

## GESTIÓN DE INCIDENTES DE SEGURIDAD

---

### 2.1 INCIDENTES DE SEGURIDAD

---

Por **Incidente de Seguridad** entendemos cualquier evento que pueda provocar una interrupción o degradación de los servicios ofrecidos por el sistema, o bien afectar a la confidencialidad o integridad de la información.

Un incidente de seguridad puede ser causado por un acto intencionado realizado por un usuario interno o un atacante externo para utilizar, manipular, destruir o tener acceso a información y/o recursos de forma no autorizada. Aunque un incidente también podría ser la consecuencia de un error o trasgresión (accidental o deliberada) de las políticas y procedimientos de seguridad, o de un desastre natural o del entorno (inundación, incendio, tormenta, fallo eléctrico...).

En España, la Ley Orgánica de Protección de Datos define una incidencia como “cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos”, en el contexto de los ficheros con datos de carácter personal.

### 2.2 IDENTIFICACIÓN Y CARACTERIZACIÓN DE LOS DATOS DE FUNCIONAMIENTO DEL SISTEMA

---

Los *logs* de los equipos informáticos (en especial, de los servidores) y de los dispositivos de red facilitan el registro de posibles incidentes y funcionamientos anómalos, la existencia de fallos en la configuración de una aplicación, la posible desconexión de algún dispositivo del sistema, los cambios realizados en la configuración de los equipos, la utilización de recursos sensibles por parte de los usuarios del sistema, etcétera. Además, proporcionan estadísticas que permiten evaluar el rendimiento del sistema informático.

No obstante, en algunos casos se podría estar registrando información que podría afectar a la privacidad de los usuarios, por lo que será necesario tener en cuenta las posibles consideraciones desde el punto de vista legal (obligación de informar a los usuarios que se está registrando su actividad en el sistema).

En lo que se refiere a los *logs* del sistema operativo, se podrían configurar para registrar los procesos en ejecución dentro del sistema, los inicios y cierres de sesión por parte de los usuarios, las llamadas al sistema, las aplicaciones ejecutadas por los usuarios, los accesos a ficheros y a otros recursos (impresoras...), los posibles problemas de seguridad (intentos de acceso no autorizado a los recursos o fallos de las aplicaciones), etcétera.

Así, por ejemplo, en los sistemas UNIX se podría utilizar la herramienta "System log", mientras que en los sistemas Windows se puede recurrir al registro de eventos (*event log*). También será necesario configurar los *logs* de los dispositivos de red (*routers*, cortafuegos...), de los servidores y de las aplicaciones instaladas en algunos equipos.

Para garantizar la adecuada protección de los *logs*, será necesario almacenarlos de forma segura en un entorno distinto al del sistema protegido, para evitar que los intrusos los puedan modificar o eliminar: grabación de los registros en discos WORM (*Write Once Read More*), generación de una copia en papel, etcétera.

En algunos casos se puede recurrir a una gestión centralizada de los *logs*, mediante un servidor de *logs* que se encargue de guardar copias de todos los registros enviados por los dispositivos de red y los servidores. Para ello, se podrían utilizar aplicaciones como *Syslog* para centralizar los registros. De este modo, se refuerza la seguridad frente a intrusos que pretendan eliminar su rastro manipulando los *logs* de los equipos.

Además, un servidor centralizado de *logs* permite conservar los registros durante un mayor período de tiempo, lo que puede facilitar el análisis detallado de estos registros, incluyendo el estudio de la relación entre eventos incluidos en los *logs* de distintos equipos y dispositivos (elementos de red, herramientas de seguridad...).

Para poder comparar los distintos *logs* conviene mantener todos los relojes de los equipos y dispositivos perfectamente sincronizados. Para ello, se podría utilizar el protocolo NTP (*Network Time Protocol*, [www.ntp.org](http://www.ntp.org)).

En los servidores Web se emplea el formato CLF (*Common Log Format*) o el ELF (*Extended Log Format*), registrando los siguientes datos de cada petición realizada por un cliente remoto:

**Tabla 2.1. Registro de las conexiones a un servidor Web**

- 
- Dirección IP o nombre de dominio de la máquina remota (cliente) que se conecta al servidor Web.
  - Identificación remota del cliente.
  - Nombre de autenticación del usuario.
  - Fecha y hora de la conexión.
  - Petición formulada por el cliente (por ejemplo: "GET/index.html HTTP/1.0").
  - Estado HTTP devuelto por el servidor al cliente.
  - Número de bytes enviados al cliente.
  - Agente de usuario (tipo de navegador utilizado): campo ELF.
  - URL de procedencia (referrer log): campo ELF.
- 

Los administradores de la red tienen a su disposición una serie de herramientas para analizar toda la información registrada en los *logs*, entre las que se encuentran distintos tipos de filtros y aplicaciones que permiten detectar de forma automática patrones de ataques o situaciones de potencial peligro.

En este sentido, se debería considerar el problema de que el exceso de información registrada en el sistema pueda llegar a desbordar a sus administradores, provocando una situación bastante habitual en muchas organizaciones: que los datos de los registros de actividad no sean analizados de forma adecuada.

Por otra parte, suele ser muy recomendable realizar un estudio previo del tráfico en la red para facilitar la posterior detección de situaciones anómalas: consumo de ancho de banda por usuarios y departamentos, patrones horarios del tráfico, servicios y protocolos utilizados... El protocolo de gestión de red SNMP se podría utilizar para recabar parte de esta información de los dispositivos de red.

En los servidores Windows se pueden utilizar tres tipos de registros:

- **Registro de Aplicación:** muestra los mensajes, la información del estado y los sucesos generados desde las aplicaciones y servicios instalados en el sistema.
- **Registro del Sistema:** incluye los errores, advertencias y sucesos generados por el propio sistema operativo y sus servicios esenciales.
- **Registro de Seguridad:** muestra los registros de éxito y de fracaso de los servicios auditados, es decir, cuando un usuario intenta acceder a un recurso auditado y se le concede (éxito) o se le deniega (fracaso) el acceso.

Mediante el Visor de Sucesos es posible acceder a la información de estos tres registros.

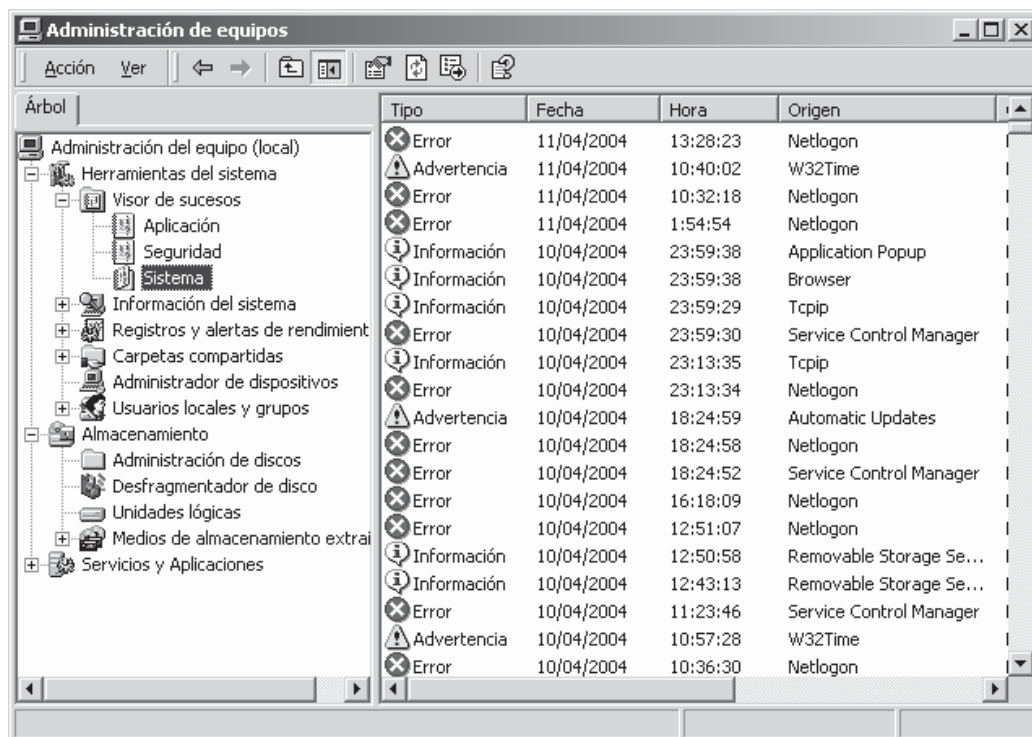


Figura 2.1. Visor de Sucesos en un equipo Windows

El Registro de Seguridad en Windows permite auditar varias clases de actividades o sucesos:

**Tabla 2.2. Sucesos que se pueden registrar en un equipo Windows**

- Eventos de inicio de sesión interactivo.
- Eventos de inicio de sesión en el dominio.
- Gestión de cuentas.
- Acceso a objetos.
- Acceso al Directorio Activo.
- Utilización de privilegios.
- Seguimiento de procesos.
- Eventos de sistema.
- Cambios de política de seguridad.

## 2.3 SISTEMAS DE DETECCIÓN DE INTRUSOS (IDS)

### 2.3.1 Características básicas de los IDS

Los **Sistemas de Detección de Intrusos** (*Intrusion Detection Systems*, IDS) son los sistemas encargados de detectar y reaccionar de forma automatizada ante los incidentes de seguridad que tienen lugar en las redes y equipos informáticos.

Para ello, estos sistemas se encargan de monitorizar el funcionamiento de los equipos y de las redes en busca de indicios de posibles incidentes o intentos de intrusión, avisando a los administradores del sistema informático ante la detección de cualquier actividad sospechosa mediante una serie de alarmas e informes.

En la arquitectura de un IDS podemos distinguir los siguientes elementos funcionales básicos:

- Una fuente de información que proporciona eventos del sistema o red informática.
- Una base de datos de patrones de comportamiento considerados como normales, así como de los perfiles de distintos tipos de ataque.
- Un motor de análisis encargado de detectar evidencias de intentos de instrucción.
- Un módulo de respuesta capaz de llevar a cabo determinadas actuaciones a partir de las indicaciones del motor de análisis.

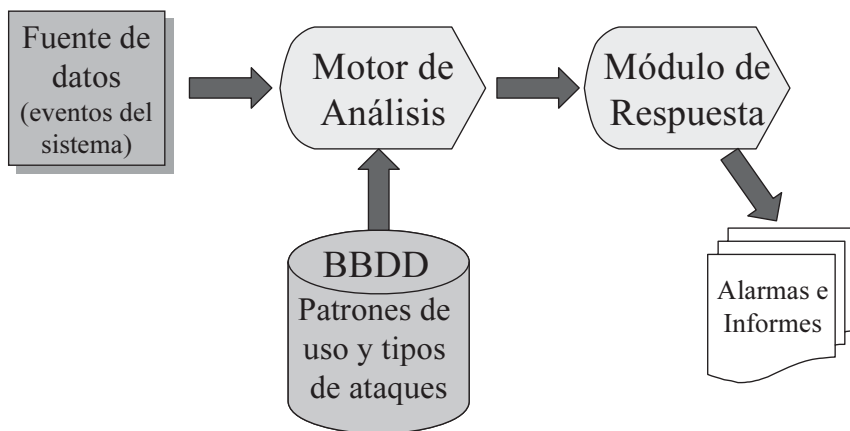


Figura 2.2. Arquitectura de un Sistema de Detección de Intrusiones (IDS)

Por otra parte, un IDS puede utilizar dos modelos de detección:

- **Detección de un mal uso** (*misuse*): tipos ilegales de tráfico, secuencias utilizadas para realizar ataques contra los equipos (*exploits*), escaneo de puertos, etcétera.
- **Detección de un uso anómalo**: análisis estadístico del tráfico en la red, monitorización de procesos y del comportamiento de los usuarios, con el fin de poder detectar aquellos comportamientos que se puedan considerar anómalos según los patrones de uso registrados hasta el momento: franjas horarias, utilización de puertos y servicios...

Se trataría, por lo tanto, de detectar cambios de comportamiento no justificados en lo que se refiere a ficheros accedidos, aplicaciones utilizadas en el trabajo, cantidad de tráfico cursado en la red, conexiones de usuarios en horarios poco habituales, etcétera.

Gracias a su módulo de respuesta, un IDS es capaz de actuar de forma automática a los incidentes detectados. Las **respuestas pasivas** se limitan a registrar las posibles intrusiones o usos anómalos, así como a generar informes y alertas dirigidas a los administradores de la red (correos electrónicos, mensajes SMS...).

Por su parte, mediante las **respuestas activas** el IDS podría responder a la situación anulando conexiones o bloqueando el acceso a determinados equipos o servicios de la red, para tratar de limitar las consecuencias del incidente.

---

**Tabla 2.3. Ejemplos de respuestas activas de un IDS**

---

- Anular las conexiones TCP inyectando paquetes de reinicio en las conexiones del atacante.
  - Reconfiguración de los cortafuegos de la red para filtrar el tráfico que pueden estar causando el incidente.
  - Desconexión automática de servidores y dispositivos de red.
  - Bloqueo de cuentas o prohibición de la ejecución de determinados comandos.
  - Localización del origen del ataque y notificación a los proveedores de acceso a Internet u organizaciones implicadas.
- 

No obstante, los sistemas IDS también presentan una serie de problemas y limitaciones, como podrían ser la generación de falsas alarmas, ya sean éstas **falsos negativos**, que se producen cuando el IDS no es capaz de detectar algunas actividades relacionadas con incidentes de seguridad que están teniendo lugar en la red o en los equipos informáticos, o bien **falsos positivos**, que se producen cuando el IDS registra y genera alertas sobre determinadas actividades que no resultan problemáticas, ya que forman parte del funcionamiento normal del sistema o red informático.

Por otra parte, en los entornos conmutados, es decir, en las redes locales que utilizan *switches*, resulta más difícil monitorizar el tráfico de la red. Por este motivo, en estos casos resulta conveniente la instalación en la red de *switches* dotados de puertos especiales, conocidos como *spanning ports* o *mirrored ports*, que faciliten la captura de todo el tráfico cursado por parte de un sistema IDS.

Así mismo, es necesario tener en cuenta la imposibilidad de analizar las comunicaciones cifradas (conexiones que empleen protocolos como SSH, SSL, IPSec...). Por este motivo, resulta conveniente examinar los datos una vez hayan sido descifrados por los equipos destinatarios dentro de la red de la organización.

Los sistemas IDS también pueden tener un cierto impacto en el rendimiento de la red y podrían ocasionar una sobrecarga de tareas administrativas si generasen un elevado número de informes y registros de actividad.

Entre los principales IDS disponibles en el mercado, podríamos citar SNORT, Real Secure de Internet Security Systems, SentiVist de la empresa NFR, NetRanger de Cisco, etcétera.

## 2.3.2 Tipos de IDS

---

### 2.3.2.1 HIDS (*HOST IDS*)

Los *Host IDS* pueden detectar las intrusiones a nivel de *host*, es decir, a nivel de un equipo informático, observando para ello si se han producido alteraciones significativas de los archivos del sistema operativo o analizando los *logs* del equipo en busca de actividades sospechosas.

Un *Host IDS* requiere de la instalación de un dispositivo sensor, conocido como "agente", en el equipo informático objeto de monitorización. Este sensor software trabaja a bajo nivel, interceptando las llamadas a las funciones básicas del sistema operativo. Además, se encarga de analizar cada actividad y proceso en ejecución dentro del equipo, razón por la que también presenta el inconveniente de disminuir el rendimiento del equipo.

Las principales tareas realizadas por un *Host IDS* son las que se presentan a continuación:

- Análisis de los registros de actividad (*logs*) del núcleo (*kernel*) del sistema operativo, para detectar posibles infiltraciones.
- Verificación de la integridad de los ficheros ejecutables. Para ello, es necesario mantener una base de datos con el estado exacto de cada uno de los archivos del sistema y de las aplicaciones instaladas, a fin de detectar posibles modificaciones

de los mismos (*integrity check*). Herramientas como *Tripwire* ([www.tripwire.org](http://www.tripwire.org)) facilitan esta función.

- Exploración periódica/planificada de programas privilegiados ("setuid" de sistemas UNIX/LINUX).
- Auditoría periódica de los permisos asignados a los recursos del sistema.
- Búsqueda y evaluación periódica de vulnerabilidades de software conocidas.
- Revisión detallada del proceso de instalación de nuevas aplicaciones en el sistema, a fin de poder detectar caballos de Troya u otros códigos malignos.

### 2.3.2.2 MHIDS (*MULTIHOST IDS*)

Este tipo de IDS permiten detectar actividades sospechosas en base a los registros de actividad de diferentes equipos informáticos (*hosts*). Por este motivo, también se les conoce como sistemas "IDS Distribuidos" (DIDS, *Distributed IDS*).

### 2.3.2.3 NIDS (*NETWORK IDS*)

Los *Network IDS* se instalan en una red de ordenadores para monitorizar el tráfico de red en busca de cualquier actividad sospechosa: escaneo de puertos; intentos de explotación de agujeros de seguridad en los servicios instalados en los equipos de la red; ataques conocidos contra determinados protocolos; intentos de ejecución de *scripts* CGI vulnerables en los servidores; etcétera.

Para ello, un *Network IDS* trata de detectar el tráfico anómalo que suele acompañar a los intentos de intrusión, analizando para ello el contenido de los paquetes de datos que se transmiten a través de la red de la organización.

Entre las distintas situaciones de tráfico anómalo, podríamos citar las siguientes:

- Enrutamiento anormal de los paquetes de datos.
- Fragmentación de paquetes deliberada.
- Utilización de una dirección IP no válida o en desuso en uno de los tramos de red internos (*IP Spoofing*).
- Afluencia de paquetes DNS con identificadores consecutivos, que incluyen la supuesta respuesta a una misma encuesta (situación típica de un ataque de *DNS Spoofing*).



- Invasión de paquetes TCP SYN desde una o varias direcciones (situación típica de un ataque de denegación de servicio del tipo de *SYN Flooding*).
- Invasión de paquetes ICMP o UDP de eco (típicos de ataques como *Smurf* y *Fraggle*).
- Falsa correspondencia entre las direcciones MAC conocidas y las direcciones IP de los equipos.
- Tormentas de tráfico ARP, que podrían revelar un intento de “envenenamiento de las tablas ARP” (situación típica de un ataque de *ARP Spoofing*).

Uno de los sistemas NIDS más conocidos es SNORT. Este sistema decide qué paquetes de los que circulan por una red resultan sospechosos, empleando para ello una base de datos de reglas que se aplican teniendo en cuenta el contenido y los formatos de cabecera de los paquetes de datos.

Además, se pueden descargar nuevas reglas directamente desde bases de datos disponibles en Internet, que permiten catalogar nuevos tipos de incidentes, *exploits* y vulnerabilidades de sistemas.

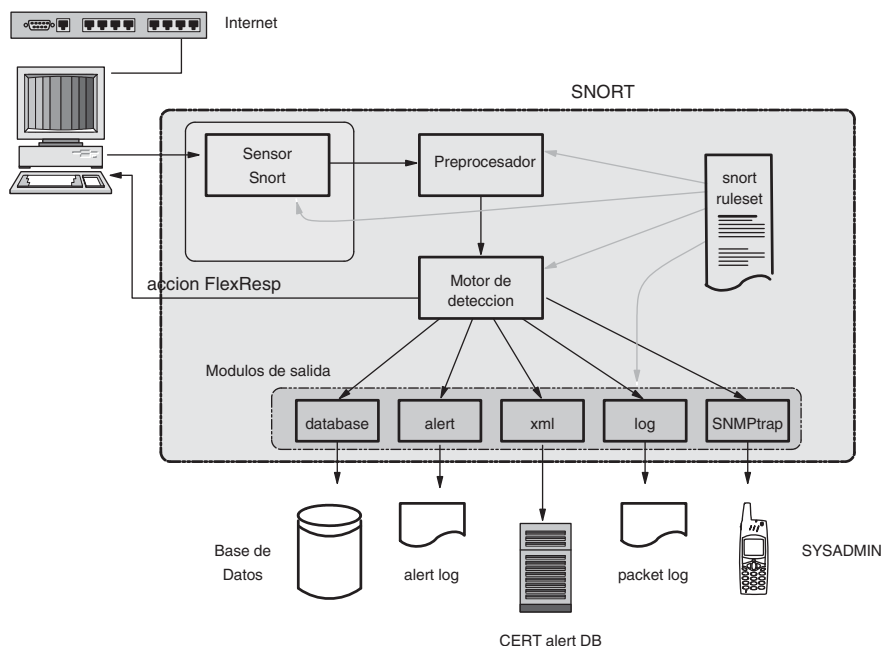


Figura 2.3. Arquitectura del IDS Snort

### 2.3.3 Arquitecturas de los IDS

---

Las arquitecturas de los IDS se han propuesto con el objetivo de facilitar la interoperabilidad y reutilización de módulos, así como la reducción de la complejidad en la gestión y configuración de los IDS.

Gracias a la aprobación de protocolos de comunicación específicos, es posible lograr el intercambio de datos entre elementos de distintos fabricantes que pueden formar parte de un IDS. De este modo, se facilita la captura de eventos generados por distintas fuentes, proporcionando una imagen más amplia y detallada de las actividades maliciosas en un determinado entorno.

En una arquitectura de IDS se distinguen los elementos Agentes (que se encargan de monitorizar la actividad en el sistema objeto de estudio), los elementos Transceptores (se encargan de la comunicación), los elementos Maestros (centralizan y analizan los datos) y una Consola de Eventos (módulo de interfaz con los usuarios).

Las arquitecturas de IDS más importantes son CIDF e IDWG.

**CIDF** (*Common Intrusion Detection Framework*) es una arquitectura promovida por la Agencia Federal de Estados Unidos DARPA (*Defense Advanced Research Projects Agency*) y finalizada en 1999, que ha tenido una escasa aceptación comercial.

Esta arquitectura está constituida por los siguientes elementos:

- **Generador de eventos:** obtención y descripción de eventos mediante objetos denominados GIDO (*Generalized Intrusion Detection Objects*).
- **Analizador de eventos:** incorpora los algoritmos de detección de ataques.
- **Base de datos de eventos:** se utiliza el lenguaje CISL (*Common Intrusion Specification Language*) para expresar los diferentes eventos.
- **Unidades de respuesta:** se encargan de cerrar las conexiones, terminar procesos, bloquear el acceso a los servidores, etcétera.

Por su parte, la arquitectura **IDWG** (*Intrusion Detection Working Group*) propone el formato IDEF (*Intrusion Detection Exchange Format*) para facilitar el intercambio de información sobre los incidentes de seguridad.

En este caso se distinguen los módulos Sensor, Analizador, Fuente de Datos y Manager:

- El **Analizador** es el componente que analiza los datos recolectados por el Sensor, buscando señales de actividad no autorizada o indeseada.

- El **Sensor** recolecta datos de la **Fuente de Datos**: paquetes de red, *logs* de auditoría del sistema operativo, *logs* de aplicaciones... (información que el IDS emplea para detectar cualquier actividad indeseada o no autorizada).
- El **Manager** es el componente desde el cual se administran los restantes elementos del IDS: se encarga de la configuración de los sensores y analizadores, de la consolidación datos, de la generación de informes, etcétera.

La arquitectura IDWG ha definido un modelo de datos orientado a objetos basado en lenguaje XML para describir los eventos, conocido como IDMEF (*Intrusion Detection Message Exchange Format*). Así mismo, IDWG prevé dos mecanismos de comunicaciones: el protocolo IAP (*Intrusion Alert Protocol*), para intercambiar datos de alertas de intrusiones de forma segura entre las entidades de detección, y el protocolo IDXP (*Intrusion Detection Exchange Protocol*), que permite intercambiar datos en general entre las entidades de detección de intrusiones.

---

## 2.4 IPS (*INTRUSION PREVENTION SYSTEMS*)

---

Un sistema IPS (*Intrusion Prevention System*) es un sistema que permite prevenir las intrusiones. Se trata, por tanto, de un tipo de sistema que pretende ir un paso más allá de los IDS, ya que puede bloquear determinados tipos de ataques antes de que estos tengan éxito.

---

## 2.5 LOS *HONEYPOTS* Y LAS *HONEYNETS* (SEÑUELOS)

---

Un *honeypot* es un servidor configurado y conectado a una red para que pueda ser sondeado, atacado e incluso comprometido por intrusos. Se trata, por lo tanto, de un equipo o sistema que actúa a modo de señuelo o trampa para los intrusos.

El concepto de sistema trampa ya fue propuesto hace algunos años por Cliff Stoll en su libro *Cuckoo's Egg*.

Por su parte, una *honeynet* (red señuelo) es una red completa que ha sido configurada y conectada a otras redes para que pueda ser sondeada, atacada e incluso comprometida por intrusos.

Los *honeypots* y *honeynets* proporcionan varios mecanismos para la monitorización, registro y control de las acciones de los intrusos. De este modo, permiten analizar cómo los intrusos emplean sus técnicas y herramientas para intentar entrar en un sistema o en una red informática (cómo consiguen analizar y explotar sus vulnerabilidades) y comprometer su

seguridad (cómo pueden alterar o destruir los datos, instalar programas dañinos o controlar de forma remota los equipos afectados). Además, estas actividades de monitorización y registro se realizan tratando de pasar de forma inadvertida para los intrusos.

Tal y como afirmaba el general chino Sun Tzu en su libro *El Arte de la Guerra* (siglo V A.C.), “lo que posibilita a un gobierno inteligente y a un mando militar sensato vencer a los demás y lograr triunfos extraordinarios es la información previa”. Además, también en palabras de este famoso estratega, “la mejor forma de protegerse es saber cómo me van a atacar”.

Por lo tanto, los *honeypots* y las *honeynets* entrarían dentro de las aplicaciones del tipo *know your enemy* (“conoce a tu enemigo”), que permiten aprender de las herramientas y técnicas de los intrusos para proteger mejor a los sistemas reales de producción, construyendo una base de datos de perfiles de atacantes y tipos de ataques. También podrían facilitar la captura de nuevos virus o códigos dañinos para su posterior estudio.

Así mismo, estos sistemas permiten desviar la atención del atacante de los verdaderos recursos valiosos de la red de la organización.

En cuanto al diseño de una *honeynet*, se han propuesto dos arquitecturas conocidas como GenI (año 1999) y GenII (año 2002), siendo la segunda más fácil de implementar y más segura para la organización.

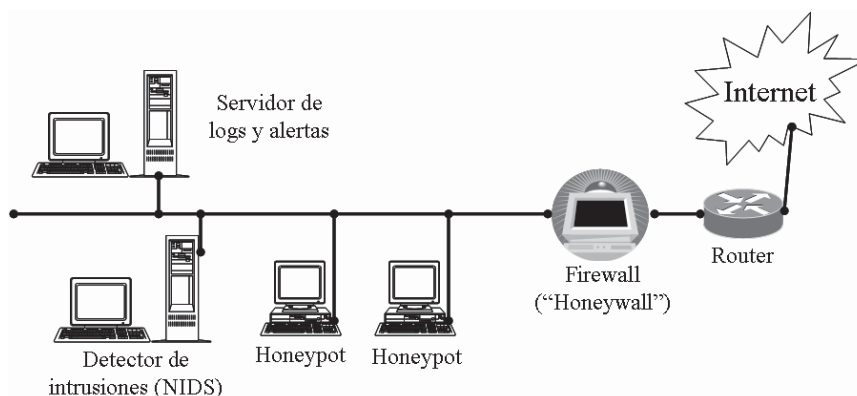


Figura 2.4. Diseño de una honeynet

Los elementos integrantes de una *honeynet*, según el esquema anterior, serían uno o varios *honeypots* (servidores que actuarían de señuelos), un sistema de detección de intrusiones en red (NIDS), un servidor de *logs*, un dispositivo que se haría pasar por un cortafuegos (*honeywall*) y un router.

También se podría considerar la posibilidad de incorporar un dispositivo que aplique la técnica de *bait and switch*, según la cual se monitoriza el tráfico procedente de Internet y se desvía aquel que pudiera ser considerado como “hostil” hacia el sistema trampa (*honeynet*), dejando que el resto del tráfico “normal” pueda dirigirse a la red interna de la organización.

En definitiva, podemos considerar que los sistemas basados en señuelos (*honeynets* y *honeypots*) ofrecen los siguientes servicios y funciones:

- Conexión segura de la red corporativa a Internet.
- Captura de datos sobre los intrusos: en el cortafuegos, en el NIDS y en los propios registros (*logs*) de los *honeypots*.
- Centralización de la información capturada en un servidor de *logs*, por motivos de seguridad.
- Control de las acciones del intruso, ya que éste debe quedar confinado dentro de la *honeynet*, sin que pueda atacar a otras redes o equipos.

En los *honeypots* se suelen instalar versiones modificadas del intérprete de comandos (*shell* en un sistema Unix/Linux o "cmd.exe" en un sistema Windows), como "ComLog", un troyano que reemplaza al "cmd.exe" para registrar y reenviar los comandos tecleados por el usuario, así como otras herramientas que permitan registrar las actuaciones de los intrusos (SpyBuddy, KeyLogger, etcétera).

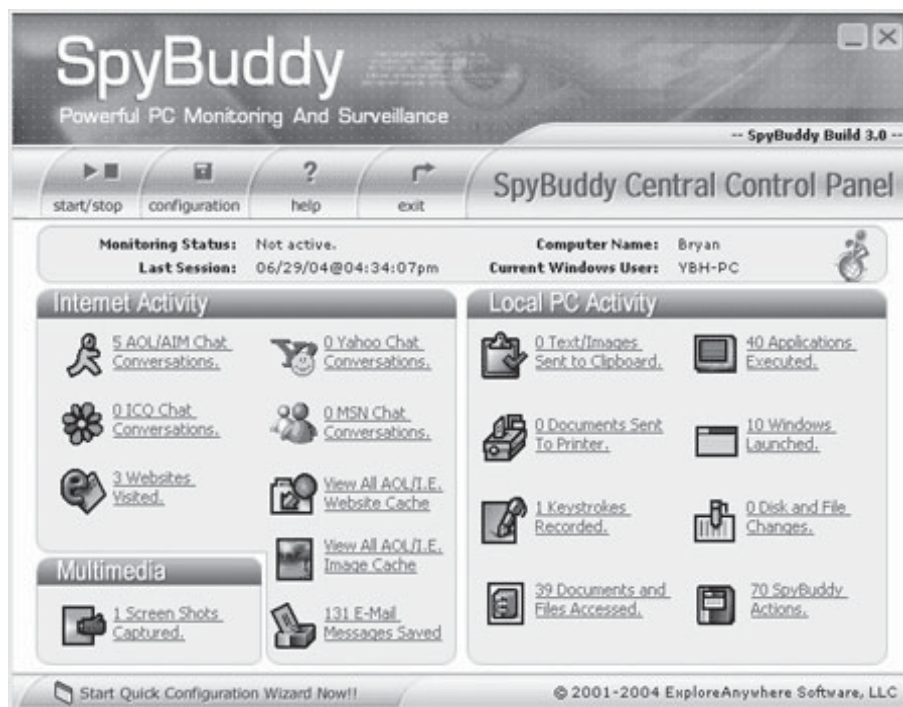


Figura 2.5. SpyBuddy

SpyBuddy es una herramienta comercial que permite registrar las teclas pulsadas por el usuario del equipo; monitorizar la creación, acceso, modificación y eliminación de ficheros y directorios; realizar un seguimiento de los programas que se ejecutan en el equipo; etcétera.

En estos últimos años se ha propuesto el desarrollo de *honeynets* virtuales, en una configuración en la que todos los equipos y servicios se ejecutan en un único ordenador, recurriendo para ello a un software de virtualización, como VMWare ([www.vmware.com](http://www.vmware.com)). Este software de virtualización permite la ejecución simultánea de varios sistemas operativos, con distintos tipos de servicios y aplicaciones, en un mismo equipo físico, de tal modo que, a pesar de compartir los recursos de este ordenador (conocido como *host* anfitrión), aparenten estar ejecutándose en máquinas distintas e independientes.

Una *honeynet* virtual presenta como ventaja unos menores costes y espacio requerido que en una red física, facilitando la gestión centralizada de todos los servicios y aplicaciones incluidos en la *honeynet*.

Por otra parte, debemos tener en cuenta otras consideraciones acerca del uso de estas herramientas, ya que se trata de proyectos de elevado riesgo, debido a las amenazas y tipos de ataques que se van a producir contra los equipos y redes de la organización. Por este motivo, en los equipos y redes señuelo no se deberían incluir datos o información sensible, ni servicios en producción.

Además, los posibles ataques contra estos equipos y redes no deberían comprometer a los usuarios y clientes de la red informática de la organización y, mucho menos, podrían afectar a terceros. Para ello, es necesario establecer las medidas de control y bloqueo de los posibles ataques e intentos de intrusión llevados a cabo contra redes y equipos de terceros desde los equipos que hayan sido comprometidos en la *honeynet*, ya que de lo contrario la organización podría incurrir en responsabilidades legales por los daños ocasionados a terceros desde sus propios equipos y redes informáticas.

Otra cuestión legal que se podría contemplar surge en torno a la discusión de hasta qué punto es lícito emplear estas herramientas para espiar a los intrusos, sin que estos hayan sido advertidos previamente de que sus actividades están siendo registradas por la organización.

Para concluir este apartado, podemos citar algunos ejemplos de herramientas y proyectos de interés relacionados con los *honeypots* y las *honeynets*.

Así, podemos encontrar en Internet aplicaciones que permiten simular determinados servicios para registrar los posibles intentos de ataque e intrusión, como *BackOfficer Friendly*, *Specter*, *Honeyd*, *Decoy Server* de Symantec, *Deception Toolkit*, etcétera.

Por su parte, el proyecto HoneyNet ([www.honeynet.org](http://www.honeynet.org)) se remonta a junio del año 2000, con el objetivo de "estudiar las técnicas, tácticas y motivaciones de la comunidad de atacantes y compartir las lecciones aprendidas". En la actualidad este proyecto está integrado por profesionales de distintos perfiles y áreas de conocimiento: informáticos, psicólogos, ingenieros de redes, etcétera.

---

## 2.6 OTRAS HERRAMIENTAS Y APLICACIONES DE UTILIDAD

---

Podemos destacar otras herramientas y aplicaciones que pueden resultar de ayuda para gestionar y supervisar la seguridad en las redes de ordenadores.

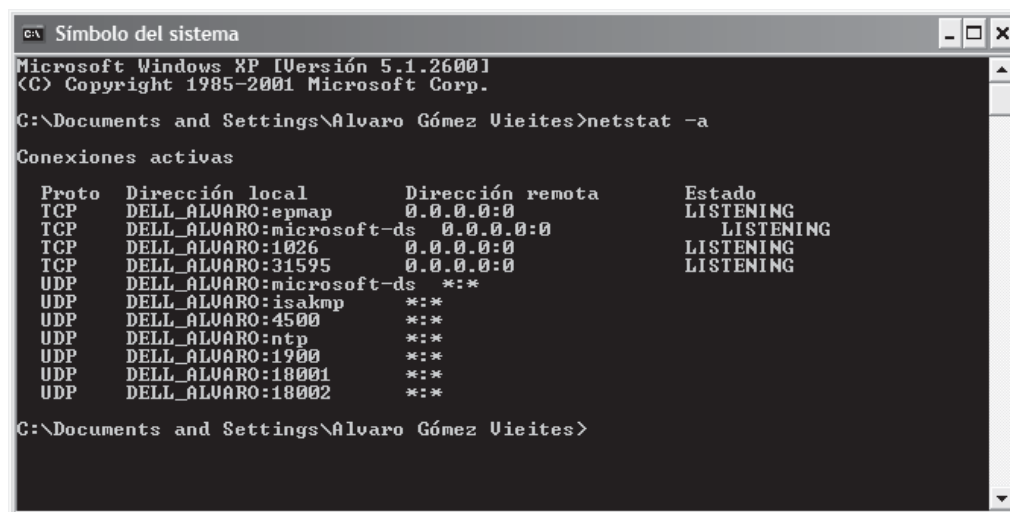
Así, por ejemplo, podríamos citar en primer lugar determinadas herramientas y comandos incluidos en el propio sistema operativo de un ordenador, entre las que destacan las siguientes<sup>8</sup>:

- **Netstat**: comando que muestra el estado de las conexiones de red.
- **NBTStat**: muestra el estado de las conexiones actuales que utilizan NetBIOS sobre TCP/IP.
- **IpConfig**: informa sobre la configuración de las tarjetas de red del equipo.
- **Ping**: envía un *ping* al equipo especificado para comprobar si se encuentra activo en la red.
- **Tracert**: informa de la ruta seguida para alcanzar un determinado equipo conectado a la red.
- **Route**: muestra y manipula las tablas de enrutamiento del equipo.
- **ARP**: muestra y modifica las tablas de conversión de direcciones IP a direcciones físicas (direcciones MAC).
- **Nslookup**: inspecciona los contenidos de los archivos de un servidor DNS.
- **Finger**: muestra información sobre un determinado usuario del sistema.
- **Whois**: relaciona nombres de dominio con direcciones IP.
- **Telnet**: permite iniciar una sesión remota en otro servidor, emulando un terminal virtual.
- **FTP**: permite enviar y descargar ficheros de otro servidor, a través del protocolo FTP.

---

<sup>8</sup> En Windows se pueden ejecutar desde el intérprete de comandos.





```

C:\Símbolo del sistema
Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Alvaro Gómez Vieites>netstat -a

Conexiones activas

Proto  Dirección local      Dirección remota      Estado
TCP    DELL_ALVARO:epmap    0.0.0.0:0             LISTENING
TCP    DELL_ALVARO:microsoft-ds 0.0.0.0:0             LISTENING
TCP    DELL_ALVARO:1026     0.0.0.0:0             LISTENING
TCP    DELL_ALVARO:31595    0.0.0.0:0             LISTENING
UDP    DELL_ALVARO:microsoft-ds *:*:
UDP    DELL_ALVARO:isakmp   *:*:
UDP    DELL_ALVARO:4500     *:*:
UDP    DELL_ALVARO:ntp      *:*:
UDP    DELL_ALVARO:1900     *:*:
UDP    DELL_ALVARO:18001    *:*:
UDP    DELL_ALVARO:18002    *:*:

C:\Documents and Settings\Alvaro Gómez Vieites>

```

Figura 2.6. Ejecución de la herramienta Netstat en un sistema Windows

Por otra parte, los *wrappers* son programas que permiten controlar el acceso y utilización de otros programas y servicios que se ejecutan en un ordenador.

A su vez, los analizadores de protocolos y *sniffers* son programas “husmeadores”, que interceptan y analizan el tráfico en la red, recurriendo para ello a la utilización de dispositivos de escucha del tráfico en la red (*network taps*), que actúan en modo promiscuo y que son difíciles de detectar ya que no tienen asociada una dirección IP.

Así, por ejemplo, podríamos citar *sniffers* y analizadores de protocolos como Nmap, Ntop, NetScanTools, LANSleuth o Ethereal, que permiten detectar protocolos y servicios no autorizados por la organización, además de llevar a cabo un completo análisis del tráfico habitual en la red de una organización (protocolos y servicios utilizados, cantidad de información transmitida, evolución de la situación por franjas horarias y por días de la semana, comportamiento por segmentos de la red...), ya que de este modo será más fácil la detección de situaciones anómalas a posteriori.

Los sistemas anti-*sniffers* son herramientas capaces de detectar la existencia de tarjetas de red que se encuentren funcionando en modo promiscuo para capturar todo el tráfico de la red.

También pueden resultar de gran ayuda las herramientas para la evaluación de vulnerabilidades. Estas herramientas, entre las que podríamos citar a Nessus o a Internet Security Scanner, se encargan de llevar a cabo un análisis automático de un sistema informático, para tratar de localizar algunas de las vulnerabilidades más conocidas.

Además, el sondeo de seguridad complementa al análisis de vulnerabilidades con tareas como la detección y la revisión de la instalación y configuración de los equipos de seguridad (cortafuegos, antivirus, IDS, etcétera).



En este caso, se podrían realizar pruebas de intrusión (tests de penetración), en las que no solo se detectasen las vulnerabilidades, sino que se tratasen de explotar aquellas que hayan sido identificadas y que pudieran comprometer el sistema, así como otros sistemas accesibles desde el afectado. Esta tarea se puede completar posteriormente con un análisis de riesgos en el sistema informático, en el que se pretende determinar cuál es el nivel de riesgo a partir del análisis de posibles amenazas y vulnerabilidades.

También podemos considerar las herramientas que se encargan de monitorizar de forma permanentemente la actividad en la red de la empresa, para evitar que determinada información o documentos "sensibles" puedan ser enviados al exterior sin la adecuada autorización, debido a distintos factores: virus informáticos, actuaciones de empleados desleales, explotación de algún agujero de seguridad en un equipo informático de la organización, etcétera.

Por último, podemos destacar que en los últimos años se han presentado en el mercado distintas soluciones integradas "todo en uno", constituidas por dispositivos que incorporan varios servicios de seguridad como el programa antivirus, el filtrado de contenidos, el filtrado de correo basura (*spam*), una herramienta para el análisis de vulnerabilidades del sistema, un Sistema de Detección de Intrusos (IDS), un cortafuegos para la seguridad perimetral y/o un servidor VPN para crear túneles seguros y habilitar las conexiones remotas. Además, estos dispositivos, que se instalan en el punto de conexión de la red corporativa de la empresa con el exterior, cuentan con un servicio de actualización y mantenimiento remoto por parte del fabricante.

Como ejemplo destacado de estos dispositivos integrados podríamos citar la gama de productos FortiGate de la empresa Fortinet ([www.fortinet.com](http://www.fortinet.com)).

---

## 2.7 DIRECCIONES DE INTERÉS

---

### Cortafuegos:

- Firewall-1 de CheckPoint: <http://www.checkpoint.com/>.
- PIX de Cisco: <http://www.cisco.com/>.
- Netscreen Firewall: <http://www.juniper.net/>.
- Watchguard Firebox: <http://www.watchguard.com/>.
- Symantec Raptor: <http://www.symantec.com/>.
- ZoneAlarm: <http://www.zonealarm.com/>.
- Fortigate de la empresa Fortinet: <http://www.fortinet.com/>.



#### Sistemas IDS:

- Tripwire: <http://www.tripwire.org/>.
- Snort: <http://www.snort.org/>.
- Specter: <http://www.specter.com/>.

#### Honeypots y honeynets:

- VMWare: <http://www.vmware.com/>.
- Honeyd: <http://www.honeyd.org/>.
- HoneyNet Project: <http://www.honeynet.org/>.

#### Otras herramientas y aplicaciones de interés:

- Nessus: <http://www.nessus.org/>.

## RESPUESTA ANTE INCIDENTES DE SEGURIDAD

---

### 3.1 DEFINICIÓN DE UN PLAN DE RESPUESTA A INCIDENTES

---

La definición e implantación de un Plan de Respuesta a Incidentes debería tener en cuenta una serie de actividades y tareas, entre las cuales podríamos destacar todas las que se presentan en la siguiente relación:

---

**Tabla 3.1. Actividades contempladas en un Plan de Respuesta a Incidentes**

---

- Constitución de un Equipo de Respuesta a Incidentes.
  - Definición de una Guía de Procedimientos.
  - Detección de un incidente de seguridad.
  - Análisis del incidente.
  - Contención, erradicación y recuperación.
  - Identificación del atacante y posibles actuaciones legales.
  - Comunicación con terceros y relaciones públicas.
  - Documentación del incidente de seguridad.
  - Análisis y revisión a posteriori del incidente.
-

### 3.1.1 Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT)

---

El **Equipo de Respuesta a Incidentes de Seguridad Informática** (CSIRT, *Computer Security Incident Response Team*) está constituido por las personas que cuentan con la experiencia y la formación necesaria para poder actuar ante las incidencias y desastres que pudieran afectar a la seguridad informática de una organización.

Generalmente solo las grandes organizaciones cuentan con un equipo de personas contratadas para cumplir con esta función. En la mayoría de las organizaciones que no cuentan con un Equipo de Respuesta formalmente constituido, será necesario identificar quiénes son las personas responsables de acometer cada una de las tareas que se hayan definido en el Plan de Respuesta a Incidentes, definiendo claramente las responsabilidades, funciones y obligaciones de cada persona implicada en dicho Plan.

La organización deberá mantener actualizada la lista de direcciones y teléfonos de contacto para emergencias, para poder localizar rápidamente a las personas clave.

En algunos casos será necesario contratar a las personas con la necesaria experiencia y cualificación profesional (conocimientos técnicos, habilidades de comunicación...). La experiencia es un factor determinante para poder actuar de forma correcta evitando errores a la hora de responder de forma rápida y eficaz ante los incidentes de seguridad.

Así mismo, conviene prestar especial atención a la formación continua de los miembros del Equipo de Respuesta a Incidentes (o de las personas que deban asumir esta responsabilidad si no existe el equipo como tal), contemplando tanto los aspectos técnicos como los aspectos legales (delitos informáticos).

Estas personas deben contar con la dotación de medios técnicos y materiales necesarios para poder cumplir con eficacia su misión. Para comprobar la idoneidad de los medios disponibles, el entrenamiento de los miembros del equipo y las actividades definidas en el Plan de Respuesta a Incidentes, conviene llevar a cabo simulacros de forma periódica en la organización.

### 3.1.2 Procedimientos y actividades a realizar

---

Como parte integrante del Plan de Respuesta a Incidentes, la organización debe definir una guía de actuación clara y detallada con los procedimientos y acciones necesarias para la restauración rápida, eficiente y segura de la capacidad de procesamiento informático y de comunicaciones de la organización, así como para la recuperación de los datos dañados o destruidos.

El objetivo perseguido con la Guía de Procedimientos es conseguir una respuesta sistemática ante los incidentes de seguridad, realizando los pasos necesarios y en el orden adecuado para evitar errores ocasionados por la precipitación o la improvisación.

Una buena Guía de Procedimientos permitirá minimizar los daños ocasionados y facilitar la recuperación del sistema afectado.

Además, esta guía debe completar la adquisición de información detallada sobre cada incidente de seguridad para mejorar los procedimientos de actuación ante futuros incidentes y reforzar la protección actual de los sistemas informáticos de la organización.

Por supuesto, también debe tratar de forma adecuada las cuestiones legales que se pudieran derivar de cada incidente de seguridad, así como los aspectos relacionados con la imagen y reputación de la organización y las relaciones públicas.

---

## 3.2 DETECCIÓN DE UN INCIDENTE DE SEGURIDAD: RECOLECCIÓN DE INFORMACIÓN

---

La organización debería prestar especial atención a los posibles indicadores de un incidente de seguridad, como una actividad a contemplar dentro del Plan de Respuesta a Incidentes. Seguidamente se presenta una relación de los principales indicadores de posibles incidentes de seguridad:

- Precursores de un ataque: actividades previas de reconocimiento del sistema informático, como el escaneo de puertos, el escaneo de vulnerabilidades en servidores, el reconocimiento de versiones de sistemas operativos y aplicaciones...
- Alarmas generadas en los Sistemas de Detección de Intrusos (IDS), en los cortafuegos o en las herramientas antivirus.
- Registro de actividad extraña en los *logs* de servidores y dispositivos de red o incremento sustancial del número de entradas en los *logs*.
- Aparición de nuevas carpetas o ficheros con nombres extraños en un servidor, o modificaciones realizadas en determinados ficheros del sistema (*librerías*, *kernel*, aplicaciones críticas...), que se pueden detectar mediante herramientas de revisión de la integridad de ficheros.
- Caída o mal funcionamiento de algún servidor: reinicios inesperados, fallos en algunos servicios, aparición de mensajes de error, incremento anormal de la carga del procesador o del consumo de memoria del sistema...
- Notable caída en el rendimiento de la red o de algún servidor, debido a un incremento inusual del tráfico de datos.

- Cambios en la configuración de determinados equipos de la red: modificación de las políticas de seguridad y auditoría, activación de nuevos servicios, puertos abiertos que no estaban autorizados, activación de las tarjetas de red en modo promiscuo (para poder capturar todo el tráfico que circula por la red interna mediante *sniffers*), etcétera.
- Existencia de herramientas no autorizadas en el sistema.
- Aparición de nuevas cuentas de usuario o registro de actividad inusual en algunas cuentas<sup>9</sup>: conexiones de usuarios en unos horarios extraños (por ejemplo, por las noches o durante un fin de semana), utilización de la misma cuenta desde distintos equipos a la vez, bloqueo reiterado de cuentas por fallos en la autenticación, ejecución inusual de determinados servicios desde algunas cuentas, etcétera.
- Informes de los propios usuarios del sistema alertando de algún comportamiento extraño o de su imposibilidad de acceder a ciertos servicios.
- Detección de procesos extraños en ejecución dentro de un sistema, que se inician a horas poco habituales o que consumen más recursos de los normales (tiempo de procesador o memoria)<sup>10</sup>.
- Generación de tráfico extraño en la red: envío de mensajes de correo electrónico hacia el exterior con contenido sospechoso, inusual actividad de transferencia de ficheros, escaneo de otros equipos desde un equipo interno...
- Notificación de un intento de ataque lanzado contra terceros desde equipos pertenecientes a la propia organización.
- Desaparición de equipos de la red de la organización.
- Aparición de dispositivos extraños conectados directamente a la red o a algunos equipos de la organización (en este último caso podrían ser, por ejemplo, dispositivos para la captura de pulsaciones de teclado en los equipos).

Conviene tener en cuenta que los ataques informáticos se están volviendo cada vez más sofisticados, por lo que es difícil conseguir detectarlos a tiempo. Incluso existen herramientas que facilitan este tipo de ataques ocultando su actividad y que se pueden obtener de forma gratuita en Internet.

Por otra parte, la gran cantidad de información que se genera en los *logs* y en las distintas herramientas de seguridad puede dificultar su posterior estudio, debido sobre todo a la pérdida de tiempo provocada por los "falsos positivos". Por este motivo, es necesario contar con herramientas y filtros que faciliten la detección y clasificación de los incidentes.

---

9 Para ello, se pueden utilizar aplicaciones como *finger* y *who* en sistemas UNIX/LINUX, que muestran los usuarios que se encuentran conectados al sistema, desde qué terminal o equipo están conectados y en qué momento iniciaron su sesión.

10 Para ello, podría resultar de utilizar el comando "*ps*" en sistemas UNIX/LINUX, que muestra la relación de procesos en ejecución en el sistema.

### 3.3 ANÁLISIS DE UN INCIDENTE DE SEGURIDAD

El Plan de Respuesta a Incidentes debe definir cómo el equipo de respuesta debería proceder al análisis de un posible incidente de seguridad en cuanto éste fuese detectado por la organización, determinando en primer lugar cuál es su alcance: ¿qué equipos, redes, servicios y/o aplicaciones se han podido ver afectados? ¿Se ha podido comprometer información confidencial de la organización o de sus usuarios y clientes? ¿Ha podido afectar a terceros?

Seguidamente, el equipo de respuesta debería determinar cómo se ha producido el incidente: qué tipo de ataque informático (si lo ha habido) ha sido el causante, qué vulnerabilidades del sistema han sido explotadas, qué métodos ha empleado el atacante, etcétera.

Se podría utilizar una **Matriz de Diagnóstico** para facilitar la actuación del equipo en momentos de máximo estrés, evitando que se puedan tomar decisiones precipitadas que conduzcan a errores, constituyendo además un valioso apoyo para el personal con menos experiencia en la actuación frente a incidentes de seguridad.

**Tabla 3.2. Ejemplo de Matriz de Diagnóstico**

| Síntoma                                  | Código malicioso | Denegación de servicio (DoS) | Acceso no autorizado |
|--|------------------|------------------------------|----------------------|
| Escaneo de puertos                       | Bajo             | Alto                         | Medio                |
| Caída de un servidor                     | Alto             | Alto                         | Medio                |
| Modificación de ficheros de un equipo    | Alto             | Bajo                         | Alto                 |
| Tráfico inusual en la red                | Medio            | Alto                         | Medio                |
| Ralentización de los equipos o de la red | Medio            | Alto                         | Bajo                 |
| Envío de mensajes de correo sospechosos  | Alto             | Bajo                         | Medio                |

Así mismo, conviene realizar una valoración inicial de los daños y de sus posibles consecuencias, para a continuación establecer un orden de prioridades en las actividades que debería llevar a cabo el equipo de respuesta, teniendo para ello en consideración aspectos como el posible impacto del incidente en los recursos y servicios de la organización y en el desarrollo de su negocio o actividad principal.

En este sentido, los documentos RFC 1244 y RFC 2196 (del IETF, *Internet Engineering Task Force*) proponen la siguiente priorización de las actividades a realizar por parte de un equipo de respuesta a incidentes:

- **Prioridad uno:** proteger la vida humana y la seguridad de las personas.
- **Prioridad dos:** proteger datos e información sensible de la organización.
- **Prioridad tres:** proteger otros datos e información de la organización.
- **Prioridad cuatro:** prevenir daños en los sistemas informáticos (pérdida o modificación de ficheros básicos para las aplicaciones y los servidores).
- **Prioridad cinco:** minimizar la interrupción de los servicios ofrecidos a los distintos usuarios (internos y externos).

---

## 3.4 CONTENCIÓN, ERRADICACIÓN Y RECUPERACIÓN

---

Dentro del Plan de Respuesta a Incidentes, el equipo de respuesta debe elegir una determinada estrategia de **contención** del incidente de seguridad. Una primera opción sería llevar a cabo una rápida actuación para evitar que el incidente pueda tener mayores consecuencias para la organización: apagar todos los equipos afectados, desconexión de estos equipos de la red informática, desactivación de ciertos servicios, etcétera. Esta estrategia de contención es la más adecuada cuando se puedan ver afectados servicios críticos para la organización, se pueda poner en peligro determinada información confidencial, se estén aprovechando los recursos de la organización para lanzar ataques contra terceros o cuando las pérdidas económicas puedan ser considerables.

Una segunda alternativa sería retrasar la contención para poder estudiar con más detalle el tipo de incidente y tratar de averiguar quién es el responsable del mismo. Esta estrategia se puede adoptar siempre y cuando sea posible monitorizar y controlar la actuación de los atacantes, para de este modo reunir las evidencias necesarias que permitan iniciar las correspondientes actuaciones legales contra los responsables del incidente. No obstante, se corre el riesgo de que el incidente pueda tener peores consecuencias para la organización o para terceros (y en este último caso la organización podría ser considerada culpable por no haber actuado a tiempo).



Por otra parte, en algunos tipos de ataque las medidas de contención adoptadas podrían desencadenar mayores daños en los sistemas informáticos comprometidos. Así, por ejemplo, un equipo controlado por un *cracker* podría estar ejecutando un servicio que se encargaría de realizar *pings* periódicos a determinados servidores o comprobar el estado de las conexiones de red, de tal modo que si se detectase una desconexión del equipo del resto de la red, se desencadenaría otro proceso encargado de eliminar todas las pruebas del disco duro del equipo.

También hay que tener en cuenta que en los ataques de Denegación de Servicio (DoS) puede resultar necesario contar con la colaboración de las empresas proveedoras de acceso a Internet o de administradores de las redes de otras organizaciones para contener el ataque.

Por su parte, la **erradicación** es la etapa del Plan de Respuesta a Incidentes en la que se llevan a cabo todas las actividades necesarias para eliminar los agentes causantes del incidente y de sus secuelas, entre las que podríamos citar posibles “puertas traseras” instaladas en los equipos afectados, *rootkits*<sup>11</sup> u otros códigos malignos (virus, gusanos...), contenidos y material inadecuado que se haya introducido en los servidores, cuentas de usuario creadas por los intrusos o nuevos servicios activados en el incidente. También será conveniente llevar a cabo una revisión de otros sistemas que se pudieran ver comprometidos a través de las relaciones de confianza con el sistema afectado.

Por último, la **recuperación** es la etapa del Plan de Respuesta a Incidentes en la que se trata de restaurar los sistemas para que puedan volver a su normal funcionamiento. Para ello, será necesario contemplar tareas como la reinstalación del sistema operativo y de las aplicaciones partiendo de una copia segura, la configuración adecuada de los servicios e instalación de los últimos parches y actualizaciones de seguridad, el cambio de contraseñas que puedan haber sido comprometidas, la desactivación de las cuentas que hayan sido utilizadas en el incidente, la revisión de las medidas de seguridad para prevenir incidentes similares y la prueba del sistema para comprobar su correcto funcionamiento.

---

## 3.5 IDENTIFICACIÓN DEL ATACANTE Y POSIBLES ACTUACIONES LEGALES

---

Dentro del Plan de Respuesta a Incidentes, la identificación del atacante es necesaria para poder emprender acciones legales para exigir responsabilidades y reclamar indemnizaciones. No obstante, conviene tener en cuenta que generalmente solo se podrá identificar la máquina o máquinas desde las que se ha llevado a cabo el ataque, pero no directamente al individuo responsable de su utilización.

---

11 Un rootkit es un programa dañino que simula actuar como una herramienta o servicio legítimo del sistema infectado. Para ello, el atacante se encarga de reemplazar el fichero original del programa que pretende suplantar.

La identificación del atacante puede ser una tarea que consuma bastante tiempo y recursos, por lo que no debería interferir en la contención y erradicación del incidente. Algunas organizaciones optan por no perseguir legalmente a los atacantes por el esfuerzo necesario: costes, trámites judiciales, publicación en los medios...

Además, los ataques realizados desde otros países con ciertas lagunas legales en el tratamiento de los delitos informáticos pueden dificultar las reclamaciones judiciales, ya que se complica en gran medida el proceso de extradición de los responsables<sup>12</sup>.

Existen distintas técnicas para determinar la dirección IP del equipo (o equipos) desde el que se ha llevado a cabo el ataque contra el sistema informático: utilización de herramientas como *ping*, *traceroute* o *whois*; consulta en los registros inversos de servidores DNS; etcétera.

No obstante, es necesario tener en cuenta una serie de obstáculos que pueden dificultar esta tarea:

- Mediante técnicas de *IP Spoofing* se podría enmascarar la dirección en algunos tipos de ataque.
- El atacante podría estar utilizando equipos de terceros para realizar sus acciones, situación que se produce con bastante frecuencia hoy en día.
- El atacante podría haber empleado una dirección IP dinámica, asignada a su equipo por un proveedor de acceso a Internet.
- El equipo del atacante podría estar situado detrás de un servidor *proxy* con el servicio NAT activo (traducción de direcciones internas a una dirección externa), compartiendo una dirección IP pública con otros equipos de la misma red.

Por este motivo, en muchos casos será necesario solicitar la colaboración de los responsables de otras redes y de los proveedores de acceso a Internet que pudieran haber sido utilizados por los atacantes.

Una tarea que también podría contribuir a la identificación del atacante es el análisis de las actividades de exploración (escaneos de puertos y de vulnerabilidades en el sistema) que suelen anteceder a un ataque, sobre todo si éstas han podido ser registradas por los *logs* de los equipos afectados o por el Sistema de Detección de Intrusiones (IDS).

En cuanto a la ejecución de acciones contra el atacante, se recomienda presentar una denuncia ante las unidades policiales especializadas en este tipo de incidentes o ataques informáticos, para poder emprender de este modo las correspondientes actuaciones policiales y judiciales.

---

<sup>12</sup> En estos casos se requiere de la existencia de un tratado de cooperación judicial entre los países involucrados en el proceso.

Conviene destacar que si la organización decidiese actuar por su propia cuenta, “tomando la justicia por su mano”, es decir, realizar ataques a modo de represalia contra los equipos desde los que aparentemente se está produciendo un intento de intrusión contra sus propios equipos y redes informáticas, esta actuación podría tener graves consecuencias para la organización. Si el atacante ha utilizado técnicas de enmascaramiento (como *IP Spoofing*), la organización podría lanzar un ataque contra equipos y redes inocentes, con las correspondientes responsabilidades legales que se derivan de esta actuación, por lo que podría ser denunciada por las organizaciones propietarias de estos equipos atacados a modo de represalia.

---

## 3.6 COMUNICACIÓN CON TERCEROS Y RELACIONES PÚBLICAS

---

El Plan de Respuesta a Incidentes tiene que contemplar cómo la organización debería comunicar a terceros la causa y las posibles consecuencias de un incidente de seguridad informática.

Así, dentro de este Plan de Respuesta deberían estar previstos los contactos con organismos de respuesta a incidentes de seguridad informática (como el CERT), con las fuerzas de seguridad (Policía o Guardia Civil en España), con agencias de investigación y con los servicios jurídicos de la organización.

También podría ser necesario establecer contactos con proveedores de acceso a Internet, ya sea el proveedor de la propia organización o el proveedor o proveedores que dan servicio a equipos desde los que se ha originado un ataque contra la organización.

Del mismo modo, en algunos casos sería recomendable contactar con los fabricantes de hardware y/o software que se hayan visto involucrados en el incidente, debido a una vulnerabilidad o una mala configuración de sus productos.

En el Plan de Respuesta a Incidentes también se deben contemplar los contactos con terceros que pudieran haber sido perjudicados por el incidente de seguridad, como en el caso de que se hubieran utilizado ordenadores de la organización para realizar un ataque contra sistemas y redes de otras entidades. De este modo, se podrían limitar las responsabilidades legales en las que podría incurrir la organización por culpa del incidente de seguridad.

Por otra parte, hay que tener en cuenta el cumplimiento de la normativa existente ya en algunos países, que obliga a la notificación de los incidentes de seguridad a determinados organismos de la Administración, así como a los ciudadanos (generalmente clientes de la organización) que pudieran verse afectados por dicho incidente. En los contactos con los clientes de la organización, el personal debería poder transmitir seguridad y tranquilidad, indicando en todo momento que “la situación está controlada”.

Por último, también será conveniente definir un Plan de Comunicación con los Medios: agencias de noticias, prensa, emisoras de radio y TV... Para ello, la organización debería establecer quién se encargará de hablar con los medios y qué datos se podrán facilitar en cada momento.

El interlocutor debería estar preparado para responder a preguntas del estilo: ¿quién ha sido el responsable del ataque o incidente?; ¿cómo pudo suceder?; ¿hasta qué punto se ha extendido por la organización?; ¿qué medidas están adoptando para contrarrestarlo?; ¿cuáles pueden ser sus consecuencias técnicas y económicas?; etcétera.

En la comunicación con los medios, la organización debería procurar no revelar información sensible, como los detalles técnicos de las medidas adoptadas para responder al incidente de seguridad, y evitar en la medida de lo posible las especulaciones sobre las causas o los responsables del incidente de seguridad.

## 3.7 DOCUMENTACIÓN DEL INCIDENTE DE SEGURIDAD

El Plan de Respuesta a Incidentes debería establecer cómo se tiene que documentar un incidente de seguridad, reflejando de forma clara y precisa aspectos como los que se presentan en la siguiente relación:

**Tabla 3.3. Documentación de un incidente de seguridad**

- Descripción del tipo de incidente.
- Hechos registrados (eventos en los logs de los equipos).
- Daños producidos en el sistema informático.
- Decisiones y actuaciones del equipo de respuesta.
- Comunicaciones que se han realizado con terceros y con los medios.
- Lista de evidencias obtenidas durante el análisis y la investigación.
- Comentarios e impresiones del personal involucrado.
- Posibles actuaciones y recomendaciones para reforzar la seguridad y evitar incidentes similares en el futuro.

La *Trans-European and Education Network Association* (TERENA) ha desarrollado un estándar para facilitar el registro e intercambio de información sobre incidentes de seguridad: el estándar RFC 3067, con recomendaciones sobre la información que debería ser registrada en cada incidente (*Incident Object Description and Exchange Format Requirements*).

Conviene destacar que una correcta y completa documentación del incidente facilitará el posterior estudio de cuáles han sido sus posibles causas y sus consecuencias en el sistema informático y los recursos de la organización. Por supuesto, será necesario evitar que personal no autorizado pueda tener acceso a esta documentación sensible.

---

## 3.8 ANÁLISIS Y REVISIÓN A POSTERIORI DEL INCIDENTE: VERIFICACIÓN DE LA INTRUSIÓN

---

Dentro del Plan de Respuesta a Incidentes se tiene que contemplar una etapa para el análisis y revisión a posteriori de cada incidente de seguridad, a fin de determinar qué ha podido aprender la organización como consecuencia del mismo.

Con tal motivo, será necesario elaborar un informe final sobre el incidente, en el que se puedan desarrollar los siguientes aspectos de forma detallada:

- Investigación sobre las causas y las consecuencias del incidente:
- Estudio de la documentación generada por el equipo de respuesta a incidentes.
- Revisión detallada de los registros de actividad (*logs*) de los ordenadores y dispositivos afectados por el incidente.
- Evaluación del coste del incidente de seguridad para la organización: equipos dañados, software que se haya visto afectado, datos destruidos, horas de personal dedicado a la recuperación de los equipos y los datos, información confidencial comprometida, necesidad de soporte técnico externo, etcétera.
- Análisis de las consecuencias que haya podido tener para terceros.
- Revisión del intercambio de información sobre el incidente con otras empresas e instituciones, así como con los medios de comunicación.
- Seguimiento de las posibles acciones legales emprendidas contra los responsables del incidente.
- Revisión de las decisiones y actuaciones del equipo de respuesta a incidentes:
- Composición y organización del equipo.
- Formación y nivel de desempeño de los miembros.

- Rapidez en las actuaciones y decisiones: ¿cómo respondió el personal involucrado en el incidente?; ¿qué tipo de información se obtuvo para gestionar el incidente?; ¿qué decisiones se adoptaron?
- Análisis de los procedimientos y de los medios técnicos empleados en la respuesta al incidente:
  - Redefinición de aquellos procedimientos que no hayan resultado adecuados.
  - Adopción de las medidas correctivas que se consideren necesarias para mejorar la respuesta ante futuros incidentes de seguridad.
- Adquisición de herramientas y recursos para reforzar la seguridad del sistema y la respuesta ante futuros incidentes de seguridad.
- Revisión de las Políticas de Seguridad de la organización.
- Definición de nuevas directrices y revisión de las actualmente previstas por la organización para reforzar la seguridad de su sistema informático.

---

## 3.9 PRÁCTICAS RECOMENDADAS POR EL CERT/CC

---

El CERT/CC (*Computer Emergency Response Team/Coordination Center*) ha propuesto una serie de actividades para mejorar la respuesta de una organización ante los incidentes de seguridad informática. Seguidamente se presenta un extracto con algunas de las principales actividades propuestas por este organismo, agrupadas en tres fases o etapas:

### 3.9.1 Preparación de la respuesta ante incidentes de seguridad

---

- Definición del plan de actuación y los procedimientos para responder a los incidentes, especificando, entre otras cuestiones, a quién se debe informar en caso de incidente o qué tipo de información se debe facilitar y en qué momento (fase del incidente).
- Documentación del plan de actuación y de los procedimientos para responder a los incidentes.
- Comprobación de que el plan de actuación y los procedimientos previstos cumplen con los requisitos legales y las obligaciones contractuales con terceros (como, por ejemplo, exigencias de los clientes de la organización).

- Adquisición e instalación de herramientas informáticas y dispositivos que faciliten la respuesta ante incidentes. Conviene disponer de equipos redundantes, dispositivos de red y medios de almacenamiento para poder recuperar el funcionamiento normal del sistema.
- Verificación de los procedimientos y dispositivos de copias de seguridad.
- Creación de un archivo de discos de arranque y un conjunto de copias con todas las aplicaciones y servicios necesarios para el funcionamiento de los sistemas informáticos, así como de los parches y actualizaciones correspondientes.
- Formación y entrenamiento del personal afectado por este plan y procedimientos de actuación.
- Mantenimiento actualizado de una base de datos de contactos (personas y organizaciones).

### 3.9.2 Gestión del incidente de seguridad

---

- Aislamiento de los equipos afectados por el incidente, realizando además una copia de seguridad completa de sus discos duros.
- Captura y protección de toda la información asociada con el incidente: registros de actividad (*logs*) de los equipos y dispositivos de red, ficheros dentro de los servidores, tráfico intercambiado a través de la red, etcétera.
- Catalogación y almacenamiento seguro de toda esta información para poder preservar las evidencias. Convendría disponer de copias de seguridad con la información del estado previo y del estado posterior al incidente de los equipos y sistemas afectados.
- Revisión de toda la información disponible para poder caracterizar el tipo de incidente o intento de intrusión. Análisis detallado de los registros de actividad (*logs*) y del estado de los equipos para determinar cuál puede ser el tipo de ataque o incidente, qué sistemas se han visto afectados, qué modificaciones han realizado o qué programas han ejecutado los posibles intrusos dentro de estos sistemas.
- Comunicación con todas las personas y organismos que deberían ser informados del incidente, cumpliendo con lo establecido en las políticas y procedimientos de respuesta a incidentes. Mantenimiento de un registro detallado de todas las comunicaciones y contactos establecidos durante la respuesta ante el incidente.
- Participación en las medidas de investigación y de persecución legal de los responsables del incidente.

- Aplicación de soluciones de emergencia para tratar de contener el incidente: desconectar los equipos afectados de la red corporativa; desactivar otros dispositivos y servicios afectados; apagar temporalmente los equipos más críticos; cambiar contraseñas e inhabilitar cuentas de usuarios; monitorizar toda la actividad en estos equipos; verificar que se dispone de copias de seguridad de los datos de los equipos afectados por el incidente; etcétera.
- Eliminación de todos los medios posibles que faciliten una nueva intrusión en el sistema: cambiar todas las contraseñas de los equipos a los que hayan podido tener acceso atacantes o usuarios no autorizados; revisar la configuración de los equipos; detectar y anular los cambios realizados por los atacantes en los equipos afectados; restaurar programas ejecutables y ficheros binarios (como las librerías del sistema) desde copias seguras; mejorar, si es posible, los mecanismos de registro de la actividad en estos equipos.
- Recuperación de la actividad normal de los sistemas afectados: reinstalación de aplicaciones y servicios, incluyendo los parches y actualizaciones de seguridad; restauración de los datos de los usuarios y las aplicaciones desde copias de seguridad; recuperación de las conexiones y servicios de red; verificación de la correcta configuración de estos equipos.

### 3.9.3 Seguimiento del incidente de seguridad

---

- Identificación de las lecciones y principales conclusiones de cada incidente, recurriendo para ello al análisis post mórtem de los equipos afectados por el incidente y entrevistando a las personas implicadas en la gestión del incidente.
- Implementación de las mejoras de seguridad propuestas como consecuencia de las "lecciones aprendidas" en cada incidente: revisión de las políticas y procedimientos de seguridad, realización de un nuevo análisis detallado de las vulnerabilidades y riesgos del sistema, etcétera.

---

## 3.10 OBLIGACIÓN LEGAL DE NOTIFICACIÓN DE ATAQUES E INCIDENCIAS

---

La obligación legal de notificación de ataques e incidencias que puedan afectar a la seguridad informática es una medida que ya ha sido adoptada por el Estado de California en Estados Unidos. Así, en este Estado desde el 1 de julio de 2003 todos los *websites* de comercio electrónico están obligados por ley a informar a sus clientes cuando se haya producido una violación de la seguridad de su sistema informático.



De hecho la "Senate Bill 1386" fue aprobada en California en septiembre de 2002, después de que tuviese lugar una intrusión en los sistemas de nóminas de este Estado, a consecuencia de la cual los datos de más de doscientos mil empleados del Estado cayeron en manos de los atacantes, con un notable riesgo de fraudes y robos de identidad.

En virtud de lo dispuesto por esta ley, toda empresa afectada por un ataque o incidencia informática deberá informar de este hecho por correo electrónico a sus clientes, indicándoles que el número de su tarjeta de crédito o algún otro dato de carácter personal podría haber sido sustraído de los ordenadores de la empresa. Esta alerta informativa se tendrá que enviar tanto en caso de robo de información como cuando hayan sido descubiertas brechas de seguridad en el *website* de la empresa.

Esta ley del Estado de California no contempla la aplicación de multas a quienes no cumplan con este requisito, pero sí abre las puertas a todo tipo de procesos legales contra las empresas afectadas.

En la actualidad se estudia la posibilidad de aplicar esta misma medida a todas las empresas que cotizan en bolsa en Estados Unidos.

---

## 3.11 PLAN DE RECUPERACIÓN DEL NEGOCIO

---

Las empresas son cada vez más conscientes de la necesidad de estar preparadas para poder responder ante todo tipo de desastres y situaciones catastróficas, como podrían ser los incendios, inundaciones, terremotos, consecuencias de huracanes, etcétera. Sin embargo, estas situaciones también se podrían producir debido a los daños ocasionados por sabotajes, robos o, incluso, por atentados terroristas.

En este contexto, la definición e implantación de un **Plan de Recuperación del Negocio**, también conocido como **Plan de Continuidad del Negocio** o **Plan de Contingencias**, constituye un elemento fundamental para poder garantizar una respuesta adecuada frente a desastres y situaciones catastróficas, asegurando la integridad y la recuperación de los datos.

En este Plan de Recuperación se deben especificar los objetivos y prioridades a tener en cuenta por la organización en caso de un desastre que pueda afectar a la continuidad de su negocio. Para ello, es necesario contemplar la disponibilidad de los recursos y medios adecuados que permitan restaurar el funcionamiento del sistema informático de la organización, así como recuperar los datos, aplicaciones y servicios básicos que se utilizan como soporte al negocio de la organización:

- Disponibilidad de un Centro Alternativo o Centro de Reserva para la ubicación de los principales recursos informáticos (servidores y bases de datos corporativas).

- Existencia de líneas de *back-up* para las comunicaciones.
- Sistemas de almacenamiento RAID en los servidores.
- Implantación de *clusters* de servidores con balanceo de carga.
- Herramientas para llevar a cabo una replicación de los documentos y las bases de datos, que puede ser síncrona, asíncrona o periódica.

Así mismo, se tiene que definir en el Plan de Recuperación del Negocio cuál va a ser la composición de un equipo de dirección que se encargará de coordinar todas las tareas de recuperación frente a un desastre, realizando esta labor desde un determinado centro de control, cuya ubicación también tiene que haber sido previamente especificada en el Plan de Recuperación.

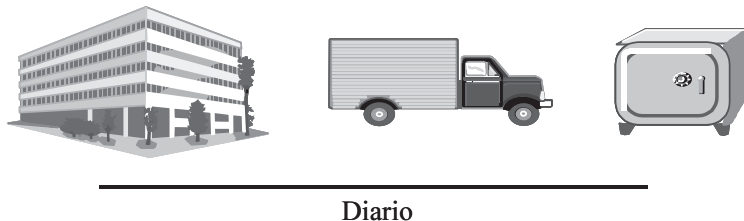
Un elemento fundamental dentro del Plan de Recuperación del Negocio es la existencia de un **Centro Alternativo**, también conocido como **Centro de Respaldo** o **Centro de Back-up**, si bien en la práctica solo las grandes empresas podrán disponer de un local o edificio dedicado exclusivamente a esta misión. Este centro tendría que estar equipado con los equipos informáticos adecuados y contar con copias de seguridad de los datos más críticos para el negocio suficientemente actualizadas.

Este Centro Alternativo debería contar con las mismas medidas de seguridad informática que las instalaciones principales de la organización. Para su correcta implantación es necesario contemplar no solo el equipamiento de hardware y de software, sino también aspectos organizativos relacionados con su gestión. Así mismo, se debe tener presente este Centro Alternativo a la hora de instalar nuevos sistemas informáticos en la organización, para que pueda estar puesto al día y sea compatible con los nuevos sistemas implantados.

Las organizaciones pueden adoptar distintas estrategias a la hora de implantar un Centro Alternativo:

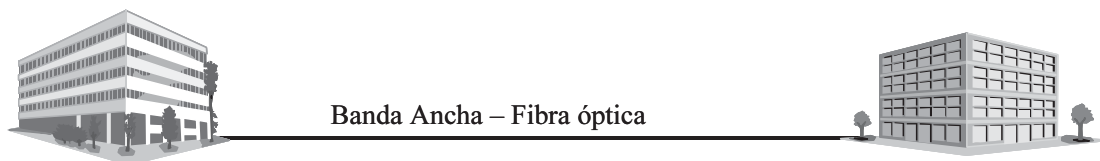
- No se dispone de un Centro Alternativo y no existen copias de seguridad externas. En esta situación el tiempo de recuperación puede ser impredecible e, incluso, dependiendo de la gravedad del desastre, es posible que nunca se puedan llegar a recuperar totalmente los datos, programas y la documentación del sistema afectado. Debemos señalar que un importante porcentaje de empresas y organizaciones de todo tipo (sobre todo las de menor tamaño) todavía se encuentra en esta situación.
- Transporte periódico de copias de seguridad a un almacén. En este caso podemos considerar que ya existe un Plan de Recuperación del Negocio, gracias a la existencia de copias de seguridad más o menos actualizadas en otra ubicación física. No obstante, el tiempo de recuperación puede ser alto, posiblemente superior a una semana, ya que no se dispone de un Centro Alternativo con

equipos adecuados para volver a poner en marcha las aplicaciones y servicios informáticos de la organización.



*Figura 3.1. Transporte de copias de seguridad a un almacén*

- Centro Alternativo "Frío": Se trata de un Centro Alternativo que cuenta con un equipamiento suficiente de hardware, software y de comunicaciones para mantener los servicios críticos de la organización. Así mismo, en este centro se guardan copias de seguridad de los datos y aplicaciones de la organización. El tiempo de recuperación puede ser de uno a varios días, ya que es necesario restaurar los datos y las aplicaciones desde las copias de seguridad, poniendo en funcionamiento los distintos equipos del Centro Alternativo.
- Centro Alternativo "Caliente": Se trata de un Centro Alternativo que cuenta con el equipamiento de hardware, software y de comunicaciones necesario para mantener los servicios críticos de la organización, y en el que además estos equipos se encuentran en funcionamiento y disponen de una réplica de todos los datos y aplicaciones del sistema informático, que se realizan de forma diaria o incluso cada hora. De este modo, el tiempo de recuperación es de unas pocas horas, inferior a un día.
- Centro Alternativo "Caliente" en una configuración en "espejo" (*mirror*): Se trata de un Centro Alternativo con el mismo equipamiento que el Centro Principal y que trabaja de un modo paralelo a éste, pudiendo entrar en acción inmediatamente a la caída del Centro Principal. Se trata, por tanto, de un sistema redundante, adecuado para situaciones que requieran de una alta disponibilidad.



*Figura 3.2. Centro Alternativo "Caliente"*

Por otra parte, debemos destacar la importancia de documentar el sistema informático al mayor nivel de detalle posible, ya que en caso de desastre no siempre se podrá disponer de las personas clave para poder disponer de esta información.

En una empresa de pequeño o mediano tamaño se podría plantear la posibilidad de subcontratar este Centro Alternativo a una empresa especializada, por ejemplo, un *Data Center* de un operador de telecomunicaciones, formalizando la relación mediante un contrato en el que se contemple las condiciones y el nivel de servicio (*Service Level Agreement*).

Un procedimiento para la recuperación frente a desastres debería contemplar las siguientes actividades:

- Detección y respuesta al desastre en el Centro Principal:
  - Adopción de las medidas de contención previstas dependiendo del tipo de desastre: incendio, inundación, explosión...
  - Comunicación a las personas y organismos externos indicados según el tipo de desastre.
- Traslado de la actividad al Centro Alternativo:
  - Traslado del personal necesario al Centro Alternativo.
  - Puesta en marcha de los servidores y equipos informáticos.
  - Volcado de los datos disponibles en las copias de seguridad más recientes.
  - Recuperación de las aplicaciones y servicios necesarios para la continuidad de las operaciones, priorizando el orden de esta recuperación en función de su importancia o criticidad para el funcionamiento de la organización.
  - Verificación del nivel de servicio recuperado.
  - Registro de todos los incidentes ocurridos durante este proceso.
- Recuperación del Centro Principal siniestrado.

El resultado de este procedimiento de recuperación se puede determinar a partir de indicadores como el RTO (*Recovery Time Objective*), que informa de en cuánto tiempo se puede recuperar el sistema informático de la organización, así como el RPO (*Recovery Point Objective*), que indica hasta dónde se puede recuperar el sistema.

Debemos destacar la importancia de llevar a cabo auditorías y pruebas periódicas para garantizar la correcta ejecución de los procedimientos previstos para la continuidad del negocio: detección y respuesta al desastre en el Centro Principal, traslado de la actividad al Centro Alternativo y recuperación del Centro Principal siniestrado. Así mismo, en todo este proceso también resulta fundamental la adecuada formación y entrenamiento periódicos del personal que pueda estar implicado en las actividades de recuperación.

## 3.12 ORGANISMOS DE GESTIÓN DE INCIDENTES

Para combatir de forma más eficaz las distintas amenazas que afectan a la seguridad de los sistemas informáticos, en estos últimos años se han creado varios organismos especializados cuya misión es alertar a los gobiernos, empresas y ciudadanos en general para poder contener y minimizar los daños ocasionados por los ataques informáticos.

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

El CERT, el “Equipo de Respuesta a Emergencias Informáticas”, es el primer y más conocido centro de respuesta, creado en diciembre de 1988 por la agencia DARPA de Estados Unidos para gestionar los incidentes de seguridad relacionados con Internet.

Se encuentra en el Instituto de Ingeniería del Software de la Universidad Carnegie Mellon. La dirección en Internet es <http://www.cert.org>.



### 3.12.2 CERT INTECO

El Centro de Respuesta a Incidentes de Seguridad fue creado en 2006 en España dentro del Instituto Nacional de Tecnologías de la Información (INTECO).

Su dirección en Internet es <http://cert.inteco.es/>.



### 3.12.3 Agencia Europea de Seguridad de las Redes y de la Información

---

Agencia europea creada por decisión del Consejo y del Parlamento (EC 460/2004) con la finalidad de alcanzar un alto nivel de seguridad en las redes y en el tratamiento de la información dentro de la Unión Europea. Esta Agencia comenzó oficialmente sus actividades en septiembre de 2005, tras fijar su sede institucional en la isla de Creta.

Su dirección en Internet es <http://www.enisa.europa.eu/>.



### 3.12.4 CSRC (Computer Security Resource Center)

---

EL CSRC, "Centro de Recursos de Seguridad Informática", es un centro dependiente del NIST (*National Institute Standards of Technology* de Estados Unidos).

Su dirección en Internet es <http://csrc.nist.gov/>.

### 3.12.5 US-CERT

---

El US-CERT es un Centro de Respuesta a Incidentes de Seguridad Informática que depende del *National Cyber Security Division* (NCSD) en el Departamento de Seguridad Interior (*Department of Homeland Security* -DHS-) de Estados Unidos.

### 3.12.6 FIRST (Forum of Incident Response and Security Teams)

---

Foro constituido en 1990 con el objetivo de facilitar el intercambio de información sobre incidentes de seguridad entre los distintos miembros que lo integran (Centros de Respuesta a Incidentes de distintos países y organizaciones), así como para la detección, prevención y recuperación de estos incidentes de seguridad.

Su dirección en Internet es <http://www.first.org/>.

### 3.12.7 Otros centros de seguridad y respuesta a incidentes

Otros países también han puesto en marcha sus respectivos centros de respuesta a incidentes de seguridad, como el AusCERT (*Australian Computer Emergency Response Team*, <http://www.auscert.org.au>) de Australia o el DFN-CERT (*Computer Emergency Response Team for the German Research Network*, <http://www.cert.dfn.de>) de Alemania.

En España también podemos destacar los servicios del IRIS-CERT, Centro de Respuesta a Incidentes de Seguridad de la Red IRIS, que da soporte a los Centros de Investigación y Universidades del país, a través de la dirección de Internet <http://www.rediris.es/cert/>.

Así mismo, el Centro de Alerta Temprana sobre Virus y Seguridad Informática fue creado en julio de 2001 por el Ministerio de Ciencia y Tecnología español, para ofrecer información, alertas y distintos recursos sobre seguridad informática a ciudadanos y empresas, a través de la dirección <http://www.alerta-antivirus.es>. En la actualidad se encuentra integrado dentro del INTECO, en la dirección <http://www.inteco.es/Seguridad>.

### 3.12.8 Bases de datos de ataques e incidentes de seguridad

También existen distintos organismos que se encargan de capturar y agrupar los registros de incidencias (*logs*) y ataques sufridos por distintas organizaciones en una base de datos. DShield (*Distributed Intrusion Detection System*, Sistema de Detección de Intrusiones Distribuido) es una de las bases de datos sobre incidentes de seguridad informática más conocida (<http://www.dshield.org/>).

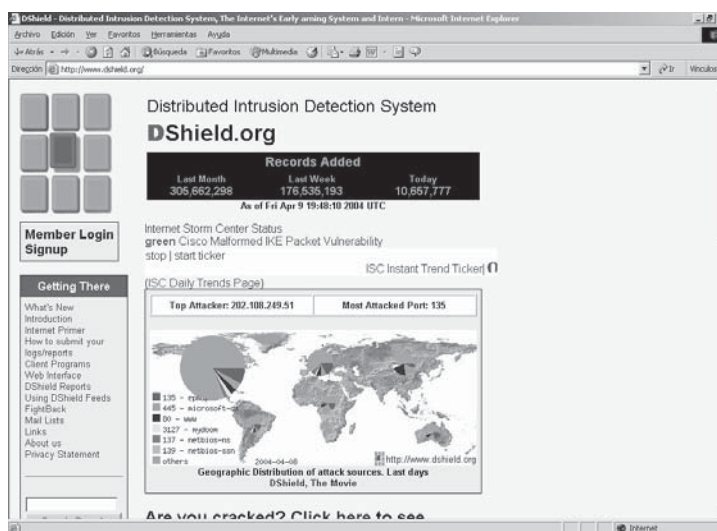


Figura 3.3. DShield.org

Otra completa base de datos con referencias sobre incidentes de seguridad se encuentra disponible en Security Focus (<http://www.securityfocus.com/>).

Así mismo, también podemos encontrar algunos servicios que se encargan de evaluar el estado del tráfico en Internet, como *Internet Health Monitoring* ([www.internetpulse.net](http://www.internetpulse.net)), que contribuye a la detección y control de los ataques de Denegación de Servicio (DoS).

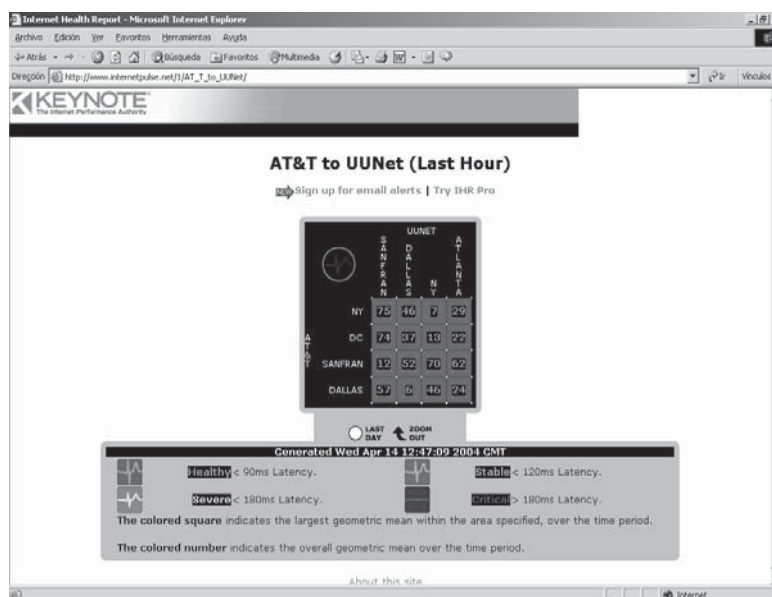


Figura 3.4. Internetpulse.net

### 3.13 DIRECCIONES DE INTERÉS

- Base de datos NSRL (National Software Reference Library) del NIST: <http://www.nsrl.nist.gov/>.
- RFC 2350 - Expectations for Computer Security Incident Response: <http://www.ietf.org/rfc/rfc2350.txt>.
- CERT: <http://www.cert.org/>.
- CERT - INTECO: <http://cert.inteco.es/>.
- ENISA: <http://www.enisa.europa.eu/>.
- US-CERT: <http://www.us-cert.gov/>.





- CSRC: *<http://csrc.nist.gov/>*.
- FIRST: *<http://www.first.org/>*.
- IRIS-CERT: *<http://www.rediris.es/cert/>*.
- AusCERT: *<http://www.auscert.org.au/>*.
- DFN-CERT: *<http://www.cert.dfn.de/>*.

