



MF0488_3: Gestión de incidentes de seguridad informática

Certificado de Profesionalidad
IFCT0109 - Seguridad informática



IFCT0109 > MF0488_3

MF0488_3:

Gestión de incidentes de seguridad informática

ÍNDICE

Capítulo 1 Sistemas de detección y prevención de intrusiones (IDS/IPS)	181
1. Introducción.....	181
2. Conceptos generales de gestión de incidentes, detección de intrusiones y su prevención	181
3. Identificación y caracterización de los datos de funcionamiento del sistema.....	186
4. Arquitecturas más frecuentes de los sistemas de detección de intrusos	189
5. Relación de los distintos tipos de IDS/IPS por ubicación y funcionalidad	194
6. Criterios de seguridad para el establecimiento de la ubicación de los IDS/IPS	203
7. Resumen	204
 Capítulo 2 Implantación y puesta en producción de sistemas IDS/IPS	206
1. Introducción.....	206
2. Análisis previo de los servicios, protocolos, zonas y equipos que utiliza la organización para sus procesos de negocio	206
3. Definición de políticas de corte de intentos de intrusión en los IDS/IPS	213
4. Análisis de los eventos registrados por el IDS/IPS para determinar falsos positivos y caracterizarlos en las políticas de corte del IDS/IPS	216
5. Relación de los registros de auditoría del IDS/IPS necesarios para monitorizar y supervisar su correcto funcionamiento y los eventos de intentos de intrusión	221
6. Establecimiento de los niveles requeridos de actualización, monitorización y pruebas del IDS/IPS.....	226
7. Resumen	229
 Capítulo 3 Control de código malicioso	231
1. Introducción.....	231
2. Sistemas de detección y contención de código malicioso	231
3. Relación de los distintos tipos de herramientas de control de código malicioso en función de la topología de la instalación y las vías de infección a controlar.....	241
4. Criterios de seguridad para la configuración de las herramientas de protección frente a código malicioso	245
5. Determinación de los requerimientos y técnicas de actualización de las herramientas de protección frente a código malicioso	250

6. Relación de los registros de auditoría de las herramientas de protección frente a códigos maliciosos necesarios para monitorizar y supervisar su correcto funcionamiento y los eventos de seguridad.....	254
7. Establecimiento de la monitorización y pruebas de las herramientas de protección frente a código malicioso.....	259
8. Análisis de los programas maliciosos mediante desensambladores y entornos de ejecución controlada.....	262
9. Resumen	264
 Capítulo 4 Respuesta ante incidentes de seguridad	265
1. Introducción.....	265
2. Procedimiento de recolección de información relacionada con incidentes de seguridad	266
3. Exposición de las distintas técnicas y herramientas utilizadas para el análisis y correlación de información y eventos de seguridad.....	276
4. Proceso de verificación de la intrusión.....	280
5. Naturaleza y funciones de los organismos de gestión de incidentes tipo CERT nacionales e internacionales.....	284
 Capítulo 5 Proceso de notificación y gestión de intentos de intrusión	289
1. Introducción.....	289
2. Establecimiento de las responsabilidades en el proceso de notificación y gestión de intentos de intrusión o infecciones.....	289
3. Categorización de los incidentes derivados de intentos de intrusión o infecciones en función de su impacto potencial.....	294
4. Criterios para la determinación de las evidencias objetivas en las que se soportará la gestión del incidente.....	299
5. Establecimiento del proceso de detección y registro de incidentes derivados de intentos de intrusión o infecciones.....	305
6. Guía para la clasificación y análisis inicial del intento de intrusión o infección contemplando el impacto previsible del mismo	309
7. Establecimiento del nivel de intervención requerido en función del impacto previsible.....	313
8. Guía para la investigación y diagnóstico del incidente de intento de intrusión o infecciones	317
9. Establecimiento del proceso de resolución y recuperación de los sistemas tras un incidente derivado de un intento de intrusión o infección	322

10. Proceso para la comunicación del incidente a terceros, si procede	326
11. Establecimiento del proceso de cierre del incidente y los registros necesarios para documentar el histórico del incidente	330
12. Resumen.....	334
 Capítulo 6 Análisis forense informático	335
1. Introducción.....	335
2. Conceptos generales y objetivos del análisis forense	335
3. Exposición del principio de Locard	339
4. Guía para la recogida de evidencias electrónicas.....	345
5. Guía para el análisis de las evidencias electrónicas recogidas, incluyendo el estudio de ficheros y directorios ocultos, información oculta de sistema y la recuperación de ficheros borrados	349
6. Guía para la selección de las herramientas de análisis forense	354
7. Resumen	356

CAPÍTULO 1 SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES (IDS/IPS)

1. INTRODUCCIÓN

En una economía donde las tecnologías de la información están cada vez más en auge y más extendidas, las organizaciones deben definir políticas de seguridad más exhaustivas en sus sistemas de información para evitar el acceso a ellos por personal no autorizado y para impedir un uso malintencionado de sus datos.

Hay numerosas motivaciones por las que un atacante puede actuar en una organización: desde motivos económicos, por simple diversión, por disconformidad con sus directrices o valores o por la mera autorrealización personal, entre muchas otras.

A medida que avance el manual se irán comentando los distintos tipos de ataques y cómo prevenirlos y combatirlos y, en este capítulo en particular se van a identificar y caracterizar los distintos datos de funcionamiento del sistema donde localizar las incidencias que le suceden.

También se van a describir y analizar varias técnicas para detectar y prevenir el ataque de intrusos mediante una serie de herramientas como son los sistemas de prevención de intrusiones o IPS y los sistemas de detección de IDS, comentando detalladamente sus características principales y sus funcionalidades.

Para concluir el capítulo, una vez que ya se han descrito las herramientas necesarias para decidir qué sistema de prevención o detección de intrusos van a implantar las organizaciones en sus sistemas de información, se aportan una serie de pautas a tener en cuenta en el momento de elegir la ubicación de estos IDS y/o IPS atendiendo a las necesidades concretas de cada organización.

2. CONCEPTOS GENERALES DE GESTIÓN DE INCIDENTES, DETECCIÓN DE INTRUSIONES Y SU PREVENCIÓN

Antes de definir los conceptos de gestión de incidentes y sus relaciones es imprescindible conocer tres conceptos básicos referentes a la información:

- **Confidencialidad:** la confidencialidad de la información es la propiedad mediante la que se garantiza el acceso a la misma solo a usuarios autorizados.
- **Integridad:** propiedad de la información que garantiza que no ha sido alterada y que se ha mantenido intacto el documento original que contenía dicha información. La información solo puede ser modificada por los usuarios autorizados.
- **Disponibilidad:** propiedad de la información en la que se garantiza que esté disponible para los usuarios cuando estos lo requieran.

Propiedades de seguridad informática



En términos de seguridad informática para que la información cumpla unos estándares de seguridad adecuados debe contener las tres propiedades mostradas en la imagen: integridad, confidencialidad y disponibilidad.

Un incidente de seguridad es cualquier evento que puede afectar a la integridad, confidencialidad y disponibilidad de la información. En otras palabras, y atendiendo a la norma ISO 27001:2005, un incidente de seguridad es un evento no deseado o no esperado que puede comprometer significativamente las operaciones de negocio y amenazar la seguridad de la información.

Nota

ISO es la Organización Internacional de Normalización. Esta organización elaboró una serie de normas internacionales que formulan recomendaciones de buenas prácticas para las empresas, entre ellas la ISO 2700:2005 que hace referencia a la seguridad de la información.

2.1.- Tipos de incidentes de seguridad

Son numerosos los tipos de incidentes de seguridad que pueden ocurrir en un sistema. Una posible clasificación sería la siguiente:

- **Accesos no autorizados:** son ingresos y operaciones no autorizadas a los sistemas, con éxito o no. Forman parte de esta categoría:
 - Robo de información.
 - Borrado de información.
 - Accesos no autorizados exitosos.
 - Alteración de la información.
 - Intentos recurrentes y no recurrentes de acceso no autorizado.

- Abuso o mal uso de los servicios informáticos (tanto internos como externos) que requieran autenticación.
- **Código malicioso o *malware*:** son incidentes que se infiltran en un sistema de información sin autorización del propietario. Son incidentes de código malicioso los siguientes:
 - Virus informáticos.
 - Troyanos: código malicioso que se introduce en el sistema informático como un programa aparentemente legítimo e inofensivo pero que, al ejecutarlo, permite el acceso remoto del sistema a usuarios no autorizados.
 - Gusanos informáticos: código malicioso que, una vez ha accedido al sistema, se va duplicando a sí mismo. No altera los archivos ya instalados pero supone un consumo de recursos importante.
- **Denegación del servicio:** eventos que producen la pérdida de un servicio en particular, impidiendo su ejecución normal. Suelen ser incidentes de denegación del servicio cuando en el sistema se nota que hay tiempos de respuesta muy bajos y servicios internos y externos inaccesibles sin motivos aparentes.
- **Pruebas,** escaneos o intentos de obtención de información de un sistema de información: son eventos que intentan obtener información sobre las acciones que se producen en un sistema informático. Algunos de estos eventos son:
 - *Sniffers:* aplicaciones cuya función es obtener la información que envían los distintos equipos de una red.
 - Detección de vulnerabilidades: aplicaciones que buscan las vulnerabilidades de un sistema de información para aprovecharse de ello maliciosamente.
- **Mal uso de los recursos tecnológicos:** eventos que atacan a los recursos tecnológicos de un sistema de información a causa de un mal uso de los mismos. Forman parte de este tipo de eventos:
 - Violación de la normativa de acceso a internet.
 - Abuso o mal uso de los servicios informáticos externos o internos.
 - Abuso o mal uso del correo electrónico.
 - Violación de las políticas, normas y procedimientos de seguridad informática de una organización.
 -

Incidentes de seguridad	
Tipo de incidente	Incidente
Acceso no autorizado	Accesos no autorizados con éxito.
	Robo de información.
	Alteración de la información.
	Borrado de la información.
	Intentos de acceso no autorizado recurrentes y no recurrentes.

Incidentes de seguridad	
Tipo de incidente	Incidente
	Mal uso o abuso de los servicios informáticos que necesitan autenticación.
Código malicioso	Virus informáticos.
	Troyanos.
	Gusanos informáticos.
Denegación del servicio o DoS	Ataques a páginas web o servidores para saturarlos.
Intentos de obtención de información	<i>Sniffers.</i>
	<i>Detección de vulnerabilidades.</i>
Mal uso de los recursos	<i>Abuso o mal uso de los servicios informáticos (internos o externos).</i>
	<i>Violación de la normativa de acceso a internet.</i>
	<i>Abuso o mal uso del correo electrónico.</i>
	<i>Violación de políticas de seguridad informática.</i>

2.2.- Gestión y medidas de incidentes de seguridad

Ante la posibilidad de que haya algún tipo de incidente de seguridad en la organización hay que tomar una serie de medidas que pueden ser:

- Medidas preventivas: aquellas medidas que se aplican para evitar la ocurrencia de incidentes de seguridad. Algunos ejemplos son: utilización de contraseñas, cifrado de información, establecimiento de *firewalls*, etc.
- Medidas de detección: medidas que sirven para detectar y controlar los incidentes de seguridad. Por ejemplo: auditorías de seguridad, revisiones de seguridad, etc.
- Medidas correctivas: medidas implementadas una vez ya ha sucedido el incidente de seguridad que sirven para evitar que no vuelvan a ocurrir y para restaurar la situación inicial antes de la incidencia. Suelen ser procedimientos de restauración, eliminación de código malicioso y auditoría forense.

La gestión de incidentes tiene como objetivo calcular y utilizar adecuadamente los recursos necesarios para aplicar correctamente estas medidas de prevención, detección y corrección de incidentes de seguridad. Se establecen unas pautas generales a seguir para que esta gestión esté bien ejecutada:

- Prevención de los incidentes: aplicación de las medidas preventivas que eviten la producción de los incidentes.

- Detección y reporte de los incidentes: en caso de producirse el incidente hay que detectarlo y reportar el mismo a los responsables de su gestión.
- Clasificación del incidente: definición del tipo de incidente que ha ocurrido (acceso no autorizado, robo de información, etc.).
- Análisis del incidente: análisis de cómo se ha producido el incidente y de los daños que ha causado.
- Respuesta al incidente: aplicación de las medidas correctivas para restaurar el sistema a la situación inicial antes de producirse el incidente.
- Registro de incidentes: registro del incidente sucedido y de las medidas aplicadas para obtener un historial y un control de todos los registros que han ido ocurriendo.
- Aprendizaje: análisis de los posibles errores causantes de la incidencia para evitar que se vuelvan a producir.

Siguiendo estas fases de gestión de incidentes, las organizaciones pueden obtener numerosos beneficios, entre ellos:

- Rápida, eficiente y sistemática respuesta ante la aparición de incidentes.
 - Rápida restauración del sistema informático garantizando **la** mínima pérdida de información posible.
 - Generación de una base de datos con **el** histórico de los incidentes y de las medidas tomadas para una mayor rapidez ante próximos incidentes.
 - Mejora continua de la gestión y tratamiento de incidentes.
 - Eliminación de **la** aparición de incidentes repetitivos (gracias al registro histórico).
 - Optimización de los recursos disponibles.
 - Mayor productividad de los usuarios.
 - Mayor control de los procesos del sistema de información y del proceso de monitorización del mismo.

Sin embargo, una gestión de incidentes deficiente puede llevar a efectos adversos importantes:

- Desperdicio y bajo rendimiento de los recursos.
- Pérdida de información valiosa para **la** organización.
- Pérdida de productividad en los servicios y, como consecuencia, peor calidad de servicio a los clientes.

2.3.- Detección de intrusiones y su prevención

Los intentos de intrusión son aquellos intentos que pueden afectar negativamente a la confidencialidad, integridad y disponibilidad de la información de un equipo o que intentan evitar los mecanismos de seguridad que hay establecidos.

Estas intrusiones pueden producirse de varios modos: desde usuarios no autorizados que acceden al sistema a través de internet, usuarios que sí están autorizados pero que intentan acceder a privilegios para los que no tienen autorización, hasta usuarios autorizados que utilizan malintencionadamente los privilegios que les han sido otorgados.

Para evitar este tipo de intrusiones están los sistemas de prevención de intrusiones o IDS que son sistemas que permiten establecer una protección adicional a los equipos y redes de una organización ante las posibles amenazas que pueden aparecer debido al uso exhaustivo de las redes y de los sistemas de información externos .

3. IDENTIFICACIÓN Y CARACTERIZACIÓN DE LOS DATOS DE FUNCIONAMIENTO DEL SISTEMA

Un *log* es un registro oficial de los eventos del sistema producidos a lo largo de un período de tiempo determinado. En los *logs* se registran datos de eventos referentes a:

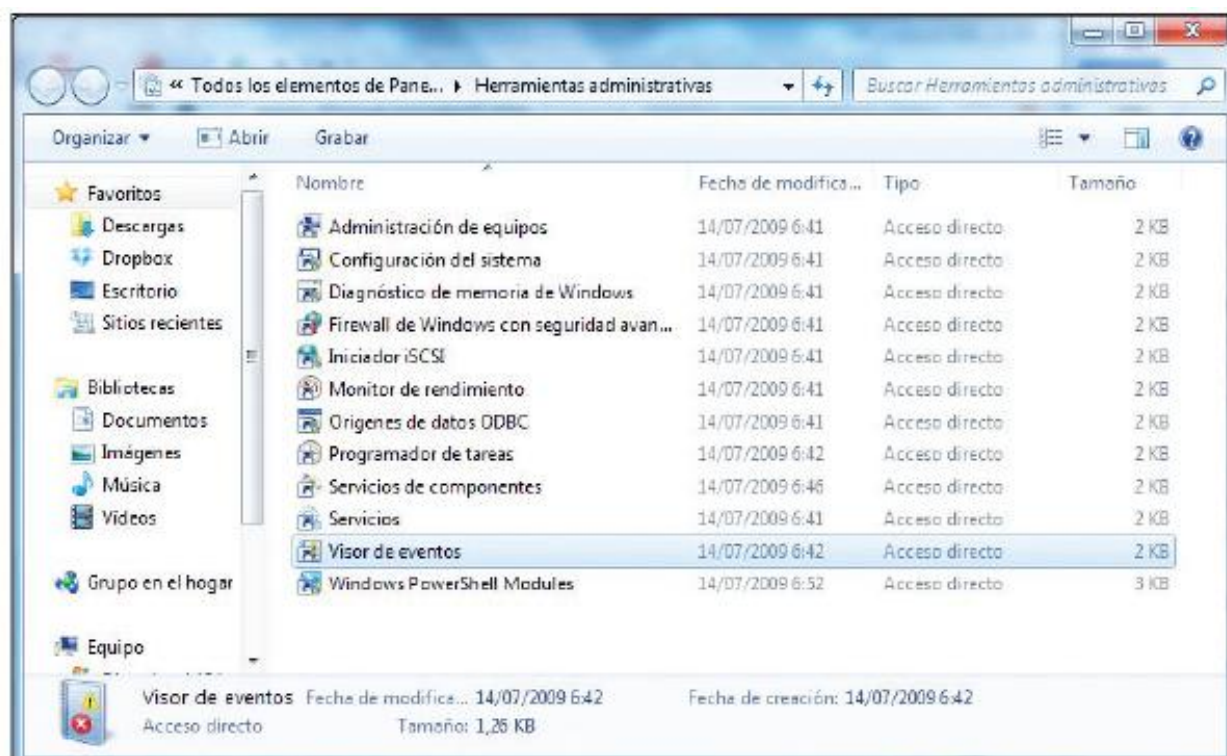
- Qué tipo de evento ha ocurrido.
- Quién ha originado el evento.
- Cuándo se ha producido el evento.
- Dónde se ha producido el evento.
- Por qué se ha producido el evento.

Así, para comprobar el correcto funcionamiento del sistema e identificar los distintos eventos sucedidos se recomienda evaluar los *logs* de los equipos, ya que se podrán detectar fallos y eventos como:

- Incidentes de seguridad.
- Funcionamientos anómalos.
- Cambios de configuración de aplicaciones o dispositivos.
- Utilización y rendimiento de los recursos.
- Intentos fallidos de acceso de usuarios no autorizados.

Tanto *Windows* como *Linux* ofrecen la posibilidad de visualizar estos *logs* y eventos para detectar y seguir los distintos eventos que han ido sucediendo en el equipo.

En *Windows* se puede utilizar el "Visor de eventos" accediendo a **Inicio -> Configuración-> Panel de control-> Herramientas administrativas ->Visor de eventos:**

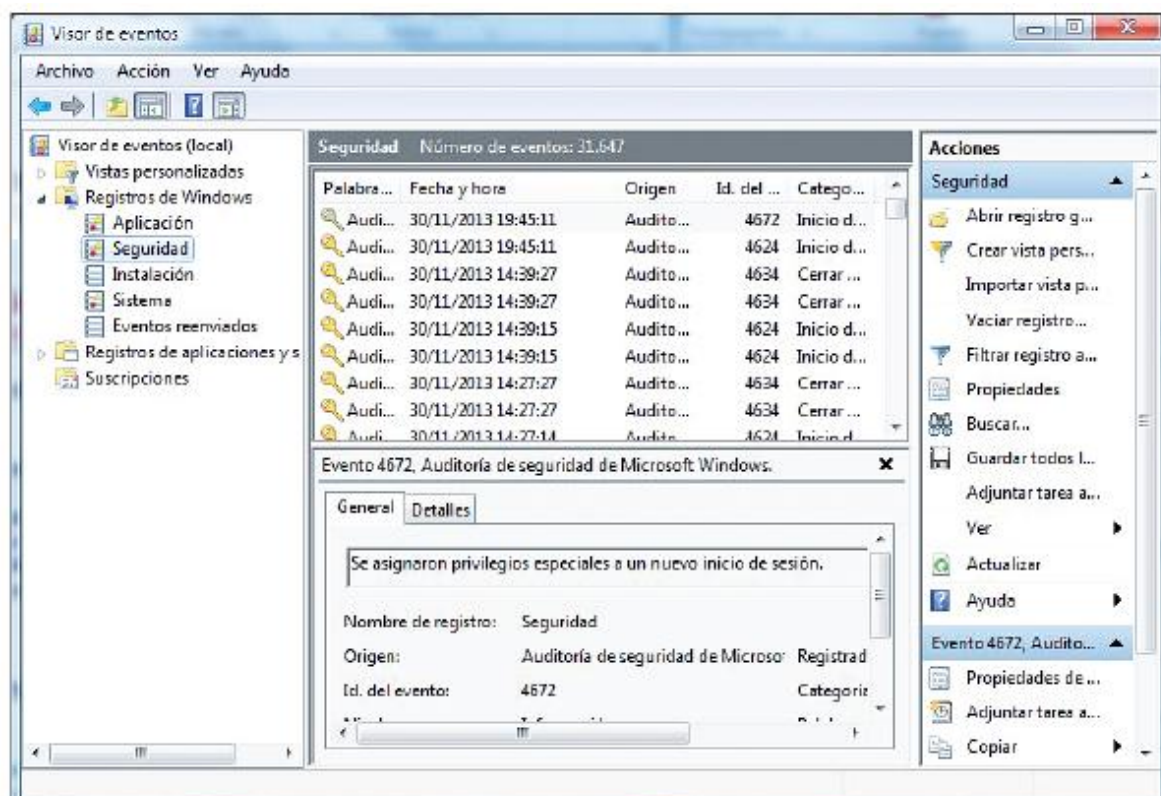


Panel de control, herramientas administrativas

Con esta herramienta se pueden visualizar distintos tipos de eventos sucedidos junto con la fecha y hora, el origen, su identificador, el usuario que lo ha generado y otras características:

- Registros de aplicación: eventos registrados por aplicaciones o programas.
- Registros de seguridad: eventos ocurridos en los accesos del sistema como los intentos de inicio de sesión (tanto exitosos como fallidos), las introducciones de contraseñas erróneas, la utilización de los recursos, etc.
- Registros de instalación: eventos que hacen referencia a la instalación de aplicaciones en el equipo. Se suelen utilizar para comprobar si se ha instalado algún código malicioso en el equipo.
- Registros de eventos reenviados: eventos que se han reenviado a este registro desde otros equipos.

En este caso, como se pretenden detectar las intrusiones y los distintos fallos de seguridad sucedidos en el equipo, el tipo de registros al que más atención habrá que prestar es a los registros de seguridad:



Visor de eventos de Windows

En cambio utilizando *Linux* no hay una aplicación gráfica que permita visualizar los eventos de un equipo. Para ello será necesario acceder a los archivos de registro iniciando la sesión como usuario "root" y utilizar una serie de comandos:

- Con el comando **tail - f** se ven las últimas líneas de un archivo y sus actualizaciones. Por ejemplo, utilizando **tail - f/var/log/auth.log** se mostrarán los últimos eventos de autenticación como sesiones nuevas.
- Con el comando **less +F** en lugar de acceder a las últimas líneas de un archivo de registro se accede a su totalidad, pudiéndose ver, incluso, las actualizaciones del mismo a tiempo real.
- Para finalizar estos comandos se pulsa la combinación de teclas (Ctrl + C) y en el caso del comando **less +F** se pulsa además la tecla [Q].

Los principales archivos de registro que se utilizan para comprobar el funcionamiento del sistema y sus problemas de seguridad se pueden observar en la tabla siguiente:

Nombre de archivo	Funcionalidad
<code>/var/log/auth.log</code>	Eventos de autenticación de usuarios y permisos.
<code>/var/log/boot.log</code>	Eventos y servicios empezados cuando se inicia el sistema.
<code>/var/log/daemon.log</code>	Mensajes sobre permisos o servicios corriendo en el sistema.
<code>/log/dmesg.log</code>	Mensajes del núcleo Linux.
<code>/var/log/errors.log</code>	Errores del sistema.
<code>/var/log/everything.log</code>	Mensajes misceláneos no cubiertos por los otros archivos.
<code>/var/log/httpd.log</code>	Mensajes y errores de Apache.
<code>/var/log/mail.log</code>	Mensajes del servidor de correo electrónico.
<code>/var/log/messages.log</code>	Alertas generales del sistema.
<code>/var/log/secure</code>	Registro de seguridad.
<code>/var/log/syslog.log</code>	Registro del sistema de registro.
<code>/var/log/user.log</code>	Muestra información acerca de los procesos usados por el usuario.

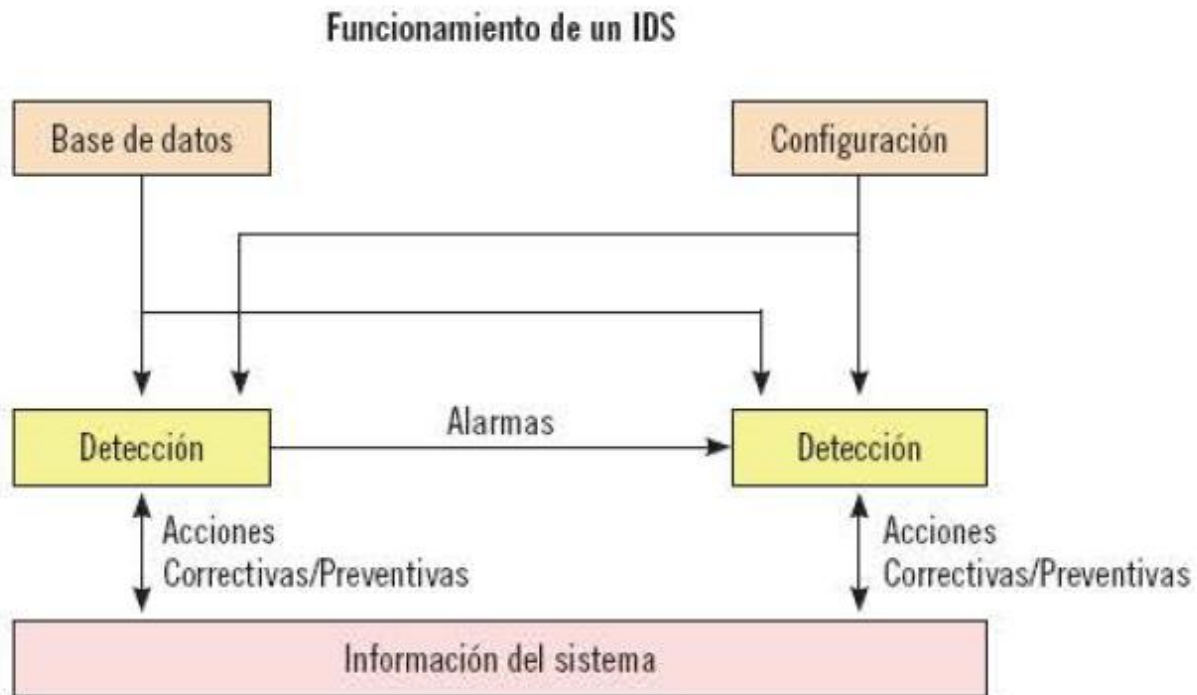
De este modo, tanto con *Windows* como con *Linux*, mediante las herramientas de visualización de *logs* y de eventos que se han visto hasta ahora, se pueden comprobar y evaluar los distintos parámetros de funcionamiento de un sistema o de un equipo. Así, se podrán detectar las distintas deficiencias de la gestión de recursos e incidentes de un sistema y analizar de dónde provienen y poder establecer una serie de medidas correctivas que permitan una eficiente gestión del equipo.

Así mismo, mediante el historial de *logs* y eventos también se pueden observar los eventos repetidos perjudiciales para el equipo y encontrar aquellas medidas que eviten que vuelvan a suceder mejorando significativamente el rendimiento del equipo y aumentando la seguridad del mismo.

4. ARQUITECTURAS MÁS FRECUENTES DE LOS SISTEMAS DE DETECCIÓN DE INTRUSOS

Los sistemas de detección de intrusos o IDS (*Intrusion Detection System*) son programas cuya utilidad es detectar las intrusiones que se pueden producir en la red o en un equipo. Se encargan de monitorizar los eventos del equipo para buscar intentos de intrusión.

Los IDS son una especie de proceso de auditoría. Son aplicaciones que mediante una amplia base de datos y una serie de configuraciones consiguen prevenir y detectar los posibles ataques que pueden producirse en un sistema. Una visión gráfica del funcionamiento de un IDS podría ser la siguiente:



Las ventajas que proporcionan los sistemas de detección de intrusos son numerosas. No obstante, son varios los motivos que justifican la utilización de IDS en las organizaciones:

- **Previenen de posibles problemas porque disuaden individuos hostiles:** los IDS posibilitan el descubrimiento de atacantes al sistema, lo que resulta un elemento disuasorio ante la posibilidad de ser descubiertos y penalizados.
- **Detectan ataques y otras vulneraciones de la seguridad que otros sistemas de protección no previenen:** en numerosas ocasiones los atacantes acceden sin autorización a los equipos aprovechando sus vulnerabilidades. Mediante los IDS se pueden detectar estos intentos de acceso y reportarlos de inmediato al administrador, de modo que puedan aplicarse medidas correctivas lo antes posible y minimizar el daño.
- **Detectan preámbulos de ataques: normalmente, antes de intentar acceder y atacar a un sistema, los atacantes suelen examinarlo y hacer pruebas para tantear el ataque.** Los IDS detectan estas pruebas de red y accesos al sistema lo que permite aumentar la seguridad cuando hay este tipo de detecciones para poder evitar futuros ataques.
- **Justifican y documentan el riesgo de la organización: en el momento en el que se elaboran las políticas de seguridad de la empresa es necesario realizar una evaluación de los riesgos justificada con indicadores y datos.** Los IDS permiten conocer estos riesgos y documentarlos, de modo que la política de seguridad establecida y las decisiones que se tomen en relación a esta estarán correctamente justificadas.

- Aportan información útil sobre las intrusiones y ataques que se producen en el equipo: aparte de bloquear los ataques e intentos de ataque del sistema, los IDS también recogen información útil de estos ataques que puede utilizarse como prueba de delito en el momento de querer emprender acciones legales.

Arquitectura de los IDS

Actualmente hay varias propuestas en el mercado sobre la arquitectura de IDS y no hay ninguna de ellas que se utilice de modo estándar, lo que provoca que las organizaciones que trabajan con distinta arquitectura IDS tengan dificultades para interoperar entre sí.

No obstante, hay ciertas peculiaridades comunes en las distintas arquitecturas de IDS:

- La fuente de recogida de datos. Las fuentes pueden ser *logs*, dispositivos de red o el mismo sistema de información.
- Las reglas que definen los patrones y directrices para detectar las anomalías de seguridad de un sistema.
- Los filtros que comparan los datos o los *logs* que se han obtenido con los patrones definidos en las reglas.
- Los detectores de los eventos anormales que suceden en el tráfico de la red.
- El sistema que genera los informes y las alarmas en caso de encontrar alguna intrusión o ataque.

Nota

La seguridad de la información en las organizaciones es un asunto primordial para garantizar su éxito. A pesar de que es imposible conocer todas las vulnerabilidades de un sistema y que cada día surgen vulnerabilidades nuevas, los IDS son una herramienta muy útil para detectarlas y solucionarlas. Aún así, como única medida de seguridad no son suficientes: es necesario establecer medidas adicionales como cortafuegos o IPS, entre otras.

A pesar de estos rasgos comunes son muchas las diferencias que hay entre las arquitecturas de los IDS. A continuación se describirán las arquitecturas de IDS más importantes en el mercado actual.

Arquitectura CIDF (*Common Intrusion Detection Framework*)

La arquitectura CIDF (*Common Intrusion Detection Framework*) fue promovida por la Agencia Federal de Estados Unidos DARPA (*Defense Advanced Research Projects Agency*) y, aunque no logró establecerse como un estándar, determinó un modelo y un vocabulario general para tratar las intrusiones.

Esta arquitectura contempla cuatro tipos básicos de equipos:

- Equipos generadores de eventos o Equipos E: equipos cuya función principal es la detección de eventos y la emisión de informes.
- Analizadores de eventos o Equipos A: equipos que reciben los informes emitidos y se encargan de realizar los análisis pertinentes.
- Base de datos de eventos o Equipos D: componentes de bases de datos que permiten ver el historial de los eventos sucedidos en el sistema.
- Equipos de respuesta o Equipos R: obtienen los datos de los demás tipos de equipos (E, A y D) y responden a los eventos sucedidos en el sistema.

Arquitectura CISL (*Common Intrusion Specification Language*)

La arquitectura CISL (*Common Intrusion Specification Language*) o lenguaje de especificación de intrusiones común surge por la necesidad de unir los cuatro tipos de equipos que se definieron en la arquitectura CISL. En esta arquitectura deben poder transmitirse los siguientes tipos de información:

- Información de eventos en grupo: une los equipos C y A definidos en la arquitectura CID F. Proporciona información sobre el tráfico de red del sistema y sobre la auditoría de registros.
- Resultados de los análisis: une los equipos A y D y facilita información como las características de las anomalías sucedidas en el sistema y de los ataques que se han detectado.
- Prescripciones de respuestas: une los equipos A y R y se encarga de detener ciertas actividades y de modificar los parámetros de seguridad de componentes para responder a posibles ataques.

Arquitectura AusCERT

La arquitectura AusCERT (CERT australiano) es mucho más simple que las dos anteriores (CIDF y CISL) y facilita en unas pocas líneas un informe en una base de datos de un incidente sucedido en el sistema.

Un ejemplo de informe que proporciona AusCERT podría ser el siguiente:

Ejemplo de informe AusCERT

```
Source: 216.37.42.84
Ports: tcp 111
Incident type: Network_scan
Re-distribute: yes
Timezone: GMT -1
Reply: yes
Time: Sat 14 November 2013 at 15:30 (UTC)
```

La ventaja principal de esta arquitectura es que es muy sencilla para construirla y analizarla. Eso sí, en el momento en el que se requiera una información detallada de los eventos e incidencias sucedidos en el sistema se deberá tener en cuenta que AusCERT es muy limitada ya que su nivel de detalle es mínimo.

Arquitectura IDWG (*Intrusion Detection Working Group*)

La arquitectura IDWG (*Intrusion Detection Working Group*) propone un nuevo formato (el formato IDEF o *Intrusion Detection Exchange Format*) cuya función principal es la definición de formatos y procedimientos de intercambio de información entre los diversos subsistemas del IDS. Facilita el intercambio de información acerca de los incidentes de seguridad.

En esta arquitectura se distinguen tres módulos distintos:

- **Sensor:** recoge los datos de la fuente de datos, datos que el IDS utiliza para detectar las actividades no autorizadas. Son ejemplos de este tipo de datos los paquetes de red, *logs* de aplicaciones, *logs* del sistema operativo, etc.
- **Analizador:** analiza los datos recopilados por el sensor para detectar los accesos y/o actividades no autorizados.
- **Manager:** componente que gestiona y administra los demás elementos del IDS. Configura los sensores y analizadores, consolida los datos obtenidos, genera los informes mediante los datos facilitados por el analizador, etc.

Con estos tres módulos de la arquitectura IDWG se obtienen resultados como los siguientes:

- Lenguaje común que describe el formato de los datos.
- Documentos que recogen los distintos requerimientos funcionales de alto nivel que permiten la comunicación entre los IDS y entre los IDS y sus sistemas de gestión de incidentes.
- Identificación y definición de los protocolos más apropiados para la comunicación entre IDS y para el establecimiento del formato de los datos.

Como resumen, en la siguiente tabla se muestran las distintas arquitecturas IDS y sus características principales:

Tipo de arquitectura IDS				Características
CIDF	(Common Intrusion Detection Framework)			Consta de generador, analizador y base de datos de eventos además de unidades de respuesta ante la aparición de incidentes. Tuvo escasa aceptación en el mercado.
CISL	(Common Intrusion Specification Language)			Une los distintos equipos que forman parte de la arquitectura CIDF y facilita información sobre información de eventos en bruto, resultados de los análisis y prescripciones de respuestas.
AusCERT				Arquitectura simple que facilita la información de las incidencias en muy pocas líneas. Es muy limitada si se pretende obtener información detallada de las incidencias.
IDWG (Intrusion Detection Working Group)				Facilita el intercambio de información sobre los incidentes de seguridad y permite definir los protocolos y formatos de intercambio de información entre los IDS.

5. RELACIÓN DE LOS DISTINTOS TIPOS DE IDS/IPS POR UBICACIÓN Y FUNCIONALIDAD

En este epígrafe se van a describir los distintos tipos de IDS/IPS por ubicación y funcionalidad distinguiendo entre los sistemas de detección de intrusiones (o IDS) y los sistemas de prevención de intrusiones (IPS).

5.1.- Tipos de IDS

Atendiendo a su ubicación hay varios tipos de sistemas de detección de intrusos o IDS que se especificarán a continuación.

IDS basados en red (NIDS)

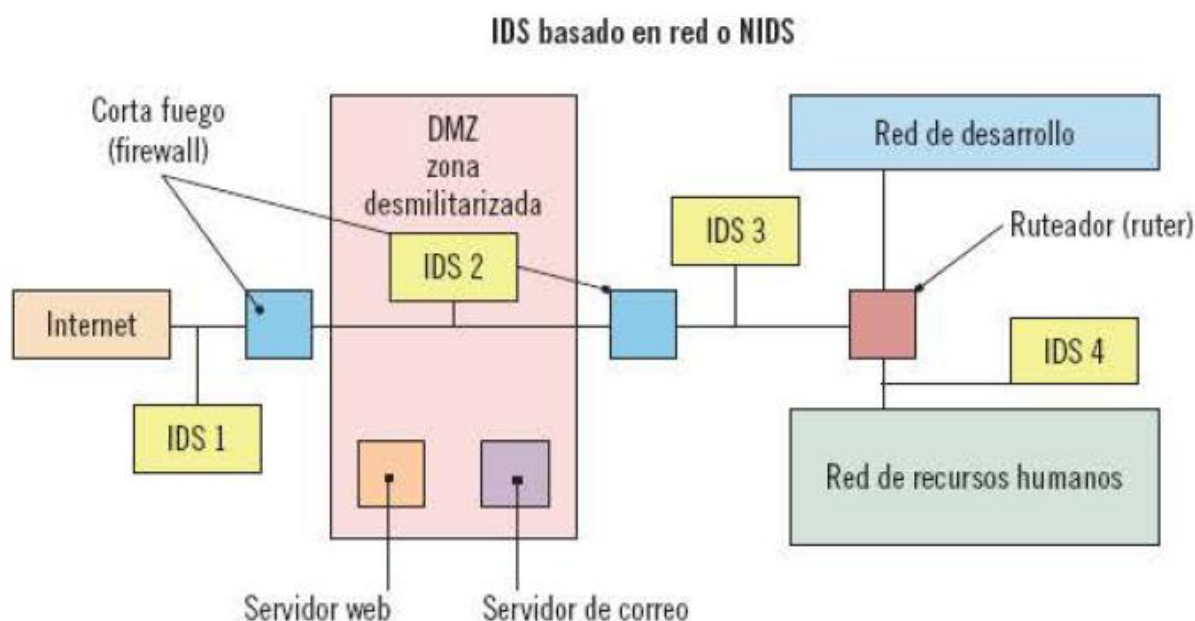
Los IDS basados en red detectan los ataques mediante la captura y análisis de los paquetes de la red. La gran mayoría de los IDS están basados en red. Una vez capturados y analizados los paquetes de la red, los IDS se encargan de buscar patrones que supongan algún tipo de ataque.

Los NIDS analizan el tráfico de toda la red examinando paquetes para buscar opciones no permitidas y diseñadas para no ser detectadas por los cortafuegos. Además, emite alertas cuando hay intentos de acceso o análisis externo de alguna vulnerabilidad del sistema.

Su funcionamiento consiste en:

- Unos sensores o agentes que se sitúan en varios puntos de la red para monitorizar el tráfico buscando tráfico sospechoso. Lo habitual es que estos sensores analicen los paquetes en modo oculto para no ser descubiertos.
- Una consola que recibe las alarmas emitidas por los sensores y que, atendiendo al tipo de alarma, producirá algún tipo de respuesta.

Un ejemplo de NIDS está reflejado en la imagen siguiente:



Como se puede observar, hay IDS (sensores) situados en varios puntos de la red que se encargan de monitorizar el tráfico que hay entre ellos.

De este modo se pueden detectar las incidencias sucedidas a lo largo de toda la red del sistema y reaccionar ante ellas.

Hay una serie de ventajas de este tipo de IDS:

- Detectan accesos no deseados en la red.
- No requieren la utilización de un *software* adicional en los servidores para poder funcionar.

- Son sistemas de fácil instalación y actualización.
- Tienen un bajo impacto en la red al no intervenir en sus operaciones habituales.
- Pueden monitorizar redes de grandes dimensiones siempre que haya capacidad suficiente para analizar todo su tráfico.

No obstante, los NIDS también conllevan una serie de desventajas:

- A pesar de poder monitorizar redes grandes pueden presentar dificultades en su procesamiento y fallar en el reconocimiento de ataques producidos en momentos de elevado nivel de tráfico de red.
- Los NIDS tienen dificultades para detectar los ataques con información cifrada.
- Los NIDS se limitan a detectar los ataques lanzados, independientemente de si han tenido éxito o no, lo que implica que ante cada ataque detectado los administradores deben analizarlo uno a uno para comprobar el éxito o fracaso del mismo.
- Pueden presentar problemas cuando tienen que detectar ataques que viajan en paquetes fragmentados.

Uno de los NIDS más utilizados es *Snort*, una herramienta que, además de facilitar la información de los paquetes de red, es diferenciada de las demás por suministrar información completa y precisa en el registro de actividades maliciosas de la red. Además, notifica a los administradores la detección de potenciales violaciones de la red. Como características principales destacan:

- Dispone de más de 700 firmas en su base de datos.
- Es de distribución gratuita.
- Analiza el tráfico de la red en tiempo real.
- Permite la utilización de filtros en la detección de ataques.

Snort IDS Console - Microsoft Internet Explorer

Address: https://localhost:8080/snort-ids-console

Snort IDS Console Unfilter Refresh every 30 secs View alerts: Since 6 AM or on

Alert Information		Sensors		Top Sources		Top Targets		Top Target Ports	
	# %	Sensor	Sigs	Alerts	IP Address	Sigs	Alerts	IP Address	Sigs
Signatures:	62		19	482	192.168.1.1	6	186	192.168.1.1	6
TCP Alerts [View]	1,126 42%		13	177	192.168.1.1	6	6	192.168.1.1	6
UDP Alerts [View]	1,523 57%		11	240	192.168.1.1	3	21	192.168.1.1	3
ICMP Alerts [View]	0 0%		11	131	192.168.1.1	2	108	192.168.1.1	2
Total Alerts [View]	2,649 100%		9	298	192.168.1.1	2	92	192.168.1.1	2

Alert Overview by Signature

Earliest Alert: 2004-12-29 06:01:03
Latest Alert: 2004-12-29 16:57:12

Prio	Signature	# Sensors	# Alerts	# Srcs	# Dests
1	WEB-MISC cross site scripting attempt [sid 1497]	2	353	2	2
1	P2P Fasttrack/Kazaa/Morpheus traffic [sid 1698]	2	145	3	49
1	MS-SQL/SMB raiseerror possible buffer overflow [sid 1396]	2	117	1	1
1	WEB-MISC NetObserve authentication bypass attempt [sid 2441]	1	110	1	1
1	MS-SQL/SMB xp_cmdshell program execution [sid 681]	2	33	1	1
1	WEB-MISC PCT Client Hello overflow attempt [sid 2515]	2	25	1	8
1	MS-SQL xp_cmdshell - program execution [sid 687]	1	17	2	1
1	MS-SQL/SMB xp_reg* registry access [sid 689]	2	12	1	1
1	MS-SQL/SMB xp_password password change [sid 677]	2	10	1	1
1	MS-SQL/SMB xp_delete alert logfile deletion [sid 678]	2	10	1	1
1	MS-SQL xp_start_job - program execution [sid 673]	2	8	1	1
1	MS-SQL sa login failed [sid 688]	1	5	1	1

NIDSSnort

IDS basados en host (HIDS)

Los IDS basados en *host* o HIDS detectan las intrusiones a nivel de un equipo informático, analizando su tráfico para comprobar si ha habido algún tipo de alteración de los archivos del sistema operativo y para localizar actividades sospechosas. Fueron el primer tipo de IDS desarrollado e implementado.

Al trabajar sobre un equipo y no sobre el tráfico de la red ofrece una gran precisión en el análisis de las actividades, pudiendo detectar de un modo exacto los procesos y usuarios que han estado involucrados en un ataque en concreto dentro de un sistema operativo.

A diferencia de los NIDS, los IDS basados en *host* informan del resultado del ataque en cuanto a su éxito o fracaso. Además, también monitorizan los ficheros y los procesos del sistema atacado para una mejor detección y respuesta ante los ataques.

Sus funcionalidades principales se concretan en:

- Análisis del tráfico sobre un servidor o sobre un equipo concreto.
- Detección de los intentos de acceso, tanto fallidos como exitosos.
- Detección de las modificaciones realizadas en archivos críticos.

Como ventajas importantes, los HIDS destacan por:

- Detectan ataques que no pueden descubrir los NIDS al poder monitorizar los eventos locales del equipo o *host*.
- Pueden operar y detectar ataques ante datos cifrados que circulan por la red porque analizan los datos en el *host* de origen antes de ser cifrados o los datos en el *host* de destino una vez ya han sido descifrados.
- Facilitan información sobre el éxito o fracaso de los intentos de ataque.

Sin embargo, los IDS basados en *host* también cuentan con una serie de desventajas:

- Suponen un coste mayor que los NIDS ya que hay que gestionarlos y configurarlos en cada *host* que se quiere monitorizar.
- No son útiles cuando se pretende detectar ataques a toda una red, ya que los HIDS solo analizan los paquetes de red que entran en el *host* en el que están instalados.
- Suponen un consumo de recursos del *host* que monitorizan, lo que implica una disminución del rendimiento del sistema.
- Los HIDS corren el peligro de ser deshabilitados por algunos DoS.

Recuerde

Los DoS son ataques de denegación del servicio. Estos ataques se realizan a equipos o a redes e impiden al usuario el acceso a un servicio o recurso determinado para el que está legitimado.

Además, los IDS también se pueden clasificar atendiendo a su funcionalidad fundamental:

- IDS de detección de abusos o firmas.
- IDS de detección de anomalías.

IDS de detección de abusos o firmas

Los IDS de detección de abusos o firmas tienen como funcionalidad principal buscar eventos que coincidan con un patrón predefinido o con una firma que describa un ataque conocido.

Entre las ventajas de este tipo de IPS destacan:

- Elevado grado de efectividad sin generar en exceso falsas alarmas.
- Rápido diagnóstico del uso de un ataque determinado.

Sin embargo, también tiene como desventaja la constante necesidad de actualización continua para que la detección de los abusos o firmas sea eficaz.

IDS de detección de anomalías

Este tipo de IDS, en lugar de buscar abusos conforme a unos patrones, tiene como función principal la detección de comportamientos in usuales que sucedan en un *host* de una red. Sus ventajas principales son:

- La elevada capacidad de detectar ataques de los que no hay un conocimiento determinado.
- La posibilidad de definir firmas en la detección de abusos con la información que obtienen.

Sin embargo, al contrario que con los IPS de detección de abusos o firmas, este tipo de IPS genera un elevado número de falsas alarmas (al no haber ningún patrón definido).

5.2.- Tipos de IPS

Los sistemas de prevención de intrusiones o IPS se desarrollaron en 1990 con la finalidad de monitorizar el tráfico de una red en tiempo real y conseguir prevenir las intrusiones al sistema. Se consideran una evolución de los sistemas de detección de intrusiones (IDS).

Los IPS tratan de prevenir que se filtre cualquier intrusión: en cuanto se produce la caída de algún paquete o se detecta que está dañado o incompleto, la red bloquea la transmisión de este paquete con el fin de prevenir un posible ataque.

Las características fundamentales que tienen en común los distintos tipos de IPS son las siguientes:

- Tienen una capacidad de respuesta automática en cuanto se produce un incidente.
- Aplican filtros nuevos conforme se van detectando ataques en progreso.
- Reducen las falsas alarmas de ataques producidos en la red.
- Bloquean automáticamente los ataques a la red en tiempo real.
- Optimizan el rendimiento del tráfico de la red al bloquear de un modo automático los ataques.

Además, los IPS conllevan una serie de ventajas:

- Ofrecen una protección preventiva antes de que se produzca el ataque.
- Ofrecen una protección y defensa completa de varios tipos de ataques como: vulnerabilidades del sistema, tráfico de red, códigos maliciosos, intrusiones, etc.
- Optimiza la seguridad y la eficiencia en la prevención de intrusiones y/o ataques a una red o sistema.
- Son fáciles de instalar, configurar y administrar.
- Son escalables, por lo que se pueden ir actualizando según las necesidades de la organización.
- En comparación con un IDS requieren de menos inversión en recursos para entrar en funcionamiento.

Los IPS se pueden distinguir en tres categorías atendiendo a la acción que realizan:

- IPS de filtrado de paquetes.
- IPS de bloqueo de IP.

- IPS con acción de decepción.

IPS de filtrado de paquetes

Los IPS de filtrado de paquetes tienen como función principal determinar el tipo de tráfico que puede entrar y salir de un equipo o servidor.

En el mercado hay varias soluciones de IPS de filtrado de paquetes, las más importantes se describen a continuación:

- **Hogwash:** es un sistema que funciona tanto como IDS, como IPS (es un IDS/IPS). Monitoriza el tráfico de una o varias redes y genera alertas. Además, puede detectar los ataques de la red y filtrarlos. Aunque es imposible que evite todos los ataques a una red, sí que descarta un elevado porcentaje de los mismos.



- **Dragon IPS:** herramienta cuya funcionalidad principal es bloquear a los atacantes, reducir los ataques DoS y prevenir el acceso a la información del sistema convirtiendo la red en una red invisible.



Herramienta Dragon IPS

- **Snort Inline:** está basado y construido sobre el IDS *Snort* mencionado anteriormente, y con la función añadida de la capacidad de cambiar o descartar paquetes mientras circulan por el *host*. Es uno de los IPS de red más conocidos y utilizados.

IPS de bloqueo de IP

Este tipo de IPS tiene como funcionalidad principal bloquear direcciones IP que puedan ser causantes de algún tipo de ataque.

Del mismo modo que con los IPS de filtrado de paquetes, son numerosas las herramientas que hay en el mercado:

- **Snortsam:** herramienta gratis y de código abierto que bloquea las direcciones IP por periodos de tiempo que pueden ir desde segundos hasta tiempo indefinido. Además, también permite determinar una serie de direcciones individuales o redes enteras que el usuario no quiere que sean bloqueadas de ningún modo aunque en ellas se genere alguna alerta.

- **Portsentry:** herramienta de libre distribución desarrollada por Cisco. Su función principal es rastrear las conexiones sobre el *host* donde es ejecutada e identificar los intentos de exploración contra dicho *host*. En cuanto se detecta algún intento *Portsentry* niega el acceso a la exploración del *host*.

IPS con acción de decepción

Los IPS con acción de decepción están basados en la decepción o en el engaño hacia el atacante, de modo que cuando se produce algún ataque el IPS remite al atacante información errónea del *host*.

Las principales soluciones de IPS con acción de decepción son las siguientes:

- **DTK** o *Toolkit Deception*: conjunto de herramientas cuya función principal es emitir respuestas falsas al atacante para que este entienda que hay un número muy elevado de vulnerabilidades en el sistema al que está atacando.
- **Honeyd**: herramienta que crea *hosts* virtuales sobre una red con el fin de crear una simulación de la misma y engañar a los atacantes.
- **Specter**: es un *honeypot* o sistema de engaño que realiza la simulación de un equipo completo para atraer a los atacantes y alejarlos de los equipos reales. Además, en el momento en el que se produce algún ataque *Specter* investiga el rastro de los atacantes.

A modo de resumen se puede observar en la siguiente tabla los distintos tipos de IPS y las principales herramientas que actualmente se comercializan:

Nombre	Acción	Funciones
Hogwash	Filtrado de paquetes	Filtra y descarta paquetes que pueden provocar ataques en el sistema.
Dragon IPS	Filtrado de paquetes	Palía los efectos de los ataques de denegación de servicio.
Snort_Inline	Filtrado de paquetes	Modifica los paquetes que circulan por la red. Basado en el IDS Snort.
Snortsam	Bloqueo de IP	Bloquea direcciones IP por un período determinado o indefinidamente.
Portsentry	Bloqueo de IP	Detecta intentos de escaneo al <i>host</i> y bloquea el acceso al escaneo.

Nombre	Acción	Funciones
DTK	Decepción	Emite una respuesta falsa al atacante haciéndole ver que el equipo tiene un número elevado de vulnerabilidades.
Honeyd	Decepción	Crea hosts virtuales sobre una red.
Specter	Decepción	Realiza una simulación de un equipo completo para atraer a los atacantes.

6. CRITERIOS DE SEGURIDAD PARA EL ESTABLECIMIENTO DE LA UBICACIÓN DE LOS IDS/IPS

Una vez decidido el tipo de IDS/IPS que se quiere implantar, una de las preguntas más importantes que deben realizarse las organizaciones es dónde localizarlo. La ubicación de los sistemas IDS/IPS dependerán del equipo que se va a utilizar y del *software* IDS/IPS que se va a implantar.

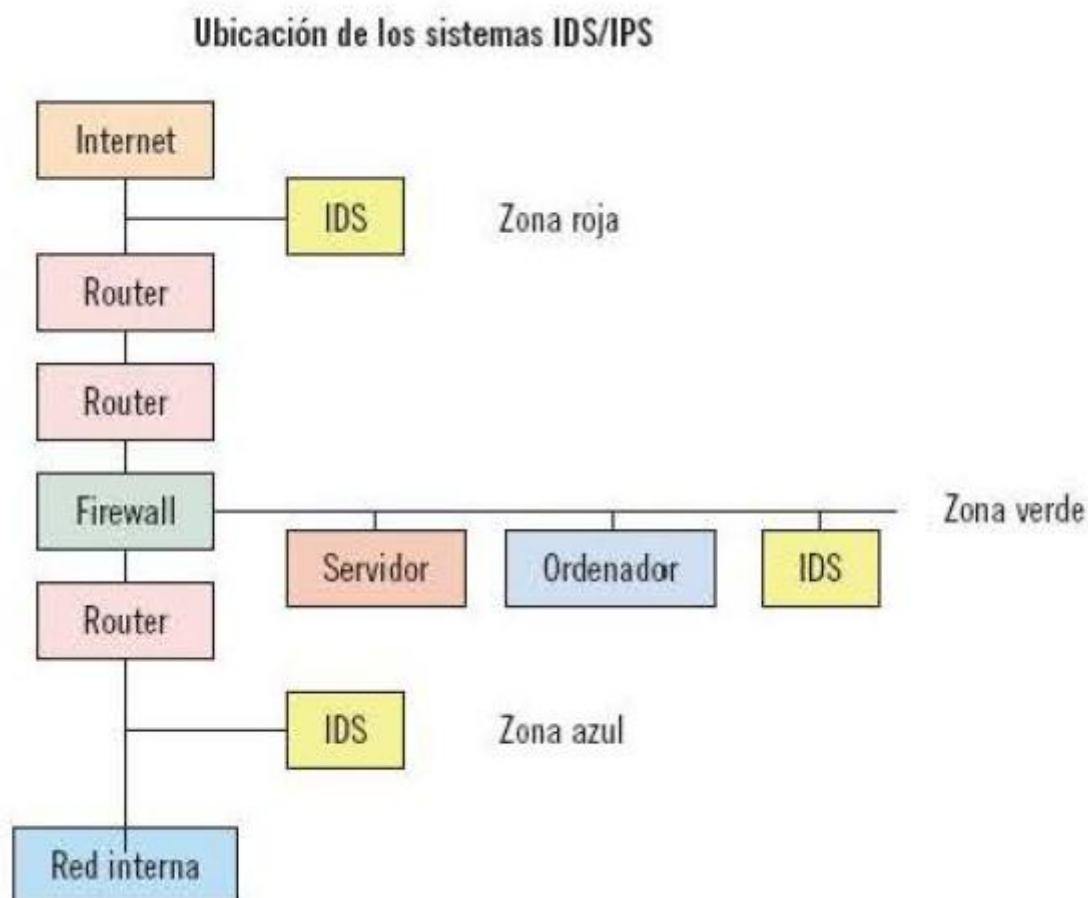
Atendiendo a los criterios de seguridad para el establecimiento de la ubicación de los IDS/IPS se distinguen tres zonas en las que se puede ubicar un sistema IDS/IPS:

- **Zona roja:** es una zona de riesgo elevado. En esta zona el sistema IDS/IPS debe configurarse de modo que tenga poca sensibilidad, ya que observará todo el tráfico de la red y habrá una elevada posibilidad de falsas alarmas.
- **Zona verde:** esta zona tiene menos riesgo que la zona roja y en ella el IDS/IPS debe configurarse de modo que tenga mayor sensibilidad que en la zona roja porque aquí el firewall o cortafuegos realiza un filtrado de accesos predefinidos por la organización. En esta zona hay menos falsas alarmas que en la zona roja.
- **Zona azul:** es la zona de confianza. En esta zona cualquier tipo de acceso anómalo que haya en la red hay que considerarlo como acceso hostil. Al haber un número inferior de accesos también se reduce considerablemente el número de falsas alarmas, por lo que es necesario que cualquier falsa alarma detectada por el sistema IDS/IPS sea analizada con detenimiento.

Nota

Aunque la zona azul se considere zona de confianza y el tráfico analizado sea muy limitado, los IDS/IPS ubicados en esta zona no forman parte de la red interna del sistema, por lo que no se analizará el tráfico interno de la red.

En la siguiente imagen se pueden observar las distintas ubicaciones de los IDS/IPS, distinguiendo entre zona roja, azul y verde:



Así, atendiendo al nivel de riesgo, al grado de falsas alarmas que se está dispuesto a asumir y al tráfico de datos que se pretenda analizar (según las preferencias de la organización) se elegirá una zona u otra para ubicar un sistema IDS/IPS en una organización.

7. RESUMEN

Un incidente de seguridad es cualquier evento que puede afectar a la integridad, confidencialidad y disponibilidad de la información. En otros términos, también se puede definir como un evento no deseado que puede comprometer significativamente las operaciones de una organización y amenazar su seguridad.

Hay numerosos tipos de incidentes de seguridad: accesos no autorizados, código malicioso, denegación de servicio, intentos de información de un sistema, uso deficiente de los recursos tecnológicos, etc. Para cada uno de ellos las organizaciones deben tomar una serie de medidas que los corrijan, los prevengan o, como mínimo, los detecten. La gestión de incidentes tiene como

objetivo la organización de los recursos para que estas medidas sean aplicadas de un modo eficiente. Para ello se puede utilizar el "Visor de eventos" de *Windows* o una serie de comandos en *Linux* que ofrecen una visión de los diferentes archivos de registro de eventos.

Una vez ya se conoce cómo localizar los eventos que ocurren en un sistema, es básica la implantación de sistemas de prevención de intrusiones o de sistemas de detección de intrusiones como complemento a las demás medidas de seguridad de la organización.

Una vez decidido el sistema IDS/IPS a implantar, otra de las decisiones fundamentales que influirán en el sistema de seguridad de una organización es elegir la ubicación de estos sistemas. Atendiendo a criterios de asunción de riesgos, grado donfianza donde el riesgo es mínimo y el número de falsas alarmas es muy limitado).

CAPÍTULO 2 IMPLANTACIÓN Y PUESTA EN PRODUCCIÓN DE SISTEMAS IDS/IPS

1. INTRODUCCIÓN

Cuando las organizaciones toman la decisión de implantar un sistema de detección y prevención de intrusos o IDS/IPS deben realizar una serie de análisis y comprobaciones previas para garantizar que la implementación se realice correctamente y sea lo más eficaz posible.

En el primer apartado de este capítulo se describen con profundidad los distintos elementos que hay que tener en consideración cuando se deben tomar las decisiones de ubicación del sistema, equipos que van a funcionar y se van a utilizar bajo los IDS/IPS y los protocolos y servicios que emplea la organización en su actividad diaria y en la transferencia y utilización de datos.

Una vez decidida la ubicación y las características de los sistemas de detección y prevención de intrusiones, en el apartado siguiente se mencionan una serie alternativas de políticas de seguridad que pueden utilizar estos sistemas en el momento en el que se detecta algún tipo de actividad sospechosa.

Aunque la detección de las intrusiones es fundamental para garantizar la eficacia del IDS/IPS hay que tener en cuenta que no todas las intrusiones detectadas tienen que ser intrusiones reales y que también puede ser que haya alguna intrusión no detectada. Por ello, en otro apartado se profundiza en estos conceptos y se formulan una serie de recomendaciones que permitan a las organizaciones configurar sus sistemas IDS/IPS para reducir las intrusiones no detectadas y las falsas detecciones.

Además, también se describen en profundidad las informaciones detalladas que deben facilitar los sistemas IDS/IPS cuando detectan alguna intrusión para que se realice una correcta monitorización de los eventos y se pueda comprobar el funcionamiento correcto del equipo y sus dispositivos.

Para finalizar el capítulo se formula una serie de recomendaciones que pueden ayudar a las organizaciones a definir los niveles adecuados de monitorización, actualización y pruebas a realizar antes de la implantación y una vez implantado el sistema de detección y prevención de intrusiones.

2. ANÁLISIS PREVIO DE LOS SERVICIOS, PROTOCOLOS, ZONAS Y EQUIPOS QUE UTILIZA LA ORGANIZACIÓN PARA SUS PROCESOS DE NEGOCIO

Los sistemas de detección y prevención de intrusiones (IDS/IPS) cada vez resultan más imprescindibles para cualquier empresa que trabaje con alguna infraestructura de red. Los intentos de intrusión y de utilización malintencionada de los datos de una organización siguen aumentando a niveles cada vez más elevados.

Aunque estos sistemas resultan muy útiles para evitar posibles intrusiones, no son suficientes: las organizaciones deben establecer una serie de medidas de seguridad adicionales que sirvan de apoyo en el momento que ocurra cualquier fallo de seguridad.

Además, suele ocurrir que los responsables de la infraestructura de la red no tengan muchos conocimientos específicos y concretos de estos sistemas.

Debido a ello es necesario que las organizaciones realicen previamente un estudio de sus infraestructuras, servicios, equipos, zonas y protocolos, entre otros muchos elementos, para que la implantación del sistema IDS/IPS y de las demás medidas de seguridad se realicen de un modo correcto y efectivo.

Por esto, el establecimiento de estos sistemas y medidas requiere un proceso previo de planificación, preparación, pruebas y formación especializada de los administradores de modo que cuando ya esté la implementación completada se pueda funcionar a pleno rendimiento y con la certeza de que el nivel de seguridad de la infraestructura de la organización es el adecuado.

La implementación de los sistemas IDS/IPS dependen en mayor parte de los recursos y políticas de la organización y debe realizarse escalonadamente para que el proceso de aprendizaje de los administradores sea profundo y basado en la experiencia que vaya adquiriendo a medida que se completa la implementación.

Recuerde

Los sistemas de detección de intrusiones (IDS) tienen como función principal detectar accesos no autorizados en los equipos o redes de una organización. Sin embargo, los sistemas de prevención de intrusiones (IPS) tienen como objetivo evitar estos accesos no autorizados.

A continuación se describirán las distintas opciones de localización de los sistemas IPS/IDS y sus características, ventajas e inconvenientes principales que deberán tener en cuenta las organizaciones en el momento de decidir qué sistema implantar en su infraestructura.

2.1.- Sistemas de detección y prevención de intrusiones en red o NIDPS

Como ya se ha comentado en el capítulo anterior y a modo de recordatorio, los sistemas de detección y prevención de intrusiones en red o NIDPS son sistemas que trabajan con los datos que circulan en una red, monitorizándola para buscar posibles accesos no autorizados y filtrando el tráfico de la red.

Son muy útiles porque proporcionan alertas cuando se produce un ataque en la red y pueden reaccionar para evitarla o para intentar que los daños sean mínimos. Además, facilitan un análisis de las intrusiones exitosas, lo que ayuda a las organizaciones a prevenir estas intrusiones en momentos futuros. No obstante, nunca deben ser sustitutos de una política de seguridad, sino que deben ser accesorios.

Estos sistemas pueden colocarse en varias ubicaciones de la infraestructura de red de una organización. Estos se mencionan a continuación.

Delante del cortafuegos o firewall

La colocación de los sistemas NIDPS delante del cortafuegos externo permite una monitorización de los ataques (tanto en tipo de ataque como en número de ataques) contra la infraestructura de una organización y detecta principalmente aquellos ataques que van dirigidos contra el *firewall* de la red.



Esta ubicación también implica una serie de desventajas:

- No detecta ataques con información encriptada.
- El NIDPS, si está mal diseñado, se puede saturar debido al elevado tráfico de red que acontece en esta zona de la infraestructura de la red.
- El exceso de información producido por el elevado tráfico de red puede ser contraproducente, ya que puede ser más difícil localizar la información importante y, por lo tanto, los ataques efectivos.
- No ofrece un elevado grado de protección ya que si algún intruso lo localiza puede dirigir sus ataques directamente a él.

No todo son ventajas, también hay que tener en cuenta una serie de desventajas:

- Solo se monitoriza el tráfico que haya entrado realmente en la red. Al estar situado posteriormente al cortafuegos, los datos que le llegan han sido previamente filtrados por la barrera *del firewall*.
- En esta ubicación tampoco se pueden identificar los ataques con información encriptada.
- Aunque la seguridad del NIDPS mejora considerablemente al estar situado a continuación del cortafuegos, esta sigue sin ser suficiente: hay que utilizar medidas de seguridad adicionales.

Detrás del cortafuegos o firewall

El sistema NIDPS se sitúa entre la red externa y la red interna en una zona llamada DMZ (zona desmilitarizada).



Esta localización permite comprobar la totalidad de los ataques que se producen en la red de la organización, tanto exitosos como no exitosos. Como ventajas de localizar los sistemas en esta zona destacan:

- En esta ubicación se monitorizan aquellas intrusiones que consiguen atravesar el cortafuegos o firewall.
- Los ataques detectados son potencialmente mucho más peligrosos que los detectados en otras ubicaciones, por lo que el riesgo de ataques exitosos disminuye considerablemente.
- Al poder identificar los ataques más comunes permite una configuración más efectiva del cortafuegos principal.
- La cantidad de logs es inferior, pero la información facilitada por estos sistemas está mejor seleccionada y es más relevante.

No todo son ventajas, también hay que tener en cuenta una serie de desventajas:

- Solo se monitoriza el tráfico que haya entrado realmente en la red. Al estar situado posteriormente al cortafuegos, los datos que le llegan han sido previamente filtrados por la barrera del firewall.
- En esta ubicación tampoco se pueden identificar los ataques con información encriptada.
- Aunque la seguridad del NIDPS mejora considerablemente al estar situado a continuación del cortafuegos, esta sigue sin ser suficiente: hay que utilizar medidas de seguridad adicionales.

Combinación de los dos anteriores

Una opción muy válida que contrarresta las desventajas de la ubicación del sistema de detección y prevención de intrusiones antes o después del cortafuegos es la combinación de ambas: situar sistemas antes y después del cortafuegos.



Esta combinación reúne las ventajas de las dos ubicaciones y además, proporciona otras adicionales:

- Hay un mayor control de las posibles intrusiones en la red.
- En el supuesto de que se deje pasar tráfico que no se debe, esta combinación permite ir mejorando la seguridad a través del aprendizaje.

- Permite una correlación entre los ataques detectados antes y después del cortafuegos. Como desventaja principal destaca el coste que implica la colocación de dos máquinas para implementar estos sistemas en dos ubicaciones.

Combinación firewall/NIDPS

Cuando la organización no dispone de máquinas suficientes para que haya una de ellas destinada exclusivamente a la detección y prevención de intrusiones, una buena alternativa es utilizar un equipo que funcione como cortafuegos y NIDPS a la vez.

Con esta opción se monitoriza todo el tráfico de la red con las ventajas y desventajas que ello implica, pero se reduce el gasto al ser necesaria una inversión menor por un solo equipo.

Equipo utilizado como cortafuegos y NIDS



Ubicación en las redes principales de la organización

Otra opción, independientemente de si se ubica el IDS/IPS antes o después del cortafuegos, es decidir entre ubicarlo en las redes principales de la organización o bien situarlo solo en las redes más críticas y valiosas.

La ubicación en las redes generales de la organización monitoriza una cantidad más elevada de tráfico, lo que aumenta las posibilidades de encontrar posibles ataques. Además, también permite detectar aquellos ataques que se producen dentro de la misma red interna de la organización, normalmente ocasionada por empleados y otro personal interno.

Aun así, también presenta una serie de desventajas:

- Tampoco se detectan ataques con información encriptada.
- Los sistemas situados en las redes generales pueden hacerlas más vulnerables ante ataques internos producidos dentro de la misma red.

Ubicación en las redes críticas de la organización

En numerosas ocasiones la información más valiosa de una organización no se almacena en sus redes generales, sino que utilizan otras subredes separadas para aumentar su nivel de seguridad y ser tratados de un modo acorde con su valor.

De este modo, la ubicación de los IDS/IPS en estas redes permite la detección y prevención de los ataques realizados específicamente contra los datos críticos y añaden un nivel de seguridad adicional a los mismos, minimizando aún más los posibles riesgos de ataques. general de la organización.

2.2.- Sistemas de detección y prevención de intrusiones en equipos (hosts) o HIDPS

Los sistemas de detección y prevención de intrusiones basados en *hosts* son los que residen en el mismo equipo que monitorizan y solo se preocupan de proteger a dicho equipo sin necesidad de monitorizar todo el tráfico de la red de una organización. Consumen menos recursos que los NIDS o NIDPS y no impiden un buen rendimiento del sistema.

Aunque implican un mejor rendimiento del sistema, estos tipos de sistema combaten las intrusiones una vez que el equipo ya está en peligro, lo que el riesgo es bastante mayor. Además, implica unas mayores medidas de seguridad en el equipo para combatir los ataques.

Los IDPS basados en *hosts* monitorizan con más profundidad los datos del equipo (que puede ser un servidor, ordenador o, incluso, alguna aplicación específica) que los IDPS basados en red como, el tráfico inalámbrico, el tráfico de red, los accesos a los archivos, los cambios de configuración en el equipo o en alguna aplicación, etc.

Aun así, y del mismo modo que en los demás sistemas mencionados, tampoco detecta los ataques con información encriptada.

2.3.- IDS/IPS en ambientes virtuales

La utilización de ambientes virtuales (información en "la nube") es cada vez mayor debido a sus numerosas ventajas:

- Hay un ahorro de energía al ser necesaria una infraestructura menor en la organización para almacenar datos.
- Suponen un coste reducido de mantenimiento, permitiendo así que los equipos tengan mayor capacidad de almacenamiento y reduciendo también el espacio físico y la reducción de costes que ello implica (menos gastos de electricidad, menos gastos de alquiler de local, etc.).

Definición**Ambientes virtuales**

Son un conjunto de herramientas de *software* que facilitan a los usuarios y organizaciones el almacenamiento de aplicaciones y datos en infraestructuras externas de la organización por un reducido coste de servicio.

El nivel de seguridad en este tipo de sistemas es bastante elevado al estar las estructuras físicas situadas fuera de la organización. Además, al utilizar soluciones de detección y prevención de ataques facilitadas por proveedores que ofrecen servicio a muchas otras organizaciones, la base de datos de posibles vulnerabilidades y ataques es mucho mayor y hay más posibilidad de detección y reacción.

2.4.- IDS/IPS inalámbricos o wireless IDS/IPS

Este tipo de sistemas analizan los protocolos inalámbricos para detectar las actividades sospechosas.

Su funcionamiento es igual a los IDPS basados en red, con servidor, consola y base de datos y permite la monitorización del tráfico de red que circula por la red inalámbrica de la organización.

Como desventaja principal cabe señalar que los análisis de estos sistemas se limitan a un solo canal, por lo que si la organización utiliza varios canales inalámbricos no podrán realizarse análisis de todos los canales simultáneamente.

2.5.- Decisiones de la organización para ubicar un sistema de detección y prevención de intrusiones

Una vez vistas varias opciones de ubicación de los sistemas de detección y prevención de intrusiones queda bastante claro que en el momento de decidir cuál de ellos implantar en la organización es necesario realizar un análisis previo y profundo que incluya varios aspectos:

- Análisis de los procesos de negocio e identificación de la información valiosa en cada uno de los procesos.
- Análisis de los protocolos de red utilizados para transferir datos entre los equipos de la organización y al exterior.
- Análisis de los protocolos y políticas de la organización para ser coherentes con su política de seguridad y su política de costes en el momento de implantar el sistema IDS/IPS apropiado.

- Análisis de las distintas zonas que forman parte de la organización y la ubicación de sus equipos y servidores para ver qué ubicación del IDS/IPS puede ser más conveniente según sus características.
- Análisis de los servicios que ofrece la organización para averiguar cuáles de ellos necesitan un nivel de seguridad especial debido a la tipología de información con la que trabajan.

Una vez realizados todos estos análisis ya se puede planificar el proceso de implantación de los sistemas de seguridad. No obstante, y como se ha repetido ya varias veces, los sistemas IDS/IPS no deben ser los únicos sistemas de seguridad implantados siendo necesarias otras medidas como *antivirus, firewalls*, etc.

3. DEFINICIÓN DE POLÍTICAS DE CORTE DE INTENTOS DE INTRUSIÓN EN LOS IDS/IPS

Una vez tomada la decisión sobre el sistema IDS/IPS que se va a implantar en la organización hay que definir una serie de políticas sobre el tipo de respuesta que debe tomar cuando haya algún intento de intrusión o ataque.

Antes de comentar las distintas políticas de corte de intentos de intrusión en los IDS/IPS es fundamental conocer los diversos tipos de análisis que realizan estos sistemas para entender sus diferentes modos de funcionamiento.

Hay dos tipos fundamentales de análisis:

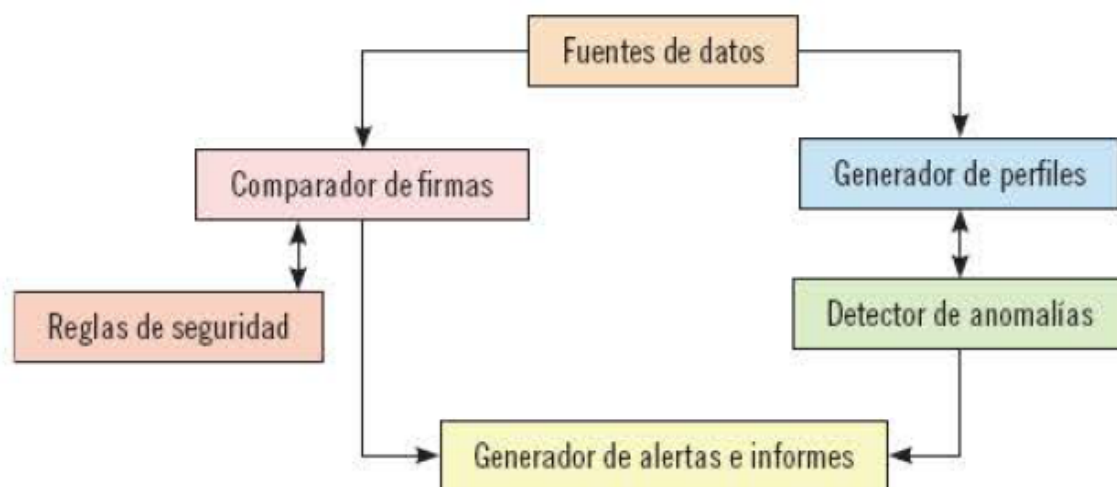
- Detección de usos indebidos (*misuse*): los IDS/IPS utilizan una base de datos para encontrar usos indebidos mediante la comparación de las firmas de la base de datos con la información recogida previamente.
- Detección de anomalías: en este caso no se utiliza una base de datos como elemento de comparación, sino que se emplean técnicas estadísticas para definir y aproximar los patrones que se corresponden con un comportamiento normal.

Nota

Las firmas en IDS/IPS se refieren a los patrones de ataques conocidos, patrones que se han repetido en varias ocasiones y que se han confirmado como comportamientos maliciosos.

En la siguiente figura se puede observar el funcionamiento de los dos tipos de análisis en los sistemas de detección de intrusiones.

Tipos de análisis de detección de intrusiones



Lo habitual en las organizaciones es que se utilice una combinación de ambos tipos de análisis para minimizar el riesgo y poder detectar todo tipo de ataques, tanto los más comunes como los más inusuales.

Otra manera de distinguir los tipos de análisis de los sistemas de detección y prevención de intrusiones es teniendo en cuenta el tiempo de realización de los análisis, distinguiendo entre:

- **Análisis por lotes (*batch mode*):** el análisis de los datos para detectar intrusiones se realiza cada cierto intervalo de tiempo definido. Al finalizar cada período de tiempo el sistema realiza el análisis de los datos recibidos en ese período. Tiene como inconveniente principal que las posibles alarmas de las intrusiones sucedidas no se hacen en tiempo real, sino que se originan después de haberse producido las intrusiones.
- **Análisis en tiempo real:** en este tipo de análisis se examinan los datos conforme se van recibiendo a tiempo real o con un retardo mínimo de tiempo. Son más utilizados ya que posibilitan responder a las posibles intrusiones a la misma vez que se van detectando.

En la siguiente tabla se resumen los distintos tipos de análisis de un sistema de detección y prevención de intrusiones:

Análisis de los datos obtenidos por los IDS/IPS	
Clasificación del análisis	Tipo de análisis
Según el procedimiento de análisis de los datos	Detección de usos indebidos
	Detección de anomalías
Según el tiempo del análisis	Análisis por lotes
	Análisis a tiempo real

Ante estos tipos de análisis las organizaciones pueden definir cuándo quieren que se realice la detección y qué tipo de detección se quiere implementar.

El siguiente paso consiste en definir las políticas de actuación del sistema IDS/IPS cuando se detecta algún intento de intrusión.

En general, una política de seguridad define las directrices de lo que se va a permitir y lo que se va a prohibir en un sistema de información.

De este modo se puede distinguir entre dos líneas actuación en cuanto a políticas de seguridad:

- **Política prohibitiva:** política en la que se prohíbe todo lo que no se ha definido como permitido expresamente.
- **Política permisiva:** esta política es todo lo contrario. En la política permisiva se define todo lo que se va a prohibir y todo lo demás se considera permitido.

Lo más habitual en las organizaciones en cuanto a políticas de seguridad es utilizar políticas permisivas, ya que las prohibitivas son demasiado restrictivas y pueden ocasionar bloqueos de acciones rutinarias o básicas que se pueden haber pasado por alto en la definición de las permisiones.

3.1.- Políticas de corte de intrusiones en sistemas IDS/IPS

En cuanto a los sistemas de detección y prevención de intrusiones, cuando se detecta alguna intrusión se pueden definir dos tipos de políticas de corte de intrusiones:

- Políticas de respuesta pasiva.
- Políticas de respuesta activa.

Políticas de respuesta pasiva

En estas políticas, cuando se detecta una intrusión, el sistema se limita a registrar y a emitir una alarma del ataque detectado. No se realiza ninguna acción para cambiar el curso del ataque.

Algunos ejemplos de políticas de respuesta pasiva son los siguientes:

- Envío de un correo electrónico a uno o varios usuarios: cuando se detecta una intrusión se envía un correo electrónico a uno o varios usuarios informando de esta intrusión.
- Registro del ataque: se almacenan los detalles de la alerta (fecha del ataque, hora, IP del intruso, IP del destino, protocolo utilizado, etc.) en una base de datos.
- Almacenamiento de paquetes sospechosos: se almacenan todos los paquetes de datos que originaron la alerta.
- Apertura de una aplicación: cuando hay algún intento de intrusión se abre una aplicación que realiza una acción específica como el envío de mensajes de texto o la emisión de algún sonido, entre otras.
- Notificación visual: cuando se produce un intento de intrusión se emite una notificación visual en las consolas de administración.

- Envío de una trampa SNMP a un hipervisor externo: se emite un mensaje de alerta (trampa) en protocolo SNMP a una consola externa.

Políticas de respuesta activa

El sistema de detección y prevención cuando detecta una intrusión, además de generar una alarma y remitirla al responsable, modifica el entorno para evitar que la intrusión tenga éxito.

Algunos ejemplos de políticas de respuesta activa ante ataques se describen a continuación:

- Envío de un *ResetKill*: en el momento de la detección de la intrusión se envía un paquete de alerta que fuerza la finalización de la conexión evitando que el atacante consiga entrar en el equipo.
- Reconfiguración de dispositivos externos: al detectarse el ataque se envía un comando para que el dispositivo externo se reconfigure de inmediato y pueda bloquear el intento de ataque.

En la tabla siguiente se pueden observar los distintos tipos de políticas de corte de intrusiones con sus respectivos ejemplos:

Políticas de corte de intrusiones	
Políticas de respuesta pasiva: se limitan a registrar los datos del intento de intrusión.	Políticas de respuesta activa: registran los datos del intento de intrusión e intentan evitarlo.
Envío de correo electrónico.	Envío de un <i>ResetKill</i> .
Envío de trampas SNMP a consolas externas.	Reconfiguración de los dispositivos externos.
Registro del ataque.	
Almacenamiento de los paquetes de datos sospechosos.	
Apertura de una aplicación.	
Notificación visual de una alerta.	

4. ANÁLISIS DE LOS EVENTOS REGISTRADOS POR EL IDS/IPS PARA DETERMINAR FALSOS POSITIVOS Y CARACTERIZARLOS EN LAS POLÍTICAS DE CORTE DEL IDS/IPS

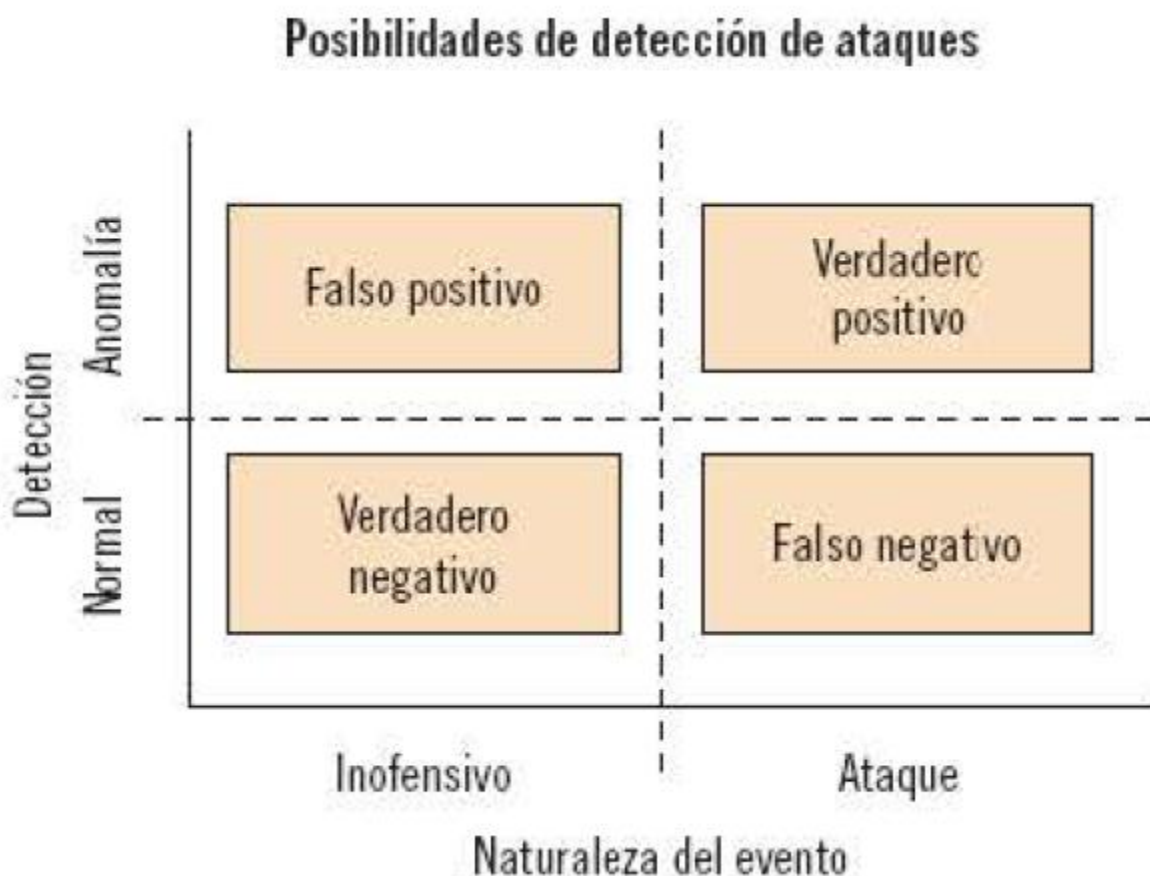
El análisis de los distintos eventos registrados en el sistema por los IDS/IPS no es impecable: es habitual que la base de datos de firmas esté desactualizada y que los métodos estadísticos de detección de comportamientos indebidos no sean perfectos.

Por ello es común que cuando los sistemas de detección y prevención de intrusiones toman decisiones sobre si un evento debe considerarse o no un ataque, se equivoquen.

En el momento de la toma de decisión de si un evento es efectivamente un ataque o no puede haber cuatro posibilidades:

- **Detección de falso positivo o falsa alarma:** cuando el IDS/IPS detecta como ataque el tráfico de datos que en verdad es inofensivo.
- **Falso negativo:** ataque que no es detectado por el IDS/IPS.
- **Verdadero positivo:** evento inofensivo que el IDS/IPS ha detectado como tráfico de red normal.
- **Verdadero negativo:** ataque detectado correctamente por el IDS/IPS.

Así, en la siguiente figura se muestran las distintas posibilidades en cuanto a la detección de ataques en los IDS/IPS.



Ante estas posibilidades el objetivo que debe establecerse en un IDS/IPS es minimizar el número de errores (falsos positivos y falsos negativos) en la detección y maximizar el número de aciertos (verdaderos positivos y verdaderos negativos) por varios motivos:

- Un elevado nivel de falsos positivos y negativos puede difuminar los motivos por los que se implantó el IDS/IPS, obteniendo bajos niveles de efectividad del sistema.

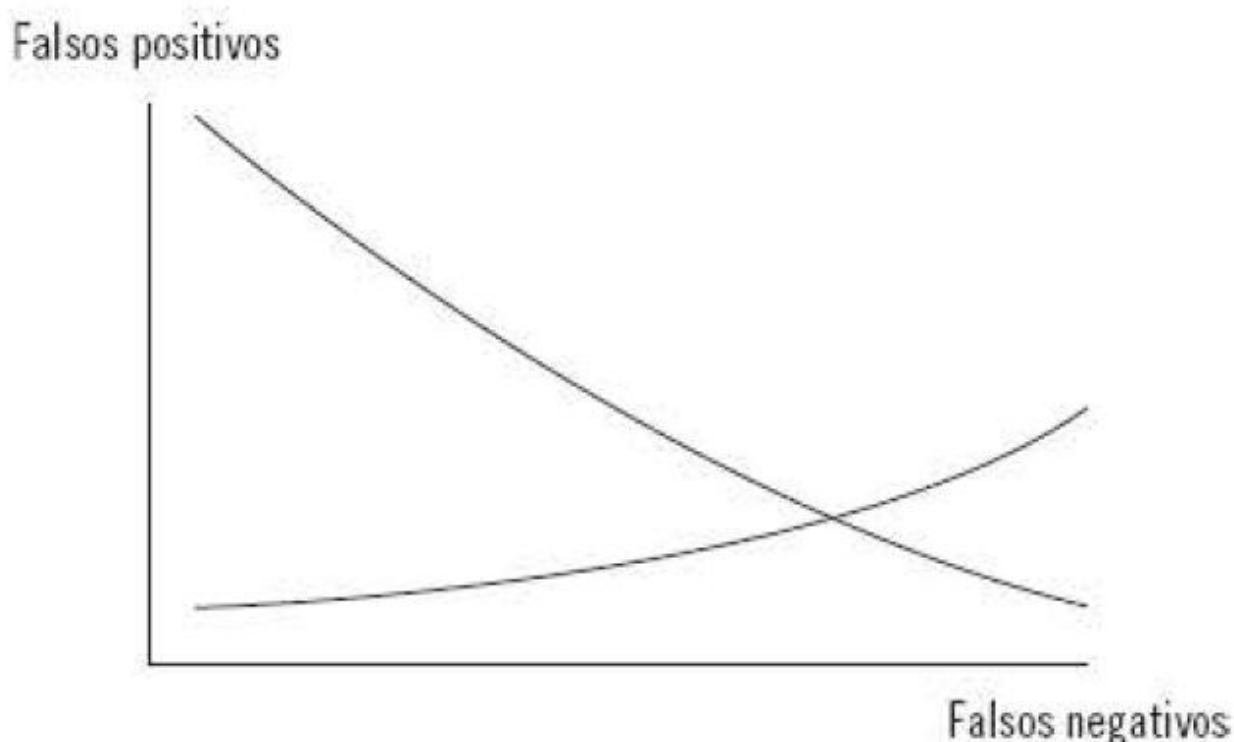
- Los falsos positivos ocupan tiempo y recursos cuando el IDS/IPS genera alarmas cuando no debe.
- La no detección de ataques (falsos negativos) puede tener graves consecuencias en la información de la organización.

Así, viendo los efectos que tiene la configuración establecida en el sistema de detección y prevención de intrusos y viendo los falsos positivos y los falsos negativos que se generan, se pueden realizar modificaciones en la configuración para conseguir la más adecuada y que trabaje con un mayor rendimiento según las características de la infraestructura de red y sus necesidades.

Para comprobar las configuraciones hay que realizar varias pruebas de referencia sobre distintas configuraciones para que se puedan hacer comparaciones de los resultados: con el análisis de las diferencias de los resultados obtenidos con las diversas configuraciones se puede detectar y eliminar la causa que provoca los falsos positivos y negativos.

Por ejemplo, de las alarmas generadas por las distintas configuraciones se puede obtener información sobre si estas se producen por un ataque real, un falso positivo o si puede determinar algún falso negativo.

El objetivo a perseguir con la configuración del IDS/IPS es conseguir un equilibrio entre los falsos positivos y los falsos negativos, consiguiendo localizarse en el cruce de las tasas de falsos positivos y negativos mostrado en el gráfico siguiente:



El gráfico de la imagen es un modelo de la tasa de error en un IDS/IPS, representando lo que ocurre cuando se reduce la sensibilidad del sistema para emitir alertas y cuando se incrementa la cantidad de paquetes inspeccionados:

- A mayor sensibilidad del sistema, mayor posibilidad de detección de falsos positivos y menor aparición de falsos negativos.
- A menor sensibilidad, menor detección de falsos positivos y mayor aparición de falsos negativos.
- A mayor cantidad de paquetes inspeccionados, mayor posibilidad de detectar falsos positivos y menor aparición de falsos negativos.
- A menor cantidad de paquetes inspeccionados, menor posibilidad de detección de falsos positivos y mayor aparición de falsos negativos.

En conclusión, en el momento de decidir la configuración de un IDS/IPS hay que encontrar a través de varias pruebas el equilibrio entre la sensibilidad del sistema y la cantidad de datos a inspeccionar, atendiendo a las necesidades de cada organización e intentando conseguir el mayor rendimiento posible.

Como recomendación, en el momento de realizar las pruebas de configuración hay que tener en cuenta algunas de las causas más frecuentes de falsos positivos:

1. **Actividad del sistema de supervisión de red:** en ocasiones, las empresas utilizan sistemas de supervisión de redes para obtener registros de la actividad que hay en sus sistemas. Muchos sistemas de detección y prevención de intrusos suelen clasificar esta actividad como hostil o sospechosa cuando en verdad es inofensiva. Como solución se recomienda configurar el IDS/IPS eliminando las alertas de este tipo de la base de datos.
2. **Escaneo de vulnerabilidad y escáneres de puertos de red:** cuando se pretende realizar una prueba de vulnerabilidad de la red o un escáner de sus puertos el IDS/IPS lo suele detectar como ataque, ya que su funcionamiento es muy similar al utilizado por los piratas informáticos en sus ataques. Se recomienda desactivar el IDS/IPS momentáneamente cuando se realiza este tipo de actividades.
3. **Actividad del usuario:** en muchos IDS/IPS viene configurado por defecto la emisión de alarmas ante comportamientos del usuario que considera como "peligrosos": compartir archivos punto a punto o utilización de mensajería instantánea, entre otras. Para evitar que se generen estas alertas es recomendable configurar específicamente las alarmas eliminando estas casuísticas.
4. **Comportamientos similares a troyanos o gusanos:** en ocasiones, la misma organización realiza acciones que son similares a las que ejecutan los gusanos o los troyanos y emite alarmas cuando realmente son acciones inofensivas. En este caso no se recomienda desactivar las alarmas, ya que dejaría al equipo desprovisto de mecanismos de detección de ataques reales de troyanos y gusanos.
5. **Cadenas largas de registro web:** hay alertas que se generan por la detección de cadenas de registro web largas, ya que algunos ataques las utilizan para desbordar la memoria del equipo y así poder acceder a su sistema. Aunque en la actualidad hay muchas webs que

utilizan cadenas largas de un modo habitual no se recomienda desactivar las alertas de su detección, ya que permitiría el acceso de ataques potencialmente dañinos.

6. **Actividad de autenticación de base de datos:** los sistemas de detección y prevención de intrusiones suelen analizar la actividad administrativa de las bases de datos porque consideran que una elevada actividad puede ser un indicio de estar sufriendo algún ataque.

Si la organización utiliza bases de datos en continua actualización y con un elevado nivel de actividad administrativa, se recomienda desactivar estas alertas para reducir el número de falsos negativos.

Si aun así se siguen teniendo dudas sobre la configuración ideal para el sistema de detección y prevención de intrusiones, hay dos metodologías de libre configuración que se utilizan para evaluar y realizar test de los distintos elementos de seguridad de una organización, entre ellos los sistemas IDS/IPS:

- Metodología OSSTM (*Open Source Security Testing Methodology*): la metodología de testeo de seguridad de código abierto ha sido elaborada por el Instituto para la Seguridad y Código Abierto (ISECOM) y ofrece una metodología de evaluación de sistemas de seguridad, sobretodo de cortafuegos e IDS/IPS.
- Metodología OSEC (*Open Security Evaluation Criteria*): el Criterio de Evaluación de Código Abierto es similar al OSSTM pero está concentrado fundamentalmente en estandarizar productos de seguridad relativos a los NIDS y a los cortafuegos.

Aparte de estas metodologías también se pueden encontrar varias herramientas de libre distribución capaces de generar elevadas cantidades de falsos ataques que pueden facilitar a la organización la configuración de los sistemas IDS/IPS. Muchas de ellas también son capaces de utilizar las propias reglas del IDS/IPS para realizar la evaluación de su capacidad de detección. Algunas de estas herramientas se muestran a continuación:

- **IDSWakeup:** genera falsos ataques desde direcciones IP que pueden ser tanto aleatorias como específicas para comprobar si el sistema IDS/IPS los detecta correctamente.
- **Sneeze:** también es un generador de falsos positivos, en este caso diseñado específicamente para Snort.
- **Stick:** herramienta que se utiliza para evaluar la capacidad del sistema para detectar intrusiones y testear las reglas del IDS y del cortafuegos.
- **Ftester:** esta herramienta envía ataques de red a equipos remotos.


```
4. / IDSWakeUp C 127.0.0.1 1 1

- IDSWakeUp: generador de falsos positivos
- Stéphane Robert
- Harve Schuster Consultants (c) 2000

- - - - -

src_addr: 0 dst_addr: 127.0.0.1 nbt: 1 ttl: 1

enviando: lágrima ...
enviando: la tierra ...
enviando: get.php ...
enviando: bind_version ...
enviando: get.php syn ack get ...
enviando: ping_of_death ...
enviando: synflood ...
enviando: synflood ...
enviando: xll ...
enviando: RMingpro ...
enviando: smtp_expn_root ...
enviando: finger redirect ...
enviando: ftp_cwr_root ...
enviando: ftp_port ...
enviando: trim00 pong ...
enviando: back_office ...
enviando: nasade ...

245.140.219.144 -> 127.0.0.1 80/tcp GET / needed / needed.dll HTTP/1.0
envio: www.ftp ...
225.158.207.188 -> 127.0.0.1 80/fragmented-tcp
GET / ... HTTP/1.0
101.114.219.120 -> 127.0.0.1 80/fragmented-tcp
GET / ... HTTP/1.0
AAAAA...
AAAAA...
.. AAAAA... / cgi-bin / php HTTP/1.0
envio: www.pastor ...
137.74.747.148 -> 127.0.0.1 80/tcp GET / HTTP/1.0
100.90.03.56 -> 127.0.0.1 80/tcp GET / / / / / HTTP/1.0
215.174.111.124 -> 127.0.0.1 80/tcp CAMEL / HTTP/1.0
101.146.51.80 -> 127.0.0.1 80/tcp CAMEL / /
137.126.215.76 -> 127.0.0.1 80/tcp / cgi-bin \ \ manager
101.226.235.216 -> 127.0.0.1 80/tcp / cgi-bin \ \ webdist.cgi
241.70.55.180 -> 127.0.0.1 80/tcp / mlog.phpml
49.155.75.176 -> 127.0.0.1 80/tcp / mlog.phpml
137.06.207.116 -> 127.0.0.1 80/tcp / CTIDE \ \ administrator \ \ startstop.html
83.90.147.104 -> 127.0.0.1 80/tcp / stopman \ \ index.htm
201.110.175.126 -> 127.0.0.1 80/tcp / mail_log_files \ \ order.log
221.226.155.208 -> 127.0.0.1 80/tcp / admin_files \ \ order.log
137.222.71.244 -> 127.0.0.1 80/tcp / cgi-bin \ \ wrdp
85.82.147.96 -> 127.0.0.1 80/tcp GET / cgi-bin/php66 HTTP/1.0
97.230.198.92 -> 127.0.0.1 80/tcp GET / HTTP/1.0 schnc.lnk
221.74.227.112 -> 127.0.0.1 80/tcp GET / HTTP/1.0 schnc.bot
201.226.207.124 -> 127.0.0.1 80/tcp GET / HTTP/1.0 schnc.url
69.194.171.192 -> 127.0.0.1 80/tcp GET / HTTP/1.0 schnc.ida
145.94.159.65 -> 127.0.0.1 80/tcp GET / default.asp : : $ HTTP/1.0 DATOS
60.215.155.216 -> 127.0.0.1 80/tcp GET / HTTP/1.0
65.166.87.92 -> 127.0.0.1 80/tcp GET / scripts / cmd.exe HTTP/1.0
132.156.155.192 -> 127.0.0.1 80/tcp GET / scripts / cmd.exe HTTP/1.0
```

Alertas generadas por IDSWakeUp

5. RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL IDS/IPS NECESARIOS PARA MONITORIZAR Y SUPERVISAR SU CORRECTO FUNCIONAMIENTO Y LOS EVENTOS DE INTENTOS DE INTRUSIÓN

Los registros de auditoría son aquellos en los que se registran las acciones realizadas por los usuarios en un sistema. Estos registros son vitales para las organizaciones, ya que cuando se produce un incidente de seguridad facilitan información sobre el usuario que haya podido cometer la infracción. El registro de auditoría no solo contiene información de los usuarios, sino que también contiene información importante sobre las infracciones de seguridad sucedidas en el sistema.

Los administradores de seguridad, por tanto, deben realizar análisis periódicos de los registros de auditoría para comprobar si la seguridad de la infraestructura de red o del equipo es la adecuada y

tomar medidas al respecto en caso de no serlo. De este modo se pueden ir ajustando los niveles de seguridad e ir detectando los defectos de seguridad que suceden en el equipo.

No obstante, hay que remarcar que no todos los registros de auditoría ponen de manifiesto fallos de seguridad. La gran mayoría de estos son meramente informativos. Por ejemplo, cuando un usuario ha intentado acceder al sistema sin éxito se genera un registro de error pero no significa que haya un fallo de seguridad, simplemente informa del intento de acceso del usuario sin más.

En el momento de establecer la política de auditoría hay que realizar un análisis previo para que la política implantada sea la adecuada. Si se auditan demasiados tipos de eventos puede sobrecargarse el sistema y reducir su rendimiento, por ello se recomienda la auditoría de solo aquellos eventos que faciliten información útil para evaluar la seguridad del sistema.

Así, para la definición de la política de auditoría se plantean una serie de recomendaciones:

- Determinar los equipos y dispositivos en los que se va a configurar la auditoría.
- Determinar los eventos que se quieren auditar (por ejemplo los accesos a archivos y carpetas, el inicio de sesión de los usuarios, el encendido del servidor, etc.).
- Determinar si se quiere auditar el éxito del evento, el fallo del evento o ambos casos.
- Determinar la necesidad real de auditar las tendencias de uso del sistema.
- Determinar la periodicidad de las revisiones de los registros de seguridad.

Un registro de auditoría puede clasificarse en una de las categorías mostradas en la tabla siguiente:

Categoría del registro	Descripción
Error	Para eventos de seguridad importantes.
Advertencia	Para eventos que no son importantes pero que pueden causar algún problema en un futuro.
Información	Para operaciones realizadas con éxito.
Auditoría correcta	En eventos ocurridos cuando la auditoría se ha realizado correctamente.
Auditoría incorrecta	En eventos ocurridos cuando ha habido algún fallo de auditoría.

Sea de la categoría que sea, un evento en el registro de auditoría contiene información sobre:

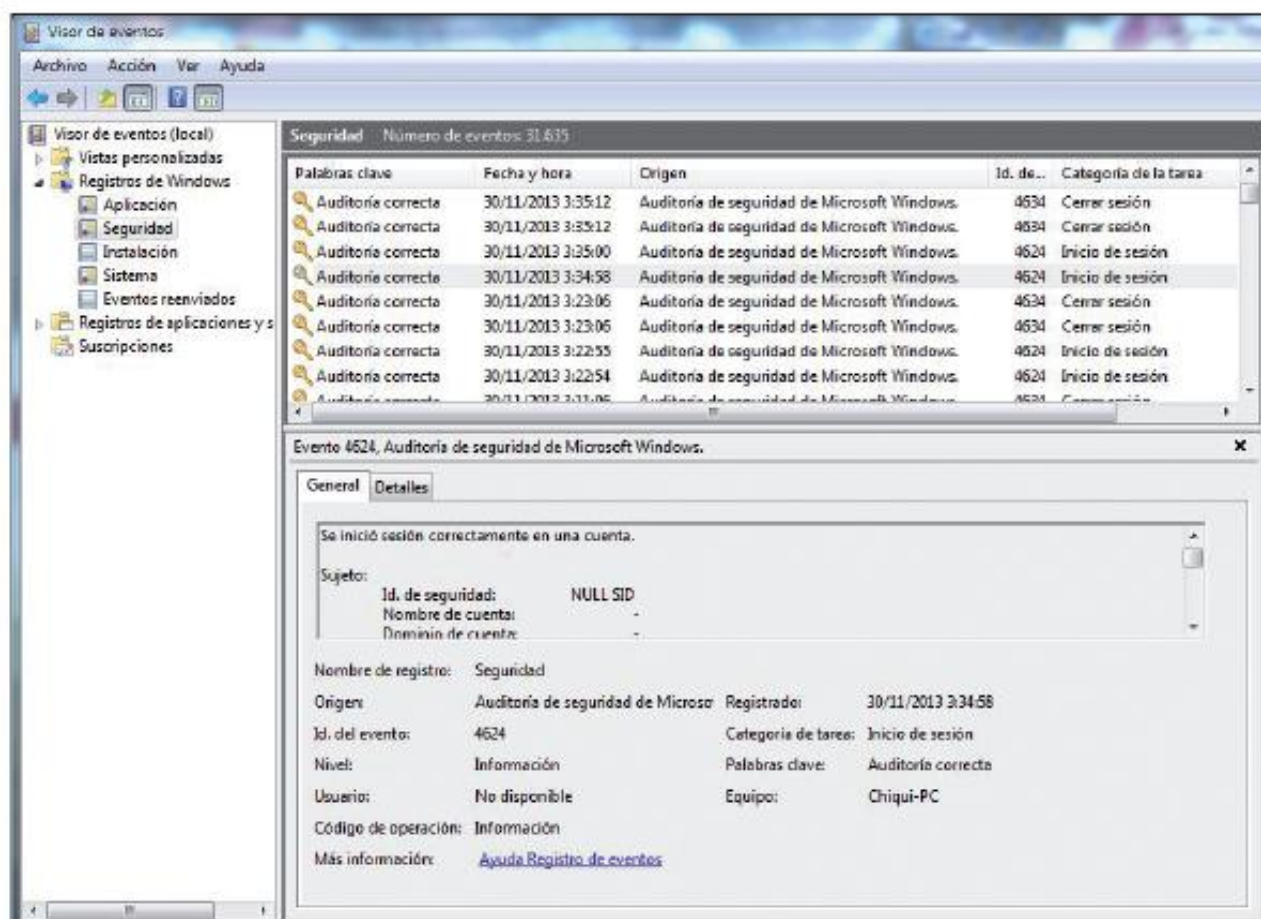
- La acción realizada.
- El usuario que ha realizado la acción.
- El éxito o fracaso del evento.
- Cuándo se ha producido el evento.
- Información adicional como, por ejemplo, el sistema desde el que se realiza la acción.

Como ya se ha comentado en el capítulo anterior, el acceso a los registros del sistema (tanto de seguridad como otros) en *Linux* se hace a través de varios comandos dependiendo del tipo de información del evento que se pretende obtener.

Para ver los registros de seguridad del sistema hay que acceder al archivo de registro de seguridad con el comando `tail -f /var/log/secure` (si solo se quieren ver las últimas líneas del registro) o con el comando `less +F /var/log/secure` (si se quiere ver el archivo de registro completo).

En *Windows* esta información se obtiene a través del "Visor de eventos" accediendo a Inicio -> Panel de Control -> Herramientas administrativas-> Visor de eventos.

En la pestaña Seguridad dentro de Registros de Windows se pueden ver específicamente los registros de seguridad con toda la información detallada.



Visor de eventos en Windows, registros de seguridad

5.1.- Relación de los registros de auditoría del IDS/IPS necesarios para un correcto control de intrusiones

Una vez visto el modo en el que están monitorizados los eventos de auditoría es imprescindible conocer cuáles son los eventos fundamentales que las organizaciones deben auditar para que la detección y prevención de intrusiones en un IDS/IPS sea lo más eficiente posible.

A continuación se describen los elementos imprescindibles que deben ser sometidos a auditoría.

Sucesos de inicio de sesión de cuenta

Es necesario configurar los IDS/IPS para que auditen los intentos de inicio de sesión de cuenta, tanto exitosos como no exitosos. Eso sí, en el momento de su configuración hay que decidir en la política de corte de ataques si se quieren auditar solo los intentos exitosos, los intentos fracasados, ambos o si directamente se decide omitir esta auditoría.

Las auditorías de inicios de sesión con éxito sirven sobre todo para poder comprobar qué ha realizado cada usuario y descubrir quién es el responsable de cualquier incidente de seguridad en el momento de su investigación: se puede comprobar quién accedió, cómo consiguió acceder y en qué equipo accedió.

Las auditorías de inicios de sesión sin éxito también resultan muy útiles para detectar intentos de intrusiones y prevenir futuros intentos.

Administración de cuentas

En estos registros de auditoría se reflejan los distintos sucesos de administración de cuentas de un equipo como, por ejemplo:

- Cuando se crea, modifica o se elimina alguna cuenta de usuario.
- Cuando se modifica alguna contraseña.
- Cuando se activa o desactiva alguna cuenta de usuario.
- Cuando se modifica el nombre de alguna cuenta de usuario.

Del mismo modo que en los registros de auditoría de inicio de sesión, también se puede decidir que el IDS/IPS elabore registros sobre los intentos exitosos, no exitosos o ambos.

Las auditorías de sucesos exitosos de administración de cuentas son muy útiles para comprobar todos los cambios producidos en las cuentas de usuario del sistema y deberían estar siempre habilitados para llevar un seguimiento de la evolución de las cuentas y de los usuarios responsables.

Sucesos de inicio de sesión

Los registros de auditoría de sucesos de inicio de sesión facilitan información de los eventos generados cada vez que un usuario inicia o cierra una sesión, además de cada vez que se realiza alguna conexión de red al equipo.

La decisión de registrar los eventos de inicio de sesión exitosos puede ser de gran utilidad, ya que se obtiene información sobre el usuario que consigue registrarse en cada equipo en el momento de investigar algún incidente de seguridad. Los registros de inicios de sesión sin éxito también son útiles (al igual que en los sucesos de inicio de sesión de cuenta) para detectar intentos de acceso de intrusos.

Nota

Hay que diferenciar los sucesos de inicio de sesión de cuenta con los sucesos de inicio de sesión. Los sucesos de inicio de sesión de cuenta hacen referencia a los intentos de acceso al equipo local a través de la red. Sin embargo, los sucesos de inicio de sesión son aquellos registrados cuando un usuario intenta iniciar la sesión desde el mismo equipo local.

Acceso a objetos

Los registros de auditoría de acceso a objetos contienen información sobre los accesos de un usuario a cualquier tipo de objeto del sistema (como carpetas, archivos, dispositivos, etc.) que esté incluido en una lista de control predefinida por el administrador.

Del mismo modo que en las anteriores, la organización también puede decidir si registrar los accesos con éxito, los intentos fracasados, ambos o, directamente, no auditar este tipo de sucesos.

Uso de privilegios

Los registros de auditoría sobre el uso de privilegios contienen información de cada evento sucedido cuando un usuario realiza alguna acción bajo unos privilegios que le han sido otorgados previamente.

Algunos de los ejemplos en los que se puede definir la generación de registros de auditoría pueden ser:

- Cuando un administrador realiza copias de seguridad de algún archivo o directorio.
- Cuando un usuario sin privilegios intenta realizar alguna acción para la que no tiene permiso (se genera un registro de error).
- Cuando el usuario con privilegios de administrador restaura algún archivo o directorio.

Seguimiento de procesos

En cuanto al seguimiento de procesos, sus registros de auditoría contienen información detallada de los sucesos ocurridos en el sistema como pueden ser: la activación de alguna aplicación, el acceso o salida a un proceso, etc.

No se recomienda la activación de este tipo de registro de auditoría, ya que debido al elevado número de procesos que acontecen en el sistema puede ser difícil localizar la información de los sucesos más valiosos.

Sucesos del sistema

Los registros de auditoría de los sucesos del sistema facilitan información sobre el reinicio o cierre de un equipo por parte de un usuario o generado por algún suceso que haya afectado a la seguridad del sistema.

Es de gran utilidad activar la generación de este tipo de registros, ya que los sucesos que acontecen son pocos y la información que se puede obtener puede ser de gran valor: siempre es útil conocer por qué se ha reiniciado o apagado el equipo para detectar qué fue lo que falló y poder evitarlo en otras ocasiones.

A modo de resumen, en la siguiente tabla se establecen los registros de auditoría de los ID SIIPS que se recomiendan para que la monitorización y evaluación de su funcionamiento sea la correcta y se pueda realizar un control eficiente de [os eventos generados por intentos de intrusión:

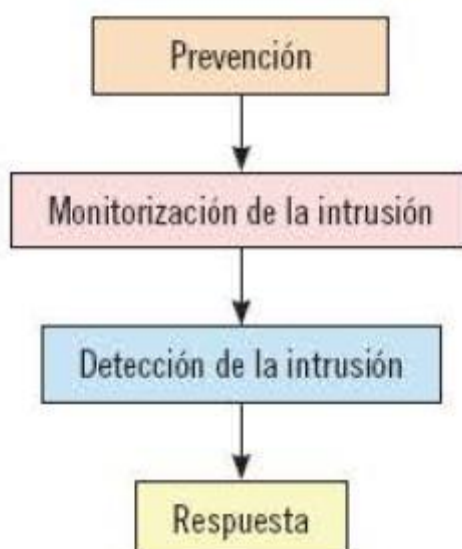
Registro de auditoría	Breve descripción
Sucesos de inicio de sesión de cuenta	En eventos de inicio o cierre de sesión de cuenta a través de la red.
Administración de cuentas	En eventos de modificaciones de las cuentas de usuario.
Sucesos de inicio de sesión	En eventos de inicio o cierre de sesión en equipos locales.
Acceso a objetos	En eventos de acceso a objetos predefinidos en una lista de control.
Uso de privilegios	En eventos de acciones de un usuario bajo unos privilegios asignados.
Seguimiento de procesos	En eventos referentes a cualquier proceso ejecutado en el sistema.
Sucesos del sistema	En eventos de reinicio o cierre de sesión provocados por algún usuario o por algún fallo de seguridad.

6. ESTABLECIMIENTO DE LOS NIVELES REQUERIDOS DE ACTUALIZACIÓN, MONITORIZACIÓN Y PRUEBAS DEL IDS/IPS

Los sistemas de detección y prevención de intrusiones siguen una serie de fases en sus procesos:

- **Prevención:** en un momento inicial, los IDS/IPS intentan evitar los ataques mediante mecanismos que dificulten el acceso de intrusos.
- **Monitorización de la intrusión:** si, a pesar de todas las medidas preventivas ha habido una intrusión o actividad sospechosa, los IDS/IPS detectan esta actividad y monitorizan el tráfico de datos sospechoso para que pueda ser analizado y revisado por el administrador del sistema.
- **Detección de la intrusión:** cuando se ha analizado el tráfico, si el IDS/IPS determina que la actividad sospechosa es efectivamente una intrusión, el sistema genera una alarma para notificar esta intrusión al administrador.
- **Respuesta:** determinada la intrusión como ataque los sistemas IDS/IPS pueden adoptar una serie de medidas que intenten bloquear el acceso del atacante al sistema.

Fases de los procesos de detección y prevención de intrusiones



Para que la implantación se realice correctamente y el funcionamiento del IDS/IPS sea realmente efectivo es necesaria la inclusión de una base de datos de firmas que permita la monitorización de los eventos y su clasificación entre actividades sospechosas, actividades no sospechosas e intrusiones reales.

Cuando la implantación ya está completada es posible que el funcionamiento del sistema no sea el adecuado debido al elevado número de falsos positivos detectados como amenaza o a ciertas intrusiones no detectadas como tal. Para solucionarlo hay que realizar una serie de pruebas (ya descritas en apartados anteriores) que permitan comparar los resultados de varias configuraciones y así conseguir definir la configuración más adecuada a las necesidades de seguridad de la organización.

Aunque ya se haya verificado que el IDS/IPS funciona correctamente, no hay que olvidar realizar comprobaciones y actualizaciones periódicas para detectar la posible obsolescencia de la base de datos de intrusiones o la pérdida de efectividad del sistema implantado.

Aunque la determinación de los niveles adecuados de monitorización, prueba y actualización de los sistemas de detección y prevención de intrusiones dependa de las directrices y requerimientos de cada organización, para medir la eficiencia del sistema IDS/IPS y establecer estos niveles se deben tener en cuenta las características siguientes:

- **Precisión:** la precisión de un sistema IDS/IPS es su capacidad para detectar ataques y diferenciarlos del tráfico normal de una red. Para medir la precisión se utiliza el porcentaje de falsos positivos (el número de veces que se detecta un ataque que es una actividad normal) y el porcentaje de falsos negativos (número de ataques no detectados por el sistema) con la fórmula siguiente:

$$\text{Precisión} = \frac{\text{Ataques reales detectados}}{\text{Ataques reales detectados más falsos positivos}}$$

Debido a que minimizar a la vez los porcentajes de falsos positivos y falsos negativos es prácticamente imposible (ya que cuando se quieren minimizar los falsos negativos se produce un aumento de los falsos positivos al aumentar la sensibilidad del sistema y viceversa), lo ideal es encontrar el equilibrio entre ambos.

En cuanto a la fórmula, la precisión será mayor cuando el ratio obtenido sea 1 o lo más cercano a 1 posible, lo que significará que la gran mayoría de ataques reales detectados son realmente ataques.

- **Rendimiento:** el rendimiento de un sistema de detección y prevención de intrusiones consiste en la cantidad de eventos que el sistema puede analizar. Aunque lo ideal sería que el sistema pudiese analizar todo el tráfico de la red habrá que limitar su rendimiento a lo que permita la capacidad de procesamiento del equipo.

De este modo las organizaciones deberán buscar un equilibrio entre la cantidad de tráfico de red a analizar y la cantidad de recursos que quieren o pueden utilizar para este análisis.

- **Complejidad:** la complejidad de un sistema IDS/IPS se consigue cuando detecta todos los tipos de ataques sucedidos en el equipo. Lo habitual es que estos sistemas no puedan detectar todos los tipos de ataques y sea necesario el establecimiento de otras soluciones que completen esta carencia. Las organizaciones deben conseguir un equilibrio entre la complejidad de un sistema y su precisión para que así se detecte el mayor número posible de ataques sin que haya un exceso de falsos positivos o falsas alarmas.

La fórmula de la plenitud de un sistema se define a continuación:

$$\text{Compleitud} = \frac{\text{Ataques reales detectados}}{\text{Ataques reales detectados más falsos negativos}}$$

En este caso también es recomendable que la ratio obtenida de la fórmula sea lo más próxima a **1** posible, ya que esto indicará que todos los ataques han sido detectados y que los falsos negativos se han reducido al mínimo.

- **Tolerancia a fallos:** la tolerancia a fallos de un IDS/IPS es su capacidad para resistir a los ataques y a los fallos del sistema (cortes de electricidad, etc.). Un IDS debe ser sólido y seguro para que un ataque no pueda inutilizarlo y dejar el sistema expuesto a todo tipo de riesgos.

Además, un IDS/IPS también debe ser capaz de recuperar la configuración establecida, los patrones para detectar intrusiones y los registros y alarma generados anteriormente.

- **Tiempo de respuesta:** el tiempo de respuesta de un IDS/IPS consiste en el período de tiempo que tarda en reaccionar cuando se produce un ataque. Esta reacción puede ser tanto la generación de alarmas como el establecimiento de medidas de corte del ataque.

Está claro que las organizaciones deben configurar estos sistemas para que el tiempo de respuesta sea lo más reducido posible, pues así se conseguirá una mayor efectividad.

7. RESUMEN

Los sistemas de detección y prevención de intrusiones son una potente herramienta para evitar posibles ataques que pueden producirse en la infraestructura de red de la organización. Son sistemas complejos y muy especializados, por lo que es vital que las organizaciones realicen un análisis previo de sus infraestructuras, servicios, equipos, zonas y protocolos utilizados para determinar el sistema a implantar, sus características y configuraciones y su localización dentro de sus instalaciones o a través de entornos virtuales.

Una vez ya tomada la decisión sobre el sistema de detección y prevención de intrusiones que se va a implantar en una organización deben decidirse qué políticas de corte de ataques se van a aplicar cuando se detecte alguna intrusión distinguiendo entre políticas de respuesta pasiva (cuando el sistema se limita a informar de los detalles de la intrusión) y políticas de respuesta activa (cuando el sistema además de informar toma medidas que frenen el ataque).

La siguiente fase en la detección y prevención de intrusiones consiste en analizar los eventos que ha registrado el IDS/IPS y que ha calificado como ataques. Estos sistemas no son perfectos y puede ser que haya falsos positivos y falsos negativos. Por ello, las organizaciones deben configurar sus sistemas para que el número de errores sea el mínimo posible consiguiendo un equilibrio entre la sensibilidad del sistema y la cantidad de datos a inspeccionar según sus requerimientos y necesidades.

Los registros de auditoría en un IDS/IPS son aquellos en los que se registran eventos realizados por los usuarios en un sistema y facilitan información tanto de los usuarios como de los demás detalles del evento realizado.

Una vez definidas las políticas de actuación y analizados los registros de auditoría, los administradores de la organización ya tienen suficiente información para comprobar la eficacia del sistema de detección y prevención de intrusiones. Aun así, siempre será necesario el establecimiento de pruebas y actualizaciones periódicas del sistema implantado que garanticen que no hay ninguna merma de eficacia mediante la comprobación de una serie de indicadores como el rendimiento, la completitud, la precisión, la tolerancia a fallos y el tiempo de respuesta del sistema.

CAPÍTULO 3 CONTROL DE CÓDIGO MALICIOSO

1. INTRODUCCIÓN

Los ataques e intrusiones que puede recibir un equipo son de lo más variados y cuantiosos. Uno de los más nocivos y habituales son los códigos maliciosos.

En este capítulo se define el concepto de código malicioso y se describen en profundidad las distintas formas que pueden tomar, cómo actúan y cuáles son los sistemas más frecuentes para su detección.

Con conocer cómo funcionan no es suficiente para evitar que se produzcan daños en el equipo, son necesarias una serie de herramientas encargadas de su control y contención que se irán describiendo junto con las distintas opciones que se pueden instalar en función de las vías de infección que se desean controlar y de la topología de la instalación de red de cada organización.

Además, es vital configurar estas herramientas siguiendo una serie de criterios definidos previamente por los responsables que sean acordes con la política de seguridad de la organización: criterios que tendrán que ver en cómo se debe actuar ante la detección de código malicioso y en la política de actualización de las herramientas de detección y contención para no rebajar el nivel de seguridad en todo lo que sea posible.

Aparte de estas herramientas, otra opción para detectar y contener código malicioso o *malware* son sus registros de auditoría: mediante una serie de aplicaciones se pueden conocer los registros de seguridad y establecer patrones de comportamiento y estadísticas de las herramientas de detección que permitirán conocer sus efectividad y saber si es necesario cambiar sus criterios o configuraciones para obtener mejoras de la seguridad.

Para terminar el capítulo, se tratarán los entornos de ejecución controlada y los desensambladores: dos tipos de herramientas que tratan de identificar los códigos maliciosos y conocer su comportamiento con el fin de establecer medidas de contención más específicas y eficaces.

2. SISTEMAS DE DETECCIÓN Y CONTENCIÓN DE CÓDIGO MALICIOSO

En este apartado se van a describir con profundidad distintos sistemas de detección y contención de código malicioso. No obstante, para entender estos sistemas y su funcionamiento es necesario tener unos conocimientos previos sobre los distintos tipos de código malicioso y su funcionamiento básico.

A continuación se concreta en estos conceptos y se aportan unos conocimientos básicos que van a permitir comprender la forma de actuar que tienen los sistemas de detección y contención para combatir estos códigos.

2.1.- Códigos maliciosos: conceptos básicos y tipos

La evolución del mundo electrónico ha provocado un crecimiento de la inseguridad de los equipos electrónicos debido al elevado número de intentos y ataques que se producen día tras día y que se propagan con más velocidad por la generalización de la banda ancha y de otras tecnologías de comunicación.

La comunidad de intrusos cada vez es más amplia y la decisión de a quién atacar puede tomar varias vertientes:

- Pueden decidir atacar a objetivos claros y específicamente definidos (un usuario u organización determinada, etc.).
- Pueden decidir atacar a un público objetivo definido atendiendo al grupo de interés. Por ejemplo, ataques a los usuarios de un sistema operativo específico, ataques a las bases de datos de un tipo de empresa definido, etc.
- Pueden decidir sus objetivos aleatoriamente sin ningún razonamiento previo.

Del mismo modo las motivaciones de los intrusos también pueden ser de lo más diversas:

- Motivaciones lucrativas: robar y vender posteriormente información de valor, entrar en bases de datos para conseguir direcciones de correo electrónico al que mandar publicidad o SPAM, etc.
- Entretenimiento: los intrusos pueden moverse por mera diversión o para aumentar su ego. También es frecuente que los intrusos utilicen códigos maliciosos para propagar elementos pornográficos.
- Motivaciones ideológicas: los intrusos pueden fundamentar sus ataques también para realizar apología del terrorismo o para difundir sus ideologías políticas, éticas o religiosas.

Nota

A pesar de la existencia de categorías de motivaciones de los intrusos bien definidas, hay que tener en cuenta que son usuarios con comportamientos variados que pueden ser tanto racionales como irracionales. De ahí surge la dificultad en muchas ocasiones de conocer los motivos reales del ataque.

Los códigos maliciosos o *malware* son una serie de programas informáticos que han sido diseñados con fines destructivos para conseguir ciertos objetivos como:

- Destruir datos, eliminando archivos o, incluso, formateando discos.
- Robar información y claves.
- Extenderse a través de un equipo a los demás equipos que forman una red o por internet.
- Comprometer sistemas operativos.

- Mostrar publicidad invasiva.

Los códigos maliciosos son cada vez más sofisticados y un mínimo cambio en ellos puede provocar que ya no sean reconocidos como maliciosos por las herramientas instaladas en el equipo para detectarlos y erradicarlos. Es por ello que cada vez hay más variedades distintas de estos tipos de códigos.

Aun así, los distintos tipos de *malware* tienen ciertos aspectos comunes:

- Suelen ser componentes de *software* diseñados con un fin específico.
- En su funcionamiento interfieren con la operación normal del sistema al que atacan.
- Es muy habitual que se instalen y ejecuten sin que haya un consentimiento expreso del usuario del equipo.
- Para lograr sus objetivos necesitan un sistema de cómputo anfitrión, un equipo en el que instalarse y propagarse.

Nota

Malware es el acrónimo en inglés de *malicious* y *software*, *software* malicioso. Forman parte de este grupo desde los clásicos virus hasta amenazas informáticas de lo más sofisticadas.

A pesar de las características comunes de los códigos maliciosos hay que remarcar que sus diferencias son numerosas, lo que clasifica los distintos tipos atendiendo a características como:

- Forma.
- Origen.
- Daños provocados.
- Finalidad para la que se diseñan.

Atendiendo a estas características se distingue entre varios tipos de *malware*:

- Virus.
- Troyanos.
- *Cookies*.
- *Keyloggers*.
- *Spyware*.
- *Worms* o gusanos.

Virus

Los virus son programas informáticos diseñados con la finalidad de producir algún tipo de daño en el equipo, trabajando sin que el usuario se dé cuenta.

Para funcionar necesitan un anfitrión o huésped en el que alojarse, que puede ser de lo más variado: desde archivos ejecutables hasta discos de arranque o unidades de memoria del equipo.

El daño que pueden producir también es variable: pueden provocar efectos menos nocivos como la aparición de mensajes en la pantalla para molestar al usuario, o efectos bastante más perjudiciales como la eliminación de archivos o la inhabilitación del acceso al sistema operativo del equipo.

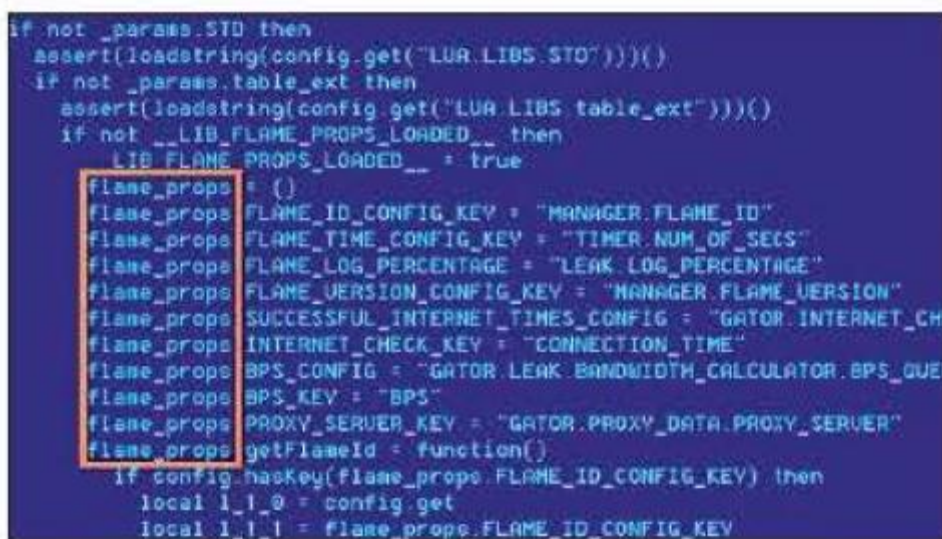
Cuando se ejecuta un virus se producen dos acciones:

- El daño al dispositivo.
- La propagación del virus infectando otros dispositivos o archivos.

El modo más habitual de contagio es por internet, pero no el único: los canales de entrada pueden ser cualquier dispositivo de almacenamiento (discos duros, *pendrives*, discos duros externos, etc.) o, incluso, redes locales (propagación del virus mediante la utilización de carpetas compartidas).

La variedad de virus también es bastante amplia, habiendo en la actualidad numerosas clasificaciones en función de varias características o criterios como, por ejemplo:

- Origen del virus.
- Modo de infección y propagación.
- Daños ocasionados.
- Lugares en los que se esconden.



```

if not _params.STD then
    assert(loadstring(config.get("LUA.LIBS.STD"))())
end
if not _params.table_ext then
    assert(loadstring(config.get("LUA.LIBS.table_ext"))())
end
if not __LIB_FLAME_PROPS_LOADED__ then
    __LIB_FLAME_PROPS_LOADED__ = true
    flame_props = {}
    flame_props.FLAME_ID_CONFIG_KEY = "MANAGER.FLAME_ID"
    flame_props.FLAME_TIME_CONFIG_KEY = "TIMER.NUM_OF_SECS"
    flame_props.FLAME_LOG_PERCENTAGE = "LEAK.LOG_PERCENTAGE"
    flame_props.FLAME_VERSION_CONFIG_KEY = "MANAGER.FLAME_VERSION"
    flame_props.SUCCESSFUL_INTERNET_TIMES_CONFIG = "GATOR.INTERNET_CHECK_TIMES_CONFIG"
    flame_props.INTERNET_CHECK_KEY = "CONNECTION.TIME"
    flame_props.BPS_CONFIG = "GATOR.LEAK.BANDWIDTH.CALCULATOR.BPS_QUEUE"
    flame_props.BPS_KEY = "BPS"
    flame_props.PROXY_SERVER_KEY = "GATOR.PROXY_DATA.PROXY_SERVER"
    flame_props.getFlameId = function()
        if config.hasKey(flame_props.FLAME_ID_CONFIG_KEY) then
            local l_1_0 = config.get
            local l_1_1 = flame_props.FLAME_ID_CONFIG_KEY
        end
    end
end

```

Virus Flame, creado por Estados Unidos e Israel para espiar y recoger información del programa nuclear de Irán.

Troyanos

Generalmente, los códigos maliciosos denominados troyanos son aquellos programas con funcionalidades ocultas diseñadas para fines maliciosos contra el usuario que los tiene instalados.

A diferencia de los virus, los troyanos no tienen capacidad de multiplicarse. Además suelen formar parte del código fuente del programa que se va a instalar, mientras que el virus se limita a suplantar el programa originario o a añadirse.

Suelen entrar en los dispositivos o sistemas como aplicaciones inofensivas y, a pesar de la variedad de troyanos existente, tienen unas finalidades comunes como:

- Capacidad para compartir archivos.
- Capacidad para apagar y/o reiniciar el sistema.
- Capacidad para recuperar contraseñas almacenadas en la memoria caché.
- Captura de pantallas del equipo infectado.
- Monitorización del tráfico de red del equipo infectado.
- Redirección de puertos y aplicaciones.
- Ejecución de aplicaciones no controladas por el usuario.
- Emisión de mensajes e imágenes en pantalla.
- Funciones *fun* o divertidas: funciones que pretenden molestar al usuario cuando utiliza el equipo. Por ejemplo, funciones de apertura o cierre del lector de CD o DVD, intercambio de teclas del teclado, ejecución de archivos de sonido, etc.

Su funcionamiento se divide en tres fases diferenciadas:

1. Entrada al dispositivo o sistema a infectar.
2. Consolidación de la posición del código malicioso.
3. Comunicación del sistema atacado con el equipo del atacante.



Detección de un troyano por parte de un antivirus

Cookies

Las *cookies* en sus inicios se diseñaron con la finalidad de que los sitios web pudiesen detectar y almacenar las preferencias del usuario en su navegación por dicha web para ofrecer servicios más acordes en sus próximas visitas. De este modo, con la expansión de la utilización de internet y servicios web, las *cookies* se han convertido en herramientas de *marketing* que permiten a las empresas conocer todo tipo de detalles del usuario cuando este navega por sus páginas web.

Las *cookies* no se consideran directamente una amenaza a los equipos o a sus archivos, pero sí pueden vulnerar la confidencialidad y privacidad de los usuarios, ya que permiten a las webs el almacenamiento de los registros de cada visita de los usuarios. Son archivos de texto que almacenan en el disco duro del usuario datos sobre la utilización de su navegador.

La introducción en el sistema se produce cada vez que el usuario visita una página web que tenga habilitada la utilización de *cookies* y su funcionamiento se establece en varias fases:

1. Las *cookies* se envían desde el servidor al navegador del usuario y se almacenan en él.

2. El navegador envía las *cookies* al servidor con el fin de identificar al usuario/diente y conocer su comportamiento de navegación.

Nota

Una de las empresas de marketing en internet más destacadas en la monitorización de la navegación de los usuarios a través de cookies es la conocida DoubleClick, llegando a monitorizar navegaciones de varios millones de equipos en todo el mundo.

Keyloggers

Los *keyloggers* son aplicaciones diseñadas con el fin de registrar el comportamiento de un usuario en un ordenador de modo remoto. Almacena todo lo que se escribe con el teclado para enviar la información al atacante o también, la almacena en el disco duro para que el atacante la pueda recuperar cuando lo requiera.

En general están diseñados para pasar inadvertidos por parte del usuario y su funcionamiento básico consiste en:

1. I. Configuración de los distintos aspectos del *keylogger* atendiendo a la información que se pretende obtener.
2. Instalación del *keylogger* en el equipo víctima.
3. Recuperación de la información obtenida y almacenada por el *keylogger*.

Actualmente, numerosos virus, gusanos y troyanos incorporan *keyloggers* en su código para obtener información de la víctima, además de las funcionalidades propias que tienen asignadas.

Nota

No todos los usos de los keyloggers son ilegales. También tienen usos legales extendidos como el control parental para que los padres vigilen a sus hijos menores de edad o el control de las empresas sobre la utilización de sus equipos por parte de sus empleados.

Spyware

De modo genérico el *spyware* se define como la aplicación diseñada para controlar el comportamiento de los usuarios con finalidades lucrativas, es decir, pretenden obtener

información del comportamiento del usuario para venderla posteriormente a terceros que suelen ser empresas publicitarias o de *marketing*. A pesar de la gran variedad de *spyware* su funcionamiento sigue el siguiente procedimiento:

1. Entrada al sistema del usuario.
2. Recolección de la información local del sistema del usuario víctima.
3. Monitorización del sistema del usuario víctima.
4. Registro de la actividad del usuario.
5. Actuación de las empresas de *marketing* y publicidad atendiendo a la información obtenida del usuario.

Aunque su procedimiento de funcionamiento sea similar, son varias e importantes las diferencias que existen entre los distintos tipos de *spyware*, distinguiendo entre:

- *Adware*: aplicaciones que incluyen ventanas de publicidad en sus interfaces de usuario.
- *Scumware*: personalizan la publicidad que se muestra en el navegador del usuario.
- *Browser Hijackers*: modifican características del explorador, actuando sobre el registro del sistema operativo.
- *Server Side Spyware*: *spyware* que se implementa en los servidores de los atacantes en lugar de instalarse en el equipo del usuario víctima.



Ventana de publicidad abierta sin consentimiento en el navegador de un usuario

Gusanos o worms

Los gusanos o *worms* son programas autocontenidos diseñados con el fin de propagarse de un sistema a otro para degradar el rendimiento de sus recursos.

Su misión es simplemente autoreplicarse, no pretenden causar daño directo aunque se pueden adjuntar a otros tipos de códigos maliciosos como complemento.

Su principal vía de infección es por archivos adjuntos en correos electrónicos, utilizando vulnerabilidades de los servicios de red y a través de redes P2P.

Nota

Las redes P2P o peer-to-peer son redes que conectan un número elevado ordenadores (nodos) para compartir información entre ellos.

Al haber aumentado la frecuencia de aparición de ventanas de publicidad es posible que el sistema esté afectado por un *spyware*, más concretamente por *adware*.

El funcionamiento de los *spyware* suele ser común en todas sus tipologías:

1. Entrada al sistema del usuario.
2. Recolección de la información local del sistema del usuario víctima.
3. Monitorización del sistema del usuario víctima.
4. Registro de la actividad del usuario.
5. Actuación de las empresas de *marketing* y publicidad atendiendo a la información obtenida del usuario.

2.2.- Sistemas de detección y contención de código malicioso

A pesar de las distintas características que tienen las tipologías de código malicioso, los sistemas utilizados para su detección y contención son comunes entre ellos:

- IDS/IPS.
- Antivirus.
- *Firewall* o cortafuegos.

IDS/IPS

A modo de recopilación y resumen, estos sistemas sirven para detectar e informar a los administradores sobre los intentos de intrusión que se producen en un equipo, red o dispositivo. Además, algunos de ellos (IPS) aparte de detectar intrusiones utilizan otros mecanismos para evitar que la intrusión se produzca con éxito.

Para su correcta utilización es necesario un alto nivel de experiencia y conocimiento del sistema de modo que sus configuraciones permitan el equilibrio entre la detección de falsos positivos y falsos negativos definido por la organización.

No obstante, con una correcta configuración de sus parámetros se consideran unas herramientas muy eficaces para la detección y prevención de accesos no autorizados.

Recuerde

Los sistemas de detección de intrusiones (IDS) son un modo de protección reactiva ante intrusiones (medidas correctivas o reactivas), mientras que los sistemas de prevención de intrusiones (IPS) ejercen protección proactiva (medidas preventivas).

Antivirus

Los antivirus son programas que tienen como función detectar y eliminar tanto virus como otros tipos de código malicioso. Para su detección disponen de una base de datos de patrones de modo que comparando cada archivo con los patrones se pueden detectar archivos contaminados.

Además de la comparación de los archivos del sistema con patrones de archivos contaminados, también tienen otras funciones:

- Revisan el correo electrónico.
- Revisan el historial de páginas web visitadas para detectar código malicioso oculto.
- Revisan los sistemas para detectar si hay algún troyano o gusano.
- Realizan tareas propias de los sistemas IDS/IPS y de los cortafuegos.

Lo habitual es que los antivirus se encuentren instalados en el sistema operativo del equipo, aunque también hay antivirus instalados en servidores o en redes que analizan el sistema del usuario de modo remoto.



*Antivirus Panda***Firewall o cortafuegos**

Como ya se sabe, los cortafuegos son elementos tanto de *software* como de *hardware* que se utilizan en un equipo o en una red de equipos como medida de control de las comunicaciones establecidas, permitiendo o denegando el acceso a los sistemas según las políticas de seguridad determinadas por la organización.

Así, un cortafuegos configurado correctamente funciona eficazmente como barrera para evitar el acceso de código malicioso a los sistemas de la organización, aunque por sí solo no es suficiente: es necesaria la instalación de medidas de protección adicionales como antivirus o sistemas IDS/IPS.

3. RELACIÓN DE LOS DISTINTOS TIPOS DE HERRAMIENTAS DE CONTROL DE CÓDIGO MALICIOSO EN FUNCIÓN DE LA TOPOLOGÍA DE LA INSTALACIÓN Y LAS VÍAS DE INFECCIÓN A CONTROLAR

La gran mayoría de usuarios han tenido alguna vez una infección con código malicioso en su equipo. Para detectar, contener y eliminar las amenazas hay muchas herramientas que se dedican a automatizar estos procesos. Por ello se debe elegir entre unas u otras dependiendo de la topología de la instalación y de las vías de infección que se pretenden controlar.

A pesar de existir una amplia variedad de herramientas, en este apartado se profundizará en tres de ellas:

- ESET NOD 32.
- Virus total.
- FileInsight.

3.1.- ESET NOD 32

ESET NOD32 es una herramienta de protección ante amenazas desarrollada por la empresa ESET y se puede utilizar en varios sistemas operativos: *Windows*, *Mac*, *Linux* e, incluso, *Android*.

La versión más avanzada aumenta la seguridad de los equipos mediante medidas antivirus, *anti-spyware*, *anti-malware* y cortafuegos, entre otras. Es una combinación de funcionalidades que permite disponer de un nivel de protección muy elevado.

Accediendo a su página web <[http:// 1descargas.eset.es/](http://1descargas.eset.es/)> se puede descargar una versión de evaluación gratuita, aunque si se quiere tener una base de datos de código malicioso actualizada pasado el período de evaluación hay que realizar una suscripción que conlleva coste adicional.



Herramienta ESET NOD32

3.2.- Virus total

A diferencia de ESET NOD32, Virus total es un servicio gratuito cuya funcionalidad es analizar archivos y URL sospechosas para detectar cualquier tipo de *malware*.

Su funcionamiento es remoto (no es necesaria realizar ninguna instalación en el equipo, se realiza todo vía web) y muy sencillo: basta con acceder a su página web <<https://www.virustotal.com/es/>>, pulsar Seleccionar y elegir el archivo del equipo que se desea analizar en búsqueda de código malicioso.

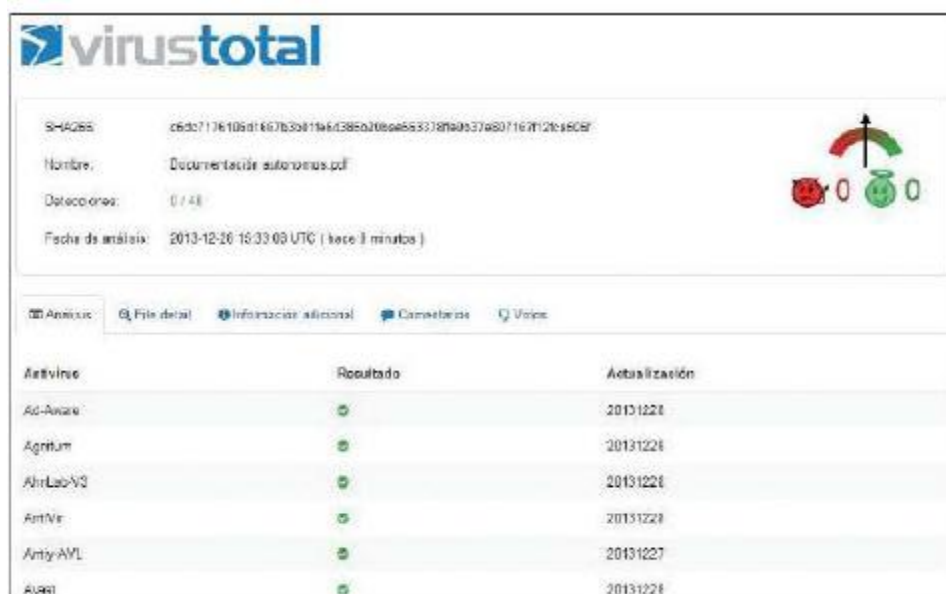


Página de inicio de la herramienta Virus total

Una vez seleccionado el archivo a analizar basta con hacer clic en **Analizar**. La herramienta procederá a analizar el archivo para conocer si este ha sido infectado o no con algún tipo de *malware*.

Como se puede observar en la imagen siguiente, la información que ofrece esta herramienta es abundante y detallada:

- Resultado positivo o negativo del análisis realizado por los distintos motores de antivirus y *anti-malware* (Avast!, Panda Antivirus, AVG, Norton Antivirus, etc.).
- Información detallada del archivo analizado: fecha y hora de la última modificación, autor, tipo de archivo, fecha y hora de creación, etc.
- Información adicional del archivo: tamaño, fecha del último análisis, identificación del archivo, etc.
- Comentarios de los usuarios sobre el archivo.
- Votos positivos o negativos de los usuarios sobre el archivo.



The screenshot shows the VirusTotal interface. At the top, the SHA256 hash is displayed: c6d0717610d1667b3d1166d385a200e65338f9d537a807167f121e5c0f. The file name is 'Documentación autorizados.pdf'. It shows 0 detections out of 48 engines. The analysis date is 2013-12-26 15:33:03 UTC (less than 3 minutes ago). Below this, there are tabs for 'Analysis', 'File details', 'Additional information', 'Comments', and 'Virus'. A table lists the antivirus engines and their results:

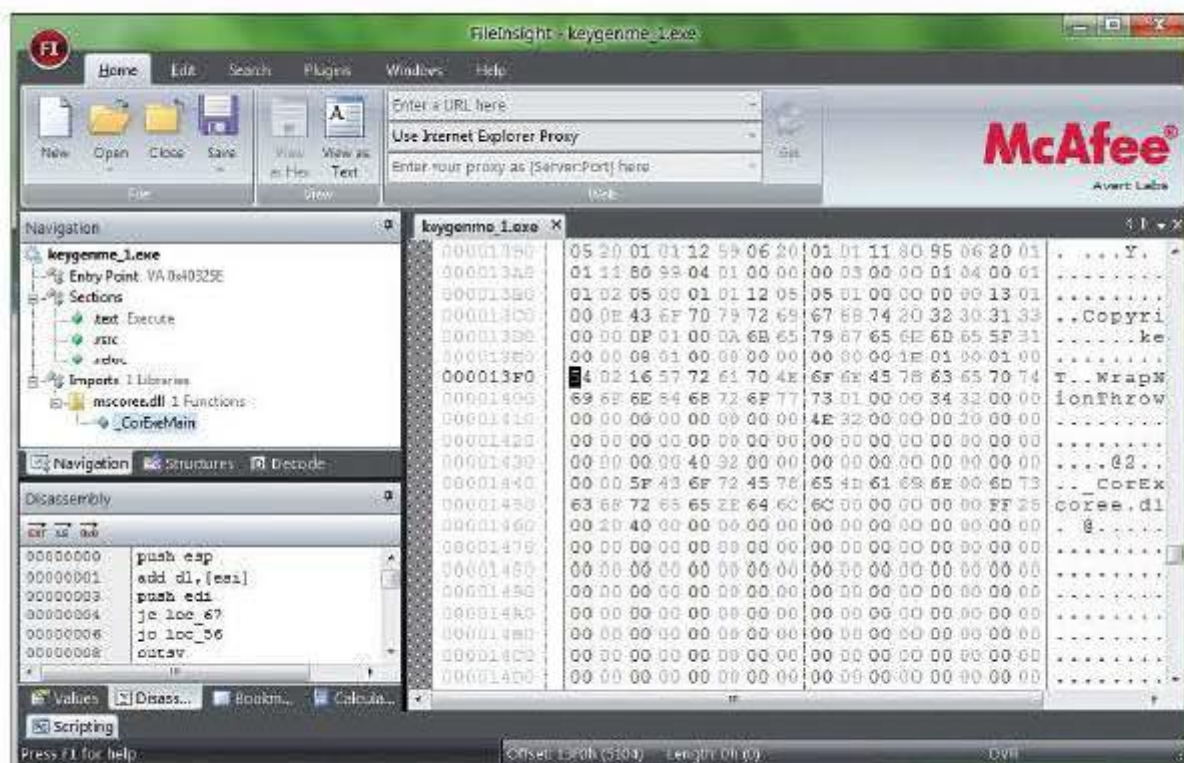
Antivirus	Resultado	Actualización
Ad-Aware	OK	20131228
Agrium	OK	20131228
AlmLab-V3	OK	20131228
AntVir	OK	20131228
Antiy-AVL	OK	20131227
Avast	OK	20131228

Herramienta Virus total, resultados del análisis

3.3.- FileInsight

FileInsight está desarrollada por la empresa McAfee Labs y se trata de una herramienta de análisis remoto (vía web también) de archivos para detectar virus y otros tipos de *malware*.

Además de analizar archivos resulta muy útil porque permite comprobar si una página web está limpia de *malware* con introducir su URL en la casilla Enter a URL, here y pulsando en Get, tal como se muestra, en la siguiente imagen.



Herramienta FileInSight

Esta herramienta resulta muy útil ya que los usuarios pueden localizar el origen de algún *malware* detectado en el sistema simplemente con buscar el historial de navegación de un equipo y comprobar si las distintas webs visitadas están limpias o infectadas.

4. CRITERIOS DE SEGURIDAD PARA LA CONFIGURACIÓN DE LAS HERRAMIENTAS DE PROTECCIÓN FRENTE A CÓDIGO MALICIOSO

Sea cual sea la herramienta de protección del equipo frente a código malicioso que se decida utilizar hay que tener en cuenta que, aunque se trate de herramientas efectivas, siempre es posible recibir algún ataque de *malware*.

Para detectar estos ataques se enumeran a continuación una serie de síntomas que pueden ser indicios de que hay una infección en el equipo o en el sistema:

- Las aplicaciones cargan lentamente o tardan en cargar (bajo rendimiento).
- Aparecen archivos desconocidos en el disco duro.
- Desaparecen del disco duro archivos necesarios para ejecutar alguna aplicación habitual.
- La pantalla no se comporta de una forma habitual.
- Hay cambios repentinos en el tamaño de los archivos respecto a su tamaño original.
- El sistema operativo se resetea inesperadamente.

- El sistema operativo muestra algún mensaje de error o no se inicia correctamente.
- Se cargan aplicaciones desconocidas o extrañas al iniciar el sistema operativo.
- Las aplicaciones tienen comportamientos erróneos o inesperados.

Cualquiera de estas situaciones y comportamientos in usuales pueden indicar que el equipo está infectado por algún código malicioso.

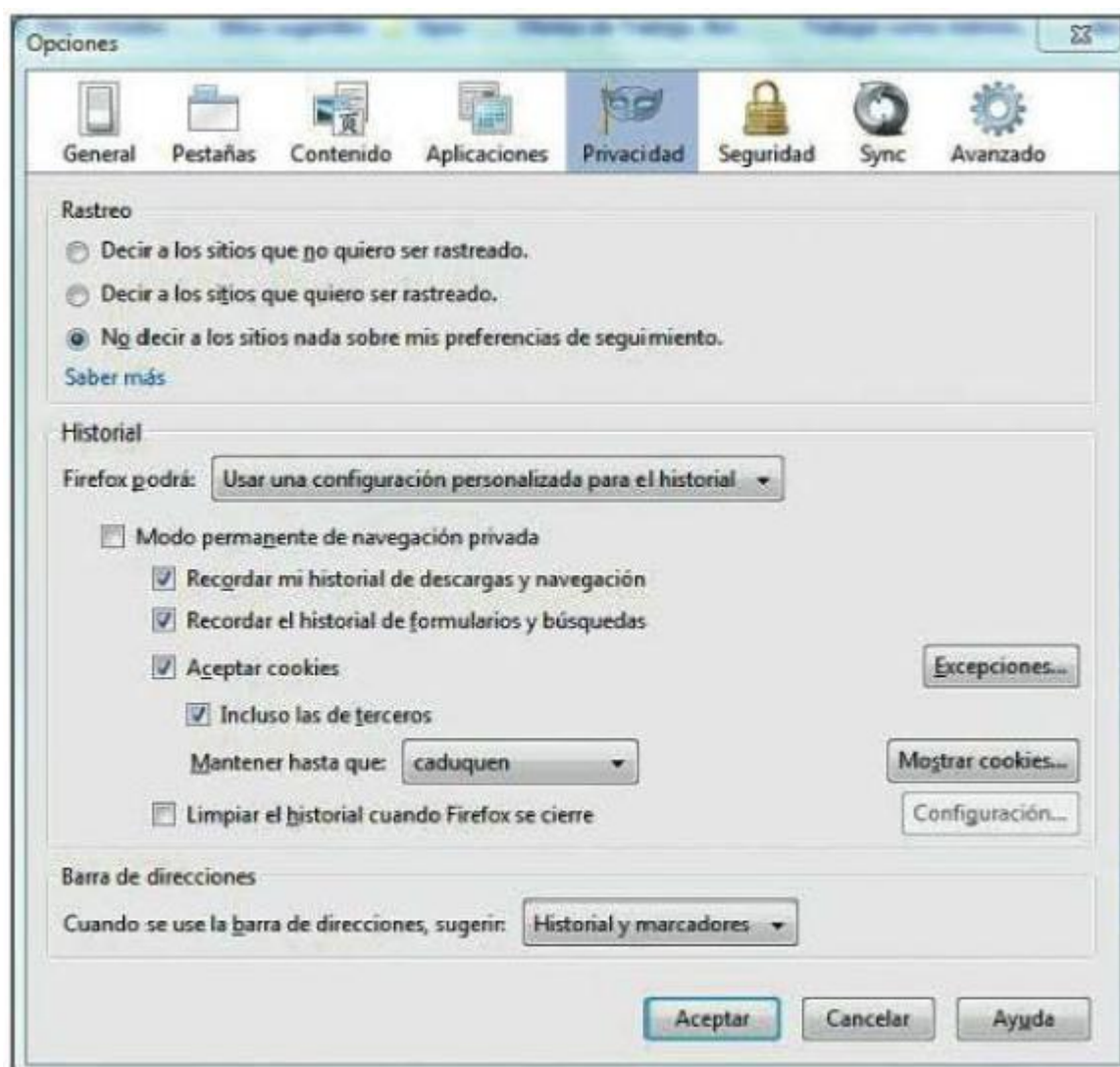
Para evitar estas infecciones e intrusiones se recomienda que las herramientas de detección y contención de código malicioso y que los sistemas operativos y aplicaciones de un equipo se configuren siguiendo unos criterios de seguridad preventivos:

- Mantener [os sistemas operativos, las herramientas y las aplicaciones actualizadas.
- Implementar *software* antivirus en equipos, archivos y servidores de correo.
- Implementar *software* de administración de contenidos.
- Configurar las herramientas de contención de código malicioso atendiendo a las políticas de filtrado de contenidos definida en la organización.
- Implementar herramientas de búsqueda y actualización de vulnerabilidades.
- Implementar un sistema de alarmas en la herramienta de contención de código malicioso.
- Utilizar claves y contraseñas de alta seguridad.
- Realización periódica de copias de seguridad del sistema operativo.
- Navegar por páginas web seguras y de confianza, configurando las herramientas y navegadores para que bloqueen temporalmente las webs potencialmente peligrosas.
- Implementar un cortafuegos.
- Configurar el navegador para que rechacen los diferentes tipos de *cookies*.

La configuración del navegador para el bloqueo de *cookies* puede variar de un navegador u otro, pero el procedimiento es bastante similar. Por ejemplo, en *Mozilla Firefox* hay que seguir los siguientes pasos:

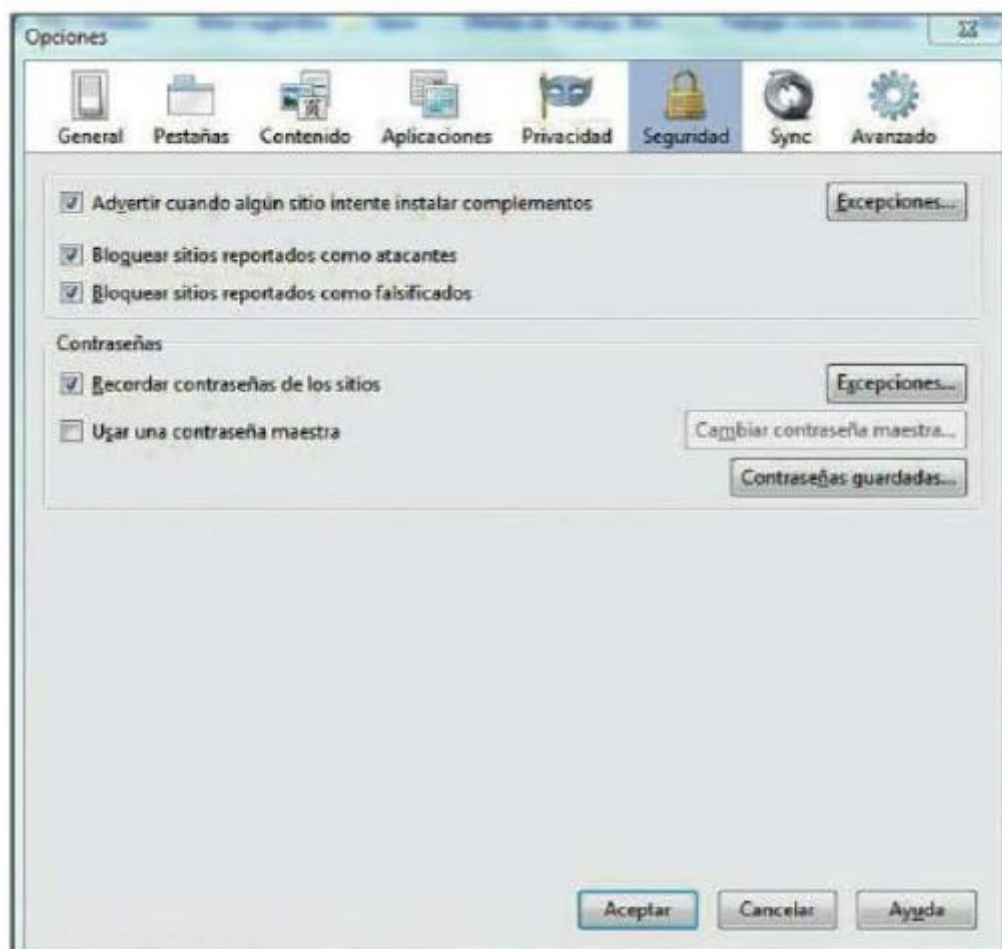
1. Hacer *clic* en Firefox -> Opciones.
2. En Historial -> Firefox seleccionar la opción Usar una configuración personalizada para el historial.
3. Desmarcar la opción Aceptar cookies.

Además, en este navegador se pueden definir excepciones de *cookies* de páginas que el usuario considere seguras y decidir, en el caso de aceptar las *cookies*, durante cuánto tiempo deben almacenarse en el navegador.



Configuración de cookies en Mozilla Firefox

En la pestaña Seguridad también se puede establecer que el navegador bloquee aquellas páginas web que considere como atacantes o falsificados: bastaría con marcar las casillas Bloquear sitios reportados como atacantes y Bloquear sitios reportados como falsificados dependiendo de lo que el usuario quiera bloquear:



Pestaña Seguridad en Mozilla Firefox

En *Internet Explorer* los mecanismos y procedimientos son similares: seleccionando **Opciones de internet -> Privacidad**, el usuario puede definir el nivel de seguridad que quiere establecer en el navegador desplazando la barra situada bajo **Seleccione una configuración para la zona de Internet**. Este nivel puede ir desde el nivel de protección máximo en el que se bloquean todas las *cookies*, hasta el nivel de protección mínimo en el que no se bloquea ninguna, habiendo varios niveles intermedios de menor a mayor nivel de restricción de *cookies* (en cada nivel de seguridad se muestra qué *cookies* se mantienen y cuáles se deshabilitan).



Configuración de cookies en Internet Explorer

Además, en la pestaña **Seguridad** también se ofrece la posibilidad de definir la seguridad (en cuanto a política de descargas, certificados válidos, habilitación o deshabilitación de medidas de seguridad) en varios niveles: navegación por sitios web de internet, navegación por sitios web de una red local, definición de sitios web de confianza y definición de sitios web potencialmente peligrosos.



Pestaña Seguridad en Internet Explorer

La configuración de las herramientas de contención y detección de código malicioso es fundamental para una protección adecuada de los equipos. Pero, después de ver estos ejemplos de configuraciones de los navegadores para definir su nivel de seguridad, se recomienda que además de las herramientas *anti-malware* se configuren los distintos elementos que forman parte del sistema operativo y de las aplicaciones para que, ante fallos de las herramientas, el equipo no quede completamente desprotegido y haya una barrera más de protección.

5. DETERMINACIÓN DE LOS REQUERIMIENTOS Y TÉCNICAS DE ACTUALIZACIÓN DE LAS HERRAMIENTAS DE PROTECCIÓN FRENTE A CÓDIGO MALICIOSO

Atendiendo a la ya mencionada norma ISO 27001, el responsable de seguridad debe definir los controles de detección y prevención para la protección contra el *software* malicioso, además debe desarrollar procedimientos adecuados de concienciación de usuarios en cuanto a seguridad, controles de acceso al sistema y administración de cambios.

5.1.- Acciones y requerimientos recomendados para un correcto control de accesos

Los controles a establecer deben comprender una serie de acciones como:

- Prohibir la instalación y uso de *software* no autorizado por la organización.
- Redactar procedimientos para evitar los riesgos relacionados con la obtención de archivos y *software* externos desde o a través de redes, o por cualquier otro medio, señalando las medidas de protección a tomar.
- Instalar y actualizar periódicamente el *software* de detección y reparación de virus, examinando los equipos y medios informáticos.
- Mantener los sistemas al día con las últimas actualizaciones de seguridad disponibles. Se recomienda realizar previamente pruebas y comprobaciones en un entorno de prueba si las actualizaciones provocan cambios críticos en el sistema.
- Revisar periódicamente el contenido del *software* y los datos de los equipos que sustentan procesos críticos de la organización.
- Verificar previamente la presencia de virus en archivos de medios electrónicos de origen incierto o en archivos recibidos a través de redes poco confiables.
- Redactar procedimientos para verificar la información relativa a *software* malicioso, garantizando que los mensajes de alerta sean exactos e informativos.
- Concienciar al personal sobre el problema de los falsos antivirus, de las cadenas falsas y de cómo proceder frente a los mismos.
- Redactar normas de protección y habilitación de puertos de conexión de dispositivos móviles y sus derechos de acceso.

Nota

Los falsos antivirus o rogué software son programas informáticos malintencionados que suelen descargarse e instalarse en el equipo de forma oculta y sin permiso del usuario con el fin de hacer creer al usuario que el equipo está infectado por un virus y que deben pagar una suma de dinero para eliminarlo.

Siguiendo las recomendaciones y controles descritos en la ISO 27001 se establecen una serie de requerimientos y técnicas de actualización para las herramientas de control y contención de código malicioso:

- Protección antivirus continua, 24 horas al día los 7 días de la semana.
- Herramientas de actualización automática.
- Herramientas de actualización que no provoquen interrupciones en el trabajo.
- Aparición rápida y continua de actualizaciones.
- Generación periódica de informes y estadísticas. Gestión avanzada de informes.
- Protección para todo tipo de servidores (*Linux, Windows, etc.*).

- Métodos de escaneo y análisis de posibles códigos maliciosos que permitan la detección de virus anómalos y desconocidos.
- Comprobación y seguridad remota del estado de los equipos y dispositivos.
- Realización de copias de seguridad y discos de arranque periódicos.
- Detección de virus en tiempo real.
- Velocidad de escaneo para una rápida detección y eliminación de cualquier código malicioso.
- Utilización de distintos métodos de escaneo, detección y eliminación de códigos maliciosos para incrementar el grado de protección de los equipos.
- Facilidad de manejo y gestión de las herramientas de protección y contención.
- Administración centralizada en la que se puedan recibir reportes de virus, actualizaciones y personalizar configuraciones según el tipo de usuario.

Nota

Resulta imprescindible remarcar la importancia de tener actualizadas las herramientas de protección ante código malicioso. Los códigos maliciosos se reproducen y tienen variaciones continuamente y la no actualización de las herramientas que los combaten deja a los equipos completamente desprotegidos ante posibles ataques.

5.2.- Herramientas de protección frente a código malicioso

Además de estos requerimientos y técnicas de actualización no hay que olvidar que las herramientas deben controlar y proteger las distintas vías de acceso de un modo personalizado para cada una de ellas:

- Sistemas de fichero.
- Red local.
- Correo electrónico.
- Navegadores.

Sistemas de fichero

Pueden ser tanto discos duros, *pendrives*, CD como cualquier otro dispositivo que soporte sistemas de archivo.

Las herramientas encargadas de proteger los sistemas de ficheros deben cumplir una serie de requerimientos:

- Los programas antivirus deben estar instalados tanto en clientes como en servidores.

- Deben realizar una gestión eficiente del escritorio, controlando y realizando un inventario del *software* instalado en el dispositivo.
- Debe gestionar las vulnerabilidades del sistema, debiendo identificarlas y parchearlas de modo automático.
- Deben ofrecer una protección especial a códigos maliciosos *adware* y *spyware*.

Red local

En una gran mayoría de veces la transmisión de códigos maliciosos se produce internamente a través de la red local en lugar de provenir del exterior. Por ello, las herramientas de detección y contención de códigos maliciosos deben prestar una protección especial a la red local para impedir su propagación.

De este modo se recomienda realizar una configuración centralizada de los cortafuegos de los dispositivos que forman parte de la red local, además del establecimiento de políticas centralizadas de seguridad y respuesta ante detección de intrusiones.

Correo electrónico

Las herramientas deben contener programas antivirus especializados para controlar y detectar códigos maliciosos en los correos electrónicos que circulan por los equipos y dispositivos de la organización.

Estos programas deben controlar y verificar la inexistencia de código malicioso en la entrada de correos electrónicos y, además, también deben estar realizando comprobaciones constantes en aquellos servidores que almacenen buzones de correo electrónico.

Todo ello debe complementarse con la implementación de políticas de seguridad específicas para correo electrónico en la gestión de la seguridad de una organización.

Recuerde

La política de seguridad de las organizaciones debe reflejar y tener en cuenta las distintas posibles vías de entrada de código malicioso, las herramientas necesarias para su protección y su configuración y políticas de respuesta ante ataques.

Navegadores

Las herramientas de protección ante códigos maliciosos deben proteger la actividad y acciones de los navegadores instalados tanto en los servidores como en los equipos cliente de la red de la organización.

Para una protección adecuada hay que configurar los navegadores correctamente y de un modo acorde a las políticas de seguridad establecidas previamente y hay que instalar programas antivirus que realicen análisis periódicos y sean capaces de detectar códigos maliciosos en los distintos navegadores de los equipos.

6. RELACIÓN DE LOS REGISTROS DE AUDITORÍA DE LAS HERRAMIENTAS DE PROTECCIÓN FRENTE A CÓDIGOS MALICIOSOS NECESARIOS PARA MONITORIZAR Y SUPERVISAR SU CORRECTO FUNCIONAMIENTO Y LOS EVENTOS DE SEGURIDAD

Las herramientas de protección frente a códigos maliciosos cada vez son más necesarias y para conseguir evitar incidentes de seguridad no es suficiente con implementar alguna de estas herramientas, hay que encontrar la cantidad de herramientas necesarias para elevar el nivel de seguridad todo lo posible de un modo acorde con el coste que debe o puede soportar la organización.

De este modo, las herramientas de protección en las organizaciones ya forman una infraestructura tan compleja que cuesta llevar a cabo un control pormenorizado y manual de todas ellas: deben ser gestionadas de modo que controlen y vigilen la aparición de los incidentes de seguridad.

Una solución útil que gestione esta infraestructura compleja de herramientas es el análisis de eventos de seguridad centralizado a través de herramientas de auditoría de seguridad informática.

La auditoría de seguridad se concibe para analizar y evaluar la planificación, el control, la eficacia y la seguridad de la estructura informática de una organización mediante una serie de pruebas realizadas por personal independiente. Estas auditorías responden a preguntas como:

- ¿Es adecuada la seguridad de los equipos y dispositivos?
- ¿La información está almacenada en medios fiables? ¿Existe la posibilidad de que haya pérdidas de información irreversibles?
- ¿La seguridad de los sistemas permite la consecución de los objetivos y las metas de la organización?
- ¿La infraestructura de seguridad es eficiente? ¿Se aprovechan los recursos de un modo adecuado?

6.1.- Requisitos y funcionalidades de las auditorías de seguridad

Con la implantación de auditorías de seguridad en las organizaciones se consigue información muy valiosa que puede determinar si las políticas y medidas de seguridad aplicadas son correctas, suficientes y adecuadas. Para ello, una auditoría de seguridad adecuada debe responder a funcionalidades como:

- Análisis de los costes que supondría una ruptura de la seguridad de la información.
 - Informe de la situación actual de los distintos equipos y dispositivos (tanto locales como remotos) y el nivel de seguridad establecido en cada uno de ellos.
 - Auditorías de seguridad de los distintos sistemas de información de la organización.
 - Pruebas y test de intrusiones.
 - Búsqueda de vulnerabilidades en los sistemas.
 - Prevención de ataques mediante antivirus y *antispyware*, entre otras herramientas de prevención.
- Control de acceso a los sistemas y a las aplicaciones instaladas en ellos.
 - Análisis de registros de seguridad (o *logs*) para detectar los ataques producidos.

6.2.- Los archivos de registro o archivos de log

Los archivos de registro o archivos de *log* (registros de auditoría sobre todo) son una fuente importante de seguridad y de solución de problemas: son archivos en los que se encuentra información diversa de un sistema. A través de ellos se puede analizar información y conocer el tráfico de la red, las aplicaciones utilizadas y los usuarios que han accedido a cada aplicación y qué han hecho con estas.

Nota

Los archivos de registro de auditoría llegan a acumular una cantidad elevada de información. La automatización del análisis de estos archivos a través de ciertas herramientas puede ahorrar a los administradores mucho tiempo ofreciéndoles solo la información imprescindible y omitiendo la información sin relevancia.

En cuanto a la seguridad del sistema, los archivos de registro permiten descubrir posibles ataques a los sistemas, detectando información sobre problemas o incidencias de seguridad producidas en ellos. Con los registros de auditoría se genera información sobre las actividades que los administradores y usuarios realizan sobre un sistema y si se emplean las herramientas y procedimientos adecuados se puede conseguir información sobre violaciones de la seguridad del sistema y otros datos que servirán para comprobar el grado de cumplimiento de las políticas de seguridad definidas en una organización.

Los *logs*, como mínimo, deben registrar información sobre los siguientes eventos:

- Intentos de acceso al sistema o a alguna aplicación, tanto exitosos como fallidos.
- Identidad del usuario.
- Fecha del intento de acceso.

- Tiempo de cada intento de entrada.
- Fecha y tiempo de salida del sistema o de la aplicación.
- Dispositivos utilizados en la conexión.
- Las actividades y funciones ejecutadas por el usuario que ha accedido.

Con esta información facilitada los registros de auditoría sirven para ayudar a los responsables de seguridad a tener controlada una serie de aspectos:

- Control de acceso: a través de los *logs* se pueden conocer las acciones que los usuarios autorizados realizan y así poder evaluar y tomar decisiones sobre la asignación de autorizaciones y permisos de usuario.
- Reconstrucción de eventos: con una revisión de los *logs* se puede realizar un seguimiento de las últimas operaciones llevadas a cabo en el sistema y detectar cómo, cuándo y por qué se ha generado cualquier incidencia de seguridad. Con el análisis de los *logs* también se puede detectar cómo se originó la incidencia, si fue por algún error del *software* o si, por el contrario, la generó algún usuario. Además, si hay alguna pérdida de datos el análisis de *logs* puede ayudar en su proceso de recuperación.
- Detección de intrusos: los registros de auditoría se pueden diseñar e implementar de modo que sean un apoyo a la detección de intrusiones. Configurados correctamente pueden llegar a detectar intrusiones a tiempo real o después de haberse producido el incidente de seguridad. Para ello es básica la monitorización de estos registros para que generen mensajes de advertencia y alarmas en cuanto se produzca algún intento de intrusión.

Nota

Los registros de auditoría están protegidos con medidas legales en numerosos países, lo que requiere su almacenamiento en lugares de alto nivel de seguridad que eviten modificaciones y eliminaciones involuntarias o malintencionadas.

Otro aspecto importante de los ficheros de registro es la necesidad de realizar revisiones periódicas para detectar las alarmas y los mensajes de advertencia generados. Estos mensajes pueden aportar información sobre los intentos de conexiones sin éxito pero también pueden dar una abundante información que no tiene nada que ver con la seguridad del sistema.

La revisión de estos mensajes puede ser una tarea bastante tediosa debido a la gran cantidad de información irrelevante y lo más habitual es la utilización de herramientas especializadas en análisis de ficheros de registro que proporcionan solo la información relevante.

Las herramientas de análisis de *logs* de auditorías pueden ejecutar los análisis de dos modos:

- Realizando comprobaciones periódicas definidas previamente por el administrador. Estos análisis tienen como ventaja que solo se ejecutan una vez cada cierto tiempo, lo que implica que la utilización de recursos es escasa y por cortos periodos de tiempo. Sin

embargo es necesario configurar las herramientas para que analicen solo los registros nuevos para evitar pérdidas de eficiencia.

- Realizando comprobaciones constantes mediante la lectura continua de los archivos de *log*. En este caso los archivos de log se van analizando conforme se van generando: consume más recursos pero la información se obtiene de un modo inmediato habiendo más posibilidades de evitar ataques.

Nota

Los archivos de log contienen registros referentes a todo lo que ocurre en un sistema operativo y los servicios que se van ejecutando en este.

Las herramientas de auditoría filtran los registros y eventos más importantes para el administrador llegando incluso a ser capaces de llevar a cabo reacciones automáticamente.

En resumen, los registros de auditoría de seguridad facilitan información de vital importancia sobre el uso ilegal o sospechoso de información y sobre los ataques de intrusos y códigos maliciosos. Las herramientas de análisis de estos registros buscan información a través de estos datos y obtienen aquella información sobre los eventos importantes.

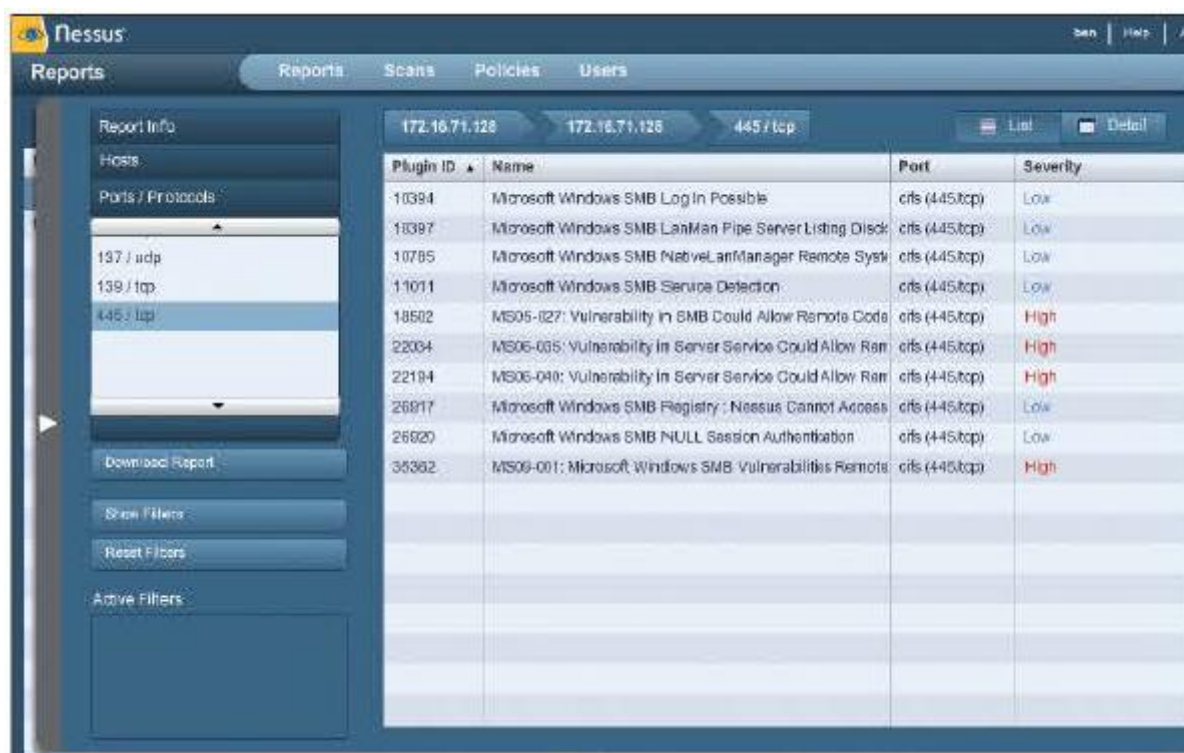
6.3.- Herramientas de auditoría de seguridad y archivos de registro

La variedad de estas herramientas es muy amplia y a continuación se expondrán dos de las más utilizadas: *Nessus* y *Ethereal*.

Nessus Security Scanner

Nessus Security Scanner es una herramienta de auditoría de seguridad que trabaja en modo remoto. Evalúa los módulos de seguridad con la finalidad de detectar vulnerabilidades que pueden repararse. Además es compatible con varios sistemas operativos como *Microsoft Windows*, *Linux*, *BSD*, *Solaris* y otros sistemas *Unix*.

Realiza numerosas pruebas de seguridad remotas, genera reportes de información y propone soluciones ante los problemas de seguridad detectados.



Herramienta de auditoría Nessus Security Scanner

Ethereal

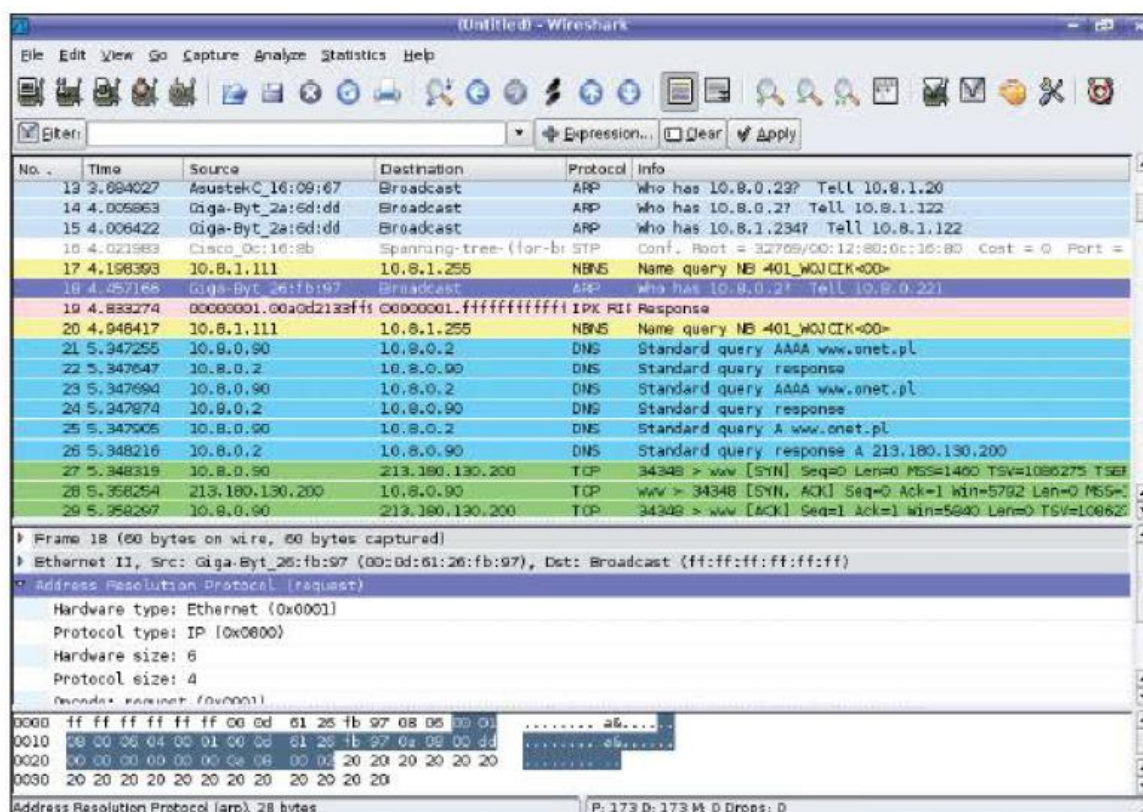
Ethereal es un analizador de protocolos de red que permite analizar el tráfico de una red o de registros de auditoría almacenados en el disco.

Con esta herramienta se puede examinar la información obtenida de forma detallada a través de una interfaz gráfica.

Además contiene una biblioteca que permite al administrador establecer filtros que definan qué tipo de información se desea obtener. También es compatible con varios sistemas operativos como *Windows*, *Unix* o *Linux*.

Desde 2006 es conocido como *Wireshark* y dispone de las características siguientes:

- Captura los paquetes directamente desde una interfaz de red.
- Permite obtener información detallada del protocolo utilizado en el paquete de datos capturado.
- Puede importar y/o exportar los registros capturados desde/hacia otras aplicaciones.
- Busca los registros de información que cumplan con un criterio establecido previamente por el usuario.
- Ofrece informes y estadísticas.



Herramienta de auditoría Ethereal!Wireshark

7. ESTABLECIMIENTO DE LA MONITORIZACIÓN Y PRUEBAS DE LAS HERRAMIENTAS DE PROTECCIÓN FRENTE A CÓDIGO MALICIOSO

La monitorización de las herramientas de protección frente a código malicioso y las pruebas que deben realizar se definen en el procedimiento establecido ante la aparición de algún código malicioso. Este procedimiento está formado por una serie de pasos:

- 1) Contención de los daños provocados por el *malware*. Si no hubiese soluciones conocidas de contención se recomienda:
 - a) Identificar el *software* malicioso y extraer una muestra.
 - b) Monitorizar las comunicaciones y los cambios que pueda ocasionar el código malicioso.
 - c) Realizar pruebas para comparar los distintos comportamientos en un entorno controlado antes y después de la ejecución del *software* malicioso observando y analizando lo siguiente:
 - La actividad de red para conocer las comunicaciones que ha realizado el *software*.
 - Los procesos del sistema que ha iniciado el *software*.
 - Los cambios que se han producido en la estructura de ficheros del sistema.
 - Los cambios producidos en los registros de los eventos.
 - d) Realizar pruebas que verifiquen el grado de confiabilidad, integridad y validez de la información facilitada por la herramienta de protección.
 - e) Realizar pruebas que verifiquen el grado de efectividad de las herramientas de protección y contención de código malicioso utilizado: pruebas en entornos controlados que permitan

comparar lo que hubiera ocurrido ante intrusiones si no estuviera instalada la herramienta de protección en el equipo.

Gracias a todos estos análisis se pueden detectar las actividades que ha llevado a cabo el código malicioso y definir con mayor rapidez las medidas que hay que tomar para gestionar el incidente y contener lo máximo posible los daños ocasionados.

- 2) Evaluación de los daños producidos por el código malicioso. Una vez contenidos los daños hay que analizarlos y evaluarlos en varios aspectos como: el coste de la pérdida de los datos eliminados, la pérdida de productividad causada, el grado de propagación del código malicioso tanto a nivel interno como a nivel externo, etc.
- 3) Reparación y revisión de la infección. En el momento de la evaluación de los daños causados por el código malicioso debe adoptarse una serie de medidas con el fin de restaurar el sistema y volver al estado anterior en el menor tiempo posible. Estas medidas consisten en la reversión de las alteraciones producidas por el código malicioso en los archivos y sistemas de los equipos afectados. Para ello se utilizan herramientas de análisis forense.

Definición

Análisis forense

Es un conjunto de técnicas especializadas que ayudan a detectar pistas sobre ataques informáticos y a posibilitar la recuperación y tratamiento de la información perdida después de que ocurra algún tipo de incidente.

Estas fases de contención, evaluación y reparación de los daños causados por los códigos maliciosos pueden ser monitorizadas a través de herramientas de protección. Con estas se pueden monitorizar funcionalidades como:

- Creación de bitácoras de herramientas habilitadas en los clientes con acceso centralizado.
- Creación del inventario de *software*: conjunto de aplicaciones instaladas en los sistemas de cada equipo.
- Sistemas de detección de intrusos.
- Creación y gestión de registros de correo electrónico.
- Creación y gestión de registros de uso de protocolos de internet como http y ftp.
- Gestión centralizada de las bitácoras del sistema.
- Gestión de acciones y medidas a tomar en caso de detección de intrusiones.
- Actualizaciones periódicas de la base de datos de códigos maliciosos y de la herramienta de protección utilizada.

El procedimiento de monitorización puede variar dependiendo de la herramienta de protección a utilizar. Por ejemplo, con el antivirus *Avast!* se pueden monitorizar las acciones que debe llevar a cabo respecto a una serie de parámetros:

- Escudo del sistema de archivos.
- Escudo de correo electrónico.
- Escudo web.
- Escudo P2P.
- Escudo de mensajería instantánea.
- Escudo de red.
- Escudo de comportamiento.



Estadísticas generadas por el antivirus Avast!

Avast! facilita información estadística de los parámetros mencionados atendiendo a los análisis realizados y a los ataques detectados. Se puede configurar el periodo de tiempo que se desea

visualizar, tanto si se quiere ver un resumen detallado de lo ocurrido los últimos días, como si se quiere visualizar la evolución de los análisis y detecciones encontradas en los últimos meses o incluso años.

Además permite la configuración de las funcionalidades indicando qué se quiere analizar y qué medidas hay que tomar ante cualquier detección.

En la imagen siguiente se puede observar la configuración de las acciones a llevar a cabo cuando se detecta un virus en el análisis web.



Configuración de acciones del antivirus Avast!

8. ANÁLISIS DE LOS PROGRAMAS MALICIOSOS MEDIANTE DESENSAMBLADORES Y ENTORNOS DE EJECUCIÓN CONTROLADA

Las técnicas y herramientas de detección y contención de códigos maliciosos que se han ido describiendo hasta el momento se refieren a un análisis dinámico de una amenaza, es decir, con estas se pretende monitorizar el comportamiento de los códigos maliciosos para obtener información valiosa y poder reaccionar al respecto.

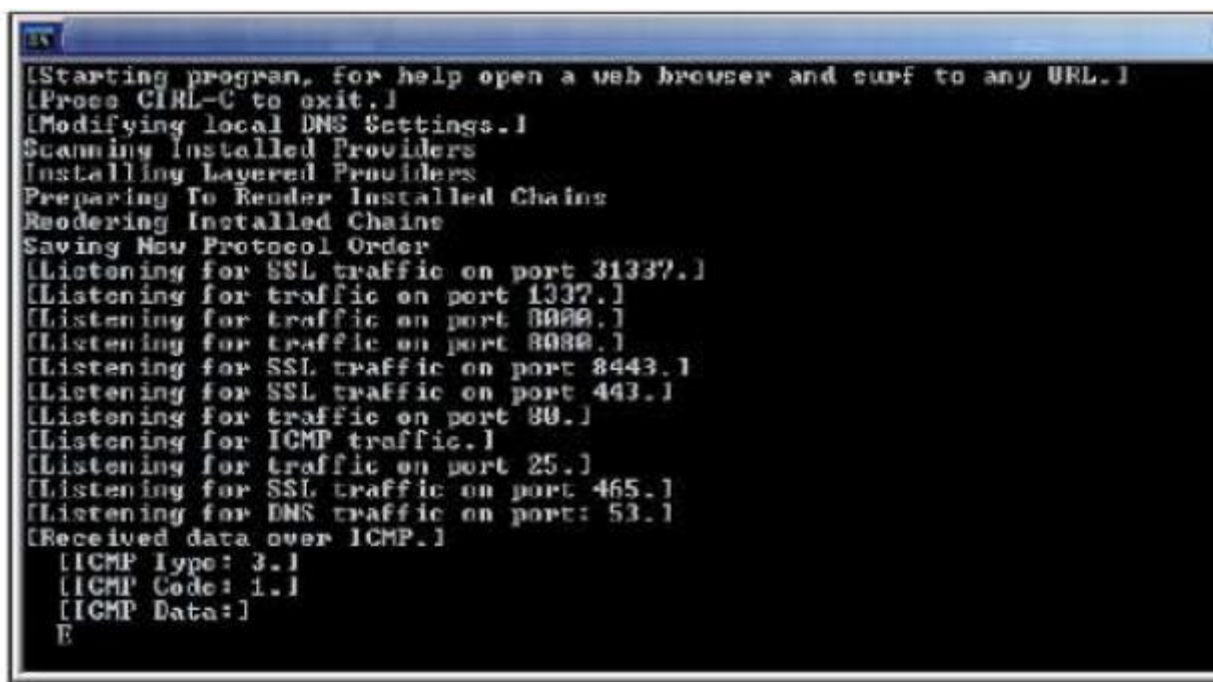
Sin embargo, en algunos casos conviene evitar la conexión real del usuario con el servidor del código malicioso, ya que puede hacer ver a los intrusos que se están realizando acciones sobre los códigos y pueden tomar medidas para evitarlo: se alerta a los intrusos de la presencia del usuario.

Una alternativa a considerar sería la simulación de ciertas situaciones. Se puede hacer creer al código malicioso que se está comunicando con los servidores maliciosos cuando, en realidad, se está comunicando con una máquina controlada por el usuario o administrador.

Esta técnica se refiere a la creación de entornos simulados de ejecución controlada. Reciben los paquetes que van llegando del *malware* y van generando respuestas falsas acordes con lo esperado por el código malicioso. Con esto se consigue un conocimiento más profundo y exacto del comportamiento del código malicioso que intenta acceder al equipo evitando que haya una conexión directa entre el equipo y el servidor malicioso.

Las herramientas con funcionalidades de simular entornos de ejecución controlada son numerosas pero merece la pena destacar dos de ellas:

- *Fakenet*: herramienta que se puede ejecutar desde la línea de comando de *Windows* y permite obtener información sobre los sitios web visitados por el *malware*. No dispone de interfaz gráfica.



```
[Starting program, for help open a web browser and surf to any URL.]
[Press CTRL-C to exit.]
[Modifying local DNS Settings.]
Scanning Installed Providers
Installing Layered Providers
Preparing To Render Installed Chains
Rendering Installed Chains
Saving New Protocol Order
[Listening for SSL traffic on port 31337.]
[Listening for traffic on port 1337.]
[Listening for traffic on port 8080.]
[Listening for traffic on port 8080.]
[Listening for SSL traffic on port 8443.]
[Listening for SSL traffic on port 443.]
[Listening for traffic on port 80.]
[Listening for ICMP traffic.]
[Listening for traffic on port 25.]
[Listening for SSL traffic on port 465.]
[Listening for DNS traffic on port: 53.]
[Received data over ICMP.]
[ICMP Type: 3.]
[ICMP Code: 1.]
[ICMP Data:]
E
```

Herramienta Fakenet

- *InetSim* : herramienta que genera un entorno virtual encargado de recibir el tráfico de red de la máquina infectada, registrar las peticiones que recibe y enviar respuestas simuladas de protocolos de red.

8.1.- Desensambladores

Otra alternativa para conocer el comportamiento de los códigos maliciosos son los desensambladores. Aunque tienen otras utilidades, se encargan de desensamblar archivos de códigos maliciosos para identificarlos y entender sus actuaciones.

Los usuarios están utilizando técnicas de ingeniería inversa: pretenden obtener información del código malicioso que ha intentado acceder al sistema para conocer cómo está diseñado, cómo funciona y cómo actúa para crear herramientas que puedan detectarlos y contenerlos con más facilidad.

Nota

La ingeniería inversa no solo se utiliza para identificar códigos maliciosos, puede utilizarse también en cualquier tipo de aplicación o, incluso, en componentes electrónicos. De hecho, algunas aplicaciones de software libre han sido diseñadas a partir de la información obtenida de la tecnología inversa.

Un buen desensamblador (que se puede utilizar tanto en *Windows*, *Linux* o *Mac*) es el llamado *IDA Pro*. Se considera uno de los mejores desensambladores del mercado al soportar casi cualquier plataforma. Su principal inconveniente es su elevado precio, aunque se puede utilizar la versión de prueba en un periodo de tiempo limitado.

La alternativa gratuita es el *software Rasta RingO Debugger*: funciona también en bastantes plataformas y tiene funcionalidades parecidas a los desensambladores de pago: ofrece información sobre el comportamiento del código malicioso y proporciona datos como sus rutinas de archivo objetos, registros, procedimientos, etc.

9. RESUMEN

La inseguridad de los equipos electrónicos ha ido aumentando con el tiempo por la gran cantidad de intentos y ataques que se producen a diario y a su alta capacidad y velocidad de propagación por las nuevas tecnologías de comunicación.

Un tipo de ataque muy común son los códigos maliciosos, para los cuales existen sistemas de detección y contención: IDS/IPS, antivirus y cortafuegos.

La elección de los sistemas de detección y contención puede variar en función de la tipología de la instalación de red de la organización y de las vías de infección que se pretenden controlar, existiendo incluso herramientas de detección *online* que no consumen recursos de memoria de los equipos y disponen de bases de datos de *malware* actualizadas en todo momento.

Sin embargo, en el instante de decidir qué herramientas y sistemas de protección implantar en la organización hay que tener en cuenta las recomendaciones de la ya mencionada norma ISO 27001, en la que se describen una serie de procedimientos de concienciación de usuarios en cuanto a seguridad y también las recomendaciones sobre los requerimientos y las técnicas de actualización para las herramientas de contención y control de código malicioso.

Una vez decididas las herramientas a implantar suele suceder que el número de herramientas es muy elevado y resulta una tarea ardua llevar a cabo un control manual de estas. Como solución a esta problemática hay varias aplicaciones encargadas de gestionar la infraestructura de herramientas de detección de la organización ofreciendo estadísticas que permiten conocer su eficacia, la evolución de detección de códigos maliciosos y las medidas que se han ido tomando en cada una de las detecciones.

Para terminar, otro tipo de herramientas muy útiles para combatir los códigos maliciosos son las herramientas que generan entornos de ejecución controlada y los desensambladores.

CAPÍTULO 4 RESPUESTA ANTE INCIDENTES DE SEGURIDAD

1. INTRODUCCIÓN

La prevención y contención de los incidentes de seguridad es vital para evitar intrusiones en los equipos y, por consecuencia, daños y pérdidas de información contenida en ellos.

No obstante, cuando, a pesar de todas las medidas de prevención y contención implantadas, se produce un incidente y consigue llegar a los equipos de una organización resulta primordial establecer un plan de respuesta que permita su eliminación y la reducción de los daños provocados al mínimo posible.

En este capítulo se procede a explicar todas las recomendaciones y fases a seguir cuando se produce un incidente de este tipo. En primer lugar, la recolección de toda la información posible del incidente para identificarlo y poder restaurar los equipos a su situación de origen.

Otra fase consiste en utilizar una serie de técnicas y herramientas que analicen la información de los eventos de seguridad para conocer con precisión qué ha sucedido durante el incidente de seguridad y obtener pistas de cómo se ha podido producir.

Ante todas estas medidas hay que recordar que estas no servirían si no se verifica la intrusión, ya que es posible que simplemente sea una falsa intrusión y se estén generando alarmas innecesariamente.

Como conclusión, en este capítulo se muestran una serie de organizaciones nacionales e internacionales que ofrecen apoyo e información a las organizaciones y usuarios ante la gestión de incidentes para complementar y ayudar a la elaboración de los planes de respuesta a incidentes y así conseguir combatirlos de un modo más eficaz minimizando los riesgos de seguridad.

2. PROCEDIMIENTO DE RECOLECCIÓN DE INFORMACIÓN RELACIONADA CON INCIDENTES DE SEGURIDAD

Como ya se sabe, un incidente de seguridad es un evento o conjunto de eventos que pueden provocar la interrupción de los servicios ofrecidos por un sistema informático e incluso la pérdida de información y de activos valiosos para la organización.

La seguridad de la información consiste en el establecimiento de una serie de medidas por parte de las organizaciones que permitan proteger la información manteniendo sus propiedades de confidencialidad, disponibilidad e integridad.

Estas medidas se clasifican en:

- **Medidas preventivas:** establecimiento de contraseñas, políticas de seguridad, cortafuegos, procedimientos de copias de respaldo, concienciación del personal, etc.
- **Medidas correctivas:** procedimientos de restauración del sistema, establecimiento de esquemas de tolerancia a fallos, etc.
- **Medidas de detección:** revisiones de seguridad, análisis de registros de auditoría, análisis de *logs*, etc.

La gestión de incidentes de seguridad es la parte de la seguridad de la información encargada de asignar los recursos adecuados y necesarios a la prevención, detección y corrección de incidentes que afecten a la seguridad de la información.

Nota

Numerosas organizaciones aprenden a responder a incidentes y a amenazas de seguridad una vez ya sufrido el ataque, lo que implica un coste mayor de recuperación del sistema. Por ello es necesario concienciar a las organizaciones de las ventajas de establecer políticas de seguridad ante incidentes.

Los beneficios de aplicar una gestión de incidentes son incalculables, pero se destacan los siguientes:

- Respuesta sistemática a los incidentes de seguridad.
- Agiliza y facilita el proceso de recuperación de equipos y sistemas ante el acontecimiento de incidentes de seguridad. Además reduce la pérdida de datos y el tiempo de interrupción de servicios.
- A través del aprendizaje se previenen los incidentes reiterados.
- Mejora continua de la seguridad de la organización y del proceso de gestión y tratamiento de incidentes.
- Facilita la gestión de los aspectos legales referentes a los incidentes de seguridad.

2.1.- Equipo de respuesta de incidentes de seguridad informática (CSIRT)

La rapidez con la que se detecte, reconozca, analice y responda a una amenaza minimiza los daños y disminuye considerablemente los costes ligados a la recuperación de la información.

El término de equipo de respuesta a incidentes de seguridad informática CSIRT (*Computer Security Incident Response Team*) surgió a finales de los 90 en EE.UU ante la necesidad de designar un conjunto de personas especializadas encargadas específicamente de la gestión y tratamiento de incidentes.

Aunque generalmente solo tengan equipos de respuesta a incidentes las grandes organizaciones, toda organización, sea del tamaño que sea, debe designar a uno o varios responsables que se encarguen de ejecutar con detalle las tareas asignadas en el plan de respuesta a incidentes definido en cada organización.

Nota

En ocasiones, las empresas tienen un tamaño tan reducido que les es imposible designar a responsables de la gestión de incidentes. Ante estas situaciones es conveniente contratar a especialistas externos que realicen estas gestiones y mantengan sus datos protegidos ante todo tipo de amenazas.

El Plan de Gestión de Incidentes está elaborado por el responsable de seguridad informática de la empresa y consiste en un conjunto de tareas y procedimientos encaminados a la correcta y adecuada gestión de incidentes de seguridad junto con las personas designadas para llevar a cabo todas y cada una de estas tareas.

Un buen Plan de Gestión de Incidentes permite a las organizaciones la automatización de numerosos procesos de respuesta ante incidentes y la reducción considerable de los daños ocasionados, a la vez que se facilita la recuperación de los sistemas afectados.

El equipo de respuesta ante incidentes de seguridad, además de la confección del Plan de Gestión de Incidentes, deberá encargarse de establecer:

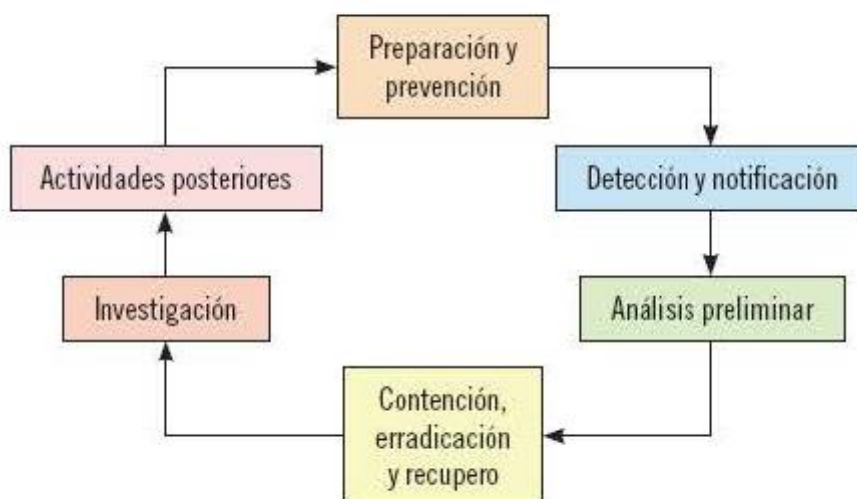
- Una política general de gestión de incidentes en la que se deberá basar el plan de gestión.
- Los procedimientos a seguir para la gestión de incidentes basados en la política e incluidos en el plan.
- Relaciones entre el equipo de respuesta a incidentes y otros grupos de la organización internos y externos.
- Las guías en las que se defina el procedimiento a seguir en la comunicación de la organización con terceros en caso de ocurrencia de incidentes.

- Organización de los responsables de la gestión de respuesta a incidentes y definición y asignación de funciones.

Ante todo, en el momento de definir el Plan de Gestión de Incidentes de seguridad hay que tener en cuenta que el procedimiento a seguir ante la posibilidad de incidentes siempre debe englobar una serie de fases:

1. Preparación y prevención de incidentes: establecimiento de medidas preventivas que minimicen el riesgo de aparición de incidentes en los sistemas de la organización.
2. Detección y notificación: establecimiento de medidas que detecten la entrada de posibles amenazas y sean capaces de notificar a los responsables su detección.
3. Análisis preliminar: análisis de la posible amenaza para ver si es una amenaza real o es una falsa alarma. En caso de ser real, análisis de la incidencia para conocer los detalles y los daños ocasionados.
4. Contención, erradicación y recuperación: establecimiento de medidas correctivas que minimicen los daños ocasionados y puedan restaurar el sistema a situaciones anteriores a la aparición de la amenaza.
5. Investigación: análisis profundo de la incidencia para conocer detalladamente su procedimiento de ataque y cómo ha podido acceder al sistema.
6. Actividades posteriores: la investigación del incidente se utiliza para llevar a cabo un procedimiento de aprendizaje que permita el establecimiento de medidas correctivas que impidan que la amenaza sucedida no pueda volver a acceder a los sistemas de la organización.

Esquema del procedimiento de gestión de incidentes



Preparación y prevención de incidentes

La fase de prevención y preparación de incidentes consiste en definir una serie de medidas que eviten lo máximo posible la entrada de intrusiones al sistema y minimicen la producción de incidentes en la organización.

En cuanto a medidas de preparación cabe destacar las siguientes:

- Definición de las políticas, normas y procedimientos para la gestión de incidentes.
- Definición de los criterios de clasificación y priorización de incidentes.
- Preparación del equipo de respuesta a incidentes de seguridad.
- Entrenamiento del personal de la organización.
- Diseño y formalización un documento en el que aparezca reflejada la topología y arquitectura de la red.
- Elaboración de un documento en el que se plasmen las configuraciones de los equipos de la organización.
- Creación de los patrones de las redes y [os sistemas.
- Activación de los *logs* en las aplicaciones y sistemas de la organización.
- Centralización y definición de una política de gestión y almacenamiento de los *logs*.
- Sincronización de los relojes de todos los equipos.
- Definición e implementación de sistemas de realización de copias de respaldo de datos.

Nota

La lista de medidas de preparación ante incidentes de seguridad es una lista abierta. En el momento de elaborar el Plan de Gestión de incidentes deberán proponerse medidas adicionales que se adapten a las características peculiares de cada sistema de información y organización.

Para una correcta aplicación de las medidas de preparación siempre resulta necesario la utilización e implantación de herramientas apropiadas que permitan la detección de incidentes, su monitorización, su análisis posterior, su documentación, etc.

Asimismo, en estas medidas se considera la categorización de los posibles incidentes que pueden ocurrir. Para ello hay que considerar dos criterios:

- **Según el tipo de incidente y los efectos negativos producidos o potenciales:** teniendo en cuenta los efectos negativos que produce o puede producir un incidente se puede elaborar una tabla de categorización de incidentes como la que se muestra:

INCIDENTE	Efectos negativos producidos O· potenciales		
	Grave	Moderado	Leve
INCIDENTE 1			

INCIDENTE 2			
INCIDENTE 3			
INCIDENTE 4			

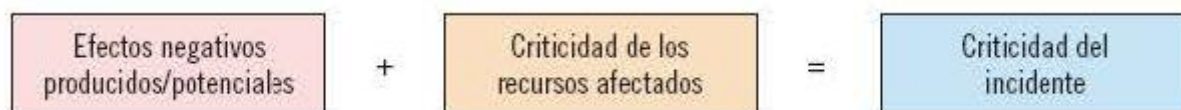
- **Según la envergadura de los daños producidos:** teniendo en cuenta la envergadura de los daños producidos y del nivel de criticidad de los recursos que han sido afectados por la incidencia, también se puede elaborar una tabla de clasificación de incidentes como la siguiente:

RECURSO	Criticidad de los recursos		
	Alta	Media	Baja
RECURSO 1			
RECURSO 2			
RECURSO 3			
RECURSO 4			

Atendiendo a estos dos criterios se establecerá el nivel de criticidad del incidente distinguiendo entre muy grave, grave, moderado y leve tal como se muestra en la siguiente tabla:

RECURSO		Criticidad de los recursos		
		Alta	Media	Baja
Efectos negativos producidos o parciales	Grave	MUY GRAVE	Grave	Moderado
	Moderado	Grave	Moderado	Leve
	Leve	Moderado	Leve	Leve

Por ejemplo, un incidente que produzca efectos negativos moderados, pero que la criticidad de los recursos a los que afecta sea alta se clasifica como incidente "grave":



De este modo, según la criticidad del incidente, dentro de las medidas de preparación será necesario establecer también el tiempo máximo en el que se deben tratar los incidentes desde el momento de su detección, siendo los siguientes:

Criticidad del incidente	Tiempo de reacción
LEVE	4 horas
MODERADO	2 horas
GRAVE	30 minutos
MUY GRAVE	10 minutos

En cuanto a las medidas de prevención de incidentes también hay que destacar algunas de ellas:

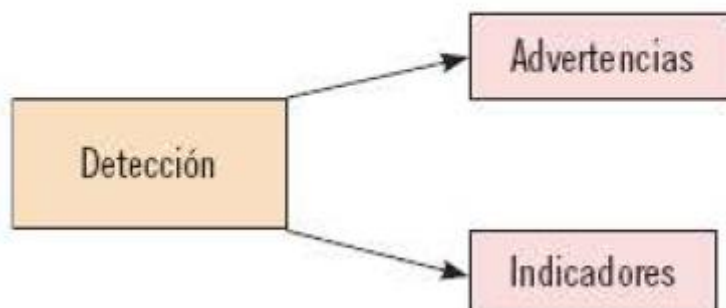
- Análisis de riesgos periódicos.
- Establecimiento de auditorías periódicas.
- Gestión eficaz de las actualizaciones.
- Establecimiento de un sistema de seguridad en la red.
- Incremento en todo lo posible de la seguridad de los equipos de la organización.
- Establecimientos de sistemas de detección y prevención de códigos maliciosos.
- Concienciación del personal de la organización.

Detección y notificación

En la fase de detección de un incidente hay que tener clara la diferencia entre advertencias e indicadores:

- Una advertencia es una señal que indica al usuario que es posible que haya ocurrido un accidente.
- Un indicador, sin embargo, señala que el incidente ya se ha producido o que se está produciendo en ese mismo momento.

Fase de detección. Advertencias e indicadores



Se consideran advertencias, por ejemplo, las amenazas de ataques web o las alertas que emiten los IDS al realizar un escaneo de la red. En cuanto a los indicadores se pueden encontrar ejemplos como:

- Detección de un virus por el antivirus.
- Ejecución lenta de las aplicaciones del equipo.
- Ralentización del acceso a webs de internet.
- Bloqueo de una cuenta de usuario por exceso de intentos fallidos de acceso.
- Cambios de configuraciones de aplicaciones sin permiso del usuario.

Para llevar a cabo la fase de detección de incidentes las organizaciones pueden implantar herramientas y técnicas de detección de incidentes como:

- Sistemas IDS/IPS.
- Antivirus.
- Sistemas de monitorización de la red.
- Análisis de los registros de auditoría o *logs*.
- Aplicaciones de control de integridad de los archivos y datos.

Recuerde

Hay que tener en cuenta que cada una de las herramientas y técnicas de detección de incidentes tiene unas características particulares, con lo que habrá que plantearse la opción de implantar varias herramientas que permitan reducir el riesgo de incidentes al mínimo y maximizar las probabilidades de detección de incidentes e intrusiones.

En cuanto a la notificación del incidente, las organizaciones, en su Plan de Gestión de Incidentes, deben diseñar un proceso de notificación en el que se incluyan las pautas, procedimientos y métodos de notificación que hay que llevar a cabo en cuanto se detecta un incidente.

En el formulario de notificaciones es imprescindible añadir una serie de datos referentes al incidente reflejados en el siguiente ejemplo:

Características del incidente	Incidente detectado 1
Datos del reporte:	
Identificación del incidente	Troyano.
Fecha y hora	25.03.2013 20:00:23
Datos del incidente:	
Clasificación	Moderado.
Breve descripción	Intento fallido de acceso del código malicioso troyano.
Efectos y daños producidos	Ninguno.
Descripción detallada	Intento de acceso de un troyano espía que ha sido interceptado por el sistema de protección del antivirus, impidiendo la producción de cualquier daño en el equipo. Reacción correcta de la seguridad del sistema.
Datos de la solución:	
Estado	Resuelto.
Fecha de cierre	25.03.2013 20:00:40
Detalles de la solución	No ha sido necesaria más intervención que la propia realizada por el antivirus.

Una vez redactado el formulario del incidente, el Plan de Gestión de Incidentes debe definir a quién hay que notificarlo, atendiendo al tipo de incidente y su relevancia. Los interesados a los que se les debe notificar pueden ser de lo más variado, siendo algunos el mismo personal de informática, el responsable de seguridad, los dueños de la información afectada, altos directivos de la organización, etc.

Análisis preliminar

La fase de análisis preliminar del posible incidente consiste en realizar un análisis de los indicadores y advertencias disponibles para detectar si realmente es un incidente de seguridad o es una falsa alarma.

En caso de ser un incidente real se debe seguir un proceso de recolección de información para analizar una serie de ítems como:

- El alcance del incidente: redes, equipos, sistemas y aplicaciones afectados.
- Qué ha sido lo que ha originado el incidente.
- Impacto del incidente en las actividades, servicios y procesos de la organización.
- Cómo ha ocurrido o está ocurriendo el incidente en cuanto a métodos y herramientas utilizadas, vulnerabilidades detectadas y explotadas, etc.

Nota

La fase de análisis preliminar es una de las fases más relevantes de la gestión de incidentes de seguridad: si la información previa se obtiene erróneamente pueden ocasionarse errores en el tratamiento del incidente y, como consecuencia, unos efectos negativos de este bastante mayores.

En cuanto al alcance del incidente se puede determinar teniendo en cuenta aspectos como:

- Cantidad de equipos comprometidos.
- Cantidad de redes afectadas.
- Nivel de privilegio alcanzado por la intrusión.
- Nivel de riesgo de las aplicaciones críticas.
- Nivel de riesgo general de los equipos y de la red.
- Nivel de conocimiento de la vulnerabilidad explotada por la intrusión. Análisis de los demás equipos para comprobar si tienen la misma vulnerabilidad.

Procedimiento de detección de incidentes



Quando se ha clasificado el incidente como real, se pueden utilizar varios métodos y formas de recolectar información para obtener un conocimiento más profundo y detallado del incidente y de su alcance:

- Indagación a los administradores del sistema.
- Indagación al personal que forma parte de la organización.
- Revisión de los reportes de los sistemas y herramientas IDS.
- Revisión de los *logs* referentes a las comunicaciones y sistemas.
- Revisión de la topología y arquitectura de la red.
- Revisión de las listas de acceso a la red.

Nota

El proceso de recolección de información del incidente de seguridad resulta especialmente útil para conocer su origen específico y detectar a su causante, pudiendo, en caso de ser procedente, emprender medidas legales contra este.

La utilización de estas herramientas y técnicas será muy útil para obtener información vital del incidente que permitirá el establecimiento de medidas de contención y erradicación del mismo, además de la propuesta de medidas correctivas para impedir futuras ocurrencias de este incidente. Algunos de los datos recolectados a través del proceso de recogida de información pueden ser:

- Información de los sucesos anormales en los sistemas y en las actividades rutinarias.
- Detección de actividades anormales.

- Conocimiento de los detalles concretos del incidente.
- Detección de cambios no autorizados.

3. EXPOSICIÓN DE LAS DISTINTAS TÉCNICAS Y HERRAMIENTAS UTILIZADAS PARA EL ANÁLISIS Y CORRELACIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD

Uno de los conceptos en los que está basada la gestión de riesgos de seguridad de la información es el análisis y la gestión de *logs* y la correlación de eventos de seguridad.

Una gestión adecuada facilitará al responsable de seguridad conocer con detalle todo lo que está ocurriendo (en términos de seguridad) en los equipos de la red a tiempo real, reducirá el tiempo de reacción y de toma de medidas correctivas ante incidentes y, como consecuencia, disminuirá considerablemente los daños que pueda ocasionar algún incidente de seguridad.

Las herramientas de correlación de eventos permiten llevar a cabo una gestión más eficiente de todos los sistemas, herramientas y aplicaciones críticas mediante su monitorización. Además, la gestión de eventos de seguridad facilita la detección de posibles vulnerabilidades y amenazas con el fin de conseguir minimizar los riesgos de intrusiones.

Las herramientas de gestión de información y eventos de seguridad son un conjunto de productos cuya función es la gestión de eventos o incidentes de seguridad en cualquiera de sus fases, tanto antes, como durante o después de la ocurrencia del incidente. Se encargan de recoger, cotejar y elaborar informes con los datos facilitados por los *logs*.

Además, también permiten llevar a cabo un tratamiento organizado de los incidentes con el fin de resolverlos en el menor tiempo posible intentando minimizar los daños ocasionados.

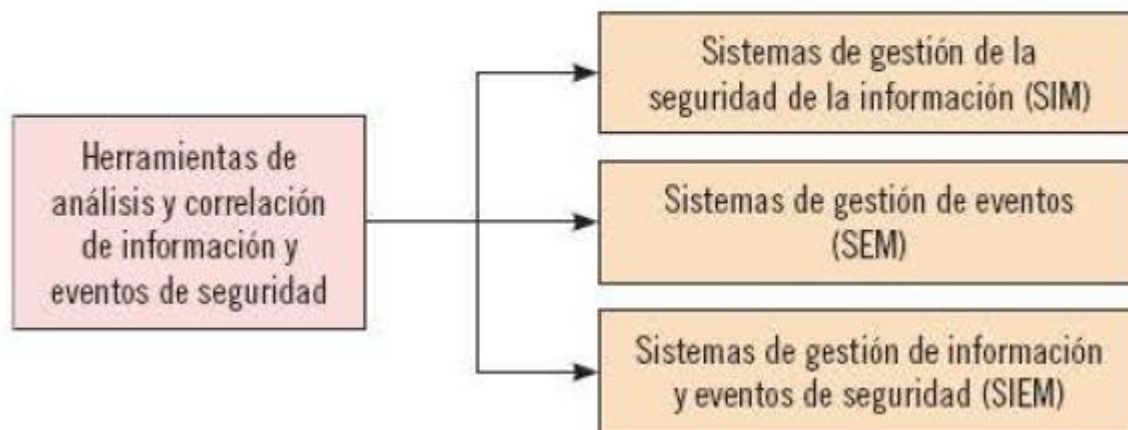
Un sistema de análisis y correlación de eventos adecuado debe permitir:

- La determinación en tiempo real de la probabilidad de materializarse una amenaza en un momento concreto.
- La detección a tiempo real del inicio de un ataque, emitiendo alertas con la menor demora posible.
- El conocimiento del éxito o fracaso de un ataque y de su impacto real sobre el sistema.
- La determinación de los patrones de materialización de las amenazas para ser utilizados en la implantación de nuevas medidas de seguridad.

Entre las técnicas y herramientas utilizadas para el análisis y correlación de información y eventos de seguridad se distinguen tres tipos de sistemas:

- Sistemas de gestión de la seguridad de la información o SIM (*Security Information Management*).
- Sistemas de gestión de eventos o SEM (*Security Event Management*).
- Sistemas de gestión de información y eventos de seguridad o SIEM (*Security Information and Event Management*).

Esquema de herramientas de análisis y correlación de información y eventos de seguridad



3.1.- Sistemas de gestión de la seguridad de la información (SIM)

Las herramientas de gestión de seguridad de la información o SIM son sistemas de supervisión cuyas metas principales son la recogida, correlación y el análisis de la información de seguridad en diferido, no a tiempo real. Estas funciones las llevan a cabo mediante la creación de una base de datos indexada basada en los datos obtenidos en las supervisiones realizadas a los equipos y dispositivos.

Entre sus funciones principales cabe destacar:

- Recogida, ordenación y correlación de información de la red.
- Automatización y monitorización de los eventos de sistemas y dispositivos de seguridad.
- Centralización, correlación y priorización de eventos con el fin de:
 - Estandarizar los eventos.
 - Reducir lo máximo posible el tiempo de detección de ataques y vulnerabilidades en la red.
 - Minimizar la información a procesar para obtener mejoras de rendimiento.

Nota

Las herramientas SIM ayudan a centralizar y administrar la información de los eventos de seguridad mediante reportes de análisis de archivos de registro y reportes de cumplimiento

Por todas estas funciones las herramientas de gestión de seguridad de la información se utilizan sobre todo para:

- Administrar la infraestructura de la red y de los activos de la organización.
- Centralizar y monitorizar los componentes de la infraestructura de seguridad de la organización.
- Analizar con mayor facilidad la información suministrada por los componentes de seguridad.
- Predecir y pronosticar amenazas.
- Correlacionar eventos de seguridad.
- Detectar, identificar y emitir reportes de eventos de seguridad.
- Realizar un análisis forense de los eventos.
- Establecer políticas de seguridad más adecuadas.

3.2.- Sistemas de gestión de eventos (SEM)

Los sistemas de gestión de eventos o sistemas SEM se encargan de monitorizar y gestionar los eventos prácticamente a tiempo real. Su función principal consiste en recoger los datos de los eventos de seguridad producidos en los distintos equipos, sistemas y dispositivos con el fin de realizar análisis a tiempo real y responder en el menor tiempo posible.

Los beneficios principales que aportan estas herramientas de gestión de eventos son:

- Acceso a los registros a través de una interfaz central consistente.
- Almacenamiento seguro de los registros, manteniendo su integridad.
- Representación gráfica de la actividad para una elaboración de informes más sencilla, visual y práctica.
- Activación de alertas programadas.
- Gestión de eventos de varios sistemas operativos.
- Recuperación de registros ante bloqueos del sistema o eliminación inesperada de registros.

Recuerde

A parte de las distintas funciones de las herramientas SIM y SEM hay que remarcar que las herramientas SIM trabajan en diferido (análisis del incidente una vez ya ha sucedido) mientras que las herramientas SEM trabajan a tiempo real (análisis del incidente cuando está ocurriendo).

En definitiva, las herramientas SEM permiten la visualización, monitorización y gestión de eventos que detecten las situaciones anómalas y automaticen las respuestas y medidas correctivas en caso de aparición de incidentes de seguridad.

3.3.- Sistemas de información y eventos de seguridad (SIEM)

Las herramientas de información y eventos de seguridad o herramientas SIEM son una mezcla de las herramientas SIM y SEM, englobando las funcionalidades de ambas: recogen los *logs* de los equipos, sistemas y dispositivos monitorizados, los almacenan a largo plazo y, además, agregan y correlacionan en tiempo real la información recibida, todo ello para lograr una detección y establecimiento de medidas más eficaz, minimizando los daños ocasionados.

Son herramientas que permiten una gestión de incidentes de seguridad más global y entre sus funciones principales destacan:

- Detección de anomalías y amenazas.
- Análisis de todas las fases del incidente.
- Captura total de los paquetes de la red.
- Conocimiento del comportamiento del usuario y su contexto.
- Cumplimiento de nuevas normativas.
- Administración más efectiva del riesgo gracias a información obtenida como:
 - Topología y arquitectura de la red.
 - Vulnerabilidades detectadas.
 - Parámetros de configuración del equipo y de los dispositivos.
 - Análisis de fallos.
 - Priorización de vulnerabilidades.
 - Correlación avanzada y profunda de los eventos.

Las herramientas SIM, SEM y SIEM disponibles en el mercado son de lo más variadas. Aun así, las herramientas SIEM generalmente suelen decantarse por disponer más herramientas SIM o SEM atendiendo a las funcionalidades que pretenden cubrir. Por ello, en el momento de elegir una herramienta, las organizaciones deben realizar un análisis previo de necesidades y prioridades para elegir la herramienta más adecuada y pertinente.

Una de estas herramientas es la ofrecida por IBM *Tivoli Security Information and Event Manager*. Esta ofrece las siguientes funciones:

- Seguimiento y gestión priorizada de los incidentes en curso.
- Consola de gestión basada en la web.
- Agregación automática de *logs* del sistema.
- Elaboración de informes.
- Acceso privilegiado a funciones de monitorización y auditoría para rastrear los eventos sin delatar al autor.
- Reflejo del análisis de los *logs* en un cuadro de mando único.



Event type	#Events	#Pol. Excp.	#Spec. Att	#Fail.
Access : Dobject / Success	3411	0	5	0
Add : User / Success	19	0	0	0
Change : Password / Success	10	0	0	0
Create : User / Success	9	0	0	0
Delete : Dobject / Success	18	0	0	0
Delete : User / Success	9	0	0	0
Enable : User / Success	9	0	0	0
Execute : Dobject / Success	8598	0	0	0
Grant : Authenticationticket / Success	23	0	0	0
Grant : Privilege / Success	1059	0	0	0
Grant : Serviceticket / Success	185	0	0	0
Insert : Dobject / Success	6	0	0	0
List : Connection / Success	3	0	0	0
Logoff : User / Success	1644	0	0	0
Login : User / Success	1608	0	0	0
Modify : Access / Success	2	0	0	0
Modify : Group / Success	20	0	20	0
Modify : Syovar / Success	16	0	0	0
Modify : User / Success	31	0	0	0
Open : Object / Success	812	0	0	0
Read : Access / Success	12	0	0	0
Read : File / Success	2337	0	0	0
Read : Syovar / Success	152	0	0	0
Refresh : Certificate / Success	10	0	0	0
Remove : User / Success	1	0	0	0

Tivoli Security and Event Manager

4. PROCESO DE VERIFICACIÓN DE LA INTRUSIÓN

En este epígrafe se describe el proceso de verificación de la intrusión, pero para ello es fundamental comentar antes las fases previas para una mayor comprensión del proceso.

4.1.- Contención, erradicación y recuperación ante incidentes de seguridad

Como ya se sabe, el incidente debe pasar por las fases de prevención y preparación, detección y notificación y análisis preliminar.

A partir de ahí, y una vez verificado que un incidente es real y concluido el proceso de recolección de información, para conocer con más profundidad sus detalles se prosigue con la fase de contención, erradicación y recuperación.

La contención consiste en evitar que el incidente siga produciendo más daños, la erradicación en eliminar aquello que provocó el incidente y todo el rastro de los daños producidos y la

recuperación en devolver los sistemas, dispositivos y equipos a su estado original antes de producirse el incidente.

Fases de contención, erradicación y recuperación



Por ejemplo, cuando se produce una infección de un virus en el equipo en las fases de contención, erradicación y recuperación debería realizarse lo siguiente:

- **Contención:** desconectar el equipo afectado de la red para impedir que se propague a los demás equipos.
- **Erradicación:** con un antivirus, localizar el virus y eliminarlo del equipo.
- **Recuperación:** restaurar el sistema dañado con la última copia de respaldo realizada con los datos del equipo.

Nota

La rapidez con la que se lleven a cabo las medidas de contención, erradicación y recuperación es de suma importancia para evitar la expansión de los posibles daños causados por el incidente de seguridad. Además, cuanto antes se recupere la situación normal, antes se podrá recuperar la actividad habitual y dar servicio al cliente minimizando las pérdidas de calidad ocasionadas por la suspensión del servicio.

4.2.- Elaboración del informe final del incidente

Cuando ya se ha eliminado el incidente y se ha podido volver a la situación original, lo siguiente que debe realizarse es el proceso de investigación del incidente y la realización de actividades posteriores (como la definición de nuevas medidas de seguridad) con la información obtenida en el proceso de investigación.

En la investigación del incidente se debe realizar la verificación de la intrusión mediante la elaboración de un informe final que deber contener, como mínimo, los aspectos que se reflejan en la tabla siguiente:

Aspectos a reflejar en el informe	Actividades a realizar
Análisis de las causas y consecuencias del incidente	Revisión exhaustiva de los logs de los equipos, sistemas y dispositivos afectados por el incidente.
	Análisis de las consecuencias que hayan podido afectar a terceros.
	Análisis de la información del incidente compartida con terceros.
	Cuantificación del coste de los daños provocados por la intrusión en la organización en cuanto a daño en equipos, aplicaciones afectadas, información perdida, personal técnico especializado contratado, etc.
	Estudio de la documentación elaborada por el equipo de respuesta a incidentes de seguridad.
Evaluación de la toma de decisiones y de las actuaciones llevadas a cabo por el equipo de respuesta a incidentes	Evaluación y control de las posibles acciones legales que se hayan podido emprender por el incidente.
	Rapidez de respuesta en decisiones y medidas tomadas por el equipo de respuesta a incidentes.
	Personal integrante, formación recibida, organización y papeles asignados en el equipo de respuesta a incidentes.
	Implementación de nuevas herramientas necesarias para evitar futuros incidentes.
Análisis de las políticas de seguridad	Evaluación de los procedimientos y de las herramientas técnicas utilizadas en la respuesta al incidente:
	<ul style="list-style-type: none"> - Los procedimientos que no hayan funcionado deben rediseñarse. - Se deben adoptar medidas correctivas que mejoren la respuesta ante futuras incidencias.
Análisis de las políticas de seguridad	Revisión de las políticas de seguridad de la información para detectar fallos y redefinir aquellas pautas ineficientes.
Análisis de directrices de la organización	Revisión de las directrices actuales de la organización e implantación de nuevas directrices para reforzar su nivel de seguridad.

Con la evaluación y análisis de todos los aspectos reflejados en el informe de verificación del incidente ya se puede obtener una imagen global de por qué sucedió la intrusión, qué es lo que ha quedado afectado, cómo se ha actuado al respecto y qué hay que modificar para que no vuelva a ocurrir.

De este modo se realiza un proceso de aprendizaje del incidente para que en futuras intrusiones la respuesta sea más rápida y efectiva y los daños ocasionados sean lo más reducidos posible.

4.3.- Documentación del incidente

Para que el proceso de aprendizaje del incidente sea más efectivo y no se olviden detalles se recomienda llevar a cabo una documentación del incidente comentando su evolución en todas las fases.

¿Qué documentar del incidente? Hay que documentar de un modo concreto y preciso los aspectos más fundamentales y que no deben olvidarse una vez solucionado el incidente. Más concretamente, la documentación del incidente de seguridad debe incluir:

- Reporte del incidente en el que se debe especificar:
 - Tipo de incidente.
 - Hechos ocurridos.
 - Daños ocasionados.
- Estado actual del incidente (fechando las distintas etapas por las que ha ido pasando el incidente).
- Conclusiones del análisis.
- Acciones y medidas tomadas para erradicar el incidente y restaurar los equipos afectados.
- Evidencias obtenidas en el proceso de análisis posterior.
- Personas involucradas, tanto a nivel interno de la empresa como a nivel externo (terceros).
- Acciones futuras y recomendaciones para aumentar el nivel de seguridad y evitar incidencias similares en próximas ocasiones.

Nota

El proceso de documentación de un incidente debe iniciarse en el momento de su detección, y debe actualizarse y continuarse a medida que va avanzando su situación.

Una adecuada documentación de los incidentes facilita el estudio e investigación posterior de sus causas y consecuencias. Hay que tener en cuenta que es información muy delicada y que afecta directamente a los recursos de una organización, por lo que hay que tener especial cuidado en que

los documentos elaborados estén bajo protección para evitar accesos de personal no autorizado que pueda utilizarlos malintencionadamente.

5. NATURALEZA Y FUNCIONES DE LOS ORGANISMOS DE GESTIÓN DE INCIDENTES TIPO CERT NACIONALES E INTERNACIONALES

Actualmente, las tecnologías de la información (TIC) se han desarrollado de tal modo que se han convertido en una de las herramientas más básicas para la gestión y el buen funcionamiento de las organizaciones hasta el punto de resultar imprescindibles.

Las TIC se han ido desarrollando a un ritmo tan veloz que es necesario aumentar las medidas para combatir problemas de seguridad, ataques, intrusiones y problemas de vulnerabilidades que cada vez son más sofisticados y dañinos.

5.1.- Organismos CERT/CSIRT

Para combatir más eficazmente estas amenazas a la seguridad de los sistemas informáticos se han ido creando estos últimos años distintos organismos encargados de realizar tareas de información y concienciación hacia los gobiernos, empresas y usuarios para conseguir contener amenazas y reducir los daños que pueden ocasionar.

Con estas motivaciones surgieron los CERT (*Computer Emergency Response Team*) o equipo de respuesta ante emergencias informáticas. Son centros de respuesta a incidentes de seguridad en tecnologías de información formados por un grupo de expertos encargados de diseñar medidas preventivas y reactivas ante incidentes de seguridad.

También surgieron los CSIRT (*Computer Security Incident Response Team*) o equipo de respuesta a incidentes de seguridad informática, organización encargada de recibir, revisar y responder a actividades y reportes de incidentes de seguridad informática ya vista anteriormente.

Nota

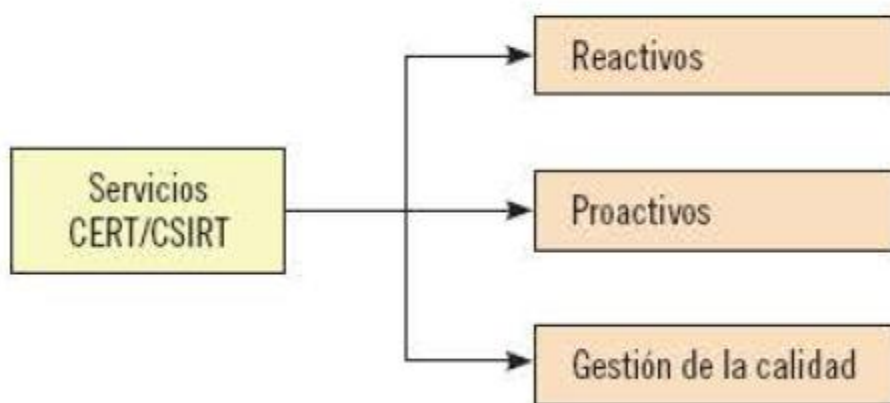
El término CSIRT suele utilizarse en Europa en lugar del término CERT al estar registrado por los Estados Unidos por el CERT Coordination Center o CERT/CC.

De los CERT/CSIRT hay que destacar tres tipos de servicios distintos:

- **Servicios reactivos:** elaboración de informes de equipos, sistemas y dispositivos afectados por amenazas, códigos maliciosos, vulnerabilidades y otros eventos de seguridad detectados en los registros. Estas actividades son las funciones principales de los CERT y CSIRT. Los servicios principales son:

- Análisis de la situación.
- Elaboración de recomendaciones para controlar la situación ante incidentes.
- Diseño de contramedidas de seguridad para reducir el riesgo de futuras amenazas.
- **Servicios proactivos:** servicios de asistencia e información para ayudar a prevenir, preparar y proteger los sistemas, equipos y dispositivos de los usuarios para reducir el riesgo de producción de amenazas e incidentes en un futuro.
- Servicios de gestión de calidad de la seguridad: servicios independientes de la gestión de incidentes encargados de buscar herramientas y medidas que mejoren la calidad de la seguridad informática. Se basan sobre todo en actividades de concienciación y educación de los usuarios.

Esquema de las funcionalidades de los servicios (CERT/CSIRT)



En cuanto a funciones de estos organismos cabe destacar las siguientes:

- Ayudar al público objetivo a prevenir y atenuar incidentes graves de seguridad.
- Ayudar a proteger informaciones y datos de gran valor.
- Coordinar centralizadamente la seguridad de la información.
- Apoyar y asistir a los usuarios para que el proceso de recuperación ante incidentes de seguridad sea lo más leve posible.
- Dirigir centralizadamente la respuesta ante incidentes de seguridad.
- Para desempeñar sus funciones los CSIRT/CERT las llevan a cabo mediante:
- El mantenimiento de una base de datos de vulnerabilidades de seguridad para consulta, seguimiento y registro histórico.
- El mantenimiento de una base de datos de incidentes de seguridad de las organizaciones integrantes.
- Provisión de un servicio de asesoramiento especializado en seguridad de la información.
- Mantenimiento de contactos con otros CSIRT /CERT del mundo y sus organizaciones para intercambiar información.

5.2.- Otros organismos de gestión de incidentes

A continuación se van a ir describiendo los organismos de gestión de incidentes más relevantes a nivel nacional e internacional.

CERT/CC (*Computer Emergency Response Team/Coordination Center*)

El CERT/CC o equipo de respuesta a emergencias informáticas fue el primer equipo de respuesta y el más conocido. Su creación se produjo en 1.988 por la agencia DARPA de EE. UU con la finalidad de gestionar aquellos incidentes de seguridad relacionados con los servicios de internet.

Se puede consultar información del CERT/CC en: <<http://www.cert.org>>.

Logotipo del organismo CERT/CC



Cert Inteco

Cert Inteco es el Centro de Respuesta a Incidentes de Seguridad en España. Fue creado en 2.006 dentro del Instituto Nacional de Tecnologías de la Comunicación y sus funciones se clasifican en tres pilares fundamentales:

- **Servicios:** Inteco ofrece servicios de seguridad para proteger la privacidad de los usuarios y desarrollar herramientas que mejoren la efectividad de las medidas de prevención y reacción ante incidentes de seguridad.
- **Investigación:** además de los servicios, también desarrolla funciones de investigación para analizar proyectos complejos de ciberseguridad y aplicar tecnologías y mecanismos emergentes en el combate de incidentes de seguridad.
- **Coordinación:** Inteco también se coordina y colabora con otras entidades (públicas y privadas, nacionales e internacionales) para intercambiar información y facilitar la inmediatez, globalidad y efectividad de las medidas a tomar ante incidentes de seguridad.

En cuanto a los servicios ofrecidos por este organismo, estos se dirigen a tres tipos de público objetivo distintos:

- Empresas y profesionales que utilizan las tecnologías de la información en su actividad económica.
- Colectivos de expertos en ciberseguridad.

- Ciudadanos: a través de la Oficina de Seguridad del Internauta (OSI) que ofrece información y servicios a los usuarios gratuitamente.

Cert Inteco	
Funciones	Servicios
	Investigación
	Coordinación
Público objetivo	Empresas y profesionales
	Expertos en ciberseguridad
	Ciudadanos
	Se

Se puede encontrar más información de los servicios y funciones de Inteco en <http://www.inteco.es>.

Logotipo del organismo Cert Inteco



Agencia Europea de Seguridad de las Redes de la Información

La Agencia Europea de Seguridad de las Redes y de la Información (*European Network and Information Security Agency*) se creó por decisión del Consejo y Parlamento Europeo para elevar los niveles de seguridad de las redes y del tratamiento de la información dentro de la Unión Europea. Se creó en 2.005 y fijó su sede en Grecia, en la isla de Creta.

Su web oficial es <http://www.enisa.europa.eu>.

Logotipo de la Agencia Europea de Seguridad de las Redes y de la Información



Forum of Incident Response and Security Teams (FIRST)

El *Forum of Incident Response and Security Teams* se creó en 1.990 con la finalidad de agilizar los procesos de intercambio de información sobre los incidentes de los centros de respuesta a incidentes de seguridad que integran la organización.

Se considera la asociación global de los CSIRT/CERT y su web oficial es <<http://www.first.org>>.

Logotipo del organismo FIRST



Resumen

La gestión de incidentes es la parte de la seguridad que se encarga de asignar los recursos a la prevención, detección y corrección de incidentes que afecten a la seguridad de la información.

Esta gestión conlleva una serie de pasos a seguir: preparación y prevención, detección y notificación, análisis preliminar, contención, erradicación y recuperación, investigación y actividades posteriores. Todos estos pasos ayudan a las organizaciones a obtener más información del incidente, evaluar los daños causados, tomar medidas al respecto y a conseguir llegar al punto inicial en el menor tiempo posible. Además, con la recolección de información se consigue analizar todo el procedimiento llevado a cabo por el incidente y elaborar medidas preventivas evitando que este incidente se vuelva a producir.

Por su parte, la gestión de riesgos de seguridad de la información basada en el análisis y correlación de información y eventos de seguridad (con herramientas SI M, SEM y SIEM) facilitará al responsable de seguridad el conocimiento de todo lo que sucede en los equipos a tiempo real y

así, conseguir establecer medidas de contención más efectivas y rápidas en cuanto se detecte algún indicio de incidente de seguridad.

Una vez detectado y eliminado el incidente y restaurada la situación original debe procederse a la investigación y verificación del incidente con el fin de elaborar un informe final que contenga aspectos fundamentales acerca de las causas y consecuencias producidas por el incidente, la evaluación de la toma de decisiones y actuaciones llevadas a cabo por el equipo de respuesta a incidentes, el análisis de las políticas de seguridad y el análisis de las directrices de la organización.

Para establecer estas medidas y herramientas hay una serie de organizaciones nacionales e internacionales conocidas como CERT o centros de respuesta a incidentes de seguridad en tecnologías de la información encargadas de diseñar medidas preventivas y reactivas, mantener bases de datos de incidentes actualizadas y, en general, de apoyar y ofrecer información valiosa a las organizaciones que les ayuden a elaborar un Plan de Gestión de Incidentes de mayor calidad.

CAPÍTULO 5 PROCESO DE NOTIFICACIÓN Y GESTIÓN DE INTENTOS DE INTRUSIÓN

1. INTRODUCCIÓN

Cuando se detecta un intento de intrusión es recomendable seguir un procedimiento definido claramente por las organizaciones para que la gestión de dicha intrusión se realice correctamente y se minimicen todo lo posible sus efectos negativos.

En este procedimiento hay que designar a una serie de responsables encargados de la gestión de la intrusión o de la incidencia que realicen búsquedas de información adicional para confirmar la intrusión o para declararla como una falsa alarma.

Si la incidencia se declara como real deberá categorizarse según su impacto potencial y deberán recogerse detalles adicionales sobre cómo ha podido acceder en el sistema y cómo ha evolucionado desde que se detectó.

En este capítulo se comentan con detalle y profundidad todas las fases de gestión de intentos de intrusión: desde la detección de indicios hasta su cierre, pasando por el procedimiento de control que hay que llevar a cabo a lo largo de toda la gestión.

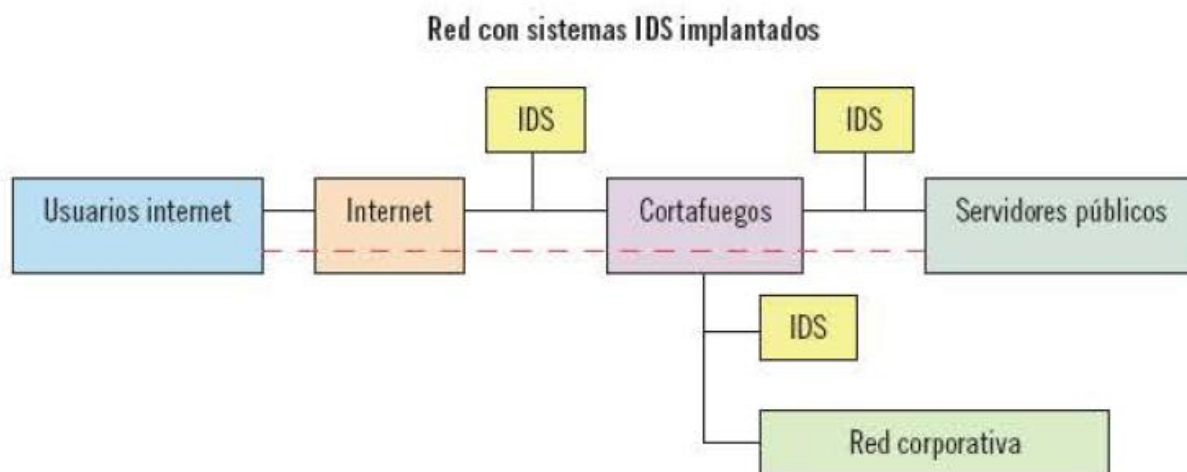
Con estos conocimientos será posible defenderse ante la presencia de intrusiones y gestionar todos los recursos de la empresa o de los equipos para contener los daños y conseguir erradicar las incidencias en el menor tiempo posible.

2. ESTABLECIMIENTO DE LAS RESPONSABILIDADES EN EL PROCESO DE NOTIFICACIÓN Y GESTIÓN DE INTENTOS DE INTRUSIÓN O INFECCIONES

Una intrusión, como ya se sabe, es un evento en el cual un usuario no autorizado intenta acceder a los equipos y/o dispositivos de una red para comprometer la integridad, confidencialidad y disponibilidad de la información poniendo en peligro su seguridad y la puesta a disposición de la misma a manos de usuarios malintencionados.

Para evitar y prevenir este tipo de intrusiones se utilizan herramientas como cortafuegos y sistemas de detección y prevención de intrusiones o IDS/IPS. La elección del IDS/IPS correcto es una decisión de gran responsabilidad por las consecuencias de las que puede derivar una mala elección. Por ello se recomienda seguir una serie de criterios en el momento de realizar la elección:

- **Escalabilidad:** capacidad de la herramienta de adaptarse a los cambios de tráfico de la red. Es recomendable que los IDS/IPS sigan funcionando correctamente tanto a niveles mínimos de tráfico de red como en momentos de hora punta en el que el tráfico es mucho más elevado.
- **Firmas de ataque utilizadas:** los IDS/IPS son de mayor calidad cuando utilizan un mayor número de firmas de ataque porque se reducen las posibilidades de obtener falsos positivos o negativos al disponer de una base de datos de ataques más amplia.
- **Capacidad de administración y gestión:** cuantas más funcionalidades de autogestión y de administración tenga el IDS/IPS, más sencilla será su utilización. Por ello se recomienda buscar herramientas que tengan funciones propias de examen de logs, capacidad de archivo, gestión de alarmas, consola centralizada, etc.
- **Tipo de estructura de hardware utilizada:** la topología de la red y la disposición de los equipos y cortafuegos también son unos elementos a tener en cuenta en el momento de elegir el IDS/IPS adecuado. Atendiendo a la ubicación del cortafuegos puede interesar un IDS/IPS con funcionalidades distintas. Por ejemplo, en la siguiente imagen se ha decidido ubicar varios IDS antes y después del cortafuegos para aumentar el nivel de seguridad de la información:



2.1.- Responsabilidades de gestión y notificación de intrusiones

La elección del correcto sistema de detección y prevención de intrusiones es fundamental para lograr una protección adecuada de la información contenida en los equipos de una organización.

No obstante, por muy bueno que sea el IDS/IPS su efectividad no servirá para nada si no hay un procedimiento adecuado de tratamiento del incidente: las organizaciones deben establecer un procedimiento de gestión y notificación de intrusiones para que el tiempo de respuesta sea lo más reducido posible y los daños producidos sean los mínimos.

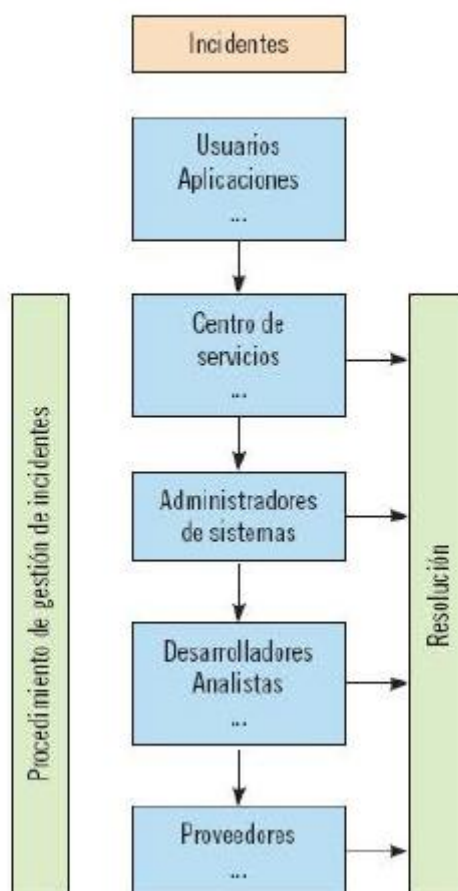
Para realizar este proceso de gestión y notificación de intrusiones es necesaria la designación de responsables cuya función principal sea la de localizar las intrusiones detectadas por los sistemas de protección y remitir la información a las personas adecuadas y encargadas de tomar medidas de respuesta ante el incidente o intrusión.

De este modo las organizaciones, atendiendo a sus necesidades de protección de datos, deberán formar una estructura integrada por varias áreas que sea capaz de:

- Detectar cualquier alteración de los servicios ofrecidos por la organización.
- Registrar y clasificar estos incidentes.
- Asignar al personal encargado de restaurar la situación al punto previo de la producción del incidente.

El proceso de gestión de incidentes debe atender a una estructura similar a la que se muestra en la siguiente imagen.

Estructura del proceso de gestión de incidentes



Como se muestra en la imagen, en el momento que los usuarios o aplicaciones detectan una intrusión hay varias áreas que se pueden encargar de llevar a cabo su gestión:

- Centro de servicios: es el primer nivel de gestión de intrusiones, el punto de contacto entre los usuarios y la gestión de estas. Se encargan de dar soporte en la gestión realizando funciones como:
 - Registro y monitorización de incidentes.
 - Aplicación de soluciones temporales y provisionales ante ataques e intrusiones.
 - Colaboran con niveles superiores en la elaboración de bases de datos de intrusiones.

Como se puede deducir son el primer punto de contacto con la intrusión y se encargan de resolver problemas básicos e intrusiones sencillas de combatir.

- Administradores de sistemas: tienen un conocimiento más profundo del funcionamiento de las intrusiones y ataques y los que realmente son capaces de desarrollar respuestas rápidas ante ataques más complejos.
- Desarrolladores y analistas: tienen conocimientos avanzados sobre las posibles intrusiones que pueden acceder al sistema, su comportamiento y su funcionamiento interno. Pueden

desarrollar herramientas de contraataque y protección avanzada ante intrusiones desconocidas.

- Proveedores: son el último escalón, cuando la organización no ha sido capaz de combatir el incidente solo queda acudir al proveedor de la herramienta del IDS/IPS implantada para que, con consultas avanzadas en sus bases de datos, puedan facilitar una solución al problema.

El nivel de complejidad de la intrusión será lo que determine la derivación de la misma a un nivel u otro de la organización para encargarse de su erradicación y de restaurar los sistemas. Así, a mayor complejidad de la intrusión, mayores serán los conocimientos que deberán tener los responsables de su erradicación y, por lo tanto, más alto será el nivel al que se deberá notificar su aparición.

De este modo, una correcta designación de responsabilidades y una elección adecuada en cuanto a la notificación de posibles intrusiones puede influir significativamente en el tiempo de respuesta a la intrusión.

Por ejemplo, si se elige derivar una intrusión compleja al nivel más bajo de responsabilidad, el centro de servicios lo único que podrá hacer es tomar medidas provisionales (efectivas o no) y remitir el incidente a niveles superiores.

Con ello se ha perdido un tiempo fundamental en el que la infección se puede expandir o los daños producidos pueden ser mayores. Si se hubiera derivado directamente a niveles más elevados la respuesta hubiera sido más rápida evitando daños innecesarios.

Nota

Hay que tener en cuenta que el nivel de seguridad y la necesidad específica de protección de la información de las organizaciones serán los que definan las áreas de respuesta a incidentes que integrarán en la organización. Una empresa pequeña que no requiera una especial protección puede no necesitar tener desarrolladores en su plantilla: con tener un centro de respuesta y un administrador puede ser más que suficiente.

2.2.- Obligaciones legales de gestión y notificación de incidentes de seguridad e intrusiones

Como ya se ha comentado, en España hay una especial protección de los datos de carácter personal con la Ley Orgánica de Protección de Datos (LOPD 15/1999) y su reglamento de desarrollo.

Esta normativa habla de la gestión de incidentes que afecten a datos de carácter personal y de la designación de responsables de su detección, notificación y gestión.

De este modo se obliga a las organizaciones a designar responsables de seguridad y, específicamente, responsables de ficheros que contengan datos de carácter personal. Todo ello

debe quedar plasmado en el documento de seguridad, en el que, atendiendo al nivel de seguridad de la información, el procedimiento de gestión y notificación de incidentes será distinto.

En las medidas de seguridad básicas el procedimiento de notificación y gestión de incidencias deberá contener necesariamente un registro en el que se haga constar:

- El tipo de incidencia.
- El momento en el que se ha producido la incidencia.
- La persona que realiza la notificación.
- A quién se le comunica.
- Los efectos que han derivado de la misma.

En las medidas de seguridad de nivel medio el procedimiento de gestión y notificación de incidencias deberá indicar, además de lo mencionado en las medidas de nivel básico, los procedimientos realizados de recuperación de los datos en los que deben constar:

- La persona que ejecutó el proceso.
- Los datos restaurados.
- Y, en su caso, qué datos han sido necesarios grabar manualmente en el proceso de recuperación.

El reglamento de desarrollo de la LOPD exige además la autorización por escrito del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos.

En cuanto a las medidas de seguridad de nivel alto no se habla específicamente de procedimientos de notificación y gestión de incidencias. En este aspecto solo cabe destacar la exigencia de conservar una copia de respaldo y que los procedimientos de recuperación de los datos estén en un lugar diferente de aquel en el que se encuentren los equipos informáticos, añadiendo una mayor protección y más posibilidades de éxito para restaurar los equipos a situaciones anteriores de producirse cualquier intrusión.

3. CATEGORIZACIÓN DE LOS INCIDENTES DERIVADOS DE INTENTOS DE INTRUSIÓN O INFECCIONES EN FUNCIÓN DE SU IMPACTO POTENCIAL

La clasificación de un incidente tiene como misión la recopilación de toda la información que pueda utilizarse para su resolución y para la restauración del sistema.

Este proceso de clasificación es necesario que contenga, por lo menos:

- Categorización del incidente: hay que asignarle una categoría (que puede contener más subcategorías) según el tipo de incidente que sea y los responsables designados para su gestión.
- Nivel de prioridad: según los daños causados y la urgencia del incidente se le asignará un nivel de prioridad u otro. A mayores daños y urgencia, mayor nivel de prioridad.
- Asignación de recursos: en el caso de que el centro de servicios no pueda combatir la incidencia deberán designarse técnicos especializados y recursos específicos para su resolución.

- Monitorización del estado del incidente y del tiempo de respuesta esperado: hay que asociar al incidente un estado (detectado, activo, resuelto, etc.) y un tiempo de respuesta y resolución atendiendo a sus niveles de prioridad y criticidad.

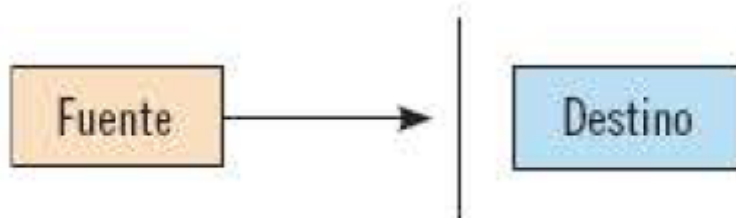
3.1.- Tipos de ataques

Antes de clasificar el incidente hay que saber qué tipo de ataque se está produciendo. En una situación normal el flujo de información circula de origen a destino sin problemas de disponibilidad, integridad y accesibilidad.

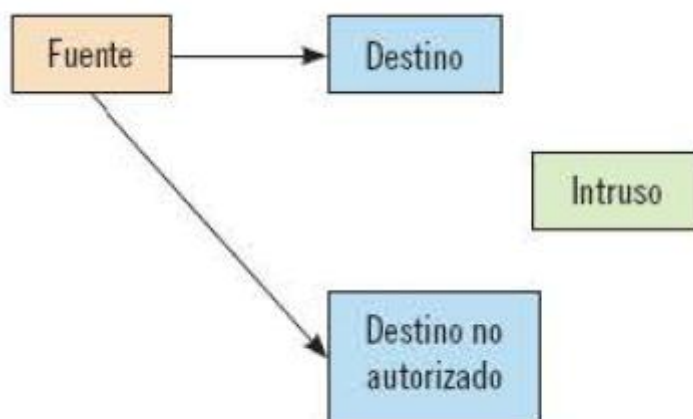


Sin embargo, en cuanto se produce un ataque se pierde alguna de las propiedades fundamentales de la información, modificándose de algún modo la recepción de la información en destino. Atendiendo a estas modificaciones los ataques deben distinguirse en:

- Ataques de interrupción: destruyen o inutilizan la información e influyen en su accesibilidad y/o disponibilidad. Son ejemplos de ataques de interrupción la destrucción de algún dispositivo o la saturación de la capacidad del procesador con el fin de dificultar la accesibilidad de los datos.



- **Ataques de interceptación:** usuarios no autorizados acceden a los datos del sistema afectando a la confidencialidad de la información. Por ejemplo, realización de copias de información no autorizadas o la obtención de contraseñas.



- **Ataques de modificación:** usuarios no autorizados modifican la información contenida en los equipos atacando a su integridad. Son ejemplos de ataques de modificación el cambio de contenidos de bases de datos, cambios en aplicaciones, cambios en datos bancarios para realizar transferencias, etc.



- **Ataques de fabricación:** los intrusos en este caso falsifican la información del sistema atacando a su autenticidad. Por ejemplo, la adición de campos o registros en bases de datos y la adición de líneas de una aplicación (adición de virus, etc.).



Todos estos tipos de ataques, a su vez, se pueden clasificar en dos grupos:

- **Ataques pasivos:** aquellos ataques en los que no hay alteración de la comunicación. En estos casos el atacante se limita a escuchar o monitorizar el tráfico de red para obtener los datos que se están transmitiendo. Son difíciles de detectar al no realizar ninguna alteración de datos.
- **Ataques activos:** en estos ataques el atacante realiza algún tipo de alteración del tráfico de red, modificándolo e incluso creando un falso tráfico. Se pueden dividir en cuatro categorías:
 - **Reactuación:** se capturan uno o múltiples mensajes legítimos para repetirlos y producir efectos no deseados por el usuario. Un ejemplo sería la repetición de transferencias a una misma cuenta sin consentimiento del usuario.
 - **Modificación de mensajes:** se altera una parte del mensaje legítimo para confundir al receptor de la información. Por ejemplo, se puede modificar un mensaje tipo "Para comprar el libro debe ingresar el dinero en la cuenta X": a otro mensaje "Para comprar el libro debe ingresar el dinero en la cuenta Y" haciendo que el receptor final del dinero no sea el destinatario legítimo.
 - **Suplantación de identidad o *phishing*:** en este caso el intruso simula ser otra entidad diferente. Es muy habitual la duplicación de páginas web bancarias haciéndose pasar por la entidad real, cuando en realidad se están facilitando datos confidenciales (contraseñas bancarias sobretodo) a usuarios no legítimos.
 - **Degradación fraudulenta del servicio:** el atacante impide la utilización normal de las comunicaciones y de los recursos informáticos. Por ejemplo, se puede interrumpir el servicio de una red lanzándole multitud de mensajes para saturarla.

En la tabla siguiente se puede observar la clasificación de los distintos tipos de ataques atendiendo al grupo al que pertenecen:

Clasificación de los ataques	Tipos de ataques
Ataques pasivos	Ataques de interceptación
	Ataques de interrupción
Ataques activos	Ataques de modificación
	Ataques de fabricación

Así, los ataques de interceptación se consideran ataques pasivos al no alterar el tráfico de red, mientras que los ataques de interrupción, modificación y fabricación son ataques activos al alterar la información que se pretende transmitir.

3.2.- Categorización de los incidentes

Cuando se produce un incidente el responsable de gestionarlo debe garantizar la recuperación de la actividad normal en el mínimo tiempo posible. Por lo tanto, un factor clave para que la recuperación sea rápida y completa es la elaboración de planes de contingencia que analicen los efectos de posibles intrusiones y la definición de procedimientos que permitan mantener la integridad, confidencialidad y disponibilidad de la información y recuperar el máximo de datos perdidos posible.

En estos planes de contingencia deben considerarse los medios que se van a utilizar para contener, erradicar y recuperar el sistema ante incidentes para que la gestión del riesgo sea eficaz.

Nota

Los planes de respuesta a incidentes y los planes de contingencia deben ser únicos para cada negocio. Cada organización debe realizar un análisis previo de necesidades de seguridad y de los recursos disponibles para que la elaboración de estos planes sea específica y adecuada.

Lo que no puede faltar en un plan de contingencia es la categorización de los incidentes derivados de intentos de intrusión o infecciones según su impacto potencial. La categorización consistirá en calcular la prioridad del incidente atendiendo a su impacto y urgencia y teniendo en cuenta:

- Los costes potenciales que se producirían si no se resuelve el incidente.
- El daño que puede causar a los distintos miembros de la organización y los costes implícitos que se pueden producir por una interrupción de la comunicación entre ellos.
- Las implicaciones legales que puede suponer.

Importante

El impacto de un incidente no tiene que ver con su complejidad. Un incidente de lo más simple puede causar numerosos daños irreparables, siendo su nivel de impacto muy elevado.

La gestión de incidentes teniendo en cuenta su nivel de impacto clasifica los incidentes del siguiente modo:

- **Incidentes de alto impacto:** son incidentes que tienen un impacto muy elevado sobre la actividad de la organización y el servicio que ofrece a los clientes.

- **Incidentes de impacto medio:** incidentes que tienen un impacto significativo sobre la actividad de la organización y sus servicios.

También están en este nivel los incidentes que tienen un impacto potencialmente elevado sobre la organización y su actividad.

- **Incidentes de impacto bajo:** no llegan a tener un impacto significativo sobre la organización, su actividad y sus servicios. Estos incidentes simplemente tienen el potencial de tener impacto significativo.

Unos ejemplos de incidentes categorizados se pueden observar en la tabla siguiente:

Impacto	Definición	Ejemplos
ALTO	Tienen impacto elevado	Infecciones por software malintencionado como virus, troyanos, etc.
		Accesos no autorizados.
MEDIO	Tienen impacto significativo o potencialmente elevado	Intentos de modificación y obtención de contraseñas.
		Contraseñas desconocidas por los usuarios por alteraciones no autorizadas.
BAJO	Tienen impacto potencialmente significativo	Escaneos del tráfico de red.
		Bloqueos inesperados por la producción de varias denegaciones de accesos.

Según la categoría que se le asigne al incidente la respuesta ante este deberá ser distinta: cuanto mayor sea el impacto que pueda producir el incidente en la organización, mayor deberá ser la implicación de los responsables de seguridad y mayores medidas deberán tomarse para evitar daños demasiado perjudiciales. Además, ante incidentes de impacto alto el tiempo de respuesta debe ser lo más reducido posible para que las medidas puedan ser efectivas y eficaces.

4. CRITERIOS PARA LA DETERMINACIÓN DE LAS EVIDENCIAS OBJETIVAS EN LAS QUE SE SOPORTARÁ LA GESTIÓN DEL INCIDENTE

Para combatir correctamente el incidente previamente hay que llevar a cabo un proceso de identificación que incluye la búsqueda y determinación de las evidencias objetivas. Con estas evidencias la decisión de las medidas a tomar puede ser más precisa y efectiva y, además, con la

información obtenida se pueden establecer medidas preventivas con las que se evitará que ese incidente se vuelva a producir.

La recolección de evidencias debe realizarse de un modo muy metódico para evitar borrar "huellas" del incidente que dificulten su identificación.

Actualmente, las herramientas que se utilizan en análisis forenses están muy avanzadas y permiten conocer exactamente los mecanismos que ha utilizado el intruso para acceder al sistema y los cambios que se han producido.

Una recomendación importante es la creación de una copia de seguridad en CD o DVD como herramienta básica para la respuesta a incidentes: hay que tener en cuenta que numerosas intrusiones pueden modificar las aplicaciones y utilidades de seguridad que incluyen los sistemas operativos y al realizar la recopilación de evidencias, si ha habido modificaciones que sean difíciles de percibir, será complicado detectarlas.

En este CD/DVD se recomienda que se incluyan las siguientes tareas:

- Enumerar los puertos TCP y UDP abiertos y las aplicaciones que llevan asociadas cada uno de ellos.
- Interpretación de los comandos en modo consola.
- Enumeración de los usuarios que se conectan al sistema tanto en local como en modo remoto.
- Obtención de la hora y fecha del sistema operativo.
- Elaboración de una lista de los procesos activos, los recursos utilizados y los usuarios o aplicaciones que los iniciaron.
- Listar las direcciones IP.
- Búsqueda de los ficheros ocultos o eliminados.
- Visualizar los distintos *logs* y registros del sistema.
- Lectura, copia y escritura a través de la red.
- Realización de copias de discos duros y particiones.
- Análisis del tráfico de datos de la red.
- Visualización de la configuración de seguridad del sistema.

Una vez elaborado el CD/DVD de respuesta a incidentes el siguiente paso consiste en la búsqueda real de los indicios del ataque. El primer sitio a buscar es en los equipos que se consideran más comprometidos pero no hay que olvidar que los atacantes han podido eliminar registros locales en estos equipos y también en equipos o dispositivos próximos a ellos: hay que buscar indicios también en escaneo de puertos y en la búsqueda de tráfico inusual en los cortafuegos y *routers* de la red.

Nota

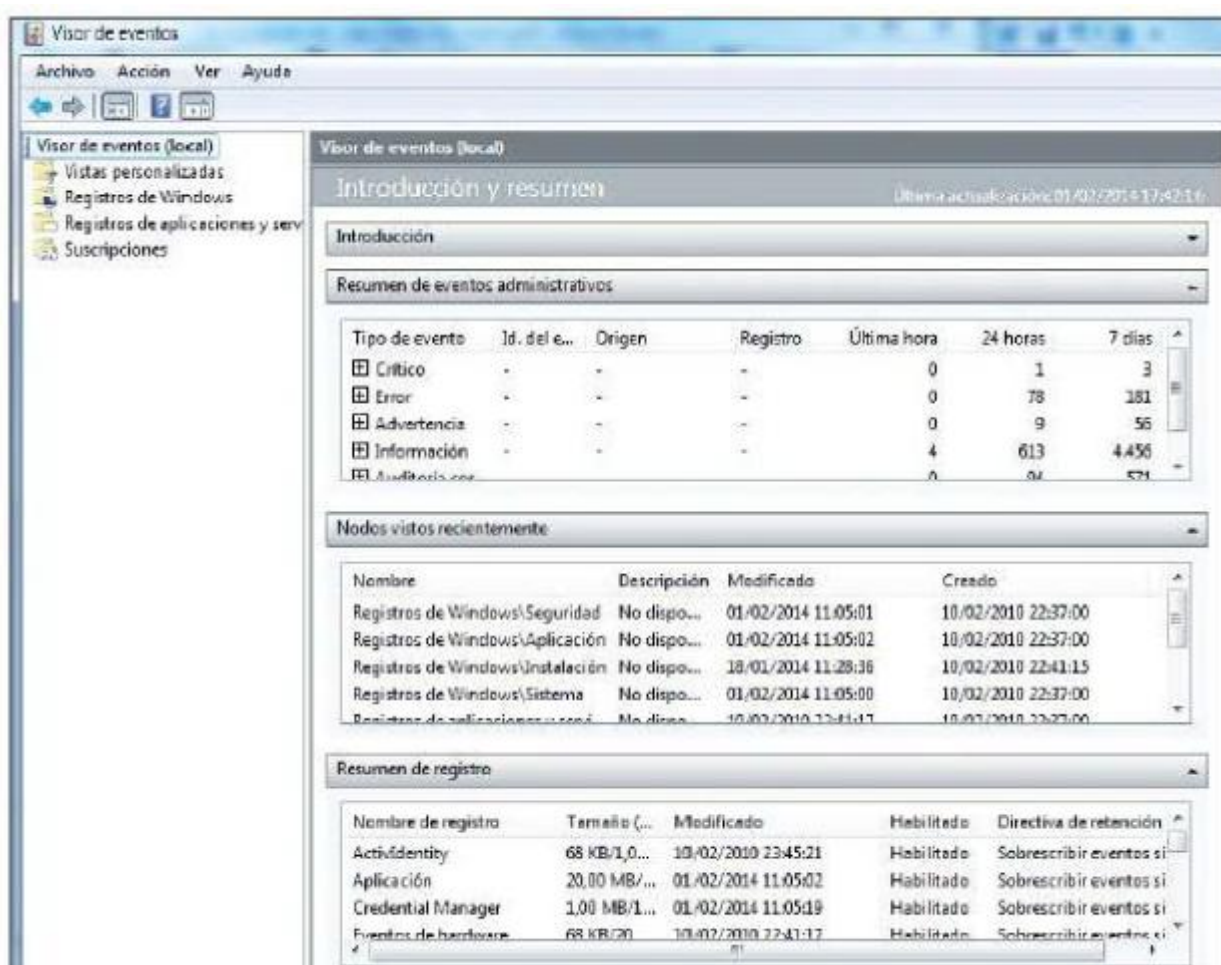
La detección de tráfico de red inusual es una evidencia clara de que se están produciendo actividades no habituales que pueden terminar siendo ataques reales.

Para conocer la actividad de los equipos y dispositivos es recomendable conocer los procesos que se ejecutan en ese momento en cada uno de ellos para buscar consumos excesivos de recursos, ubicaciones de archivos poco frecuentes, utilización de puertos no habituales, etc.

Si se encuentran indicios de posibles intrusiones el siguiente paso es obtener los archivos de registro del sistema y *logs* para detectar accesos no autorizados, conexiones fallidas, avisos sobre fallos de instalación, etc.

Como ya se ha sabido, la observación de los archivos de registro varía según el sistema operativo que se utiliza.

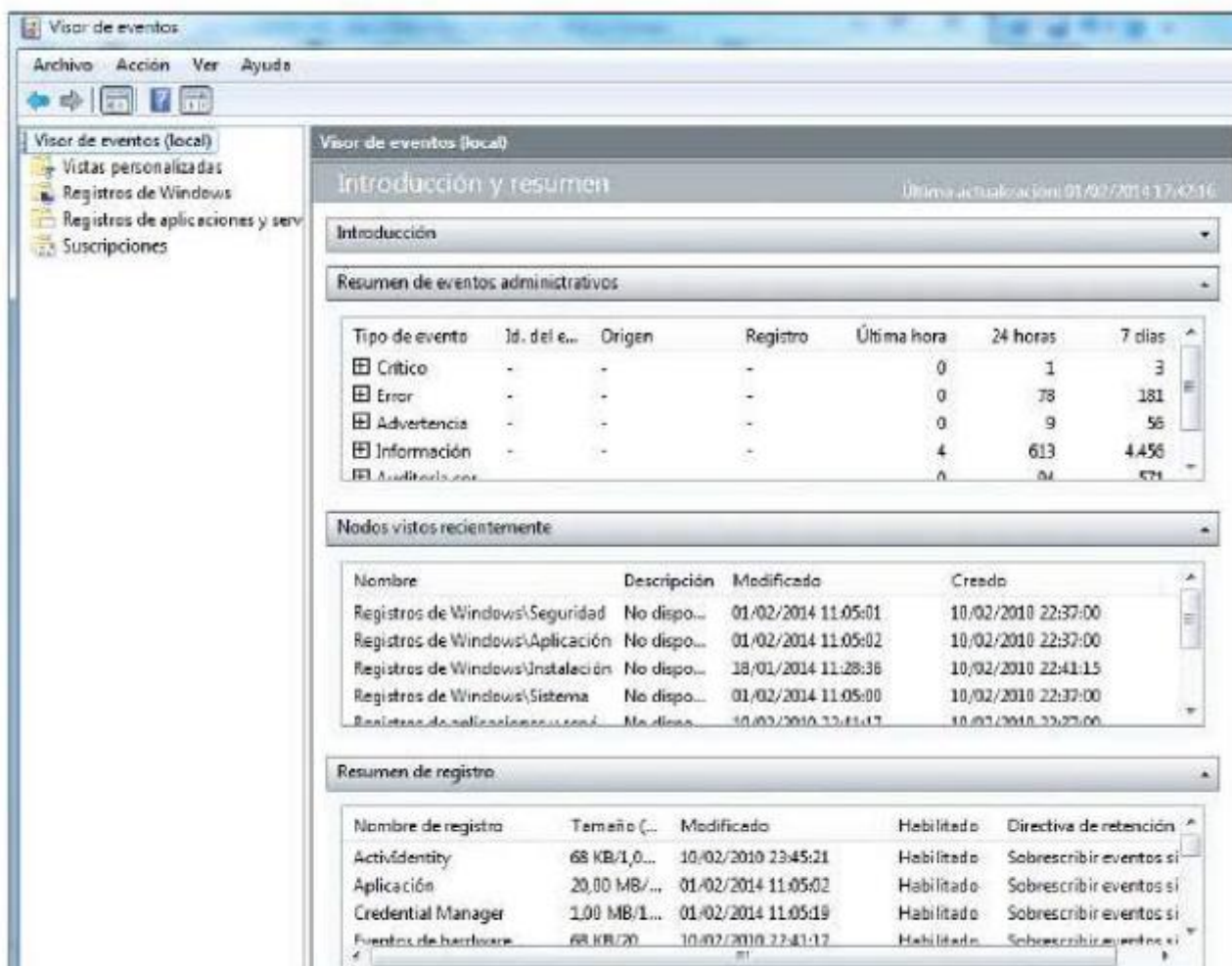
En *Microsoft Windows* se puede acceder al "Visor de eventos" a través de **Inicio -> Herramientas administrativas -> Visor de eventos**. En este se pueden observar todos los eventos acontecidos en el sistema, además de los registros de *Windows* y de las aplicaciones y servicios del equipo.



Visor de eventos de Microsoft Windows

Otra herramienta de búsqueda de evidencias es "Servicios" en la que se accede seleccionando **Inicio -> Panel de control -> Herramientas administrativas -> Servicios**.

La herramienta "Servicios" proporciona información acerca de todos los servicios que se ejecutan en el sistema indicando su descripción, estado actual y el modo y la forma en los que se inician:



Herramienta "Servicios" de Microsoft Windows

El sistema operativo *Linux*, sin embargo, no dispone de interfaz gráfica que permita ver los eventos del sistema. Para detectar evidencias en los archivos de registros se encontrarán utilizando los comandos **tail -f** (para ver las últimas líneas del registro) y **less +F** (para ver el archivo de registro entero) en los archivos de registro más importantes como:

- **/var/log/messages:** contiene los mensajes generales del sistema.
- **/var/log/secure:** almacena los sistemas de autenticación y seguridad.
- **/var/log/wtmp:** almacena un historial de los inicios y cierres de sesión acontecidos.
- **/var/log/btmp:** almacena los inicios de sesión fallidos o erróneos.

Además de los archivos de registros mencionados también se pueden detectar evidencias de incidentes en archivos como:

- **/etc/passwd:** contiene información de las claves del sistema.
- **/etc/shadow:** incluye información de los usuarios.
- **/etc/group:** incluye información sobre los grupos del sistema.

Con la realización de los pasos mencionados y la observación de los archivos de registro ya es suficiente para confirmar la existencia de ataques o intrusiones en el sistema. Aun así, será necesario un análisis más profundo y exhaustivo para conocer su comportamiento. Para ello se utilizarán una serie de criterios mencionados en el siguiente apartado.

4.1.- Criterios para la recolección de evidencias

Para llevar a cabo la recolección de evidencias se recomienda tener en cuenta una serie de criterios. Estos se describen a continuación.

Criterios de sensores basados en equipo o Host Based Sensors

Se encargan de obtener información de los eventos a nivel del sistema operativo (intentos de conexión, accesos al sistema operativo, etc.).

Como ventaja es importante destacar que la información que recogen es de calidad. Además se configuran con facilidad y suministran información con altos niveles de precisión.

Como inconveniente cabe decir que estos sensores pueden afectar considerablemente a la eficiencia del sistema en el que se ejecutan al consumir un elevado nivel de recursos.

Nota

Los sensores basados en equipo o Host Based Sensors son software instalados en un solo equipo que supervisan la actividad de todos sus elementos para mantenerlos protegidos adecuadamente.

Criterios de sensores basados en aplicación o Application Based Sensors

La función principal de estos sensores es obtener información de las aplicaciones que se ejecutan en el sistema: son una peculiaridad de los sensores basados en equipo.

Las ventajas e inconvenientes son los mismos que en los sensores basados en equipos: obtienen información de calidad, son fáciles de configurar y, por el contrario, tienen un consumo intensivo de los recursos del sistema.

Importante

La distinción de los criterios de sensores basados en sistema y en aplicación es necesaria tenerla en cuenta. Aunque los criterios de aplicación son una vertiente de los de sistema, aportan información más detallada y profunda de sus funciones, prestaciones y accesos.

Criterios de sensores basados en red o Network Based Sensors

Recolectan información de los eventos que suceden en el tráfico de datos de la red. Permiten trabajar y obtener información sin afectar a los recursos del equipo ni a la infraestructura de red.

Su nivel de seguridad es más elevado que los demás criterios, ya que no tienen que estar necesariamente instalados en el equipo que se pretende analizar y, por lo tanto, tienen más nivel de resistencia ante posibles ataques.

La ventaja principal, además de las comentadas, es la capacidad de obtener información que los otros sensores no ofrecen. La información a nivel de red no puede ser obtenida con los sensores basados en equipo o aplicación.

La decisión de qué criterio es mejor ha sido ampliamente debatida en estos últimos años, ya que cada criterio ofrece prestaciones que los demás no facilitan. Dependiendo del tipo de información que se pretenda obtener (a nivel de sistema, a nivel de aplicación o a nivel de red) deberá decidirse la utilización de unos criterios u otros.

Ante la duda, los IDS/IPS ofrecen soluciones híbridas que unifican las tres opciones (suministrando información de los equipos protegidos y de los datos que circulan entre ellos) y facilitan información más completa y extensa.

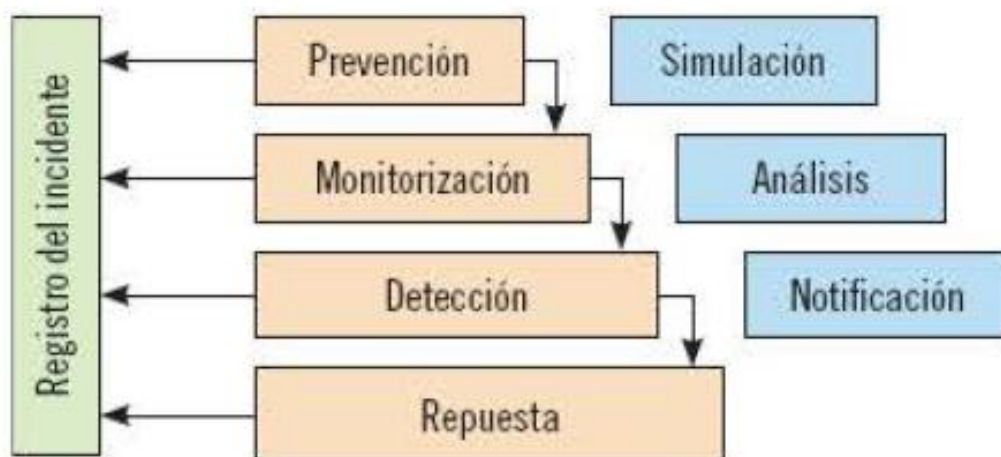
5. ESTABLECIMIENTO DEL PROCESO DE DETECCIÓN Y REGISTRO DE INCIDENTES DERIVADOS DE INTENTOS DE INTRUSIÓN O INFECCIONES

Para la detección de los incidentes relacionados con intentos de intrusión o infecciones se utilizan sobre todo herramientas ya mencionadas anteriormente como los sistemas de detección de incidentes o IPS, por lo tanto, su proceso de detección estará muy relacionado con el funcionamiento de estas herramientas.

Una vez detectado el incidente, ya serán los responsables designados los que deben encargarse de tomar medidas de respuesta y de registrar todos los eventos producidos y acciones ejecutadas.

Así, las fases de detección y registro de incidentes se pueden observar en la siguiente imagen.

Fases de detección y registro de incidentes



Fase de prevención de incidentes

Antes de intentar las intrusiones e infecciones lo primero que hay que hacer es prevenirlas.

Para ello, los sistemas de prevención de intrusiones son herramientas fundamentales y eficaces encargadas de evitar que cualquier tipo de intrusión acceda a los equipos y dispositivos de una red.

Estas herramientas realizan simulaciones con el tráfico de la red para identificar actividades que pueden llegar a ser intrusiones reales.

A continuación se resumen sus tipologías clasificadas según el modo en el que detectan el tráfico de red malicioso:

- Detección basada en firmas: compara la actividad de la red en búsqueda de posibles intrusiones registradas en su base de datos.
- Detección basada en políticas: detecta las intrusiones atendiendo a las políticas de seguridad marcadas por la organización.
- Detección basada en anomalías: compara la actividad de la red con actividades in usuales para analizarlas y detectar posibles anomalías e intrusiones.
- Detección *honey pot* jarra de miel: previene las intrusiones usando un equipo configurado específicamente para atraer intrusiones y conseguir desviar su atención de los equipos que contienen la información importante.

Tipos de detecciones	¿Cómo detectan?
Basadas en firmas	Buscan elementos reconocidos en su base de datos como intrusiones.

Tipos de detecciones	¿Cómo detectan?
Basadas en políticas	Siguiendo directrices marcadas por la política de seguridad.
Basadas en anomalías	Buscan actividad anómala para su análisis y detección de intrusiones.
Honey pot o jarra de miel	Utilizan señuelos para atraer intrusiones.

Fase de monitorización de incidentes

Si, a pesar de todas las medidas de prevención tomadas, se detecta algún tipo de actividad inusual o sospechosa hay que proceder a su monitorización.

En esta fase se monitoriza el tráfico de red del sistema con la finalidad de poder analizarlo y comprobar que todo funciona como se espera o, en caso contrario, incidir en el análisis para averiguar con profundidad los detalles de la actividad inusual.

Con la monitorización de la actividad de red y de los equipos se ayuda fervientemente a la detección de intentos de intrusión y permite ejecutar medidas de respuesta más rápidamente antes de que se produzcan daños más graves.

Para que la monitorización sea más efectiva se recomienda configurar un sistema de alertas que avise mediante mensajes en pantalla, envío de correos electrónicos a los responsables u otros métodos cuando se detecte cualquier tipo de actividad sospechosa como procesadores sobrecargados, consumo excesivo de recursos, etc.

Con la utilización de estos sistemas de alertas se consigue una reacción más rápida y, por tanto, unas medidas más eficaces que consigan contener y eliminar la intrusión con mayor rapidez y menor cantidad de daños originados.

Recuerde

Los sistemas de detección y prevención de intrusiones (IDS/IPS) son una de las herramientas más efectivas para monitorizar los procesos y servicios de los equipos y sistemas y detectar anomalías y posibles intrusiones.

Fase de detección de la intrusión

Con la monitorización del tráfico de red y de los procesos que se están ejecutando ya habrá indicios suficientes que determinarán si la actividad sospechosa es realmente una intrusión o no.

En este caso la configuración de los IDS/IPS debe realizarse por técnicos experimentados que prueben la sensibilidad de la herramienta y encuentren el punto de equilibrio entre la detección de amenazas reales y la detección de falsas alarmas.

Este punto puede ser un hándicap para las organizaciones, ya que una mayor sensibilidad evita que algunas intrusiones pasen desapercibidas, pero también detecta como posible intrusión un mayor número de falsas alarmas.

Por el contrario, una configuración de poca sensibilidad detectará pocas intrusiones que sean falsas alarmas pero, sin embargo, dejará de detectar otras intrusiones reales que pueden tener graves efectos sobre el sistema al que accedan.

Respuesta

Los sistemas IDS, en general, no pueden combatir y eliminar la amenaza, simplemente se limitan a su detección y a la generación de alertas que permitan a los responsables la toma de medidas reactivas.

Sin embargo, en la actualidad hay sistemas IDS más sofisticados que incluyen medidas de contingencia o cuarentena para evitar daños mayores ante la detección de intrusiones: cierre de puertos, bloqueo de tráfico de red, etc.

Las respuestas que pueden generar los sistemas IDS se pueden clasificar en:

- Respuestas pasivas: notificación a los responsables de seguridad de la intrusión o ataque detectado.
- Respuestas activas: realización de acciones automáticas configuradas específicamente para que obtengan más información sobre el posible ataque. Otro tipo de respuestas activas también serían las medidas de contingencia o cuarentena mencionadas anteriormente como: filtrado de información en el *router*, cierre de sesión del sistema, bloqueo de la dirección IP del intruso, etc.

Nota

Las respuestas activas intentan bloquear la intrusión o, por lo menos, evitar en todo lo posible la propagación de los daños. Sin embargo, con las respuestas pasivas la intrusión se sigue extendiendo y produciendo daños. Estas se limitan simplemente a avisar a los administradores y responsables de seguridad.

Registro del incidente

Esta fase del proceso de gestión de incidentes no tiene un momento temporal específico, sino que se debe producir a lo largo de todo el incidente, desde la detección previa de posibles indicios de intrusión hasta el momento en el que se restaura la situación incluyendo el momento anterior de la entrada de la intrusión.

El procedimiento de registro del incidente consiste en la generación de un archivo de registro en el que se vayan almacenando todos los detalles detectados de la intrusión y todas las acciones tomadas a cabo para su contención, erradicación y restauración del sistema.

El registro de los incidentes es una herramienta muy útil en el momento de realizar un análisis forense de la intrusión, ya que facilita información sobre todo lo que ha estado ocurriendo en el desarrollo de la misma junto con el orden cronológico de las acciones tomadas.

Nota

Además de toda la información relativa a la intrusión, también debe incluirse en los archivos de registro cualquier información que pueda ser relevante para la resolución del incidente. En el caso de que la intrusión pueda afectar a otros usuarios, estos deberán ser avisados para que sean conocedores de la incidencia y de las medidas a tomar en caso de detectarla.

Con un análisis profundo de los archivos de registro los analistas forenses pueden conocer con detalle cómo y por dónde ha conseguido acceder la intrusión y qué es lo que ha podido fallar en su detección y prevención.

De este modo y mediante el análisis forense de la información aportada por los archivos de registro se puede realizar un proceso de aprendizaje que culmine en el diseño de nuevas medidas que eviten que incidentes futuros parecidos a los ya sucedidos no puedan volver a acceder a los sistemas de la organización.

6. GUÍA PARA LA CLASIFICACIÓN Y ANÁLISIS INICIAL DEL INTENTO DE INTRUSIÓN O INFECCIÓN CONTEMPLANDO EL IMPACTO PREVISIBLE DEL MISMO

Para clasificar y llevar a cabo un análisis inicial del intento de intrusión hay que tener en cuenta el impacto que se prevé que va a haber ya que, si el impacto es elevado, es necesario que las medidas de contención y respuesta se tomen con más agilidad y rapidez.

Según el impacto que pueda provocar se deberán tomar medidas de urgencia o se podrá demorar su eliminación ante otras prioridades. No obstante es recomendable previamente clasificar los intentos de intrusión atendiendo a su naturaleza:

- **Intrusiones de uso erróneo:** intrusiones diseñadas para atacar los puntos débiles de un sistema. Se pueden detectar con la observación de acciones sucedidas en dicho sistema.

- **Intrusiones de anomalía:** intrusiones que atacan desviando las acciones de un sistema de su utilización habitual. Se pueden detectar guardando los perfiles del sistema en situaciones normales y comparándolas periódicamente para detectar alteraciones y anomalías importantes.

Además, para clasificar la intrusión también es importante conocer cómo y en qué vías pueden acceder los intrusos al sistema, categorizándolos en otras tipologías:

- **Intrusión física:** el intruso accede al equipo a través de un medio físico • (por ejemplo, con el teclado).
- **Intrusión del sistema:** el intruso utiliza una cuenta de usuario del sistema con pocos privilegios sobre la que actuará para que se le asignen otros privilegios más significativos y poder atacar en consecuencia.
- **Intrusión alejada:** el intruso accede al sistema con acceso remoto a través de la red.

INTRUSIONES	
Clasificación	Tipo
Según su naturaleza	Intrusiones de uso erróneo
	Intrusiones de anomalía
Según el modo de acceso al sistema	Intrusión física
	Intrusión del sistema
	Intrusión alejada

6.1.- Clasificación de los intentos de intrusión según su impacto

Como ya se ha mencionado anteriormente, el impacto sobre los activos de la organización de una intrusión es uno de los elementos fundamentales a tener en cuenta para su clasificación.

Así, atendiendo a este criterio se pueden distinguir varios tipos de intrusiones.

Intentos de entrada

Los intentos de entrada se producen cuando hay usuarios no autorizados que pretenden acceder al sistema para llevar a cabo acciones malintencionadas. El impacto de esta intrusión puede considerarse alto ya que, si este usuario consigue acceder y obtener los privilegios apropiados, puede llegar a dañar el sistema en su totalidad.

Ataques enmascarados

En este caso no se trata de usuarios nuevos que intentan acceder al sistema. Aquí el intruso utiliza usuarios ya registrados a través de los cuales intentar atacar.

El impacto de este tipo de intrusión es inferior a los intentos de entrada, ya que cabe la posibilidad de que el usuario a través del que se accede al sistema tenga menos privilegios y, por lo tanto, el daño que pueda realizar sea menor.

Importante

A pesar de tener un impacto inferior que los intentos de entrada, los ataques enmascarados no deben subestimarse: su daño potencial puede ser igual o mayor que las otras intrusiones.

Eso sí, si accede a través del administrador los efectos pueden ser nefastos. Como no es seguro y el daño en este caso se considera potencialmente significativo, el impacto será medio.

Penetraciones en el sistema de control

En las penetraciones en el sistema de control los intrusos intentan acceder a las herramientas de control del sistema con el fin de alterarlas.

Las penetraciones pueden ser:

- Internas: si se producen desde el mismo sistema.
- Externas: si proceden de otro equipo o de la red.

Su impacto puede ser alto, ya que los procesos de control de un sistema suelen controlar todos los demás procesos, usuarios, rendimientos y demás características y contenidos del equipo al que se está administrando.

Se suelen detectar mediante la observación de las actividades con comportamientos especiales fuera de lo habitual.

Fuga

La finalidad de las intrusiones tipificadas como "fuga" es principalmente utilizar de modo exhaustivo los recursos de un sistema para conseguir su saturación e impedir su funcionamiento y rendimiento habitual.

El impacto de estas intrusiones se considera bajo, ya que no se elimina información, simplemente se impide que el sistema desarrolle su actividad con normalidad.

Importante

Aunque el impacto de las intrusiones tipificadas como fuga sea bajo, este puede conllevar elevados costes derivados de pérdidas de calidad del servicio al ralentizar los equipos e impedir un desarrollo normal de las actividades del equipo y de la oferta de servicios habitual.

Para su detección se recomienda observar el rendimiento de los procesos y aplicaciones para detectar aquellos que tienen un consumo de recursos excesivo en comparación con su rendimiento habitual.

Denegación de servicio

Los intrusos que acceden al sistema de una organización con ataques de denegación de servicio (*DoS* o *Denial of Service*) tienen como objetivo limitar e incluso impedir el acceso a los recursos y servicios de una organización durante un período de tiempo indeterminado o indefinido.

Su impacto es bajo, ya que aunque impide la actividad habitual de una organización no hay alteración ni borrado de datos. Lo habitual es que estos ataques se lleven a cabo para dañar la imagen y reputación de las organizaciones al impedir que los clientes puedan acceder a ellas y que estas no puedan ofrecer sus servicios con facilidad.

Su detección es bastante simple aunque su prevención es más dificultosa. La detección de los ataques de denegación de servicio se produce al observar la dificultad de ofrecer los servicios a los usuarios por parte de la organización.

Uso malicioso

Los ataques por uso malicioso se producen cuando el intruso se infiltra o causa daños en un equipo o sistema sin autorización.

Dependiendo del tipo de *software* malicioso o *malware* utilizado el impacto será distinto: desde saturación de servidores, borrado de datos, aparición de ventanas molestas, observación de actividad, envío de *spam*, etc.

Este tipo de intrusiones, a pesar de su gran variedad, se suele detectar por los modelos de comportamiento atípico del sistema o de alguna aplicación o proceso concreto.

En la siguiente tabla se observan los distintos tipos de intrusiones clasificados por su impacto:

Tipo de intrusión	Impacto
Intentos de entrada	Alto

Penetraciones en el sistema de control	Alto
Ataques enmascarados	Medio
Fuga	Bajo
Denegación de servicio	Bajo

7. ESTABLECIMIENTO DEL NIVEL DE INTERVENCIÓN REQUERIDO EN FUNCIÓN DEL IMPACTO PREVISIBLE

El impacto previsible de una intrusión viene determinado también por los efectos negativos producidos o potenciales que se pueden originar y por la criticidad de los recursos que se van a ver afectados por dicha intrusión.

7.1.- Clasificación de los incidentes según su nivel de criticidad

Los efectos negativos producidos o potenciales y la criticidad de los recursos son los que determinarán el nivel de criticidad del incidente atendiendo a su impacto.

El Esquema Nacional de Seguridad clasifica los incidentes según su criticidad en cinco categorías o niveles:

Nivel	Nombre
5	Crítico
4	Muy alto
3	Alto
2	Medio
1	Bajo/Nulo

Nivel de criticidad crítico

En este nivel se encuentran las intrusiones de las que se tiene constancia que han producido un impacto muy significativo, afectando tanto a la confidencialidad, como a la disponibilidad o a la integridad de los datos.

Los recursos afectados por las intrusiones clasificadas como críticas contienen información crítica y especialmente relevante para la buena marcha de la organización.

Este tipo de intrusiones suelen afectar a los servicios de la organización utilizados por un elevado número de usuarios, a recursos que afectan sustancialmente a la seguridad del sistema y de la red e incluso pueden llegar a provocar pérdidas irreversibles de información crítica.

Nivel de criticidad muy alto

Tienen nivel de criticidad muy alto las intrusiones de las que se tiene constancia que han producido un impacto considerable (y no muy significativo) en recursos clasificados como críticos.

Sus efectos también afectan a la integridad, disponibilidad y confidencialidad de los datos críticos y amenazan a un número limitado de sistemas no críticos.

A pesar de la no criticidad de los sistemas, su contención y resolución conlleva un trabajo laborioso y considerable para los responsables de seguridad.

Importante

Cuanto más nivel de criticidad tenga el intento de intrusión o infección, menos deberá tardarse en su notificación y menor deberá ser el tiempo de respuesta para la toma de medidas y su erradicación.

Nivel de criticidad alto

Las intrusiones con nivel de criticidad alto son aquellas que tienen un impacto considerable en recursos e información considerados como no críticos por la organización.

Suelen ser intrusiones a equipos y sistemas muy limitados (normalmente solo a un equipo) que no contienen información relevante.

Nivel de criticidad medio

El impacto de las intrusiones con nivel de criticidad medio es limitado y afecta a recursos e información considerados como no críticos.

En general, las organizaciones deberían estar capacitadas para combatir intrusiones de este nivel sin necesidad de recurrir a agentes externos.

También deberían disponer controles y herramientas que permitan la detección y prevención de estas intrusiones, así como de la reducción de los riesgos que ello implica.

Aunque estos incidentes no requieren ser reportados en el momento de su detección, sí es recomendable la elaboración de informes periódicos de estas intrusiones para llevar un control y comprobar la efectividad de las medidas de prevención implantadas.

Nota

Suele ser habitual que las organizaciones pospongan excesivamente o que no traten los incidentes con criticidad media o baja (cayendo en un error grave de seguridad), lo que supone una pérdida de eficiencia en sus operaciones y una merma de la calidad en sus servicios.

Nota

Suele ser habitual que las organizaciones pospongan excesivamente o que no traten los incidentes con criticidad media o baja (cayendo en un error grave de seguridad), lo que supone una pérdida de eficiencia en sus operaciones y una merma de la calidad en sus servicios.

Nivel de criticidad bajo

Las intrusiones de criticidad bajo tienen un impacto nulo o insignificante para las organizaciones y suelen ser detectadas y erradicadas por sus sistemas y herramientas de seguridad.

Del mismo modo que con las intrusiones de criticidad baja, aunque no es necesario hacer un reporte cada vez que se producen, sí se recomienda la elaboración periódica de informes que las contengan para llevar un control de la efectividad de las medidas y controles de prevención.

En resumen, el nivel de criticidad de las intrusiones en función de su impacto se recoge en la tabla siguiente:

Nivel de criticidad	Impacto	Recursos afectados
CRÍTICO	MUY CONSIDERABLE	CRÍTICOS
MUY ALTO	CONSIDERABLE	CRÍTICOS
ALTO	CONSIDERABLE	NO CRÍTICOS
MEDIO	LIMITADO	NO CRÍTICOS
BAJO	NULO	NO CRÍTICOS

7.2.- Nivel de intervención requerido en función del impacto y criticidad de la intrusión

En el momento que se confirma que el intento de intrusión es real y no es una falsa alarma es de vital importancia que el tiempo de reacción sea el adecuado, teniendo en cuenta su nivel de criticidad.

Por ello, las empresas y organizaciones deberán registrar y gestionar cada intrusión individualmente según los recursos afectados y su nivel de impacto: a mayor criticidad de los recursos y mayor nivel, menor deberá ser el tiempo pasado desde su detección hasta su registro.

Concretamente y teniendo en cuenta su criticidad deberán registrarse las intrusiones según estas pautas:

- Las intrusiones con nivel de criticidad crítico deben notificarse como muy tarde en el plazo de una hora desde su detección.
- Las intrusiones con nivel de criticidad muy alto deberán notificarse dentro de las 12 h oras siguientes de su detección.
- Las intrusiones con nivel de criticidad alto se notificarán como muy tarde dentro de las 48 horas siguientes de su detección.
- Las intrusiones con nivel medio de criticidad deberán notificarse lo antes posible, pero no puede pasar más de una semana desde su detección.
- Las intrusiones con nivel bajo de criticidad se notificarán también lo antes posible, aunque no debería pasar más de un mes desde su detección.

De un modo más resumido y visual, en la siguiente tabla se recogen los tiempos máximos de notificación de las intrusiones según su nivel de criticidad:

Nivel de criticidad	Tiempo máximo para su registro
CRÍTICO	1 HORA
MUY ALTO	12 HORA
ALTO	24 HORA
MEDIO	1 Semana
BAJO	1 mes

Intervención para la contención y erradicación de la intrusión según su impacto y criticidad

Aunque cada intrusión es distinta y la casuística puede ser de lo más variada, las organizaciones, igual que con el registro y notificación, deben establecer un tiempo "objetivo" máximo de contención y erradicación de la intrusión.

Es decir, debe existir un plazo máximo para que la intrusión esté controlada (y deje de producir daños sustanciales) y para que la intrusión se cierre definitivamente, quedando restaurada la situación inicial del sistema.

Aunque son tiempos "objetivo" no es recomendable superarlos, pudiendo excederse solo en intrusiones y circunstancias muy especiales y debidamente justificadas.

De este modo, los tiempos máximos de contención y erradicación de la intrusión según su nivel de criticidad quedan reflejados en la tabla siguiente:

Nivel de criticidad	Plazo máximo de contención	Plazo máximo de erradicación
CRÍTICO	8 horas	24 horas
MUY ALTO	48 horas	72 horas
ALTO	4 días naturales	14 días naturales
MEDIO	1 mes	1 mes
BAJO	3 meses	3 meses

De este modo, y viendo lo que indica la tabla, cuanto más nivel de criticidad tenga la intrusión, menor plazo deberá pasar desde su detección hasta su contención y erradicación.

Hay que darse cuenta que la variación de tiempos según la criticidad es muy amplia (puede variar el tiempo para su contención desde ocho horas hasta tres meses), por lo que queda de manifiesto la especial importancia de clasificar las intrusiones correctamente.

Si una intrusión de nivel de criticidad muy alto se clasifica como bajo, los daños que se pueden llegar a causar serán numerosos y especialmente nocivos. Al dejar pasar demasiado tiempo desde su detección hasta la aplicación de medidas se va expandiendo el daño sobre recursos críticos pudiendo afectar significativamente a la actividad estratégica de la organización.

8. GUÍA PARA LA INVESTIGACIÓN Y DIAGNÓSTICO DEL INCIDENTE DE INTENTO DE INTRUSIÓN O INFECCIONES

Hasta ahora se han ido explicando medidas para detectar incidentes y qué hay que hacer para comprobar si el incidente es una amenaza real o es solo una falsa alarma.

También se han ido mencionando los tipos de respuesta que se pueden tomar y los tiempos máximos para evitar daños mayores en los sistemas de la organización.

Cuando se tienen sospechas de que ha habido algún ataque o intrusión en el sistema hay que tener en cuenta los siguientes aspectos:

- Si es realmente una amenaza o ataque.
- Si ha sido un ataque con éxito o fallido.
- Los daños producidos y el nivel de compromiso del sistema afectado por el ataque.

En el momento que se tiene confirmada la presencia de un ataque en el sistema, el primer paso a realizar para investigar su procedencia será comprobar si los usuarios que utilizan el sistema en ese momento pueden ser sospechosos y, en caso afirmativo, comprobar cuáles son los sistemas

que se están ejecutando y quién los está ejecutando para tener controlados los usuarios que han podido ser causantes del ataque.

Nota

Hay que tener presente que en numerosas ocasiones los ataques y amenazas provienen de usuarios internos de la organización, hecho que no hay que pasar por alto en el momento de realizar un control de usuarios.

Nota

Hay que tener presente que en numerosas ocasiones los ataques y amenazas provienen de usuarios internos de la organización, hecho que no hay que pasar por alto en el momento de realizar un control de usuarios..

Para averiguar los usuarios que están utilizando las aplicaciones y sistemas en el momento de la intrusión y los detalles de estos habrá que seguir una serie de pasos:

- Visualizar los usuarios logueados en el sistema: lo primero que hay que averiguar son los usuarios que están utilizando el sistema, dónde están, qué aplicaciones están usando y cuánto tiempo llevan registrados.

Si hay un usuario con comportamientos inusuales como el tiempo excesivo de utilización (en comparación con su tiempo habitual) o la utilización de aplicaciones poco frecuentes, podrá ser indicio de que ese usuario sea el causante de la incidencia.

- Visualizar los procesos activos: aunque no se observe ningún comportamiento inusual en los usuarios del sistema es posible que alguno de ellos haya dejado ejecutando un proceso sin estar conectado un tiempo excesivo.

Por ello, y para no pasar por alto ningún detalle, es necesario observar cuáles son los procesos activos en ese momento y si hay alguno de ellos sospechoso de ser una amenaza. Serán indicios de amenaza:

- Procesos que llevan activos un largo período de tiempo.
- Procesos que se inician en horas poco habituales.
- Procesos que consumen un nivel elevado de CPU.
- Procesos que no están ejecutados desde un terminal.

Nota

Las medidas de visualización de usuarios logueados y de procesos activos son medidas útiles cuando el intruso sigue dentro del sistema. En cuánto este salga habrá que utilizar otras medidas para detectar el rastro que haya podido dejar.

8.1.- Investigación y diagnóstico de una incidencia ya ocurrida

Cuando a pesar de ejercer un control de los usuarios y de los procesos del sistema la incidencia ha ocurrido sin conocer quién la ha provocado, hay una serie de recomendaciones y pasos a tener en cuenta para encontrar indicios y señales que permitan detectar las huellas que el intruso ha podido dejar sin darse cuenta.

Las recomendaciones imprescindibles se mencionan a continuación.

Examen de los archivos de registro o logs

Con el examen de los archivos de registro o logs se podrá obtener información sobre conexiones a lugares poco frecuentes, utilización de aplicaciones in usuales y otras actividades sospechosas de intrusión.

Por ejemplo, se puede observar el último acceso al sistema de un usuario, las aplicaciones y procesos que ha ejecutado y las contraseñas con las que ha conseguido acceder.

Si se detecta que ese usuario no tiene acceso a alguno de los procesos o aplicaciones ejecutadas o que ha utilizado contraseñas que no debería conocer, son claros indicios de que este es el causante de la incidencia.

Comprobación de los permisos del sistema

Es necesario comprobar los permisos de los usuarios del sistema para detectar si alguno de ellos dispone de permisos para más acciones de las que debería estar autorizado. Una mala asignación de permisos puede ser causante de incidencias.

Recuerde

La asignación de permisos de administrador debe estar limitada exclusivamente a aquellos usuarios con alta responsabilidad en el sistema de seguridad de la organización. En el proceso de revisión de permisos se puede aprovechar para quitar los permisos de administración a usuarios que no deberían disponer de ellos.

Chequeo de los archivos binarios del sistema

Es habitual que los intrusos modifiquen los archivos binarios del sistema para ocultarse e intentar borrar huellas. Por ello se recomienda realizar una profunda revisión de los mismos con el fin de comprobar que no han sufrido ninguna alteración.

Comprobación de los puertos abiertos

Cuando se ha producido una intrusión y el intruso ya no está en el sistema es posible que se haya dejado un puerto de conexión abierto.

Se recomienda comprobar todos los puertos de conexión abiertos y detectar si hay alguno en especial que no lo debería estar. En caso de ser así sería aconsejable comprobar si hay alguna relación entre los últimos usuarios del sistema y la utilización de los puertos abiertos para detectar cuál de ellos se ha dejado el puerto abierto.

Comprobar la existencia de sniffers

Como ya se sabe, los sniffers son programas encargados de monitorizar el tráfico de red. Ante la posibilidad de que haya instalado algún sniffer sin autorización en el sistema se recomienda Visualizar los procesos activos para detectar la ejecución de sniffers que no hayan sido instalados voluntariamente o sin autorización.

Nota

Aunque en numerosas ocasiones los sniffers tengan usos malintencionados, también pueden resultar útiles como herramienta de control para conocer el tráfico interno de la red de la organización y saber en todo momento los datos que se están transfiriendo.

Para detectar estas aplicaciones también se pueden observar los archivos de registro y las conexiones al exterior como, por ejemplo, el envío de correos electrónicos a cuentas desconocidas y sospechosas.

Esta medida es fundamental, ya que puede haber instaladas aplicaciones de monitorización del tráfico de red para observar todo el tráfico de datos, incluyendo datos comprometidos y contraseñas que pueden ocasionar daños muy perjudiciales en el caso de caer en manos de intrusos malintencionados.

Comprobar la existencia de servicios no autorizados

Se aconseja comprobar si hay dado de alta en el sistema algún servicio no autorizado.

También es recomendable comprobar todas las autorizaciones de servicios que se hayan habilitado y deshabilitado anteriormente para detectar si ha habido alguna alteración: es posible que algún intruso haya habilitado sin dejar rastro algún servicio que previamente se haya deshabilitado por seguridad.

Comprobar las contraseñas del sistema

Se recomienda realizar una comprobación de todas las contraseñas del sistema para detectar si ha habido alguna modificación no autorizada de las mismas.

Comprobar la configuración del sistema y de la red

Hay que examinar los accesos en los archivos de configuración del sistema y de la red para detectar algún acceso no autorizado que haya podido modificar cualquier propiedad o herramienta del sistema.

Buscar todos los archivos ocultos o poco habituales

Otro modo de comprobar la existencia de amenazas en el sistema es mediante el chequeo de todos sus archivos.

Es muy frecuente que los intrusos se oculten en el sistema mediante archivos ocultos o inusuales en los que puedan ocultar herramientas y aplicaciones que les permitan saltar los sistemas de seguridad del sistema y acceder a archivos comprometidos y/o críticos.

Suelen ser indicios de intrusiones los directorios ocultos con nombres tipo “...” o “..”.

También es importante analizar todos los directorios FTP para detectar si hay alguno de ellos escrito por usuarios anónimos en los que se almacene información.

Definición

FTP

Del inglés File Transfer Protocol. Es un protocolo de red que permite la conexión de equipos cliente a un servidor para el intercambio de archivos entre ellos.

Examinar todos los equipos de la red local

No solo hay que examinar el equipo del que se sospecha que ha podido sufrir un ataque, también se deben examinar todos los equipos que formen parte de su red para comprobar si han sido afectados.

Es muy habitual que si un equipo ha sido atacado y no se ha detectado a tiempo, el ataque se haya expandido a varios equipos de su red incrementando los daños causados.

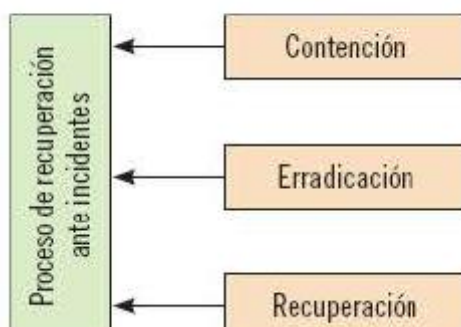
9. ESTABLECIMIENTO DEL PROCESO DE RESOLUCIÓN Y RECUPERACIÓN DE LOS SISTEMAS TRAS UN INCIDENTE DERIVADO DE UN INTENTO DE INTRUSIÓN O INFECCIÓN

Una vez confirmado y diagnosticado el incidente es el momento de proceder a su resolución y a la recuperación de los sistemas a la situación previa a su aparición.

9.1.- Proceso de resolución y recuperación de incidentes

Esta fase de resolución y recuperación se divide en tres apartados:

Proceso de recuperación de incidentes



Contención del incidente

En un primer momento, y antes de proceder a la eliminación del incidente, es necesario desarrollar una estrategia de contención del incidente de seguridad.

Esta estrategia consiste en realizar todas las medidas necesarias para impedir que el incidente de seguridad siga propagándose y dañando al sistema. Se recomienda que la ejecución de estas medidas sea lo más rápida posible para minimizar los riesgos y daños del sistema.

Unos ejemplos podrían ser la desconexión de los equipos de la red o la desactivación de ciertos servicios para evitar daños mayores.

A pesar de la recomendación, en ciertas ocasiones, cuando la información o los recursos afectados no son críticos puede ser muy útil retrasar la contención para averiguar más detalles de la incidencia y, con el aprendizaje, implantar nuevas medidas preventivas que eviten que vuelva a ocurrir. También serviría para recoger evidencias de las incidencias y de los atacantes que permitan ejercer medidas legales contra ellos.

No obstante, hay que tener mucho cuidado con esta técnica debido a los daños irreparables que puede causar el retraso de la implantación de las medidas de contención.

Nota

La decisión de implantar medidas de contención inmediatamente o de retrasar su implantación dependerá de la criticidad de los recursos afectados y de la gravedad de la intrusión. Las organizaciones deberán encontrar un equilibrio en mantener la intrusión para obtener más información y la cantidad de daños que se está dispuesto a asumir.

Medidas de erradicación

En esta etapa, cuando el incidente ya está contenido, ya se puede proceder a su eliminación: se llevarán a cabo todas las actividades y medidas necesarias que permitan asegurar que el incidente deja de estar presente en los equipos y recursos afectados.

Para ello se recomienda analizar todos los equipos afectados para buscar y eliminar archivos introducidos por el intruso y cuentas de usuario que crearon para acceder a los sistemas.

Hay que revisar los servicios y procesos afectados para comprobar que no queda ningún indicio de presencia de intrusos. Además es importante revisar los demás equipos que formen parte de la red (aunque en un principio no estuviesen afectados) para cerciorarse de la erradicación completa de la intrusión.

Recuperación

Cuando ya se ha confirmado la eliminación de la intrusión y del incidente se puede iniciar la fase de recuperación. Esta fase consistirá en tareas de restauración de los sistemas para que puedan volver a su funcionamiento habitual. Es recomendable la realización de tareas como la utilización de copias de respaldo para reinstalar el sistema operativo y las aplicaciones, además de las actualizaciones de seguridad básicas. También hay que volver a definir contraseñas nuevas para minimizar el riesgo de intrusiones.

9.2.- El plan de recuperación ante desastres

En cuanto a las organizaciones, se recomienda la implantación y desarrollo de un plan de recuperación ante desastres en el que se establezcan los procedimientos a seguir para la recuperación de la información en caso de incidencias y desastres.

Nota

El término "desastre" en términos de tecnología de la información se refiere a cualquier causa natural, intencionada o involuntaria que afecte a su infraestructura (tanto datos, como aplicaciones, como hardware) e impida la continuidad de la actividad de la organización.

El diseño de este plan se llevará a cabo por una serie de objetivos:

- Determinación de las vulnerabilidades que puedan interrumpir el servicio ofrecido y definición de las medidas preventivas que permitan reducir al mínimo la probabilidad e impacto de estas interrupciones.
- Identificación y análisis del coste, imagen y otras consecuencias que deriven de la interrupción de la actividad de la organización a causa de la intrusión.
- Determinación de las necesidades inmediatas, tanto a medio como a largo plazo, de recuperación del servicio y de los recursos que sean necesarios para ello.

- Identificación de las distintas alternativas posibles y selección de las más rentables para facilitar las operaciones de copia de seguridad y de restauración de la actividad a tiempo.
- Desarrollo e implantación de planes de contingencia que se encarguen de ejecutar las medidas inmediatas y de largo plazo.

Con el plan de recuperación ante desastres de calidad se consigue reducir al mínimo el tiempo de inactividad de la organización por producirse alguna intrusión y también reducir la pérdida de datos al mínimo posible.

Para su elaboración hay que realizar un análisis de impacto a la organización o al negocio: un informe en el que se muestren los costes que puede conllevar la aparición de una intrusión o incidencia y la interrupción de la actividad provocada por dicha intrusión.

Nota

La finalidad del análisis de impacto al negocio es priorizar las etapas del procedimiento de recuperación atendiendo a la criticidad de los recursos afectados y a la clasificación de riesgos.

La estructura de un plan de recuperación de desastres debería contener, como mínimo, lo siguiente:

- Plan de trabajo con la planificación de actividades de recuperación de la información.
- Informes de evaluación de la seguridad y la vulnerabilidad de los sistemas.
- Análisis de impacto al negocio.
- Definición de los requisitos de la organización en cuanto a las necesidades de recuperación, el ámbito de aplicación y sus objetivos.
- Plan de desarrollo de la organización en el que se establezcan las normas de recuperación, los responsables de seguridad y las copias de respaldo de la información.
- Programa de pruebas en el que se establezcan las estrategias de la organización para ejecutar pruebas, ensayos y ejercicios con el fin de comprobar la seguridad de sus equipos y sistemas.
- Programa de mantenimiento en el que se establezcan todas las medidas de actualización de sistemas y de aplicaciones de los equipos de la organización.
- Prueba inicial del plan de recuperación de desastres e implantación.

Hay que tener en cuenta que las organizaciones están en continuo cambio y, por tanto, el plan de recuperación ante desastres no debe ser estático, todo lo contrario, debe revisarse y actualizarse periódicamente para adaptarse a las características de los datos de la organización y a las necesidades de seguridad y recuperación de datos.

Nota

Del mismo modo que las organizaciones deben contar con responsables de seguridad, también deben tener personal con tareas de responsabilidad para la aplicación y control del plan de

La correcta definición e implantación de un plan de respuesta a incidentes, para terminar, implica numerosos beneficios para las organizaciones.

Se destacan los siguientes:

- Reducción de daños y pérdidas ante la presencia de un incidente.
- Mayor capacidad de protección de los sistemas críticos para la organización.
- Reducción del riesgo de interrupción de la actividad.
- Minimización de la toma de decisiones en caso de detección de incidentes.
- Mejora de la eficiencia general de la organización con la identificación de sus recursos y activos críticos.
- Reducción de las responsabilidades legales que puedan venir ocasionadas por la producción de incidentes.
- Garantía de la fiabilidad de los sistemas reserva de la organización.

Con estos planes de recuperación ante desastres las organizaciones disponen de una herramienta fundamental que les permitirá la reducción de riesgos y la recuperación de su actividad habitual sin pérdidas graves de información que impidan una interrupción larga de sus servicios.

10. PROCESO PARA LA COMUNICACIÓN DEL INCIDENTE A TERCEROS, SI PROCEDE

Cuando ya se ha llegado a controlar el incidente y se ha conseguido restaurar la situación inicial es el momento de evaluar si procede comunicar los hechos sucedidos a terceros que no tengan que ver con la organización.

En el plan de respuesta a incidentes de las organizaciones se deberían reflejar los aspectos referentes a la comunicación a terceros de las incidencias producidas, los efectos causados, sus causas y las posibles consecuencias que hayan podido suceder.

Los principales agentes y acciones recomendables a los que se les debería facilitar información sobre la ocurrencia de un incidente de seguridad son los que se describen a continuación.

Asesoramiento

Se recomienda a las organizaciones que intenten asesorarse ante profesionales especializados que evalúen las acciones y decisiones tomadas con el fin de mejorar para futuras incidencias.

Aunque siempre hay que hacer un análisis interno de la evolución y de las decisiones tomadas ante la detección de un incidente, siempre es aconsejable la opinión de un ente profesional externo.

Proveedores

Si se ha comprobado que los sistemas de detección y prevención de incidentes han fallado, hay que recurrir a los proveedores de dichas herramientas para que sean conscientes de los fallos de su aplicación. Cualquier incidencia desconocida por el proveedor, en el caso de detectarse en la organización, debería ser reportada para que dispongan una base de datos de intrusiones de mayor calidad y realicen actualizaciones que impidan la sucesión de estas incidencias en el futuro.

También es recomendable valorar las alternativas de otros proveedores analizando el coste que supondría la implantación de nuevas herramientas y las ventajas que esa implantación puede suponer.

Nota

Hay que valorar los daños que se pueden evitar con la implantación de un sistema IDS/IPS de calidad. Es posible que el coste de esta herramienta sea elevado pero que compense asumirlo por el alto valor de los recursos que pretenden protegerse.

Comunicación a terceros

Aparte de los proveedores es posible que la incidencia haya afectado a datos y recursos de terceras personas y/o organizaciones.

Es conveniente comunicar a estos terceros la detección de la incidencia, las principales actuaciones realizadas y las consecuencias de la misma para que sean conscientes del fallo y puedan colaborar en la restauración de la situación original.

Por ejemplo, es posible que se hayan perdido facturas de unos proveedores. En esta ocasión sería necesario comunicarles la situación y la incidencia sucedida para que remitan copia de dichas facturas que compensen la pérdida de la información.

Fabricantes de software y hardware

En el momento en el que la incidencia ha afectado a algún componente de software o hardware de la organización se recomienda comunicarlo a sus proveedores y fabricantes para que evalúen los daños causados y las posibles consecuencias que puedan aparecer. También se aconseja contactar con ellos para comprobar si no ha sido alguna vulnerabilidad de sus aplicaciones o dispositivos los que hayan permitido el acceso del intruso al sistema.

Nota

Cuando sucede alguna incidencia o intrusión también se recomienda evaluar la eficacia y la seguridad de las aplicaciones del sistema. Es posible que con la utilización de aplicaciones bajo contraseña (en lugar de aplicaciones sin protección) se hubiesen podido evitar daños y pérdidas de información innecesarios.

Comunicación a terceros perjudicados

No solo hay que comunicar a los terceros cuyos recursos han sido afectados a nivel interno de la organización.

Hay que evaluar los daños provocados por el incidente y los datos modificados o perdidos para comprobar si se ha puesto en peligro la seguridad, privacidad e integridad de datos de terceros.

Por ejemplo, una organización que ha sido espiada por algún tipo de spyware mediante el que los intrusos han conseguido los datos bancarios de los clientes. Se recomienda avisar a los clientes para que tomen precauciones y tengan un control de sus cuentas por si los intrusos han realizado alguna actividad en ellas.

Comunidad general

Cuando la gravedad de la incidencia supone consecuencias graves para la organización e incluso daños y consecuencias perjudiciales para la comunidad, es recomendable comunicar la aparición de dicha incidencia y de las consecuencias de su infección en los sistemas y aplicaciones de una organización y/o usuario particular a través de un plan de comunicación con los medios.

Nota

En el momento de comunicar un incidente a la comunidad general hay que tener sumo cuidado para no revelar información sensible que provoque especulaciones innecesarias. Habrá que designarse un responsable de comunicación encargado de la redacción del plan y su ejecución.

Un ejemplo claro de necesidad de comunicación a la comunidad general fue la aparición del primer gusano "1 love you": Este gusano llegó a infectar en el año 2.000 a 50 millones de equipos a través de un archivo adjunto en un correo electrónico, provocando pérdidas valoradas en más de 5.500 millones de dólares.

A pesar de la gravedad de los daños causados por su rápida propagación y mutación, si no se hubiera comunicado convenientemente a la comunidad general, las pérdidas hubieran sido bastante mayores.

Fuerzas de seguridad

En el caso de haberse producido delito informático por parte del atacante hay que comunicar todo lo sucedido a la policía o agente de seguridad análogo para que recaben todo tipo de pruebas y huellas y conseguir localizarle para que cumpla con los requerimientos legales.

Organismos de respuesta a incidentes

Las organizaciones deben estar en contacto con los organismos de respuesta a incidentes como Cert Inteco en España u otros organismos internacionales.

Estos organismos facilitarán un apoyo constante y ayuda en el momento de combatir incidencias que puedan surgir en la organización.

También es recomendable comunicar la incidencia para que sea evaluada por un equipo de expertos y, en caso de ser necesario, incorporarla a su base de datos para poner en conocimiento público su posible aparición y cómo detectarla y combatirla.

En resumen, las acciones a tomar en cuanto a comunicaciones a terceros se resumen en la tabla siguiente:

Comunicaciones a terceros cuando proceda:
Asesores externos
Proveedores
Terceros
Fabricantes de software y hardware
Terceros perjudicados
Comunidad general
Fuerzas de seguridad
Organismos de respuesta a incidentes

11. ESTABLECIMIENTO DEL PROCESO DE CIERRE DEL INCIDENTE Y LOS REGISTROS NECESARIOS PARA DOCUMENTAR EL HISTÓRICO DEL INCIDENTE

Durante todo el ciclo de vida del incidente hay que elaborar y mantener un registro sobre todas las acciones que se van tomando y su evolución para que los agentes encargados de la solución y los usuarios afectados dispongan de información actualizada sobre el estado del incidente.

Cuando ya se ha solucionado hay que llevar a cabo una serie de acciones que permitan cerrar el incidente:

- Comprobar con los usuarios que el incidente ha sido solucionado satisfactoriamente.
- Incorporar las acciones y medidas tomadas para la resolución del incidente en la base de datos de su histórico.
- Reclasificar el incidente como "resuelto" o "cerrado".
- Actualizar la información (en la base de datos de la organización) de las configuraciones del sistema que han intervenido en el proceso de gestión del incidente.
- Cerrar el incidente.

Recuerde

El proceso de registro y documentación del incidente debe realizarse a lo largo de toda su gestión, desde su posible detección hasta su cierre.

Incluso se recomienda realizar revisiones periódicas que actualicen el registro.

A pesar de estar resuelto y solucionado el proceso de gestión del incidente no termina ahí, sino que será necesario la elaboración de informes que sirvan para comparar futuras incidencias y comprobar la eficacia de las medidas tomadas.

Estos informes deberán aportar información básica como los elementos que se mencionan a continuación:

- Gestión de los niveles de servicio: los clientes deben estar informados convenientemente sobre los servicios ofrecidos por la organización y su nivel de cumplimiento. En caso de haber algún incumplimiento en el ofrecimiento del servicio deberán tomarse las medidas oportunas para su corrección.
- Monitorización del rendimiento del centro de servicios: hay que realizar encuestas y entrevistas a los clientes para conocer su nivel de satisfacción por el servicio prestado y para controlar que la atención al cliente está disponible en todo momento.

- Optimización de la asignación de recursos: debe realizarse una evaluación del proceso de gestión del incidente para comprobar que no ha habido duplicidades y consumo de recursos innecesarios.
- Identificación de los errores: cabe la posibilidad que el procedimiento seguido para gestionar la incidencia no sea fiel a las directrices de la organización, a su estructura o a las necesidades. En caso de ser así habrá que adoptar medidas correctivas para que en futuras incidencias no vuelva a ocurrir.
- Disposición de información estadística: en el informe se recomienda incluir información estadística sobre ciertos parámetros significativos de la organización (como consumo de recursos, costes del servicio, tiempo de respuesta, etc.) para hacer previsiones de futuras actuaciones ante apariciones de incidentes de seguridad.

Además de la realización del informe se recomienda la utilización de métricas e indicadores que sirvan de guía de comparación con futuras actuaciones para un correcto seguimiento del incidente. Los principales aspectos a considerar son los siguientes:

- Cantidad de incidentes clasificados temporalmente y por prioridades.
- Ratio en porcentaje de los incidentes (clasificados por prioridades) resueltos en una primera instancia.
- Nivel de cumplimiento de la oferta de servicios a clientes.
- Costes asociados a la aparición y resolución de la incidencia.
- Recursos utilizados para la resolución de la incidencia.
- Nivel de satisfacción de los clientes.
- Tiempos de respuesta y resolución según el impacto y la urgencia de los incidentes.

Importante

No hay que olvidar la clasificación de los incidentes por prioridad. Los incidentes graves con daños significativos deben contener un registro más profundo y detallado que los incidentes inocuos o sin gravedad.

11.1.-Soporte de incidentes

En conclusión, desde que se detecta un incidente hasta que se cierra hay una serie de acciones de soporte que deben llevarse a cabo para tener un control adecuado de su evolución y de todas las acciones realizadas para su resolución y cierre. Los pasos a tomar se describen a continuación.

Reporte del incidente

Nada más detectar la posibilidad de sufrir algún ataque o incidencia (aunque posteriormente sea una falsa alarma) es necesario realizar su reporte para que esta se atendida.

De este modo, cualquier funcionamiento anormal o actividad inusual deberá reportarse a los responsables de la gestión de incidentes mediante correo electrónico, teléfono, personalmente o cualquier otro medio de comunicación establecido que asegure su recepción.

Registro y documentación del incidente

El responsable de la gestión del incidente se encargará de identificar el tipo de incidente remitido por los usuarios y si este es un incidente real o, por el contrario, es una falsa alarma.

Con la recolección de información que confirme la incidencia real se procederá a registrar todos sus datos y a su clasificación según su prioridad, teniendo en cuenta su impacto y la criticidad de los recursos afectados.

Consejo

El registro de la información del incidente y su documentación debe ser lo más detallada posible para poder identificar incidentes similares en un futuro y tomar decisiones de actuación de un modo más rápido y eficaz.

Preparación de la solución del incidente

Una vez registrada la información básica del incidente debe asignarse un tiempo máximo de respuesta, contención y resolución atendiendo a la prioridad designada a dicho incidente.

Debe realizarse un proceso de consulta en la base de datos de incidentes antiguos para comprobar si hay algún caso similar y cómo se ha solucionado anteriormente para intentar aplicar medidas parecidas ante el incidente actual.

Aplicación de soluciones con software de apoyo

Dentro del tiempo máximo de resolución del incidente se procederá a enviar alertas y notificaciones a los usuarios responsables de dicha resolución en caso de ser necesario.

También se llevarán a cabo tareas de carácter interno para completar y apoyar las actividades y medidas que se tomarán para la resolución del incidente.

Asimismo se irá comunicando periódicamente de los avances en su resolución a los usuarios implicados en la incidencia.

Identificación y solución de problemas

En el proceso de resolución de la incidencia se comprobará el histórico de .incidencias. Si se comprueba la sucesión de incidencias recurrentes habrá que detectar si hay alguna causa común que las pueda provocar para evitar incidencias futuras y mejorar la seguridad de la organización.

Cierre del incidente con éxito

Debe comunicarse el cierre del incidente a los usuarios que han visto afectado sus datos indicando que se han cumplido los plazos previstos y las políticas de gestión utilizadas para la resolución del incidente.

También se incluirá el cierre y las soluciones aplicadas a la base de datos de incidentes como soluciones sugeridas en futuras incidencias.

A modo de resumen, en la siguiente tabla se mencionan todos los pasos a seguir recomendados para realizar un soporte del incidente correcto

que permita un seguimiento adecuado y sea un elemento de ayuda ante futuras incidencias.

No hay que olvidar en ningún momento la necesaria capacidad de aprendizaje que deben tener las organizaciones. Estas deben aprender de todas las acciones tomadas, teniendo en cuenta los errores cometidos para que no se repitan en un futuro y que la gestión de incidencias sea más rápida y eficaz.

Pasos de soporte de incidentes	Descripción
Reporte del incidente	Comunicación de las sospechas de incidente a los responsables.
Registro y documentación	Obtención de información adicional y clasificación de la incidencia.
Preparación de la solución	Asignación de tiempos máximos de contención y respuesta.
Aplicación de soluciones mediante software de apoyo	Remisión a los interesados de información referente a la evolución del incidente.
Identificación y solución de problemas	Búsqueda de causa común con incidentes anteriores.
Cierre del incidente con éxito	Comunicación del cierre exitoso del incidente a

todos los interesados.

12. RESUMEN

Las intrusiones son un conjunto de eventos ocurridos cuando un usuario intenta acceder al sistema sin autorización por varios motivos. Las organizaciones deben ser capaces de establecer una serie de herramientas y controles que prevengan la aparición de estos intrusos y eviten su acceso.

Aun así, cuando se detecta una posible intrusión es necesario llevar a cabo una serie de pasos establecidos para que se gestione del modo más eficiente posible. Se comienza con la recolección de información adicional para comprobar si la amenaza es real o por el contrario es una falsa alarma.

En el caso de ser una amenaza real se debe proceder a un análisis de la incidencia y a su clasificación según criterios de criticidad de los recursos e impacto potencial en la organización.

Atendiendo a esta clasificación se deberán definir los tiempos máximos de contención y resolución del incidente, debiendo resolverse en menor tiempo a medida que aumenta la prioridad de la incidencia.

Una vez tomadas las medidas correctivas y resuelta la incidencia debe valorarse la posibilidad de comunicar su ocurrencia a terceros que puedan verse implicados por la utilización de sus datos.

Para concluir y una vez resuelto el problema y realizadas las comunicaciones pertinentes se procederá al cierre del incidente, registrando toda la información sobre su evolución, las medidas que se han tomado, los errores cometidos y sus soluciones para aumentar la eficiencia ante incidencias futuras.

Un correcto registro del incidente permitirá a las organizaciones obtener un aprendizaje de las acciones tomadas que consiga evitar nuevos incidentes que sean similares a los ya sucedidos, reduciéndose así tiempo y daños producidos.

CAPÍTULO 6 ANÁLISIS FORENSE INFORMÁTICO

1. INTRODUCCIÓN

La evolución de las Tecnologías de la Información y la Comunicación (TIC) brinda a las organizaciones innumerables herramientas para la gestión de la información convirtiendo a esta en uno de sus principales activos.

Por este motivo, la información de las empresas y organizaciones se ha convertido en un aspecto atractivo para atacantes que se dedican a generar intrusiones y usos indebidos con fines de lo más variado.

Aunque la cantidad de herramientas y sistemas de protección sea la adecuada, siempre es posible que ocurra cualquier incidente y por ello es necesario detectar al responsable para poder reclamarle exigencias legales y económicas si procede.

Una de las principales herramientas para conseguir detectar a estos responsables es el análisis forense informático, una ciencia que se dedica a obtener "huellas" en los incidentes sucedidos para lograr encontrar a un culpable de un modo razonable y correctamente justificado.

En este capítulo se desarrolla con más detalle el concepto de informática forense, sus procesos y las mejores herramientas para obtener unos resultados más efectivos atendiendo al sistema operativo que se está utilizando.

2. CONCEPTOS GENERALES Y OBJETIVOS DEL ANÁLISIS FORENSE

El análisis forense es una disciplina dentro de la seguridad informática cuya función es analizar los incidentes de seguridad a posteriori con la finalidad de reconstruir los hechos para responder preguntas como:

- ¿Quién ha sido el atacante?
- ¿Cómo se ha producido el incidente de seguridad?
- ¿Cuáles han sido las vulnerabilidades explotadas?
- ¿Cuáles fueron las acciones del intruso cuando consiguió acceder al sistema?

El número de incidentes de seguridad crece día a día, lo que hace justificable invertir en herramientas de análisis forense para localizar a los atacantes y condenarles por ello.

En el gráfico siguiente (obtenido de *RediRJS*) se puede observar la evolución del número de incidentes de seguridad desde 2.004 hasta 2.012.



Nota

RedIRIS es una red académica y de investigación española financiada por el Ministerio de Economía y Competitividad, cuya función principal es facilitar infraestructura de red y servicios complementarios a la comunidad académica y científica española. Se puede obtener más información en <https://www.rediris.es>.

En el gráfico se muestra que después del pico de 2009 hay un descenso de los incidentes de seguridad, pero hay que tener en cuenta que en términos absolutos el número de incidentes puede resultar alarmante.

En la siguiente tabla se puede observar la diferencia desde 1999 a 2012 en cuanto a cantidad de incidentes:

Año	Incidentes totales	Incremento	Año	Incidentes totales	Incremento
1999	195	---	2006	1.973	13.45%
2000	416	113.333%	2007	3.473	76%
2001	1.038	149.51%	2008	3.119	-10.19%
2002	1.495	44.02%	2009	8.045	157.93%
2003	1.294	-13.44%	2010	5.337	-33.66%
2004	2.682	107.26%	2011	3.469	-35%
2005	1.739	-35.16%			

Con la tabla se puede observar con más claridad la importancia de disponer de herramientas de seguridad contra intrusiones y de su evolución.

En 1999 apenas se producían incidentes (195). Sin embargo, en 2009 se obtuvieron los peores datos llegando a remitirse a *RediRIS* un total de 8.045 incidentes.

Desde entonces se han ido reduciendo, muy probablemente, por la concienciación de los usuarios de la utilización de herramientas de protección y de la mayor eficacia de estas.

No obstante, para que siga este ritmo decreciente no hay que bajar la guardia y emplear herramientas de protección y herramientas de análisis forense informático que permitan condenar a los culpables y conocer con más detalle cómo combatir las intrusiones.

2.1.- Objetivos y usos de la informática forense

El análisis forense informático consiste en capturar, procesar e investigar la información de los sistemas informáticos en búsqueda de evidencias utilizando la metodología apropiada para que la investigación pueda utilizarse con fines legales.

El objetivo principal de esta metodología es recoger las evidencias digitales presentes en cualquier tipo de incidencia y delito informático.

Además de este objetivo principal hay que destacar otros objetivos secundarios:

- Compensar los daños causados por los intrusos.
- Perseguir y aplicar medidas judiciales a los atacantes.
- Crear e implantar medidas para prevenir incidentes futuros similares.

Los usos de la informática forense pueden ser de lo más variado. A continuación se describen los más importantes:

- **Persecución criminal:** la informática forense permite obtener evidencias que incriminen a los culpables de muchos tipos de delitos como, por ejemplo, fraudes financieros, tráfico de drogas, pornografía infantil, evasión de impuestos, etc.

- **Litigación civil:** esta disciplina permite aportar pruebas que ayuden a la resolución de conflictos de tipo civil como divorcios, fraudes, problemas de discriminación, etc.
- **Investigación de seguros:** en la actualidad, los delitos relacionados con fraudes a compañías de seguros (robos falsos sobretodo) están en proceso de crecimiento. La informática forense permite la recolección de evidencias que ayuden a las compañías de seguros a detectar estos casos de fraude y disminuir así sus costes.
- **Mantenimiento de la ley:** la informática forense puede utilizarse también para llevar a cabo búsquedas iniciales en investigaciones con órdenes judiciales. Con los resultados obtenidos se puede ampliar la orden judicial y poder realizar búsquedas más exhaustivas de evidencias.
- **Usuario final:** cada vez es más frecuente que los usuarios finales utilicen herramientas de informática forense para la recuperación de archivos eliminados, la encriptación de archivos y datos y para rastrear correos electrónicos, entre otros.
- **Organizaciones y temas corporativos:** la informática forense es cada vez más una herramienta fundamental para obtener evidencias y perseguir delitos relacionados con el uso malintencionado o la apropiación de información confidencial de organizaciones. También sirven de apoyo para la resolución de delitos relacionados con el espionaje industrial.

Nota

Los delitos informáticos están tipificados específicamente en el Código Penal y se definen como cualquier acto delictivo en el que se utiliza la informática como medio o fin del mismo para llevarlo a cabo. Son ejemplos de delitos informáticos aquellos que pretenden destruir y/o dañar equipos informáticos, redes u otros medios electrónicos, además de otros delitos tradicionales como el fraude, las amenazas, falsificación, chantaje, etc.

2.2.- Metodología del análisis forense informático

El análisis forense informático es una parte fundamental dentro del procedimiento de gestión de incidentes de seguridad. Con estos análisis se consigue averiguar cómo, quién y qué daños ha causado cualquier tipo de intrusión o ataque.

Las técnicas de análisis forense se llevan a cabo dentro de las fases de "análisis preliminar" e "investigación" del proceso de gestión de incidentes.



Procedimiento de gestión de incidencias

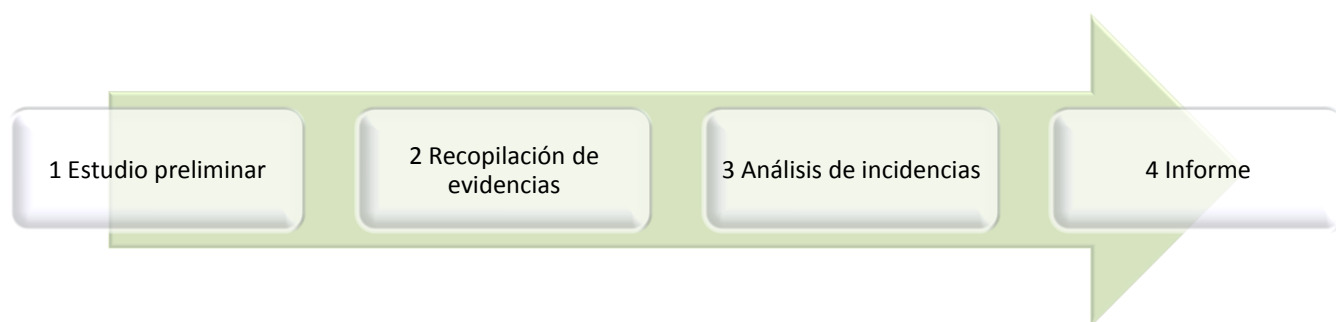
No obstante, pese a formar parte del proceso de gestión de incidentes, sus utilidades son de lo más variadas, por lo que resulta imprescindible conocer más en profundidad su procedimiento concreto.

Así, el procedimiento de análisis forense informático se lleva a cabo a través de varias fases:

- **FASE 1:** estudio preliminar. En esta fase se lleva a cabo un estudio inicial en el que se realizan entrevistas y se revisa la documentación inicial obtenida del incidente para identificar las fuentes disponibles que pueden resultar útiles para la investigación.
- **FASE 2:** adquisición de datos y recopilación de evidencias. La finalidad de la segunda fase es la recolección y obtención de los distintos tipos de evidencias e informaciones fundamentales para la investigación. Se recomienda realizar copias de los dispositivos que han estado implicados para que puedan ser analizados posteriormente.
- **FASE 3:** análisis e investigación de las evidencias. Con los datos obtenidos en la segunda fase se lleva a cabo un análisis más exhaustivo para reconstruir el timeline (la línea temporal) del ataque y llegar al inicio del mismo para detectar al atacante.
- **FASE 4:** confirmación de las pruebas realizadas y realización del informe. Una vez analizadas las evidencias y obtenidos los resultados debe plasmarse todo el procedimiento en un informe que se remitirá a la dirección o a los responsables de seguridad de la organización.

En caso de delito digital, este informe se podrá incorporar a la denuncia que se formule a las autoridades competentes.

En la siguiente imagen se pueden observar de un modo más visual las distintas fases del análisis forense digital:



Fases del análisis forense digital

En los siguientes apartados se irán detallando con más profundidad las distintas fases del análisis forense informático para aprender a desarrollar el proceso completo.

3. EXPOSICIÓN DEL PRINCIPIO DE LOCARD

La ciencia forense fundamenta los principios y técnicas que se pueden y deben utilizar para investigar cualquier delito criminal. En otros términos, esta ciencia incluye los principios y técnicas que se utilizarán para identificar, recuperar, reconstruir y analizar las evidencias que forman parte

de un delito. En cuanto a los principios, todo procedimiento de recolección y análisis de evidencias debe tener en cuenta y llevar a cabo los siguientes aspectos:

- Recogida y examen de las huellas dactilares y ADN.
- Recuperación de los documentos de los dispositivos dañados.
- Realización de copias exactas de las evidencias digitales detectadas.
- Generación de una huella digital de los textos y evidencias para asegurarse que no se modifican.
- Utilización de la firma digital para confirmar la autenticidad de los documentos y mantener la cadena de custodia de evidencias.

Nota

La cadena de custodia de una evidencia es un procedimiento controlado de recolección y análisis de evidencias que tiene como finalidad la preservación de su integridad, evitando que su manejo no provoque vicios o alteraciones.

Los forenses en general, y más concretamente los informáticos, se encargan de aplicar su conocimiento para ayudar a los investigadores a encontrar evidencias y pistas y así poder reconstruir el crimen.

Utilizando un método científico crean hipótesis sobre lo que ha sucedido mediante el análisis de las evidencias, pruebas adicionales y una serie de controles que confirmen o invaliden las hipótesis formuladas.

Los forenses informáticos no pueden conocer todo el pasado, simplemente pueden formular hipótesis y teorías de qué ha podido ocurrir en función de la información limitada de la que se dispone.

3.1.- El principio de intercambio o transferencia de Locard

Uno de los principios más relevantes y utilizados en la ciencia forense es el principio de intercambio o transferencia de Locard.

Edmond Locard (Francia, 1877-1966), criminalista francés, fue uno de los pioneros en criminología y fundó el Instituto de Criminología de la Universidad de Lyon. Es conocido por enunciar el famoso principio de intercambio o transferencia de Locard.

Sabía que ...

Edmond Locard recibió el nombre del Sherlock Holmes francés por su gran admiración hacia ese personaje. También trabajó para los servicios secretos franceses en la Primera Guerra Mundial aportando sus conocimientos criminalísticos para conocer los pasos que habían seguido los soldados y los prisioneros.

Este principio se utiliza muy frecuentemente para relacionar al criminal con el crimen que ha cometido y, en términos generales, dice que cualquiera o cualquier objeto que forma parte de la escena del crimen deja un rastro en la escena o en la víctima y viceversa, el objeto o criminal se llevará consigo algo de la escena del crimen.

Concretamente, el principio de Locard se define como:

"Cada contacto deja un rastro"

Siempre que dos objetos entran en contacto hay una transferencia de parte de algún material de un objeto al otro. Cuando un criminal entra en una escena del crimen o entra en contacto con una víctima, la víctima se queda con algo del criminal pero este también se lleva algo a cambio.

En otras palabras, cuando un contacto entra en la escena del crimen deja siempre alguna huella (pelo, sudor, huellas dactilares, etc.) pero también se lleva algo consigo cuando abandone la escena (barro, olores, fibras, etc.). Con la detección y análisis de estas evidencias se podrá demostrar con altas probabilidades la presencia de algo o alguien en la escena del crimen.

En la ciencia forense tradicional se distinguen distintos tipos de evidencias físicas:

- **Evidencias transitorias:** son evidencias temporales que solo permanecen en la escena del crimen en un período de tiempo generalmente corto. Por ejemplo, temperatura, olor, etc.
- **Evidencias curso o patrones:** evidencias que se han producido por efectos de contacto, han tenido que ser tocadas por el atacante o por la víctima. Son ejemplos los muebles cambiados de sitio, la trayectoria de una bala, etc.
- **Evidencias condicionales:** evidencias que se han originado por alguna acción o evento sucedidos en la escena del crimen. Por ejemplo, localización de evidencias según la ubicación del cuerpo (víctima), ventanas abiertas o cerradas, televisión encendida/apagada, etc.
- **Evidencias transferidas:** son las evidencias que se originan por el contacto entre varias personas, entre varios objetos o entre personas y objetos. En estas evidencias entra en juego el concepto de relación entre personas, objetos o ambos.

Nota

La primera referencia del principio de Locard encontrada fue en *"The Police and Crime-Detection Today"* en 1.956, publicación en la que se reconoce por primera vez como principio esencial para los forenses de todo el mundo.

En resumen, el principio de intercambio de Locard se compone de tres elementos:

1. El sospechoso se llevará con él algún rastro o huella de la escena y de la víctima.
2. El sospechoso dejará rastros en la víctima y la víctima puede dejar algún rastro sobre el sospechoso.
3. El sospechoso dejará también algún rastro en la escena del crimen.

De este modo, el objetivo principal del desarrollo de este principio es conseguir establecer relaciones entre los distintos elementos que forman parte del crimen:

- La víctima.
- El sospechoso.
- La evidencia.
- La escena del crimen.

El concepto de relación entre estos elementos es fundamental para una correcta resolución del crimen: si no hay relación alguna no se podrá acusar directamente a un criminal al no haber pruebas que lo incriminen.

Nota

El descubrimiento de la relación entre los elementos de un crimen es lo que llevará al éxito o al fracaso de la investigación. Por eso, el principio de intercambio de Locard fundamenta su definición en el concepto de relación.

En cuanto a las evidencias según Locard, estas pueden ser transferidas de dos modos diferentes:

- **Mediante transferencia directa:** cuando la evidencia se transfiere de origen a destino directamente, sin intermediarios.
- **Mediante transferencia indirecta:** cuando la evidencia es transferida a una localización y, posteriormente, se transfiere de nuevo a otra localización.

En resumen, el principio de intercambio de Locard se refleja en la siguiente tabla:

Principio de intercambio de Locard	
"Cada contacto deja un rastro"	La víctima deja rastro en la escena del crimen y en el sospechoso.
	El sospechoso deja rastro en la víctima y en la escena del crimen.
	Tanto la víctima como el sospechoso tendrán algún rastro de la escena del crimen.
Tipos de evidencias físicas	Evidencias transitorias.
	Evidencias curso o patrones.
	Evidencias condicionales.
	Evidencias transferidas.
Métodos de transferencia de evidencias	Transferencia directa.
	Transferencia indirecta.

3.2.- 3.2. Aplicación del principio de Locard al análisis forense digital

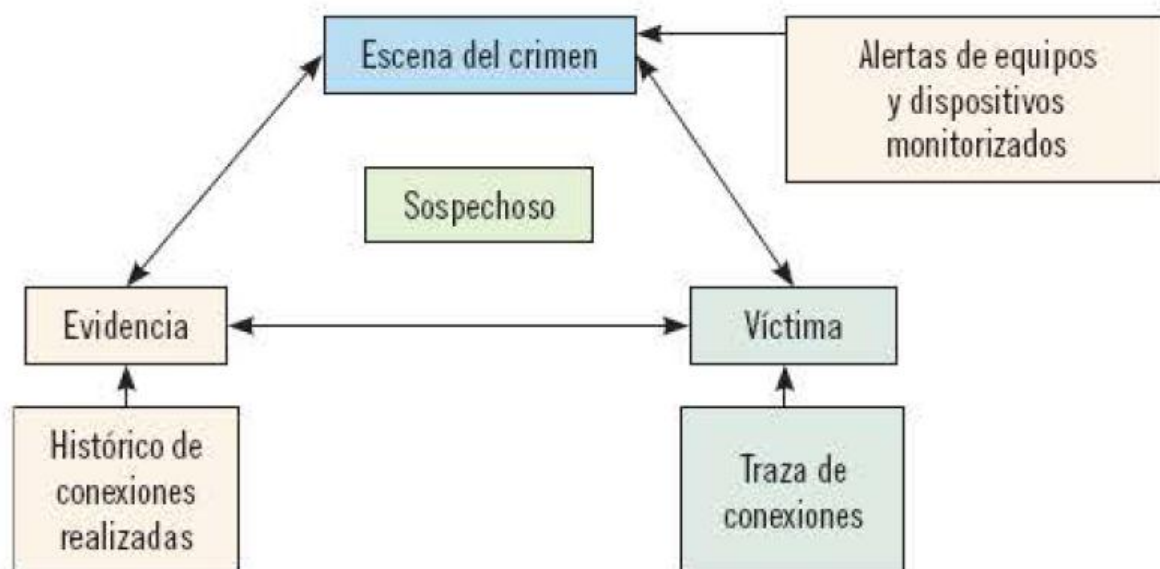
Los conceptos del principio de intercambio de Locard son perfectamente trasladables al análisis forense informático o digital y tiene plena validez en las evidencias electrónicas.

Cualquier atacante deja siempre algún tipo de "huella digital" en el sitio atacado además de llevarse algo con él. Con el análisis de las huellas digitales y de las evidencias se podrá reconstruir qué ha ocurrido para relacionar al atacante con la víctima y, a su vez, con la escena del crimen (en este caso los equipos o dispositivos afectados).

A través de la determinación de ¿cómo ha sucedido?, ¿dónde ha sucedido? Y ¿qué se ha afectado? se podrán detectar las evidencias digitales y relacionarlas entre ellas para resolver el crimen.

Por ejemplo, con la detección de quién fue la última persona que escribió en un archivo relacionado con una intrusión se pueden localizar sospechosos de la misma.

Principio de Locard trasladado a la versión digital



En el gráfico se muestran rastros de los distintos elementos:

- En la escena del crimen se puede encontrar algún resto del crimen con el análisis de las alertas emitidas por los dispositivos y equipos que han sido monitorizados previamente.
- En cuanto al sospechoso, este ha podido dejar algún rastro en la escena del crimen. Se podrá encontrar algún rastro observando el histórico de las conexiones realizadas para encontrar a posibles sospechosos.
- Analizando a la víctima (en este caso, los equipos afectados) se puede obtener un trazado de ruta de las conexiones realizadas que permita obtener el camino paso a paso de un paquete de datos desde su origen hasta su destino y así encontrar a los atacantes desde su origen.
- Además, se produce también una relación entre el atacante sospechoso y el equipo víctima, ya que generalmente hay algún archivo que haya sido utilizado y/o modificado por ambos.

Para finalizar, no se puede relacionar el principio de Locard al mundo digital si no se conoce el concepto de "evidencia digital": Una evidencia digital, a diferencia de las evidencias físicas, es cualquier documento, fichero, registro, etc. que está contenido en un soporte informático o digital y que es susceptible de tratamiento. Son ejemplos de evidencias digitales cualquier documento de ofimática (archivos Excel, Word, etc.), imagen, base de datos, registro de actividad, comunicación digital (correo electrónico, etc.), etc.

Las evidencias digitales son uno de los pilares más importantes de la informática forense, ya que suministran un gran valor en las investigaciones y pueden aportarse en procesos judiciales.

Su validez jurídica ha sido y sigue siendo un tema controvertido sometido continuamente a debate entre juristas y expertos técnicos. Para conocer más detalladamente el concepto de evidencias electrónicas y sus aplicaciones se recomienda acceder al foro de las Evidencias Electrónicas (<<http://www.evidenciaselectronicas.org>>) y conocer los debates actuales sobre su utilización en procedimientos judiciales.

4. GUÍA PARA LA RECOGIDA DE EVIDENCIAS ELECTRÓNICAS

La recopilación de evidencias electrónicas es una de las fases más críticas y vitales del análisis forense digital. Si la recopilación no se realiza bien puede invalidarse todo el análisis posterior, ya que la información obtenida no sería correcta y los resultados pueden ser erróneos.

Por ello, la recogida de evidencias electrónicas debe ser un proceso meticuloso en el que debe tratarse de no realizar ningún cambio sobre las mismas para no incurrir en vicios que lleven a errores de análisis.

Más concretamente, cuando hay que recoger evidencias electrónicas hay que tener en cuenta una serie de conceptos imprescindibles:

- Evidencias volátiles y no volátiles.
- Etiquetado de evidencias.
- Cadena de custodia.
- Ficheros y directorios ocultos.
- Recuperación de ficheros borrados.

4.1.- Evidencias volátiles y no volátiles

Las evidencias digitales se clasifican en evidencias volátiles y no volátiles:

- Las evidencias volátiles son aquellas que se pierden cuando se apaga el equipo (estado de la memoria, procesos en ejecución, etc.).
- Las evidencias no volátiles, sin embargo, se almacenan en el sistema de ficheros y no se pierden al apagar el equipo (aplicaciones, configuraciones, etc.).

Asimismo, la primera decisión a tomar es si apagar el equipo o no apagarlo. Esta decisión puede ser crucial, ya que al apagar el equipo pueden perderse evidencias volátiles importantes como los usuarios conectados, las conexiones existentes en ese momento, etc.

Debido a la relevancia de las evidencias volátiles se recomienda preservar la evidencia más volátil en el momento inicial del análisis forense digital, debiendo atender las evidencias digitales en el orden (relacionado con su grado de volatilidad) de la tabla siguiente:

Orden de preservación de las evidencias digitales:
Registros, memoria caché, memoria de periféricos
Memoria física
Estado de las conexiones de red
Ficheros temporales del sistema
Procesos que se están ejecutando en ~se momento
Discos duros, rígidos
Archivos de backups
Registros y datos de monitorización remotos relevantes
Configuración física y topología de la red
CD-ROM, impresiones

4.2.- Etiquetado de evidencias

Para que las evidencias se puedan admitir como tal deben cumplir con una serie de requisitos:

- Deben conservarse en un estado lo más parecido posible al estado en el que se encontraron.
- En la medida de lo posible, debe realizarse una copia exacta de la evidencia original para realizar los trabajos de investigación sobre la misma y no dañar los datos originales.
- Las copias realizadas deberán realizarse en medios estériles, es decir, en medios que no hayan contenido ningún dato anteriormente.
- Las evidencias deberán etiquetarse y documentarse debidamente en la cadena de custodia. Además, cada acción realizada sobre la evidencia o sobre su copia deberá ser también documentada con detalle.
- Las evidencias digitales deberán documentarse con firmas digitales del investigador para garantizar que nadie más realiza ninguna acción sobre ellas.

En el momento de etiquetar las evidencias digitales hay que tener en cuenta que se clasifican en varias categorías:

- **Registros generados por ordenador:** se generan por la programación de un equipo y son inalterables por un usuario. Estos registros son los llamados registros de eventos de seguridad o *logs* y se utilizan como medio probatorio para demostrar el correcto o incorrecto funcionamiento del sistema cuando se generó el registro.
- **Registros almacenados por ordenador es:** estos registros no son generados por un equipo, los genera una persona y posteriormente son almacenados en un equipo (por

ejemplo, un documento de Word). De estos registros se puede deducir la identidad del usuario que los generó y probar hechos que estén contenidos en este.

- **Registros híbridos:** son registros que combinan acciones realizadas por personas y acciones realizadas por el equipo.
- **Registros de cada servidor:** son los registros del sistema y de los programas en ejecución.
- **Registros de tráfico de red:** registros que incluyen la actividad de red generada en el equipo.
- **Registros de aplicación:** estos registros son almacenados por cada aplicación e incluyen datos sobre el acceso de usuarios, los errores ocurridos e información sobre las acciones que ha realizado cada usuario.

Teniendo en cuenta estas categorías, la evidencia digital deberá considerar una serie de criterios para decidir su admisibilidad reflejados en la tabla siguiente:

Criterios de admisibilidad de evidencias electrónicas	
Autenticidad	La evidencia debe haber sido generada y registrada en la escena del crimen y debe mostrar que los medios utilizados no se han modificado.
Confiabilidad	Las evidencias serán confiables si el sistema que las produjo no ha sido violado y estaba funcionando correctamente cuando se recibió, almacenó o generó la prueba.
Completitud o suficiencia	La evidencia debe estar completa, tiene que haberse mantenido su integridad.
Respeto por las leyes	Las técnicas de recolección y tratamiento de la evidencia deben cumplir las normativas legales vigentes en el ordenamiento jurídico.

4.3.- Cadena de custodia

Como ya se ha indicado anteriormente, la cadena de custodia está formada por una serie de procedimientos y documentos relacionados con la recolección, copia, traslado, tratamiento, verificación y análisis de las evidencias encargados de su preservación para evitar que la manipulación de estas pueda llevar a error en los resultados del análisis.

La cadena de custodia debe realizarse en todas las fases del análisis forense digital, desde el momento de la recolección hasta la emisión del informe final.

En un primer momento deberán utilizarse métodos adecuados para la identificación, documentación, etiquetado y almacenamiento de las evidencias añadiendo firmas temporales que permitan temporalizar cada acción realizada sobre las mismas.

Además, en su tratamiento las evidencias deberán protegerse de factores ambientales (lluvia, campos magnéticos, etc.) que puedan provocar pérdidas de datos. Se recomienda mantener los soportes informáticos donde se registran las evidencias en bolsas de plástico antiestáticas que los protejan de estos factores.

Para una correcta preservación de la cadena de custodia es necesario que las evidencias sean tratadas por profesionales con conocimientos especializados y correctamente identificados. En la documentación de la evidencia debe plasmarse quién realizó cada acción, cuándo la realizó y dónde la realizó para evitar problemas de falta de integridad en los datos de la evidencia.

Nota

El mantenimiento de la cadena de custodia de las evidencias adquiere mayor importancia desde un punto de vista legal. La pérdida de integridad o la alteración de datos en evidencias puede invalidar pruebas en procesos judiciales.

El mantenimiento de la cadena de custodia de las evidencias adquiere mayor importancia desde un punto de vista legal. La pérdida de integridad o la alteración de datos en evidencias puede invalidar pruebas en procesos judiciales.

En concreto, la cadena de custodia debe:

- Reducir todo lo posible la cantidad de agentes que traten las evidencias.
- Mantener la identidad de las personas implicadas en todo el proceso de gestión de la evidencia.
- Asegurar la firmeza de las evidencias cuando estén almacenadas para asegurar su protección.
- Registrar los tiempos firmados por cada agente en los intercambios de evidencias entre ellos para detectar al responsable de su tratamiento en cada momento.

4.4.- Ficheros y directorios ocultos

En el momento de realizar la recolección de evidencias hay que tener en cuenta que puede haber evidencias escondidas en ficheros o directorios ocultos.

Es más, los atacantes suelen esconderse en archivos ocultos, por lo que es fundamental averiguar su localización y de qué tipo son para considerar si pueden ser evidencias ocultas o si deben descartarse por ser archivos inofensivos.

Nota

Los atacantes no solo se esconden en archivos ocultos, en ocasiones también se dedican a ocultar archivos y directorios ya existentes previamente, por lo que conviene realizar una búsqueda de los archivos ocultos para detectar evidencias de estos hechos.

4.5.- Información oculta del sistema

No solo hay que localizar los archivos y directorios ocultos en el sistema, también deben encontrarse los distintos parámetros e informaciones del sistema que se han mantenido ocultos para protegerlos de atacantes para comprobar si han sido alterados.

De estas alteraciones, con herramientas de análisis adecuadas, se podrán encontrar evidencias electrónicas y pruebas que podrán utilizarse para incriminar al atacante.

Hay que tener en cuenta que la información oculta del sistema contiene detalles importantes sobre la utilización del equipo como puede ser el historial de páginas web visitadas, correos electrónicos enviados y recibidos, documentos creados, modificados y eliminados, etc.

4.6.- Recuperación de ficheros borrados

En general, cuando un archivo se elimina no es borrado definitivamente, sino que se mantiene en la papelera de reciclaje durante un período determinado. Es más, cuando este archivo se borra de la papelera de reciclaje queda marcado como borrado pero sigue físicamente en el disco duro a pesar de estar oculto para los usuarios.

En cuanto al análisis forense se recomienda localizar estos archivos eliminados que no han desaparecido definitivamente del equipo para intentar descubrir archivos sospechosos y, por lo tanto, posibles evidencias digitales.

5. GUÍA PARA EL ANÁLISIS DE LAS EVIDENCIAS ELECTRÓNICAS RECOGIDAS, INCLUYENDO EL ESTUDIO DE FICHEROS Y DIRECTORIOS OCULTOS, INFORMACIÓN OCULTA DE SISTEMA Y LA RECUPERACIÓN DE FICHEROS BORRADOS

Una vez recopiladas las evidencias digitales y almacenadas adecuadamente, el análisis forense digital debe encargarse de la reconstrucción y temporalización de los hechos ocurridos con los datos recopilados. Con este análisis deberán recopilarse los hechos desde el momento inicial del

incidente hasta su descubrimiento y se dará por finalizado cuando se detecte quién realizó el ataque, cómo se produjo, cuál fue su objetivo y bajo qué circunstancias se cometió.

El proceso de análisis de evidencias se divide en varias fases que se irán describiendo a continuación.

5.1.- Preparación del entorno de trabajo para el análisis

Antes de empezar el análisis deberá prepararse el entorno de trabajo para que sea adecuado para llevar a cabo las investigaciones previstas. Se recomienda no tocar los dispositivos originales y trabajar con las copias de las evidencias.

Para ello se aconseja preparar dos estaciones de trabajo:

- Una de ellas deberá contener dos discos duros: en uno se instalará el sistema operativo que servirá de anfitrión y con el que se realizará el análisis de las evidencias y en otro se volcará la imagen del disco duro del equipo atacado.
- En la otra estación de trabajo se instalará un sistema operativo configurado exactamente igual que el equipo atacado.

Nota

La preparación del entorno de trabajo requiere la comprobación y anotación de todos los parámetros de configuración importantes para el análisis, de modo que sea posible identificar cualquier cambio realizado desintencionadamente.

De este modo se podrán analizar los cambios producidos en ambos equipos pudiendo detectar los efectos ocasionados por los ataques sufridos en el equipo.

5.2.- Reconstrucción de la secuencia temporal del ataque

Una vez preparado el entorno de trabajo para un análisis forense adecuado, el siguiente paso a realizar será la creación de una secuencia temporal de los sucesos que se produjeron durante el ataque.

Para ello se deberá recopilar y analizar la siguiente información de los ficheros:

- Tamaño y tipo de fichero.
- Usuarios y grupos a los que pertenece el fichero.
- Permisos de acceso.
- Detección sobre si el fichero fue borrado o no.
- Trazado de ruta completo.
- Marcas de tiempo: fecha y hora de su creación, modificación, borrado y acceso.

Nota

Con la reconstrucción temporal del ataque se puede conseguir llegar al origen del mismo y localizar al atacante, además de conocer todos los pasos que ha ido tomando. Esto se podrá utilizar como prueba real para inculpar al atacante en caso de proceder a la ejecución de

Con ello se pretende encontrar ficheros y directorios (tanto visibles como ocultos) que han sido creados, modificados o eliminados recientemente que se encuentren en rutas poco comunes. En esta fase hay que vigilar con detalle los archivos ocultos y los eliminados, ya que en ellos suelen esconderse las huellas de los atacantes (deberán intentar recuperarse en la medida de lo posible los archivos eliminados, además de analizar los archivos ocultos y la información oculta del sistema).

Hay que tener en cuenta que los atacantes en general instalarán sus herramientas y crearán archivos y directorios en rutas poco comunes que no se visualicen con frecuencia por los usuarios habituales. Una ubicación bastante utilizada son los directorios temporales.

5.3.- Determinación de cómo se realizó el ataque

Cuando ya se ha determinado el orden de los acontecimientos producidos en el ataque deberá realizarse un análisis para detectar cómo se accedió al sistema, investigando las vulnerabilidades de las que se haya podido aprovechar el atacante para acceder a este.

También se deberá investigar cuáles fueron las herramientas utilizadas por el atacante que le permitieron aprovecharse de la vulnerabilidad o fallo de administración y acceder al sistema.

Para ello se realizarán consultas y se analizarán archivos de *logs*, registros, cuentas de usuarios, etc.

Recuerde

Los archivos de registro o archivos de lag son archivos que incluyen mensajes e información del sistema y de las aplicaciones que se ejecutan en él.

5.4.- Identificación del atacante o atacantes

La identificación del atacante o atacantes es fundamental sobre todo cuando la organización quiere tomar acciones legales contra los responsables.

En el proceso de identificación deberá intentar averiguarse inicialmente la dirección IP del atacante mediante la revisión de los registros de las conexiones de red.

La identificación será posible sobre todo con el análisis de las evidencias volátiles, ya que son los que contienen información sobre conexiones fallidas, archivos temporales, archivos eliminados, información sobre correos electrónicos, etc.

5.5.- Evaluación del impacto causado

En el análisis de las evidencias es fundamental analizar el impacto causado por el atacante en el sistema: hay que averiguar qué han hecho los atacantes una vez han accedido al sistema y si dicho ataque ha podido comprometer la información de los equipos.

Se distinguirán dos tipos de ataques: activos y pasivos.

Tipos de ataques	
Activos	Ataques en los que se altera la información del sistema, poniendo en compromiso su funcionamiento habitual.
Pasivos	Ataques limitados a observar y escuchar los equipos sin alterar sus datos.

No solo deberá analizarse el impacto causado, también deberá intentar deducirse el impacto potencial del ataque (el impacto que hubiera tenido si no se hubieran tomado medidas a tiempo) para ayudar a definir medidas de prevención de ataques futuras.

5.6.- Documentación del ataque

Como ya se ha comentado, debe llevarse a cabo la documentación de todas las acciones realizadas en la recolección y análisis de las evidencias.

Así, tan pronto como se haya detectado el ataque, es imprescindible dejar anotadas todas las actividades ejecutadas para aumentar la eficiencia del análisis forense y disminuir las posibilidades de error en la obtención de resultados. Para que la documentación sea correcta y efectiva se recomienda la utilización de formularios que deberán ser rellenados por los responsables de la gestión del ataque y de las evidencias.

En concreto deberían elaborarse formularios como mínimo de los siguientes aspectos:

- Cadena de custodia de la evidencia.
- Identificación de los equipos, componentes y dispositivos.
- Ataques tipificados.
- Recolección y almacenamiento de las evidencias.
- Discos duros de la organización.

Nota

La utilización de formularios para documentar los ataques crea un protocolo de actuación implícito que facilitará la consulta del histórico de incidentes y de las acciones tomadas en cada momento.

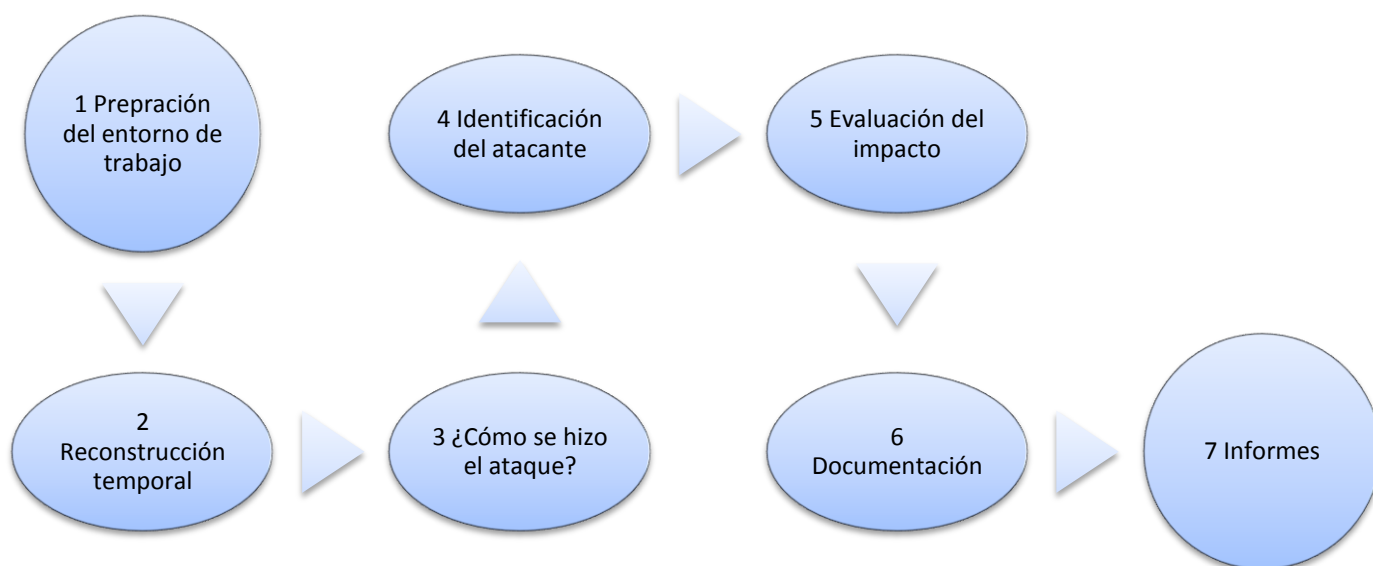
5.7.- Elaboración del informe

Cuando ya se ha terminado el análisis de las evidencias y se han obtenido los detalles de los ataques detectados deberá elaborarse un informe en el que se describan herramientas, metodología, técnicas utilizadas y los hallazgos obtenidos.

En general, este informe deberá contener los aspectos siguientes:

- Antecedentes del ataque.
- Recolección previa de datos y evidencias.
- Descripción de la evidencia.
- Herramientas utilizadas en el análisis.
- Análisis de la evidencia (incluyendo toda la información de los equipos y dispositivos analizados).
- Descripción de los hallazgos encontrados (huellas del ataque, vulnerabilidades aprovechadas, origen del ataque, alcance, etc.).
- Cronología del ataque.
- Conclusiones.
- Recomendaciones.

En resumen, las fases de análisis de evidencias se encuentran reflejadas en el siguiente gráfico:



No hay que olvidar la importancia de la preservación de la cadena de custodia en todas y cada una de las fases del análisis de las evidencias.

Cualquier variación de la información puede llevar a errores en los resultados finales.

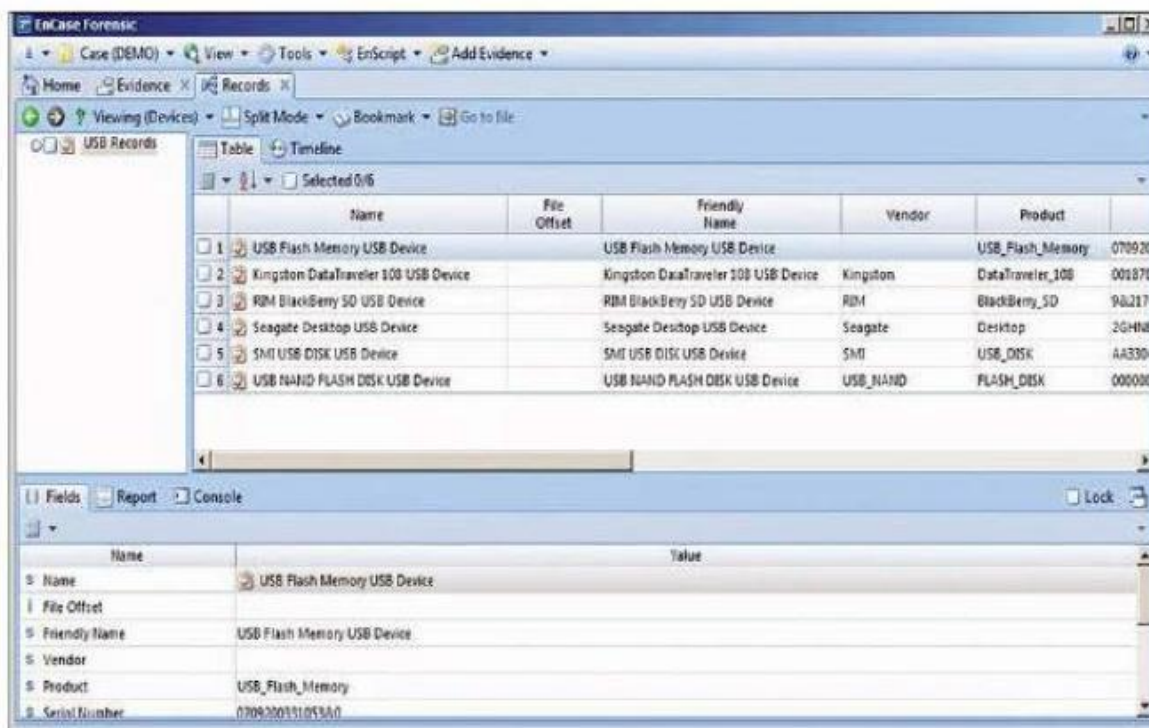
6. GUÍA PARA LA SELECCIÓN DE LAS HERRAMIENTAS DE ANÁLISIS FORENSE

Los atacantes cada vez utilizan técnicas más sofisticadas para llevar a cabo sus ataques y, por ello, la detección de evidencias y el posterior análisis de las mismas puede ser una tarea bastante tediosa para los investigadores si no utilizan herramientas específicas que completen y añadan eficacia a la investigación. La elección de la herramienta adecuada dependerá del sistema operativo utilizado y de la preferencia entre *software* comercial y *software* libre.

Teniendo en cuenta estos criterios, las herramientas más utilizadas para el análisis forense son las que se describen a continuación.

EnCase

Esta herramienta es un *software* comercial de pago que se utiliza sobre todo para analizar los medios de comunicación digitales. Incluye herramientas de recopilación de datos, recuperación de archivos, análisis y búsqueda de archivos. Actualmente es una de las herramientas líderes de análisis forense aunque no hay versión íntegra en español de la aplicación.



Herramienta EnCase

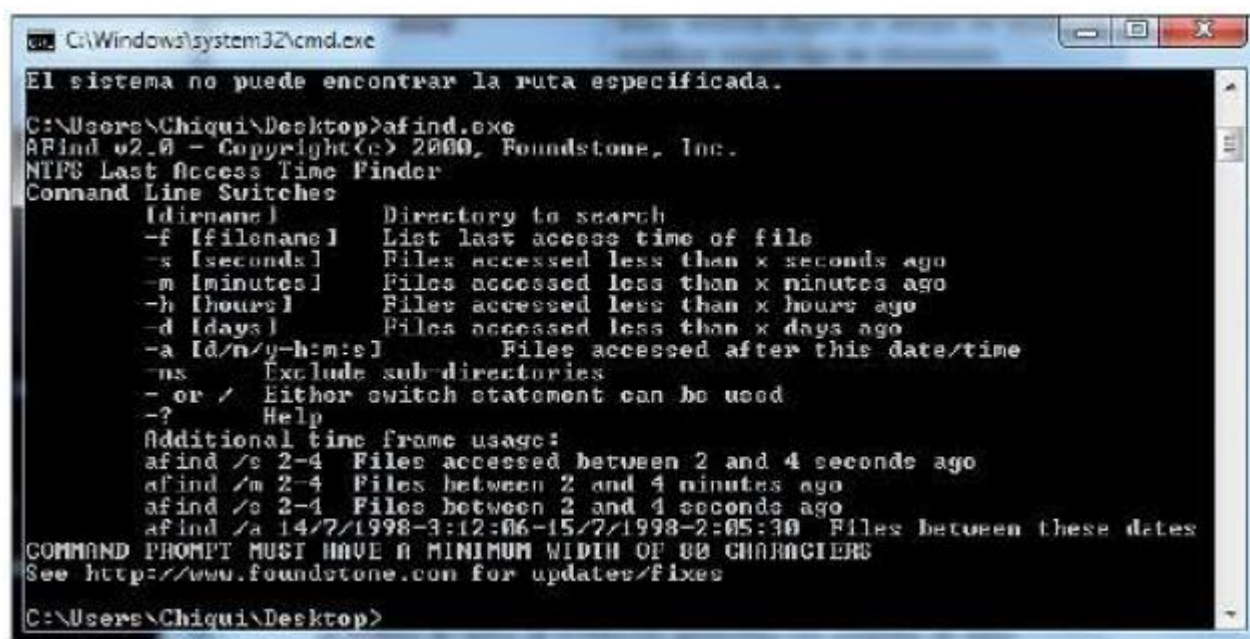
The Forensic ToolKit

En este caso *The Forensic Too/Kit* es una aplicación de *software* libre diseñado para utilizarse en *Microsoft Windows*. Con esta herramienta se puede recopilar información sobre los ataques y dispone de una serie de funcionalidades que permiten la generación de informes y estadísticas del sistema de archivos que se pretende investigar.

Se puede descargar en www.foundstone.com y funciona a través de un intérprete de comandos.

En la siguiente tabla se describen los comandos principales de la herramienta y sus funcionalidades básicas:

Comando	Función
afind	Busca archivos según su tiempo de acceso sin modificar ningún tipo de información.
hfind	Busca archivos ocultos.
sfind	Busca flujos de datos ocultos en el disco duro que aparecen con las herramientas habituales del sistema operativo.
filestat	Facilita una lista detallada de los atributos del archivo indicado.



```

C:\Windows\system32\cmd.exe
El sistema no puede encontrar la ruta especificada.
C:\Users\Chiqui\Desktop>afind.exe
AFind v2.0 - Copyright(c) 2000, Foundstone, Inc.
NTFS Last Access Time Finder
Command Line Switches
  [dirname]      Directory to search
  -f [filename]  List last access time of file
  -s [seconds]   Files accessed less than x seconds ago
  -m [minutes]   Files accessed less than x minutes ago
  -h [hours]     Files accessed less than x hours ago
  -d [days]     Files accessed less than x days ago
  -a [dd/mm/yyyy-hh:mm:ss] Files accessed after this date/time
  -ns           Exclude sub-directories
  -or /         Either switch statement can be used
  -?           Help
Additional time frame usage:
afind /s 2-4    Files accessed between 2 and 4 seconds ago
afind /m 2-4    Files between 2 and 4 minutes ago
afind /s 2-4    Files between 2 and 4 seconds ago
afind /a 14/7/1998-3:12:06-15/7/1998-2:05:30 Files between these dates
COMMAND PROMPT MUST HAVE A MINIMUM WIDTH OF 80 CHARACTERS
See http://www.foundstone.com for updates/fixes
C:\Users\Chiqui\Desktop>

```

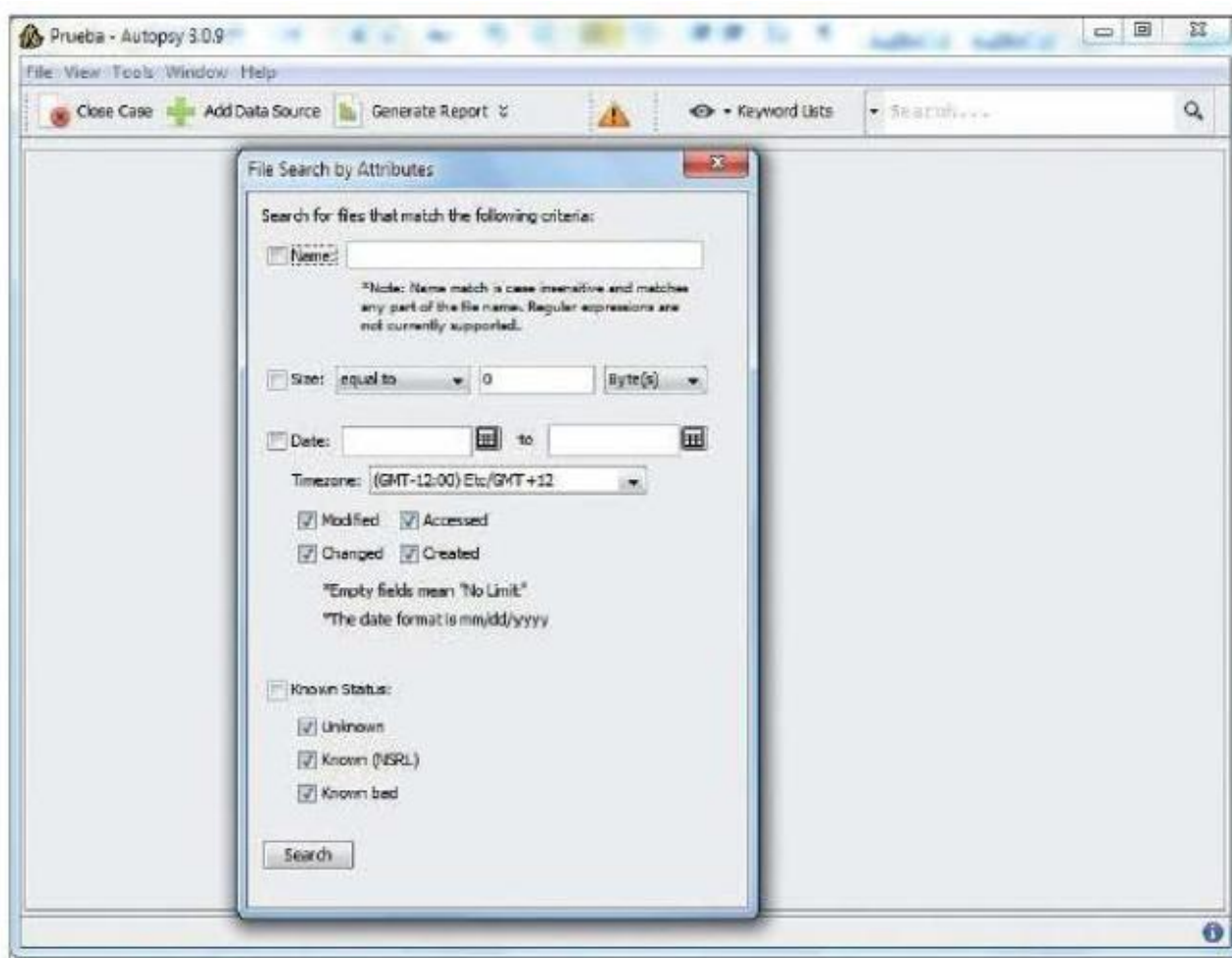
Comando *afind* de la herramienta *The Forensic Toolkit*

The Sleuth Kit y Autopsy

Se trata de un conjunto de herramientas forenses diseñadas para sistemas operativos *UNIX/Linux* y *Microsoft Windows* cuya función principal es el análisis de datos de evidencias generadas con unidades de disco.

También permite acceder a archivos eliminados, genera la línea temporal de actividad de los archivos y crea informes y notas del investigador entre otras muchas funcionalidades.

Es una herramienta gratuita y se puede descargar en <<http://www.sleuthkit.org>>.



Herramienta Autopsy

7. RESUMEN

Debido a la presencia creciente de incidentes de seguridad surgieron las herramientas de análisis forense digital. Se trata de una disciplina dentro de la seguridad informática que se encarga de

analizar los incidentes de seguridad y los delitos digitales a posteriori para reconstruir los hechos y conseguir detectar al atacante y averiguar cómo ha accedido a los equipos.

Los usos y objetivos de estos análisis son de lo más variados y pueden utilizarse tanto para aportar pruebas para investigar delitos de fraude con compañías de seguros, como para realizar investigaciones con órdenes judiciales, entre otros.

Para desarrollar las técnicas de análisis forense digital debe seguirse una metodología con unas fases perfectamente definidas: estudio preliminar, recopilación de evidencias, análisis de evidencias y elaboración de informes con los resultados.

Con la correcta aplicación de estas fases y un mantenimiento adecuado de la cadena de custodia de las evidencias (que impida que la información recopilada se modifique y pueda llevar a resultados erróneos) se puede llegar a descubrir el origen del ataque, localizar al atacante e, incluso, tomar medidas legales contra este para exigirle responsabilidad por los daños causados.

Por este motivo, los distintos atacantes cada vez utilizan técnicas más sofisticadas para ocultar sus huellas y evitar ser descubierto pero, aun así, se pueden encontrar en el mercado varias herramientas (tanto de pago, como gratuitas y para varios sistemas operativos) que consiguen recoger evidencias y detectar al culpable con bastante probabilidad.