propio sistema operativo o por aplicaciones específicas, conteniendo datos sobre accesos al equipo, errores de inicialización, creación o modificación de usuarios, estado del sistema, etc. Por lo que tendrá que buscar entradas extrañas y compararlas con la actividad de los ficheros. Editar también el archivo de contraseñas y buscar la creación de usuarios y cuentas extrañas sobre la hora que considere se inició el ataque del sistema.

4) Examinar los fragmentos del archivo /var/log/messages, que es donde se detectan y registran los accesos FTP, esto nos permitirá descubrir si sobre esa fecha y hora se crearon varios archivos bajo el directorio /var/ftp de la máquina comprometida[19], además se debe tener presente que este directorio puede ser borrado por el atacante y deberá ser recuperado.

3.3. Determinación de cómo se realizó el ataque

Una vez obtenida la cadena de acontecimientos que se han producido, se deberá determinar cuál fue la vía de entrada al sistema, averiguando qué vulnerabilidad o fallo de administración causó el agujero de seguridad y que herramientas utilizó el atacante para aprovecharse de tal brecha. Estos datos, al igual que en el caso anterior, se deberán obtener de forma metódica, empleando una combinación de consultas a archivos de logs, registros, claves, cuentas de usuarios, etc. El siguiente proceso permitirá conocer que acciones realizo el atacante:

1) Revisar los servicios y procesos abiertos que se recopilaron como evidencia volátil, así como los puertos TCP/UDP y conexiones que estaban abiertas cuando el sistema estaba aún funcionando. Examinar con más detalle aquellas circunstancias que resultan sospechosas cuando se buscó indicios sobre el ataque, y realizar una búsqueda de vulnerabilidades a través de Internet, emplear Google o utilizar páginas específicas donde se encuentran perfectamente documentadas ciertas vulnerabilidades, tal como se mostro en la corrección de vulnerabilidades.

2) Si ya se tiene claro cuál fue la vulnerabilidad que dejó el sistema desprotegido, es necesario ir un paso más allá y buscar en Internet algún exploit anterior a la fecha del incidente, que utilice esa vulnerabilidad. Generalmente se encontrará en forma de rootkit[20] y un buen lugar donde comenzar la búsqueda es, nuevamente, Google aunque también será de utilidad utilizar la información presentado en la corrección de vulnerabilidades sobre reporte de vulnerabilidades así como la siguiente dirección: http://www.packetstormsecurity.org

3) Reforzar cada una de las hipótesis empleando una formulación causa-efecto, también es el momento de arrancar y comenzar a utilizar la máquina preparada como "conejillo de Indias". Probar sobre la máquina los exploits que se encontró, recordar que en el análisis forense un antecedente es que los hechos han de ser reproducibles y sus resultados verificables, por lo tanto comprobar si la ejecución de este exploit sobre una máquina igual que la afectada, genere los mismos eventos que ha encontrado entre sus evidencias.

Una forma de ganar experiencia y estar listos ante cualquier eventualidad es recurrir a las bases de datos sobre ataques de los honeypots[21], herramientas de seguridad informática, cuya intención es atraer a crackers o spammers, simulando ser sistemas vulnerables o débiles a los ataques, esto permite recoger información sobre los atacantes y las técnicas empleadas.

3.4. Identificación del atacante

Si ya se logro averiguar cómo entraron en el sistema, es hora de saber quién o quiénes lo hicieron. Para este propósito será de utilidad consultar nuevamente algunas evidencias volátiles que se recopiló en las primeras fases, revisar las conexiones que estaban abiertas, en qué puertos y qué direcciones IP las solicitaron, además buscar entre las entradas a los logs de conexiones. También se puede indagar entre los archivos borrados que se recuperó por si el atacante eliminó alguna huella que quedaba en ellos.

Si se tiene pensado llevar a cabo acciones legales o investigaciones internas a la Universidad, se debe realizar este proceso caso contrario se debe saltar y empezar con la recuperación completa del sistema atacado y mejorar su seguridad.
Pero si se decide perseguir a los atacantes, se deberá:

1) Realizar algunas investigaciones como parte del proceso de identificación. Primero intentar averiguar la dirección IP del atacante, para ello revisar con detenimiento los registros de conexiones de red y los procesos y servicios que se encontraban a la escucha. También se podría encontrar esta información en fragmentos de las evidencias volátiles, la memoria virtual o archivos temporales y borrados, como restos de email, conexiones fallidas, etc.

2) Al tener una IP sospechosa, comprobarla en el registro RIPE NCC (www.ripe.net) a quién pertenece. Pero ojo, no sacar conclusiones prematuras, muchos atacantes falsifican la dirección IP con técnicas de spoofing. Otra técnica de ataque habitual consiste en utilizar "ordenadores zombis", éstos son comprometidos en primera instancia por el atacante y posteriormente son utilizados para realizar el ataque final sin que sus propietarios sepan que están siendo cómplices de tal hecho. Por ello, para identificar al atacante se tendrá que verificar y validar la dirección IP obtenida.

3) Utilizar técnicas hacker pero solo de forma ética, para identificar al atacante, por si el atacante dejó en el equipo afectado una puerta trasera o un troyano, está claro que en el equipo del atacante deberán estar a la escucha esos programas y en los puertos correspondientes, bien esperando noticias o buscando nuevas víctimas. Aquí entra en juego nuevamente el equipo "conejillo de indias".

Si se procede de esta forma, se puede usar una de las herramientas como nmap[22], para determinar qué equipos se encuentran disponibles en una red, qué servicios (nombre y versión de la aplicación) ofrecen, qué sistemas operativos (y sus versiones) ejecutan, qué tipo de filtros de paquetes o cortafuegos se están utilizando y así muchas mas características que poseen los equipos.

3.5. Perfil del atacante

Otro aspecto muy importante es el perfil de los atacantes y sin entrar en muchos detalles se podrá encontrar los siguientes tipos:

- ✓ ***Hackers:*** Son los más populares y se trata de personas con conocimientos en técnicas de programación, redes, Internet y sistemas operativos. Sus ataques

suelen tener motivaciones de tipo ideológico (pacifistas, ecologistas, anti globalización, anti Microsoft, etc.) o simplemente lo consideran como un desafío intelectual.

- ✓ ***SciptKiddies:*** Son una nueva especie de delincuentes informáticos. Se trata de jóvenes que con unos conocimientos aceptables en Internet y programación emplean herramientas ya fabricadas por otros para realizar ataques y ver que pasa. Su nombre viene de su corta edad y del uso de los scripts, guías de ataques que encuentran por Internet.
- ✓ ***Profesionales:*** Son personas con muchísimos conocimientos en lenguajes de programación, en redes y su equipamiento (routers, firewall, etc.), Internet y sistemas operativos tipo UNIX. Suelen realizar los ataques taques bajo encargo, por lo que su forma de trabajar implica una exhaustiva preparación del mismo, realizando un estudio meticuloso de todo el proceso que llevará a cabo, recopilando toda la información posible sobre sus objetivos, se posicionará estratégicamente cerca de ellos, realizará un tanteo con ataques en los que no modificará nada ni dejará huellas cuando lo tenga todo bien atado entonces atacará, este tipo de atacantes se encuentra muy poco y además se dedica a dar grandes golpes.

3.6. Evaluación del impacto causado al sistema

Para poder evaluar el impacto causado al sistema, el análisis forense ofrece la posibilidad de investigar qué es lo que han hecho los atacantes una vez que accedieron al sistema. Esto permitirá evaluar el compromiso de los equipos y realizar una estimación del impacto causado. Generalmente se pueden dar dos tipos de ataques:

- ✓ ***Ataques pasivos.-*** En los que no se altera la información ni la operación normal de los sistemas, limitándose el atacante a fisgonear por ellos.
- ✓ ***Ataques activos***.- En los que se altera y en ocasiones seriamente tanto la información como la capacidad de operación del sistema.

Se deberá tener en cuanta, además otros aspectos del ataque como los efectos negativos de tipo técnico que ha causado el incidente, tanto inmediatos como potenciales además de lo crítico que eran los sistemas atacados. Por ejemplo ataques al cortafuegos, el router de conexión a Internet o Intranet, el servidor Web, los servidores de bases de datos, tendrán diferente repercusión según el tipo de servicio que presta la Universidad y las relaciones de dependencia entre los usuarios.

4. Fase de Documentación y Presentación de las pruebas

Es muy importante comenzar a tomar notas sobre todas las actividades que se lleven a cabo. Cada paso dado debe ser documentado y fechado desde que se descubre el incidente hasta que finaliza el proceso de análisis forense, esto permitirá ser más eficiente y efectivo al tiempo que se reducirá las posibilidades de error a la hora de gestionar el incidente.

4.1. Utilización de formularios de registro del incidente

Es importante que durante el proceso de análisis se mantenga informados a los administradores de los equipos y que tras la resolución del incidente se presenten los informes Técnico y Ejecutivo.
El empleo de formularios puede ayudarle bastante en este propósito. Éstos deberán ser rellenados por los departamentos afectados o por el administrador de los equipos. Alguno de los formularios que debería preparar serán:

- ✓ Documento de custodia de la evidencia
- ✓ Formulario de identificación del equipos y componentes
- ✓ Formulario de incidencias tipificadas
- ✓ Formulario de publicación del incidente
- ✓ Formulario de recogida de evidencias
- ✓ Formulario de discos duros.

4.1.1. Informe Técnico

Este informe consiste en una exposición detallada del análisis efectuado. Deberá describir en profundidad la metodología, técnicas y hallazgos del equipo forense. A modo de orientación, deberá contener, al menos, los siguientes puntos:

- ✓ Introducción
- ✓ Antecedentes del incidente
- ✓ Recolección de los datos
- ✓ Descripción de la evidencia
- ✓ Entorno del análisis
  - ➢ Descripción de las herramientas
- ✓ Análisis de la evidencia
  - ➢ Información del sistema analizado
    - ❖ Características del SO
    - ❖ Aplicaciones

- ❖ Servicios
- ❖ Vulnerabilidades
- ❖ Metodología

- ✓ Descripción de los hallazgos
  - ➢ Huellas de la intrusión
  - ➢ Herramientas usadas por el atacante
  - ➢ Alcance de la intrusión
  - ➢ El origen del ataque
- ✓ Cronología de la intrusión
- ✓ Conclusiones
- ✓ Recomendaciones específicas
- ✓ Referencias
- ✓ Anexos

4.1.2. Informe Ejecutivo

Este informe consiste en un resumen del análisis efectuado pero empleando una explicación no técnica, con lenguaje común, en el que se expondrá los hechos más destacables de lo ocurrido en el sistema analizado. Constará de pocas páginas, entre tres y cinco, y será de especial interés para exponer lo sucedido al personal no especializado en sistemas informáticos, como pueda ser el departamento de Recursos Humanos, Administración e incluso algunos directivos. En este informe constara lo siguiente:

- ✓ ***Introducción***.- Descripción del objetivo del análisis del sistema previamente atacado y comprometido, también se incluye la información de la evidencia proporcionada.
- ✓ ***Análisis.-*** Descripción del entorno de trabajo y de las herramientas de análisis forense seleccionadas así como la cantidad de tiempo empleado en el mismo.
- ✓ ***Sumario del incidente.-*** Resumen del incidente tras el análisis de la evidencia aportada.
- ✓ ***Principales Conclusiones del análisis.-*** Detalle de las conclusiones a las que se llego una vez terminado el proceso de análisis.
- ✓ ***Solución al incidente.-*** Descripción de la solución para recuperación del incidente.
- ✓ ***Recomendaciones finales.-*** pasos que se deben realizar para garantizar la seguridad de los equipos y que el incidente no vuelva a suceder.

METODOLOGÍA PARA LA ATENCIÓN A INCIDENTES DE SEGURIDAD

Un incidente de seguridad[23] es cualquier evento, ataque o actividad maliciosa que busca comprometer la confidencialidad, integridad, disponibilidad, legalidad o confiabilidad de la información.

Siendo así podemos decir que, todas las áreas de la universidad han sufrido algún incidente de seguridad, que muchas de las veces no fue reportado y los conocidos no se los trato a tiempo, por lo que muchos servicios y aplicaciones sufrieron cambios que ocasionaron el mal funcionamiento ó suspensión del servicio.

Entre los incidentes[24] más conocidos tenemos:

- ✓ Virus/gusanos en Windows
- ✓ Intrusiones en el sistemas
- ✓ Envío de correo spam
- ✓ Sospechas de personas que accedieron a archivos personales sin autorización
- ✓ Abuso de recursos que afectan otras redes

Con el desarrollo de la presente metodología se busca que el equipo de seguridad y auditoría, estén en la capacidad de dar respuesta inmediata a cualquier incidente de seguridad, limitando el daño y bajando los costos de recuperación, ayudándose de recursos especializados en procesos preventivos y correctivos.

La metodología de atención a incidentes de seguridad busca, la asignación oportuna de recursos necesarios con el objeto de prevenir, detectar y mitigar cualquier tipo de incidente que afecte la seguridad de la información.

La siguiente metodología esta basada en tres fases principales como:

1. Prevención
2. Identificación
3. Corrección

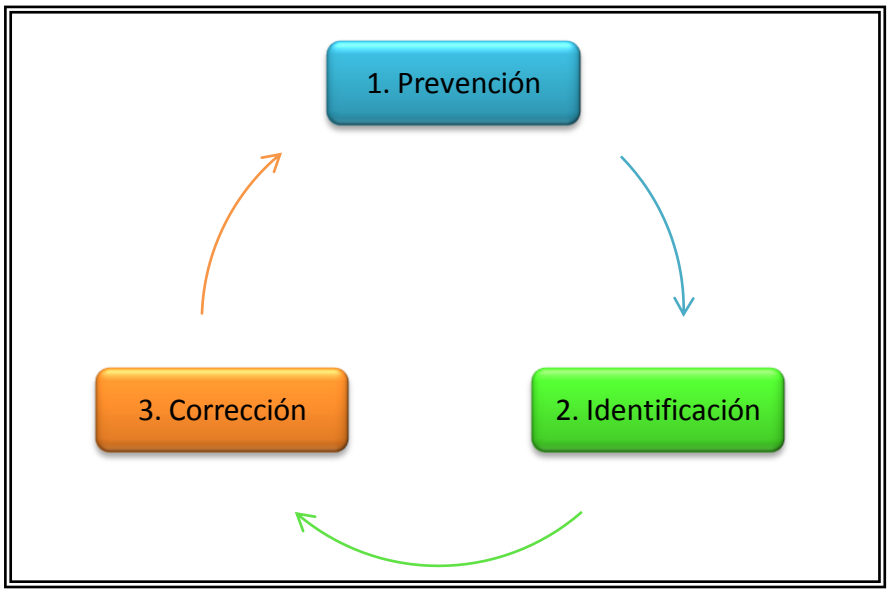


Figura 19: Proceso de atención a incidentes de seguridad.

Figura 20: Fase de Prevención de incidentes de seguridad.

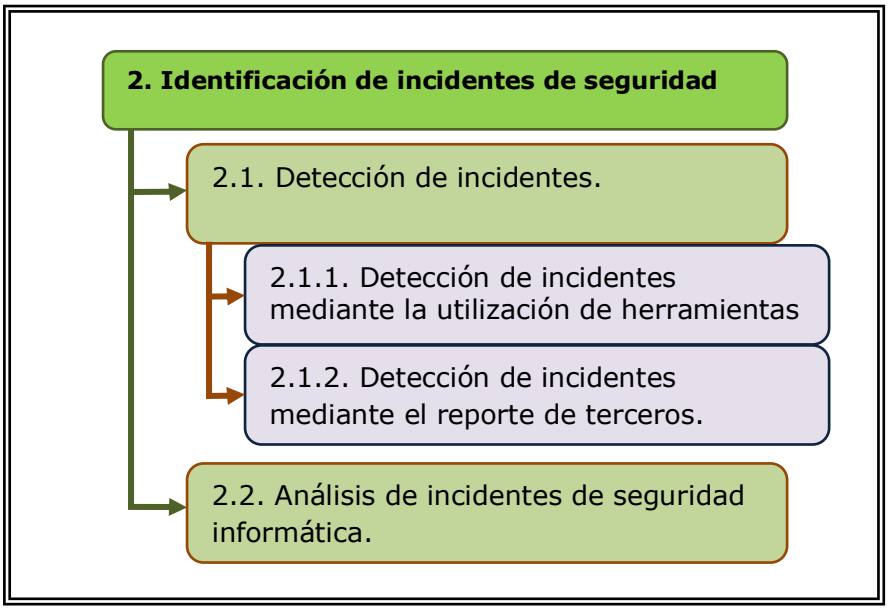


Figura 21: Fase de Identificación de incidentes de seguridad.

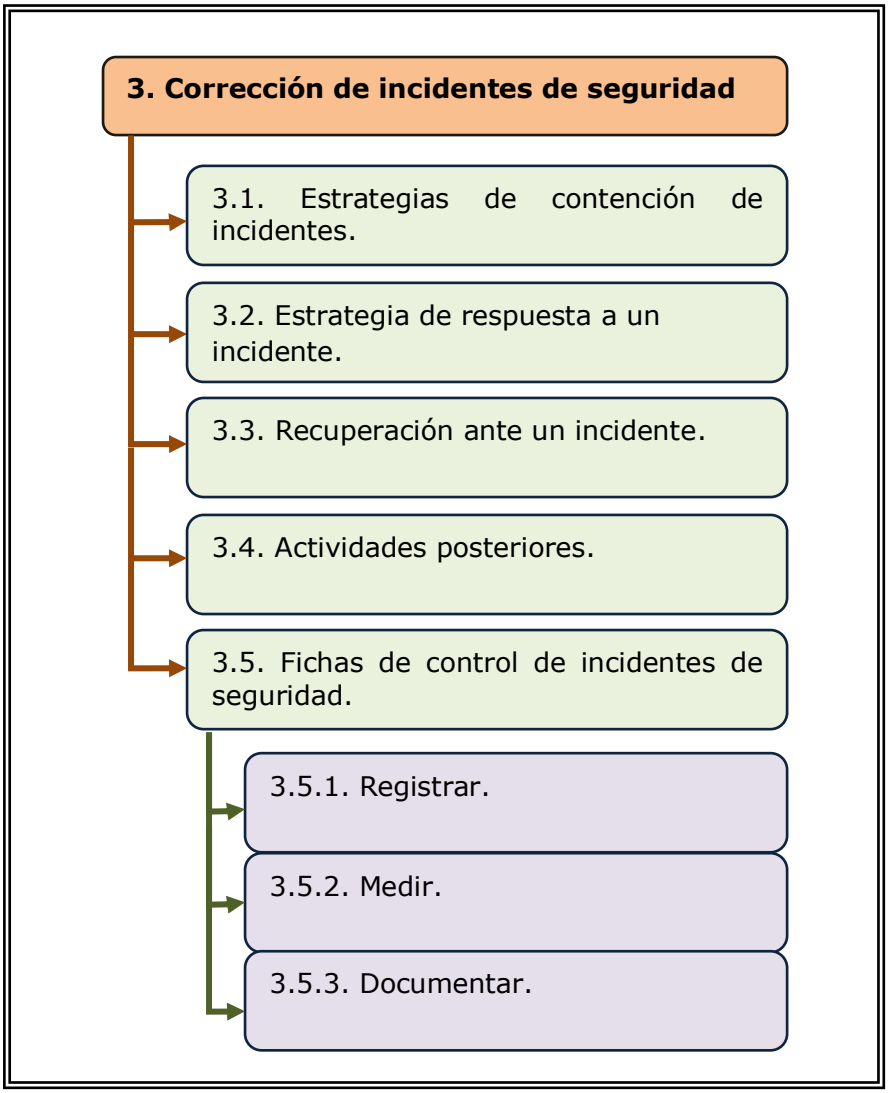


Figura 22: Fase de Corrección de incidentes de seguridad.

1. Prevención de incidentes de seguridad.

Esta fase se divide en dos procesos muy importantes para la prevención y preparación de incidentes de seguridad, que busca lograr:

- ✓ Atender cualquier eventualidad de una forma sistemática
- ✓ Maximizar la recuperación rápida y eficiente de incidentes de seguridad
- ✓ Minimizar la pérdida de información e interrupción de servicios
- ✓ Mejorar continuamente el marco de seguridad y el proceso de tratamiento de incidentes
- ✓ Manejar correctamente los aspectos legales que pudieran surgir en el tratamiento de incidentes.

1.1. Implementación de medidas de seguridad.

Para mejorar el proceso de seguridad de los servidores y enfrentar cualquier eventualidad de forma oportuna es también necesario prevenirlas, mediante la implementación de medidas de seguridad[25] tales como:

- ✓ Definir políticas, normas y procedimientos para la gestión de incidentes
- ✓ Creación del Equipo-CERT
- ✓ Capacitar al personal
- ✓ Documentar un mapa de la topología y arquitectura de la red
- ✓ Documentar la configuración del equipamiento
- ✓ Crear esquemas de redes y sistemas
- ✓ Comprender el funcionamiento normal
- ✓ Activar los logs en las diferentes plataformas y aplicaciones
- ✓ Mantener los relojes de todos los equipos sincronizados
- ✓ Crear sumas de comprobación
- ✓ Definir e implementar esquemas de resguardo de datos
- ✓ Contraseñas
- ✓ Planes de contingencia
- ✓ Políticas de seguridad
- ✓ Utilización de Firewalls
- ✓ Procesos de backup
- ✓ Cifrado de datos
- ✓ Parches y Service Packs actualizados para el servidor
- ✓ Configuración segura
- ✓ Evitar instalaciones de software por defecto
- ✓ Eliminar demos y aplicativos que no se utilicen
- ✓ Controlar y realizar una programación responsable de las aplicaciones web

- ✓ Realizar checklists de seguridad

La aplicación de estas medidas correctivas, nos ayudará a reducir la aparición de incidentes de seguridad que afecten la red, las aplicaciones, los servidores y los usuarios.

1.2. Preparación ante un incidente de seguridad.

También tenemos la preparación ante un incidente de seguridad, que nos permitirá saber que es lo que se debe hacer cuando una eventualidad este sucediendo o haya pasado.

1.2.1. Categorización de incidentes.

En este proceso se buscan criterios de categorización[26] que nos permita clasificar los incidentes. Entre los criterios de categorización tenemos:

- ✓ TIPO DE INCIDENTE
  - ✓ Denegación de servicio
  - ✓ Código malicioso
  - ✓ Acceso no autorizado
  - ✓ Uso inapropiado del equipo
  - ✓ Incidente múltiple

- ✓ EXTENSIÓN DE DAÑOS PRODUCIDOS
  - ✓ Alta
  - ✓ Media
  - ✓ Baja

1.2.2. Clasificación de incidentes.

Una forma de clasificar los incidentes es saber que tan críticos son y lo podemos encontrar aplicando la siguiente formula:

$$\text{CRITICIDAD DE LOS DAÑOS} = \text{Extensión de daños producidos} + \text{Criticidad de los recursos afectados}$$

- ✓ La extensión de lo daños producidos es:

  - ➢ Graves.- Que el incidente produjo daños muy severos sobre los servicios o información.

- Moderados.- Que el incidente causo molestias y pérdida de información.
- Leves.- Que el incidente producido no tiene mayor importancia, no se produjo ningún tipo de perdida pero si un corte o molestia en los servicios.

✓ La criticidad de los recursos afectadoses:

- Alta.- Los recursos afectados son muy importantes dentro de la universidad y como tal comprometen el normal funcionamiento y prestación de servicios.
- Media.- Los recursos afectados causan molestias a un área de la universidad.
- Baja.- Los recursos afectados causan ciertas molestias pero se puede seguir con el normal funcionamiento de los equipos.

Un claro ejemplo de como obtener la criticidad de los daños producidos es utilizando las siguientes tablas:

Efectos del incidente y Recursos afectados						
Incidente	**Daños producidos**			**Criticidad de los recursos afectados**		
	Graves	**Moderados**	**Leves**	**Alta**	**Media**	**Baja**
Acceso no autorizado						
✓ Servidor Web	***X***			***X***		
✓ Servidor de archivos		***X***			***X***	
✓ Servidor de aplicaciones	***X***			***X***		
Infección de virus						
✓ Servidor			***X***		***X***	
✓ Estación de trabajo	***X***					***X***
✓ Etc.						

Estado de los recursos				
		Criticidad de los recursos afectados		
		Alta	**Media**	**Baja**
Daños producidos	**Graves**	Muy grave	Grave	Moderado
	Moderados	Grave	Moderado	Leve
	Leves	Moderado	Leve	Leve

Tiempo máximo que puede tardarse en atender cada incidente	
Estado	Tiempo
MUY GRAVE	10 minutos
GRAVE	30 minutos
MODERADO	2:00 horas
LEVE	4:00 horas

1.2.3. Utilización de herramientas.

En este proceso, se busca un conjunto de herramientas que permitan automatizar todo el proceso de atención a incidentes de seguridad, esto significa que las herramientas seleccionadas serán las más idóneas y que cumplan con los procesos de:

- ✓ Detección de incidentes
- ✓ Monitoreo
- ✓ Análisis de incidentes, análisis forense, identificación de vulnerabilidades
- ✓ Documentación de incidentes

1.2.4. Implementación de políticas.

Definir las políticas de seguridad informática a emprender y elegir las personas a contactar en caso de detectar un posible incidente

- ✓ Análisis periódicos de riesgos
- ✓ Mejores prácticas de seguridad
- ✓ Auditorías periódicas
- ✓ Administración de actualizaciones
- ✓ Fortalecimiento de la seguridad de los equipos
- ✓ Seguridad en la red
- ✓ Prevención de código malicioso
- ✓ Concientización y capacitación de usuarios
- ✓ Contactos

2. Identificación de incidentes de seguridad.

En esta fase se busca toda posible señal de ocurrencia de un incidente, señal de que un incidente de seguridad ocurrió o está ocurriendo en un determinado momento.

2.1. Detección de incidentes

La detección de incidentes permite tener una idea clara de lo sucedido así como el estado actual del ataque o imprevisto este proceso se la realiza de dos formas:

2.1.1. Detección de incidentes mediante la utilización de herramientas.

La detección de incidentes es un proceso que permite saber si el sistema esta en peligro o si los servidores corren el riesgo de detener sus servicios. La utilización de estas herramientas dan alertas que se puede interpretar para conocer que sucesos se están presentando y estas pueden ser:

- ✓ IDS - Sistemas de detección de intrusiones de red (NIDS) o de host (HIDS)
- ✓ Software de antivirus
- ✓ Software de control de integridad de archivos
- ✓ Sistemas de monitoreo de red (NMS)
- ✓ Análisis de registros de auditoría (logs)
- ✓ Información pública
- ✓ Usuarios de la universidad (internos o externos)
- ✓ Etc.

2.1.2. Detección de incidentes mediante el reporte de terceros.

Al presentarse un fallo ó incidente de seguridad a nivel general de la universidad, ya sea en sus aplicaciones, información o equipos a los que cada uno presta sus servicios los responsables seguir el siguiente proceso tal como se muestra en la figura 2.1.2. En el que el usuario notifica del incidente al equipo de seguridad el cual esta encardado de atender cualquier evento que ponga en riesgo los equipo.

El equipo de seguridad y auditoria será idóneo para resolver y atender cualquier inconveniente a más de ello se presenta el formato de los reportes tanto inicial como final.

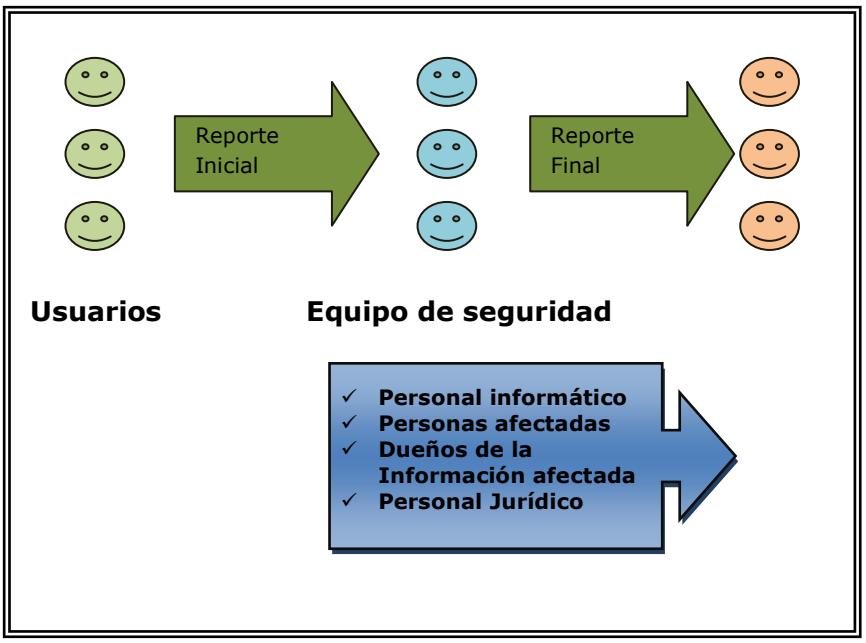


Figura 23: Proceso de Reporte de incidentes de seguridad informática.

Reporte inicial.

REPORTE DE INCIDENTES DE SEGURIDAD INFORMÁTICA

1. DESCRIPCIÓN DEL INCIDENTE N°_____

Fecha del incidente: _____

Si se puede establecer, ¿cuál fue la duración del incidente?_____

En pocas palabras, enumere los detalles del incidente

¿Cómo se descubrió el incidente?

_____
_____
_____

Si es posible realizar un diagnóstico, brevemente describir el método utilizado para obtener acceso al equipo o sistemas afectados y qué vulnerabilidades fueron aprovechadas (clave fácil, deficiencia en los controles, etc.).

_____
_____
_____

Describa las medidas que fueron tomadas para atender el incidente:

- ☐ Ninguna en especial
- ☐ Reinstalación del sistema
- ☐ Aplicación de parches
- ☐ Recuperación de copias de seguridad (Backups)
- ☐ Cambio de equipo
- ☐ Otra _____

Si existía algún plan escrito para manejar el incidente, describa de forma breve los pasos que siguió o anexe el documento.

Si en su opinión existen otros aspectos que se consideren importantes en el incidente, por favor descríbalos

_____
_____
_____

2. INFORMACIÓN GENERAL

Área: _____

Nombre de la dependencia: _____

Responsable del sistema afectado
(Persona con quién el equipo de seguridad & auditoria informática puede comunicarse y que conoce los detalles del incidente)

Nombres y Apellidos: _____

Cargo: _____

E-mail:_____ Teléfono: _____

Extensión: _____ Celular: _____ Fax: _____

Si sabe de otro equipo o sistema que haya sufrido el mismo problema o uno similar, diga cuál(es)

_____
_____
_____

3. INFORMACIÓN SOBRE EL EQUIPO AFECTADO
(Información sobre hardware, software y red. Si hay más sistemas, llene otro formato)

Dirección IP: _____ Nombre del equipo: _____

Marca y modelo: _____

Capacidad de la RAM: _____ Capacidad del disco duro: _____

Modelo del procesador: _____

Sistema operativo (nombre y versión): _____

Función del equipo: _____
_____
_____

Tipo de información procesada por el equipo: _____
_____

Observaciones:
_____
_____
_____

Reporte Final.

REPORTE DE INCIDENTES DE SEGURIDAD INFORMÁTICA

Incidencia N°_____

Incidente_____ _____
_____

Nombre y apellidos de la persona que envía este informe: _____
_____

Fecha de solución del incidente: _____

Explique con detalle el motivo que causó el incidente: _____
_____
_____
_____
_____
_____
_____
_____

Explique con detalle los pasos que ha realizado para solucionar el incidente y para evitar que vuelva a suceder en el futuro: _____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

_____
_____
_____
_____
_____
_____

Por favor, añadir cuanta información extra, comentarios o sugerencias le parezca pertinente.

Enviando el presente informe, se solicita se dé por atendido el incidente y se vuelva a permitir el acceso a la red del servidor afectado.

2.2. Análisis de incidentes de seguridad informática.

En este proceso se busca analizar cada reporte de incidentes presentado tanto por los usuarios como por las herramientas con la finalidad de cerciorarse si realmente se trata de un incidente de seguridad.

La información recolectada es la que analizaremos:

- ✓ Alcance del incidente, es decir, redes, sistemas y aplicaciones afectadas
- ✓ Qué originó el incidente
- ✓ Cómo ocurrió o está ocurriendo el incidente, reporte de incidentes, herramientas utilizadas, vulnerabilidades explotadas, etc.
- ✓ El impacto que tendrá en las actividades de cada servidor afectado

3. Corrección de incidentes de seguridad.

En esta etapa se da la solución a cada incidente y se corrigen todos los fallos que permitieron que los servidores estén bajo determinados riesgos.

3.1. Estrategias de contención de incidentes

La ejecución de estrategias permitirá delimitar cada incidente, de manera que se minimice el alcance del ataque o riesgo. Las estrategias tomadas deben evitar o precautelar cada una de las siguientes situaciones:

- ✓ Daño potencial de recursos
- ✓ Necesidad de preservación de evidencia
- ✓ Tiempo y recursos necesarios para poner en práctica la estrategia
- ✓ Efectividad de la estrategia
- ✓ Duración de las medidas a tomar

3.2. Estrategia de respuesta a un incidente

Establecer las estrategias a tomar ante un incidente de seguridad, es la clave para marcar la diferencia entre el éxito y el fracaso de una correcta respuesta a cualquier situación que ponga en peligro el correcto funcionamiento de un servidor. Para ello se deben considerar los siguientes factores para la selección de una correcta y oportuna estrategia:

- ✓ Criticidad de los sistemas afectados
- ✓ Características de los posibles atacantes
- ✓ Nivel de intrusión, de ser necesario
- ✓ Si el incidente es de conocimiento público
- ✓ Pérdida económica
- ✓ Posibles implicancias legales
- ✓ Relación costo-beneficio de la estrategia
- ✓ Experiencias anteriores

3.3. Recuperación ante un incidente

La recuperación ante un incidente de seguridad consiste en restablecer los servicios y para ello se debe:

- ✓ Volver el sistema, red o entorno a su estado original, antes de ocurrir el incidente.
- ✓ Definir medidas adicionales a implementar para prevenir nuevos incidentes, de ser necesario.

3.4. Actividades posteriores

Lo que se aconseja después de ser atendido un incidente y haberse dado una correcta recuperación del mismo es:

- ✓ Organizar reuniones
- ✓ Mantener la documentación
- ✓ Crear bases de conocimiento de los incidentes, que sucedió y como se resolvió el incidente
- ✓ Integrar la gestión de incidentes al análisis de riesgos
- ✓ Implementar controles preventivos
- ✓ Elaborar Tableros de Control

3.5. Fichas de control de incidentes de seguridad

Estas fichas permiten tener un historial o una base de ayuda y conocimiento de cada incidente ocurrido, en las diferentes aéreas de la universidad así como de cada uno de sus equipos y aplicaciones. Para ello debemos registrar, medir y documentar cada incidente de seguridad.

3.5.1. Registrar:

- ✓ Cantidad de incidentes tratados
- ✓ Tiempo asignado a los incidentes
- ✓ Daños ocasionados
- ✓ Cantidad de personas responsables de atender un incidente

3.5.2. Medir:

- ✓ Vulnerabilidades explotadas
- ✓ Frecuencia de ataques
- ✓ Pérdidas
- ✓ Demora en la respuesta de un incidente

3.5.3. Documentar:

- ✓ Estado actual
- ✓ Resumen del incidente
- ✓ Método de detección
- ✓ Conclusiones del análisis
- ✓ Acciones tomadas
- ✓ Evidencias
- ✓ Próximas acciones

CONCLUCIONES

- ✓ La metodología desarrollada tienen las alternativas suficientes y necesarias para dar solución a los problemas de vulnerabilidades, amenazas y riesgos que rodean a los recursos críticos, así como para solucionar la problemática de los usuarios finales en el manejo de información.

- ✓ La importancia de enfocar el proyecto de tesis a los servidores de Universidad radicó en la falta de seguridad, el desconocimiento de la importancia que ésta tiene dentro de la UTPL, inexistencia de metodologías o procesos formales aplicados a la identificación de vulnerabilidades, análisis forense y atención a incidentes de seguridad, lo que hace que los requerimientos de seguridad como la integridad y confidencialidad no se los practique de manera adecuada.

- ✓ Las encuestas realizadas al equipo de seguridad y auditoría para obtener información de los procesos que realizan para la seguridad informática; permitieron una correcta evaluación de los niveles de seguridad que actualmente posee la UTPL y de la falta de métodos formales que garanticen los resultados obtenidos en los servidores.

- ✓ El requerimiento de seguridad de mayor prioridad para el equipo de seguridad y auditoría fue la disponibilidad de procesos formales y la capacitación en cuanto a la identificación de vulnerabilidades análisis forense y atención a incidentes de seguridad, debido a que necesitan estar capacitados y contar con los recursos necesarios para cumplir con sus actividades diarias.

- ✓ Es fundamental para el éxito de la metodología que tanto los administradores como el equipo de seguridad participen en la investigación con la finalidad de lograr el compromiso, respaldo, credibilidad, colaboración y cumplimiento de los procesos relacionados con el análisis forense.

- ✓ Para futuras actualizaciones de la metodología se debe tomar en cuenta el estado del arte y que los cambios incluyan también los recursos

computadores personales, debido a que son recursos físicos manejados por los usuarios y mucha de la información almacenada es crítica.

- ✓ Para lograr el éxito de la implementación de la metodología es necesario que tanto los administradores como el equipo de seguridad se comprometan a colaborar en todo lo requerido por la metodología de tal forma que se facilite la evaluación y aprobación de resultados e implementación de planes de difusión dentro de la UTPL, con la finalidad de garantizar la seguridad en el manejo de la información.

- ✓ La metodología podría utilizarse en proyectos en donde se desee determinar las vulnerabilidades y mitigación de riesgos a los que están expuestos ciertos recursos.

ANEXOS 1:

PLANTILLA DE REGISTRO DE VULNERABILIDADES

Objetivo

Tener una bitácora o base de conocimiento donde se pueda ir agregando la información de los escaneos de vulnerabilidades y dar una correcta atención a cada vulnerabilidad encontrada.

"Tabla de registro de Vulnerabilidades"			
Servidor			
Dirección IP		***Nombre de dominio***	
Sistema O.		***Fecha***	

Puerto	***Protocolo***	***Servicio***	***Detalles del servicio***

Id	***Vulnerabilidad***	***Correctivo***	***Estado***

ANEXOS 2:

PLANTILLA DE REGISTRO DE SERVIDORES

Objetivo

Tener una bitácora o base de conocimiento de los servidores analizados, de esta forma contar con un historial de los servidores puertos que utiliza, usuarios y aplicaciones instaladas

"Tabla de registro de Servidores"			
Servidor			
Dirección IP		***Nombre de dominio***	
Sistema O.		***Administrador***	

Fecha destinada al escaneo de vulnerabilidades	***Horario para el escaneo de Vulnerabilidades***

Usuario	***Tipo de usuario***	***Funciones***

Puerto	***Protocolo***	***Servicio***	***Detalles del servicio***

Software	***Detalle***

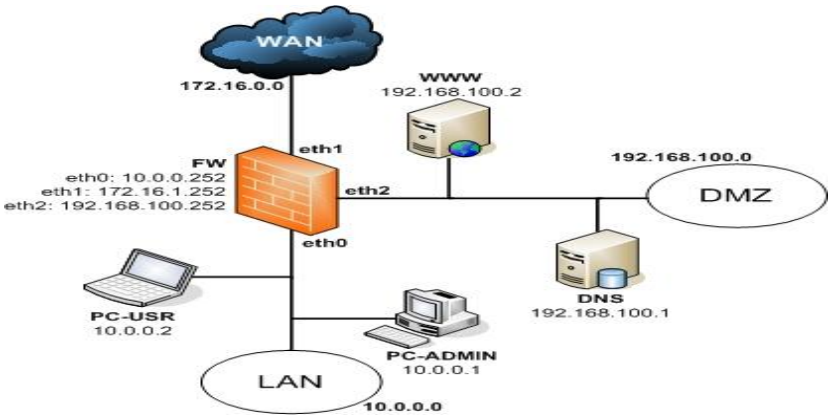
ANEXOS 3:

PLANTILLA DEL ESQUEMA DE RED

Objetivo

Tener una plantilla de red del servidor nos permitirá saber con que recursos hardware y software cuenta el equipo para su protección a mas de ello el saber si un corte en sus servicios a que equipos afectara.

"Esquema de Red"			
Servidor			
Dirección IP		***Nombre de dominio***	
Sistema O.		***Administrador***	



ANEXOS 4:

PLANTILLAS DE REGISTRO DE VULNERABILIDADES EXTERNAS E INTERNAS

Objetivo

Registrara en estas plantillas los resultados obtenidos por las diferentes herramientas que se utilicen en un escaneo para luego del análisis registrarlas en la tabla de vulnerabilidades del servidor

"Tabla de registro de Vulnerabilidades Externas"			
Servidor			
Dirección IP		***Nombre de dominio***	
Sistema O.		***Fecha***	
Herramienta			
Vulnerabilidad	***Correctivo***	***Estado***	

"Tabla de registro de Vulnerabilidades Internas"			
Servidor			
Dirección IP		***Nombre de dominio***	
Sistema O.		***Fecha***	
Herramienta			
Vulnerabilidad	***Correctivo***	***Estado***	

ANEXOS 5:

PLANTILLA DEL INFORME FINAL PARA LA PRESENTACIÓN DE LAS VULNERABILIDADES ENCONTRADAS

Objetivo

Este informe se lo emite al administrador de los servidores indicando el final del proceso de identificación de vulnerabilidades.

REPORTE DE VULNERABILIDADES

1. INFORMACIÓN GENERAL

Área: _____

Nombre de la dependencia: _____

Responsable del equipo
(Persona con quién el equipo de seguridad & auditoria informática puede comunicarse y que conoce los detalles del incidente)

Nombres y Apellidos: _____

Cargo: _____

E-mail:_____ Teléfono: _____

Extensión: _____ Celular: _____ Fax: _____

2. INFORMACIÓN SOBRE EL EQUIPO

Dirección IP: _____ Nombre del equipo: _____

Sistema operativo (nombre y versión): _____

Función del equipo: _____
_____
_____

Tipo de información procesada por el equipo: _____
_____

Observaciones:

_____
_____
_____
_____
_____
_____
_____

Estado del servidor:

_____
_____
_____
_____
_____
_____

3. INFORMACIÓN DEL EQUIPO DE SEGURIDAD

Área: _____

Nombre de la dependencia: _____

Datos del oficial de seguridad

Nombres y Apellidos: _____

Cargo: _____

E-mail:_____ Teléfono: _____

Extensión: _____ Celular: _____ Fax: _____

Por favor, añadir cuanta información extra, comentarios o sugerencias le parezca pertinente.

ANEXOS 6:

PLANTILLA DE LA SOLICITUD FORENSE

Objetivo

Solicitar la acción del equipo de seguridad informática en la atención de un incidente y para ello se brinda toda la información de la escena del crimen.

ANÁLISIS FORENSE INFORMÁTICO

1. DESCRIPCIÓN DEL DELITO INFORMÁTICO

Fecha del incidente: _____

Si se puede establecer, ¿cuál fue la duración del incidente?_____

En pocas palabras, enumere los detalles del incidente

¿Cómo se descubrió el incidente?

_____
_____

Si es posible realizar un diagnóstico, brevemente describir el método utilizado para obtener acceso al equipo o sistemas afectados y qué vulnerabilidades fueron aprovechadas (clave fácil, deficiencia en los controles, etc.).

_____
_____

Describa las medidas que fueron tomadas para atender el incidente:

- ☐ Ninguna en especial
- ☐ Reinstalación del sistema
- ☐ Aplicación de parches
- ☐ Recuperación de copias de seguridad (Backups)
- ☐ Cambio de equipo
- ☐ Otra _____

Si existía algún plan escrito para manejar el incidente, describa de forma breve los pasos que siguió o anexe el documento.

Si en su opinión existen otros aspectos que se consideren importantes en el incidente, por favor descríbalos

_____
_____

2. INFORMACIÓN GENERAL

Área: _____

Nombre de la dependencia: _____

Responsable del sistema afectado
(Persona con quién el equipo de seguridad & auditoria informática puede comunicarse y que conoce los detalles del incidente)

Nombres y Apellidos: _____

Cargo: _____

E-mail:_____ Teléfono: _____

Extensión: _____ Celular: _____ Fax: _____

Si sabe de otro equipo o sistema que haya sufrido el mismo problema o uno similar, diga cuál(es)

_____
_____

3. INFORMACIÓN SOBRE EL EQUIPO AFECTADO
(Información sobre hardware, software y red. Si hay más sistemas, llene otro formato)

Dirección IP: _____ Nombre del equipo: _____

Marca y modelo: _____

Capacidad de la RAM: _____ Capacidad del disco duro: _____

Modelo del procesador: _____

Sistema operativo (nombre y versión): _____

Función del equipo: _____
_____
_____
Tipo de información procesada por el equipo: _____
_____

Observaciones:
_____
_____
_____

BIBLIOGRAFÍA

Identificación de vulnerabilidades

- ✓ **OSSTMM 2.1.** (Open Source Security Testing Methodology Manual)
  Manual de la Metodología Abierta de Testeo de Seguridad
  [Disponible en]
  http://www.isecom.info/mirror/osstmm.en.2.2.pdf

- ✓ **OCTAVE** (Operationally Critical Threat, Asset, and Vulnerability Evaluation)
  Amenazas Críticas Operacionales, Activos, y Evaluación de Vulnerabilidad
  [Disponible en]
  www.cert.org/octave

- ✓ **OVAL** (Open Vulnerability Assessment Lenguaje)
  Lenguaje Abierto para la Identificación de Vulnerabilidades
  [Disponible en]
  http://oval.mitre.org/index.html

- ✓ **CVE** (Common Vulnerabilities and Exposures)
  Vulnerabilidades y Exposiciones Comunes
  [Disponible en]
  http://cve.mitre.org/

- ✓ ***Metodología de Análisis de vulnerabilidades.***
  [Disponible en]
  http://www.verisign.es/security-intelligence-service/methodology/index.html

- ✓ ***Seguridad Informática.***
  [Disponible en]
  http://www.auditoriasistemas.com/seguridad_informatica.htm

- ✓ ***Un debate online sobre la vulnerabilidad informática de las empresas***.
  [Disponible en]
  http://weblogs.clarin.com/conexiones/archives/000507.html

- ✓ ***OSSTMM - Open Source Security Testing Methodology Manual***.
  [Disponible en]
  http://www.isecom.org/osstmm/

- ✓ ***El Common Vulnerability Scoring System***.
  [Disponible en]
  http://www.clcert.cl/show.php?xml=xml/editoriales/doc_07-06.xml&xsl=xsl/editoriales.xsl

- ✓ ***Seguridad Informática.***
  [Disponible en]
  http://ciberhabitat.gob.mx/museo/cerquita/redes/seguridad/intro.htm

- ✓ ***Identificación de Vulnerabilidades.***
  [Disponible en]
  http://www.segu-info.com.ar

- ✓ ***Políticas de Seguridad.***
  [Disponible en]
  www.seguritos.org

- ✓ ***Metodología CTG's SAF*** (Safety architecture Framework)
  [Disponible en]
  www.seguritos.org/Reforzando%20la%20seguridad.html

- ✓ ***Vulnerabilidades de seguridad***
  [Disponible en]
  - ➢ http://www.seguridad.unam.mx/vulnerabilidadesDB/
  - ➢ http://www.vnunet.es/Seguridad/Vulnerabilidades
  - ➢ http://www.alerta-antivirus.es/seguridad/busca_vulns.php

- ✓ ***Boletines de Vulnerabilidades***
  [Disponible en]
  - ➢ http://www.cert.org.mx/boletin/
  - ➢ http://www.vnunet.es/Seguridad/Sistemas_de_protecci%C3%B3n
  - ➢ http://www.segu-info.com.ar/boletin/

- ✓ ***Organizaciones y empresas de seguridad informática***
  [Disponible en]
  - ➢ Cybex, http://www.cybex.es
  - ➢ Germinus, http://www.germinus.com
  - ➢ Guidance Software, http://www.guidancesoftware.com
  - ➢ LogiCube, http://www.logicube.com
  - ➢ RedIRIS, http://www.rediris.es

- Revista Red Seguridad , http://www.borrmart.es
- RNP-CAIS http://www.rnp.br/cais
- S21Sec, http://www.s21sec.com
- Sarenet, http://www.sarenet.es
- SANS, http://www.sans.org
- UNAM-CERT http://www.seguridad.unam.mx

Análisis forense

- ✓ ***Cyber Forensics: Una Perspectiva de Operaciones Militar***
  [Disponible en]
  http://citeseer.ist.psu.edu/giordano02cyber.html

- ✓ ***An examination of Digital Forensic Models***
  [Disponible en]
  http://people.emich.edu/pstephen/other_papers/Digital_Forensic_Models.pdf

- ✓ ***Computer Forensics-- We've had an incident, who do we get to investigate?***
  [Disponible en]
  http://eevidencelabs.com/article/WeveHadAnAccident.pdf

- ✓ ***Análsis Forense de Sistemas Linux***
  [Disponible en]
  http://memnon.ii.uam.es/descargas_web/cursos_verano/20040801/JuanMa_Canelada/Analisis_forense_de_sistemas.pdf

- ✓ ***The Linux Kernel and the Forensic Acquisition of Hard Disks with an Odd Number of Sectors***
  [Disponible en]
  http://www.utica.edu/academic/institutes/ecii/publications/articles/A0B8BE05-BD96-240E-F1BE517A38B48665.pdf

- ✓ ***Seguridad Informática***
  [Disponible en]
  http://www.auditoriasistemas.com/seguridad_informatica.htm

- ✓ ***Digital Forensics CP4DF***
  [Disponible en]

http://cp4df.sourceforge.net/

- ✓ ***Selección de links Honeynet, IDS, Computer Forensics***
  [Disponible en]
  http://voodoo.somoslopeor.com/forensics/bookmarks/

- ✓ ***Una completa lista de enlaces sobre ITSecurity en general***
  [Disponible en]
  http://www.dgonzalez.net/secinf

- ✓ ***La más completa lista de enlaces sobre Evidencia Electrónica***
  [Disponible en]
  http://www.e-evidence.info

- ✓ ***Importance of a standard methodology in computer forensics***
  [Disponible en]
  http://www.giac.org/practical/Jim_McMillan_GSEC.doc

- ✓ ***Computer Forensics Tool Testing (CFTT) Project***
  [Disponible en]
  http://www.cftt.nist.gov

- ✓ ***Open Source Software As A Mechanism To Assess Reliability For Digital Evidence***
  [Disponible en]
  http://www.vjolt.net/vol6/issue3/v6i3-a13-Kenneally.html

- ✓ ***Open Source Digital Forensics Tools: The Legal Argument***
  [Disponible en]
  - http://www.atstake.com/research/reports/acrobat/atstake_opensource_forensics.pdf
  - Trends & Issues in Crime and Criminal Justice
    http://www.aic.gov.au/publications/tandi/index.html

- ✓ ***Recovering and Examining - Computer Forensic Evidence***
  [Disponible en]
  http://www.fbi.gov/hq/lab/fsc/backissu/oct2000/computer.htm

- ✓ ***Autopsy***

[Disponible en]
http://www.sleuthkit.org/autopsy/download.php

Atención a incidentes de seguridad

- ✓ ***Seguridad Informática***
  [Disponible en]
  http://www.auditoriasistemas.com/seguridad_informatica.htm

- ✓ ***Seguridad Informática***
  [Disponible en]
  http://ciberhabitat.gob.mx/museo/cerquita/redes/seguridad/intro.htm
- ✓ ***Políticas de Seguridad***
  [Disponible en]
  http://www.seguritos.org

- ✓ ***FIRST Forum of Incident Response and Security Teams***
  [Disponible en]
  http://www.first.org

- ✓ ***CERT Computer Emergency Response Teams***
  [Disponible en]
  http://www.cert.org

- ✓ ***UNAM-CERT***
  [Disponible en]
  http://www.unam.mx

- ✓ ***ArCERT Coordinación de Emergencias en Redes Teleinformáticas de la Administración Pública Argentina***
  [Disponible en]
  http://www.arcert.gov.ar

REFERENCIAS

Identificación de vulnerabilidades

[1] Las tres fase de identificación de vulnerabilidades fueron tomadas del proyecto **OVAL,** Lenguaje Abierto para la Identificación de Vulnerabilidades
[Disponible en]

- ✓ http://www.germinus.com/sala_prensa/articulos/proyecto_oval.pdf

[2] ***Las tareas y procesos, Manual de seguridad en redes ArCERT***
[Disponible en]

- ✓ http://www.arcert.gov.ar

[3] ***Evaluación de Riesgos***
[Disponible en]

- ✓ http://www.segu-info.com.ar/politicas/

[4] ***Identificación de amenazas, amenazas existentes***
[Disponible en]

- ✓ http://www.ibiblio.org/pub/Linux/docs/LuCaS/Manuales-LuCAS/doc-unixsec/unixsec-html/node336.html

[5] ***Clasificación y tipos de ataques contra sistemas de información***
[Disponible en]

- ✓ http://www.navactiva.com/web/es/atic/doc/nociones/2004/06/27147.php

Diferentes tipos de intrusiones o ataques
[Disponible en]

- ✓ http://www.terra.es/tecnologia/articulo/html/tec10590.htm

TIPOS BÁSICOS DE ATAQUE EN REDES Y SERVIDORES
[Disponible en]

- ✓ http://www.kernelnet.com/content/view/172/2/

Seguridad Informática / Amenazas Lógicas - Tipos de Ataques
[Disponible en]

- ✓ http://www.segu-info.com.ar/ataques/ataques.htm

[6] ***Intrusiones***
[Disponible en]

- ✓ http://www.cybsec.com

[7] ***Punto de Equilibrio***

[Disponible en]

- ✓ http://www.segu-info.com.ar/politicas/costos.htm

[8] ***Identificación de vulnerabilidades externas e internas***

[Disponible en]

- ✓ http://www.germinus.com/sala_prensa/articulos/proyecto_oval.pdf

[9] ***Top 10 Vulnerability Scanners***

[Disponible en]

- ✓ http://sectools.org/vuln-scanners.html

Análisis Forense

[10] ***Delitos Informáticos***

- ✓ [Disponible en] http://www.microsoft.com/spain/empresas/legal/delitos_informaticos.mspx?gclid=CPbTu4-RkpMCFQUDkgodMXvlSw

[11] ***Análisis forense informático, Definiciones***

[Disponible en]

- ✓ http://www.acis.org.co/fileadmin/Revista_96/dos.pdf

[12] ***Evidencia Digital***

[Disponible en]

- ✓ www.tb-security.com/articles/incidentes.pdf

[13] ***Introducción a la informática forense***

[Disponible en]

- ✓ www.acis.org.co/fileadmin/Revista_96/dos.pdf
- ✓ www.compuven.net/Contenidos/Introduccion-a-la-informatica-forense-en-Windows.pdf

[14] ***Oficial de seguridad***.- Es el personal del equipo de seguridad, quien realiza el análisis forense.

[15] ***Herramientas forenses***

[Disponible en]

- ✓ http://inza.wordpress.com/2006/11/28/herramientas-de-informatica-forense-para-recuperar-datos-de-disco-duro/
- ✓ http://vtroger.blogspot.com/2006/08/herramientas-forenses-del-sistema-de.html
- ✓ http://vtroger.blogspot.com/2008/01/suite-completa-para-informtica-forense.html

Atención a Incidente de seguridad

[16] ***Sistemas Embebidos***

La denominación de Sistemas embebidos (embedded) refleja que son una parte integral (interna) del sistema, y en general son dispositivos utilizados para controlar o asistir la operación de diversos equipamientos.

[Disponible en]

- ✓ http://www2.unam.edu.ar/subprograma/metod_anex1.htm

[17] ***Identificar las evidencias***

[Disponible en]

- ✓ www.oas.org/juridico/spanish/cyb_analisis_foren.pdf
- ✓ www.securityfocus.com/archive/128/457634/30/30/threaded
- ✓ www.rediris.es/cert/doc/reuniones/fs2004/archivo/USC-Forense.pdf

[18] ***Máquinas virtuales.-*** *V*arios equipos lógicos independientes funcionando sobre un único equipo físico

[19] ***Directorio de la maquina afectada por el incidente,*** /var/ftp directorio raíz del servicio ftp en sistemas UNIX/Linux

[20] ***Rootkit***.- Es un conjunto de herramientas usadas frecuentemente por los intrusos o crackers que consiguen acceder ilícitamente a un sistema informático. Estas herramientas sirven para esconder los procesos y archivos que permiten al intruso mantener el acceso al sistema, a menudo con fines maliciosos. Hay rootkits para una amplia variedad de sistemas operativos, como Linux, Solaris o Windows.

[21] ***Honeypot.-*** Se denomina Honeypot al software o conjunto de computadores cuya intención es atraer a crackers o spammers, simulando ser sistemas vulnerables o débiles a los ataques.

Es una herramienta de seguridad informática utilizada para recoger información sobre los atacantes y sus técnicas. Los Honeypots pueden distraer a los atacantes

de las máquinas más importantes del sistema, y advertir rápidamente al administrador del sistema de un ataque, además de permitir un examen en profundidad del atacante, durante y después del ataque al honeypot.

Algunos honeypots son programas que se limitan a simular sistemas operativos no existentes en la realidad y se les conoce como honeypots de baja interacción y son usados fundamentalmente como medida de seguridad. Otros sin embargo trabajan sobre sistemas operativos reales y son capaces de reunir mucha más información; sus fines suelen ser de investigación y se los conoce como honeypots de alta interacción.

También se llama honeypot a un website o sala de chat, que se ha creado para descubrir a otro tipo de usuarios con intenciones criminales.

[22] ***Nmap.-*** Este mapeador de redes es una utilidad de código abierto, por lo tanto gratuita para exploración de redes y auditoría de seguridad. Se diseñó para analizar rápidamente grandes redes, aunque funciona muy bien contra equipos individuales. Nmap utiliza paquetes IP crudos de forma novedosa.

[23] ***GESTIÓN Y TRATAMIENTO DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN***

[Disponible en]

- ✓ http://www.arcert.gov.ar/ncursos/material/Gestion_de_Incidentes_parte1_vf.pdf
- ✓ http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/fundamentos_de_la_gestion_TI/vision_general_gestion_servicios_TI/vision_general_gestion_servicios_TI.php

[24] ***Los principales incidentes de seguridad según el CERT***

[Disponible en]

- ✓ http://bulma.net/body.phtml?nIdNoticia=873

[25] ***Aplicación de las Medidas de Seguridad***

[Disponible en]

- ✓ http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/gestion_de_la_seguridad/proceso_gestion_de_la_seguridad/aplicacion_medidas_de_seguridad.php

[26] ***Categorización de incidentes***

[Disponible en]

- ✓ http://www.e-gestar.com/itil/doc/!SSL!/WebHelp/SS_-_Gestion_de_Incidentes.htm
- ✓ http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/gestion_de_incidentes/proceso_gestion_de_incidentes/registro_y_clasificacion_de_incidentes.php

Informe de incidentes de seguridad

[Disponible en]

- ✓ http://www.rediris.es/cert/doc/informes/2002-06/