Unión Internacional de Telecomunicaciones

**CUESTIÓN 9-1/2**

*Identificación de los temas que estudian las Comisiones de Estudio del UIT-T y el UIT-R que son de particular interés para los países en desarrollo*

**UIT-D** COMISIÓN DE ESTUDIO 2 3.º PERIODO DE ESTUDIOS (2002-2006)

# *Informe sobre las infraestructuras nacionales de seguridad del ciberespacio*

Unión Internacional de Telecomunicaciones

## LAS COMISIONES DE ESTUDIO DEL UIT-D

Las Comisiones de Estudio del UIT-D se establecieron de conformidad con la Resolución 2 de la Conferencia Mundial de Desarrollo de las Telecomunicaciones (CMDT) celebrada en Buenos Aires (Argentina) en 1994. Para el periodo 2002-2006, se encomendó a la Comisión de Estudio 1 el estudio de siete Cuestiones en el campo de las estrategias y políticas de desarrollo de las telecomunicaciones y a la Comisión de Estudio 2 el estudio de once Cuestiones en el campo del desarrollo y de la gestión de los servicios y redes de telecomunicaciones. Para este periodo y a fin de responder lo más rápidamente posible a las preocupaciones de los países en desarrollo, en lugar de aprobarse durante la CMDT, los resultados de cada Cuestión se publicarán a medida que vayan estando disponibles.

**Para toda información**

*Sírvase ponerse en contacto con:*


Sra Fidélia AKPO
Oficina de Desarrollo de las Telecomunicaciones (BDT)
UIT
Place des Nations
CH-1211 GINEBRA 20
Suiza
Teléfono: +41 22 730 5439
Fax: +41 22 730 5484
E-mail: fidelia.akpo@itu.int


**Para solicitar las publicaciones de la UIT**

*No se admiten pedidos por teléfono. En cambio, pueden enviarse por telefax o e-mail.*


UIT
Servicio de Ventas
Place des Nations
CH-1211 GINEBRA 20
Suiza
**Fax: +41 22 730 5194**
**E-mail: sales@itu.int**


**La Librería electrónica de la UIT: www.itu.int/publications**

Unión Internacional de Telecomunicaciones

***CUESTIÓN 9-1/2***

*Identificación de los temas que estudian las Comisiones de Estudio del UIT-T y el UIT-R que son de particular interés para los países en desarrollo*

**UIT-D** COMISIÓN DE ESTUDIO 2 3er PERIODO DE ESTUDIOS (2002-2006)

# *Informe sobre las infraestructuras nacionales de seguridad del ciberespacio*

Unión Internacional de Telecomunicaciones

**CLÁUSULA LIBERATORIA**

**El presente informe es obra de muchos voluntarios de diferentes Administraciones y empresas. La mención de empresas o productos específicos no implica respaldo o recomendación alguna por parte de la UIT.**

# Informe sobre las infraestructuras nacionales de seguridad del ciberespacio

## ÍNDICE

*Página*

# Prefacio

*GALILEO conmocionó la ciencia y la tecnología hace cinco siglos al afirmar que la naturaleza estaba escrita en términos numéricos. La nueva revolución de las tecnologías anuncia que la sociedad está escrita en términos de información. El 0 y el 1 son los ladrillos del futuro y sólo dos cifras forman el alfabeto del fenómeno más complejo que existe: las tecnologías de la información y la comunicación.*

El decenio de 1990 se ha caracterizado por la explotación de los sistemas de comunicaciones, que han permitido el desarrollo a gran escala de los intercambios electrónicos, tanto en el ámbito industrial y bancario como en el del comercio en línea y, más recientemente, el de las relaciones entre los ciudadanos y las administraciones. Como es lógico, en los primeros años se dio prioridad a la creación y al interfuncionamiento de redes y sistemas así como a su rendimiento en detrimento de la seguridad, mientras que recientemente, los actores de las nuevas tecnologías han tomado conciencia de los problemas que se plantean y han comenzado a reflexionar sobre la seguridad de las redes de información y la comunicación, o TIC.

Las ventajas que pueden ofrecer las TIC únicamente pueden hacerse realidad si estamos convencidos de que estas tecnologías y redes son fiables y seguras y no se utilizan de manera indebida. La creación de un marco y acuerdos nacionales compatible, estable y reconocido, constituye un elemento fundamental de la edificación de la sociedad de la información y es una condición importante para instaurar la confianza, que depende también de la existencia de un marco normativo y jurídico que permita sobre todo resolver los problemas que plantean la ciberdelincuencia, la seguridad de las redes de información y comunicación, la protección del ámbito privado, los elementos jurídicos del comercio electrónico y la protección de los derechos de propiedad intelectual. Todos esos elementos deberían estudiarse en el plano internacional, con la participación activa de todas las partes interesadas.

Debido a la proliferación de piratas y virus informáticos, es necesario idear sistemas de seguridad eficaces para las redes de información y comunicación. Para ello, es imprescindible la colaboración internacional entre los Estados, el sector privado y la sociedad civil a fin de coordinar las medidas adoptadas y elaborar disposiciones jurídicas apropiadas para garantizar la protección y seguridad de las infraestructuras, los sistemas y los servicios que nos ofrece poco a poco la sociedad mundial de la información.

Cabe señalar que en la Decisión 8 de la Conferencia de Plenipotenciarios de Marrakech, celebrada en 2002 (PP-02) se da la siguiente directriz sobre la confidencialidad y la seguridad en la utilización de las nuevas tecnologías de la comunicación y la información: los socios públicos y privados no deben dudar en tomar las medidas necesarias si el contexto local de trabajo presenta factores de riesgo. Uno de los elementos más importantes del desarrollo de las nuevas tecnologías de la comunicación y la información es el establecimiento de un entorno seguro. Además, con arreglo a la Resolución 130, la Conferencia de Plenipotenciarios de Marrakech, celebrada en 2002 (PP-02), pidió a la UIT que organizara actividades en materia de seguridad de las redes de información y comunicación. Esta decisión se completó con el Anexo 1 a la citada Resolución 130 de la PP-02. Además, la Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), celebrada en octubre de 2004 (Florianópolis, Brasil), adoptó una serie de Resoluciones destinadas especialmente a los trabajos relativos a la seguridad de las redes de telecomunicaciones y la información. El presente Informe, en el que se toman en consideración estas importantes decisiones, es una contribución del Grupo de Trabajo 9-1/2 del UIT-D sobre este tema.

# 1 Introducción

La sociedad de la información ofrece grandes posibilidades de promover el desarrollo sostenible, la democracia, la transparencia, la responsabilidad y la buena gobernanza. La explotación de las nuevas oportunidades que ofrecen las tecnologías de la información y la comunicación (TIC) y su asociación con los medios de comunicación tradicionales, así como la adopción de medidas adecuadas para solucionar los problemas de la brecha digital, son elementos básicos de toda estrategia, nacional o internacional, destinada a alcanzar los objetivos de desarrollo fijados en la Declaración del Milenio de la Asamblea General de las Naciones Unidas.

Entre los principales problemas que afrontan los Estados cabe señalar las cuestiones relativas a la seguridad de la información, la complejidad, la capacidad y las repercusiones crecientes de las tecnologías de la información, el anonimato que dichas tecnologías permiten lograr y la internacionalización de las redes de comunicación. Las infraestructuras básicas de los países se componen de instituciones públicas y privadas en los ámbitos de la agricultura, la alimentación, el agua, la salud, los servicios de urgencias, los servicios públicos y de defensa nacional, la información y las telecomunicaciones, la energía, el transporte, los servicios financieros, los servicios relativos a la química y el correo. El **ciberespacio** es su sistema «nervioso», es decir, el sistema de control del país. El ciberespacio está integrado por cientos de miles de servidores, ordenadores, encaminadores, conmutadores interconectados y sistemas de transporte de la información (cables, satélites, medios radioeléctricos) que permiten un funcionamiento armonioso de las infraestructuras básicas. Por ende, el correcto funcionamiento del ciberespacio es fundamental para la economía nacional (e internacional) y la seguridad nacional. Habida cuenta de la necesidad de garantizar a todos los países un acceso equitativo y adaptado a las TIC, no hay que olvidar que estas tecnologías pueden utilizarse con fines incompatibles con los objetivos de mantener la estabilidad y la seguridad internacionales, y pueden resultar perjudiciales para la integridad de las infraestructuras estatales, en perjuicio de la seguridad de los países. Para solucionar estos problemas, es imprescindible actuar desde varios frentes y luchar por todos los medios contra la ciberdelincuencia. Garantizar la seguridad del ciberespacio es una tarea estratégica difícil que exige a todos los actores de la sociedad de la información coordinar sus esfuerzos.

a) La utilización de las TIC debe ser fiable y segura para generalizar su uso y lograr una mayor confianza de los usuarios. Para ello, es necesario:

   - proteger la confidencialidad de los datos y los intereses de los consumidores;
   - asegurar la fiabilidad de las transacciones electrónicas y el comercio en línea, e instaurar el control de los mismos;
   - elaborar normas técnicas mundiales y regionales que faciliten la instalación y utilización de las TIC;
   - mejorar la calidad de las redes mundiales y regionales, así como mantener la interconexión y el interfuncionamiento de las mismas;
   - reforzar la cooperación internacional para luchar contra la ciberdelincuencia;
   - crear mecanismos apropiados que den a conocer la importancia de la seguridad de las redes de información y comunicación y de los recursos de que dispone la comunidad internacional en este ámbito;
   - analizar las amenazas (reales y potenciales) que se ciernen en la seguridad de estas redes, sobre todo en lo que respecta a la piratería y los virus informáticos en internet, y estudiar los métodos que permitan poner fin a los mismos,
   - mejorar los intercambios de información técnica y la cooperación internacional en el ámbito de la seguridad de las redes de información y comunicación.

   En los Capítulos 2 y 3 se describen los mecanismos que pueden utilizar los actores de las TIC para proteger las redes de comunicación e información, así como los métodos utilizados por los «piratas» para atacar esas redes.

En el Capítulo 4, titulado «Centro de control y adquisición de transmisiones de datos, incluida internet», se da el ejemplo de un sistema que permite a la autoridad reguladora velar por la seguridad y el control de las redes de comunicación e información.

b) Ante el progreso sin precedentes de las TIC, es necesario tomar nuevas medidas destinadas a fortalecer la aplicación de los derechos humanos y las libertades fundamentales, en particular, el derecho a la libertad de opinión y expresión y a la confidencialidad de los datos, a saber:

- aplicar disposiciones jurídicas que garanticen el acceso a la información y el derecho del público a acceder a la información;
- elaborar un marco jurídico nacional sobre la libertad de expresión,
- aplicar la legislación de la comunicación y la información en el ciberespacio.

Este tema se aborda en el Capítulo 5, titulado «Aspectos jurídicos (ciberdelincuencia)», en el que se destacan los trabajos y los estudios realizados por la ONU, la OCDE, el Consejo de Europa, la Unión Europea y Estados Unidos que han culminado en la elaboración de Informes. En el Capítulo 6 se da a conocer la situación de las normas ISO y en el Capítulo 7, los resultados de la Cumbre Mundial sobre la Sociedad de la Información (CMSI – Ginebra, diciembre de 2003) sobre la seguridad de la información.

En el Capítulo 8 se describen los trabajos que ha realizado o está realizando la UIT.

En el Capítulo 9 se expone un ejemplo de sistema de control de datos, incluida internet.

En el Capítulo 10 se abordan estudios de casos importantes y, en particular, la lucha contra el envío masivo de correo electrónico no solicitado (spam).

# 2 Seguridad y protección de las redes

La noción de sistema de gestión y protección de las redes de telecomunicaciones (seguridad) fue incorporada en el plano internacional a través de las normas ISO 9000 e ISO 14000 y el Informe Técnico TR 13335 de la ISO («*Management of information, communications technology security*»).

El sistema de seguridad de las redes debe basarse en un conjunto de elementos correlacionados o interactivos (políticos, técnicos, de procedimiento y humanos) que permita:

- definir el método de gestión de los riesgos y aplicar y verificar/mantener/mejorar permanentemente la seguridad de la información en el marco de un organismo. En cuanto a las redes, es preciso tener en cuenta que todas las informaciones y todos los sistemas que las procesan carecen del mismo valor, no están amenazados de la misma manera y no son vulnerables a los mismos factores. Se trata de un proceso continuo en el que se han de tomar en consideración y abordar las limitaciones evolutivas de los entornos interno y externo.

## 2.1 Concepto

Las empresas reaccionan de manera relativamente distinta ante la amenaza que representan los piratas (*hackers*), lo cual, en la práctica, les lleva a instalar infraestructuras de seguridad. Se debe crear una política de seguridad cuya actualización y observancia puedan llevarse a cabo.

La instalación de una arquitectura de seguridad obliga a realizar varias tareas, que pueden realizarlas la propia empresa o un contratista, en función de la dimensión y los recursos de la empresa. En cualquier caso, es necesario realizarlas.

- Tener en cuenta el objetivo del proyecto: del simple acceso a internet a la creación de un portal para que los socios puedan consultar los datos del sistema de información.
- Elaborar una lista de las funcionalidades previstas.
- Elaborar una lista de los flujos generados.
- Adaptar las necesidades a la política de seguridad (*se debe aplicar una política de seguridad*).

- Evaluar las incidencias en el resto del sistema de información. Sincronización con los distintos responsables de ámbitos funcionales.
- Buscar instrumentos o tipos de configuración que garanticen la seguridad del conjunto de los flujos: autenticación, integridad, criptación, disponibilidad, etc.
- Escoger otros instrumentos que respondan al pliego de condiciones.
- Definir la arquitectura de seguridad con todos los elementos que la componen.
- Definir el plan de direccionamiento.
- Instalar una maqueta para validar las funcionalidades y la seguridad del sistema.
- Redactar procedimientos de explotación, administración y aplicación de un procedimiento de escalada en caso de ataque.
- Transferir competencias a las entidades de explotación y los administradores.
- Crear un sitio piloto.
- Realizar una prueba de intrusión.
- En su caso, modificar la arquitectura de seguridad o los procedimientos.
- Aplicar la solución en varios sitios.

## 2.2 Las tecnologías

Hoy en día, las tecnologías de seguridad permiten instalar equipos cada vez más eficaces y robustos, que suelen proponerse en forma de «cajas negras» especializadas. (Encaminadores de alto nivel, conmutadores, programas informáticos.)

Actualmente, la elección de las soluciones depende del costo, la evolución, la administración, la política de concesión de licencias, la compatibilidad con las normas de la industria, etc. La administración sigue siendo un elemento importante porque cuanto más fácil resulte manipular la estructura de interfaz, más interesante puede ser la solución. De hecho, algunas empresas no tienen equipos dedicados a la seguridad, las personas encargadas de la red son las que se ocupan de gestionar los elementos de seguridad.

Por otra parte, las extensiones inmediatas de un cortafuegos (*firewall*) pueden repercutir rápidamente en la elección porque en cuanto se instala un cortafuegos suelen adquirir importancia soluciones como la autenticación y el cifrado con ayuda de túneles VPN.

Además del cortafuegos existe todo tipo de complementos que deben utilizarse en asociación con los cortafuegos para reforzar realmente la eficacia de la seguridad:

- retransmisoras de mensajes,
- antivirus,
- *Proxy*, HTTP, FTP, *news*,
- programas de optimización de la banda de paso,
- sistemas y programas de cifrado,
- sistema de análisis de registros cronológicos,
- sistema de detección de ataques e intrusión (SDI),
- equipos destinados a la autenticación de usuarios,
- conmutadores web «inteligentes»,
- herramientas de detección de puntos de vulnerabilidad,
- memorias cache.

Los enlaces inalámbricos (Wireless LAN) son redes por las que las conexiones y los datos que transitan no son realmente fiables y cuya confidencialidad no puede garantizarse sin un dispositivo de seguridad. He aquí una situación que ya es habitual en internet. A los mismos problemas se aplican las mismas soluciones: aislamiento del sistema de información mediante la creación de una zona desmilitarizada (DMZ) específica y aplicación de la seguridad en una capa superior (cifrado, firma ...). En el punto 2.9 del presente documento se estudia más detenidamente este tema.

## 2.3 Los encaminadores

Un encaminador es un computador conectado a varias redes por otras tantas interfaces y cuya tarea consiste en hacer pasar un datagrama (o paquete) de una red a otra en función de la dirección de destino que figura en el encabezamiento del paquete. Por defecto, un encaminador deja pasar todos los paquetes sin excepción, permite el acceso distante (Telnet con autenticación) a través de todas sus interfaces para la configuración y ofrece la posibilidad de actualizar programas a través de la red así como aplicaciones de lectura y escritura distantes en el entorno del protocolo de gestión de red simple (SNMP).

Antes de instalar un cortafuegos (encaminador filtrante cuyas decisiones de encaminamiento pueden modificarse con reglas de acceso), se ha de configurar ante todo el encaminador de origen del tráfico entrante. Para ello, es necesario empezar por dimensionar de manera adecuada la conexión a la red pública. El encaminador conectado puede, según su configuración, limitar la utilización de ciertos protocolos con objeto de evitar una saturación de la banda de paso. De este modo, da igual que la línea dé acceso a internet o a un sitio asociado, sólo pueden pasar los flujos declarados útiles, lo cual evita todo ataque por «inundación» de paquetes. Una vez finalizada esta etapa, se puede proceder a instalar el cortafuegos.

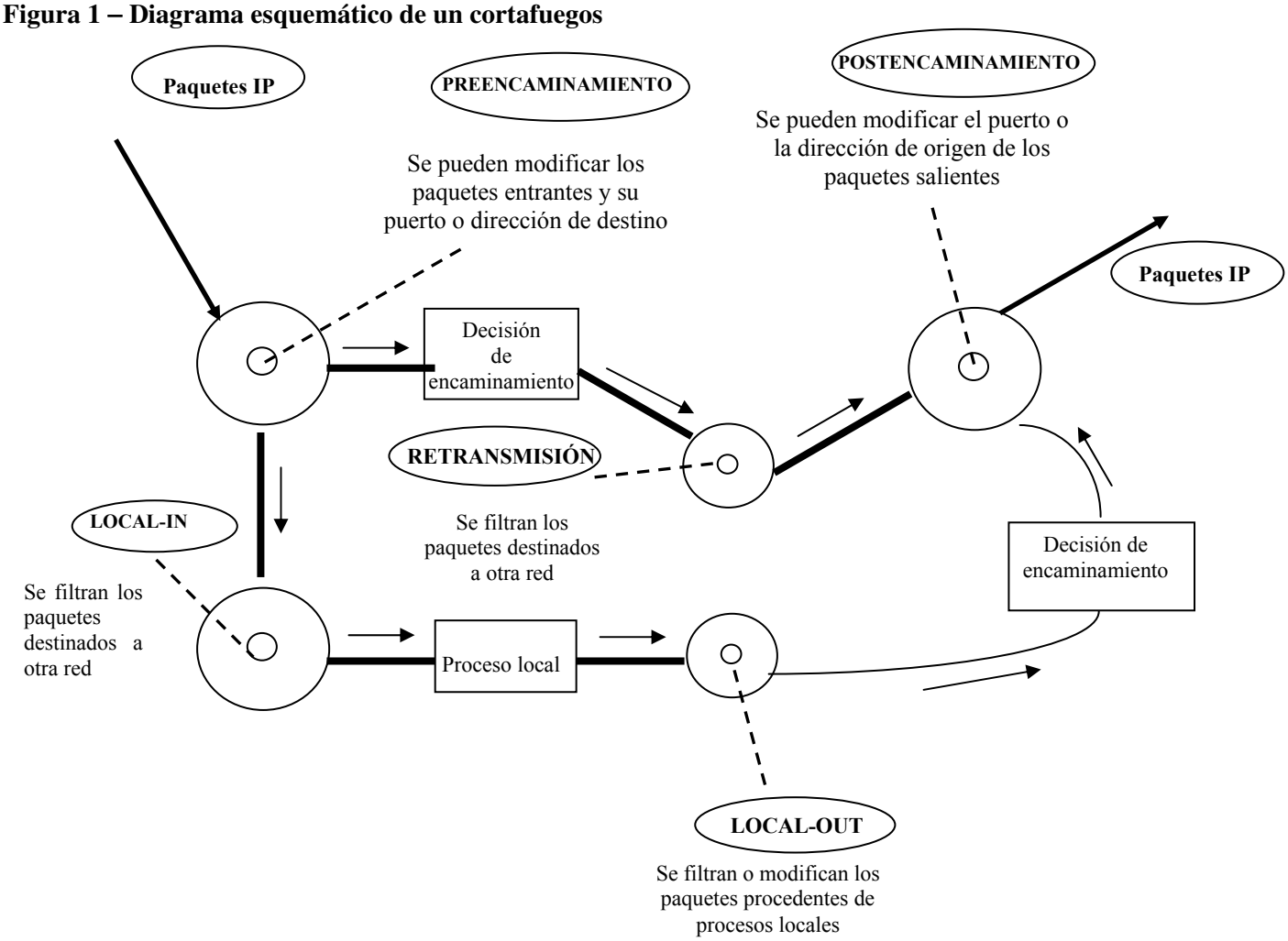
## 2.4 Los cortafuegos (*firewall*)

Los límites del perímetro de seguridad suelen quedar determinados por uno o varios elementos cortafuegos, cuya administración debe estar obligatoriamente centralizada. El nombre genérico de cortafuegos se da a numerosos programas y equipos que desempeñan todos la misma función: aislar de manera selectiva la red empresarial respecto de las demás redes (blindaje contra los *hackers*, filtrado contra los curiosos). En consecuencia, la creación de un perímetro de seguridad consiste en designar la(s) red(es) de máquinas o recursos que han de protegerse. El límite de este perímetro designa la zona donde se controlan todas las conexiones entrantes y salientes. La autorización para que el paquete pueda atravesar el cortafuegos queda definida por reglas como, por ejemplo:

- la dirección de origen o destino del paquete,
- el protocolo utilizado,
- el puerto de conexión.

El cortafuegos constituye la única pasarela de comunicación para todos los huéspedes situados dentro de la zona protegida. Para que este perímetro de seguridad sea realmente eficaz, todas las comunicaciones entrantes o salientes establecidas han de transitar por el cortafuegos. Este elemento desempeña pues una función esencial para solucionar el problema, puesto que protege el famoso perímetro de seguridad. Para ello, el cortafuegos pone en marcha un mecanismo de filtrado dinámico de paquetes. También comprende un «controlador» de sesiones y un dispositivo que analiza todas las capas de red. Así pues, el análisis de los paquetes va más allá del encabezamiento IP, sea cual sea el protocolo de transporte explotado (TCP, UDP, ICMP, RPC). Cada sesión se autoriza o rechaza en función de las reglas de filtrado establecidas. El proceso se registra con todo detalle (puertos de origen y destino, hora, fecha, número de regla aplicada ...) y queda almacenado en una base de datos.

**Figura 1 – Diagrama esquemático de un cortafuegos**

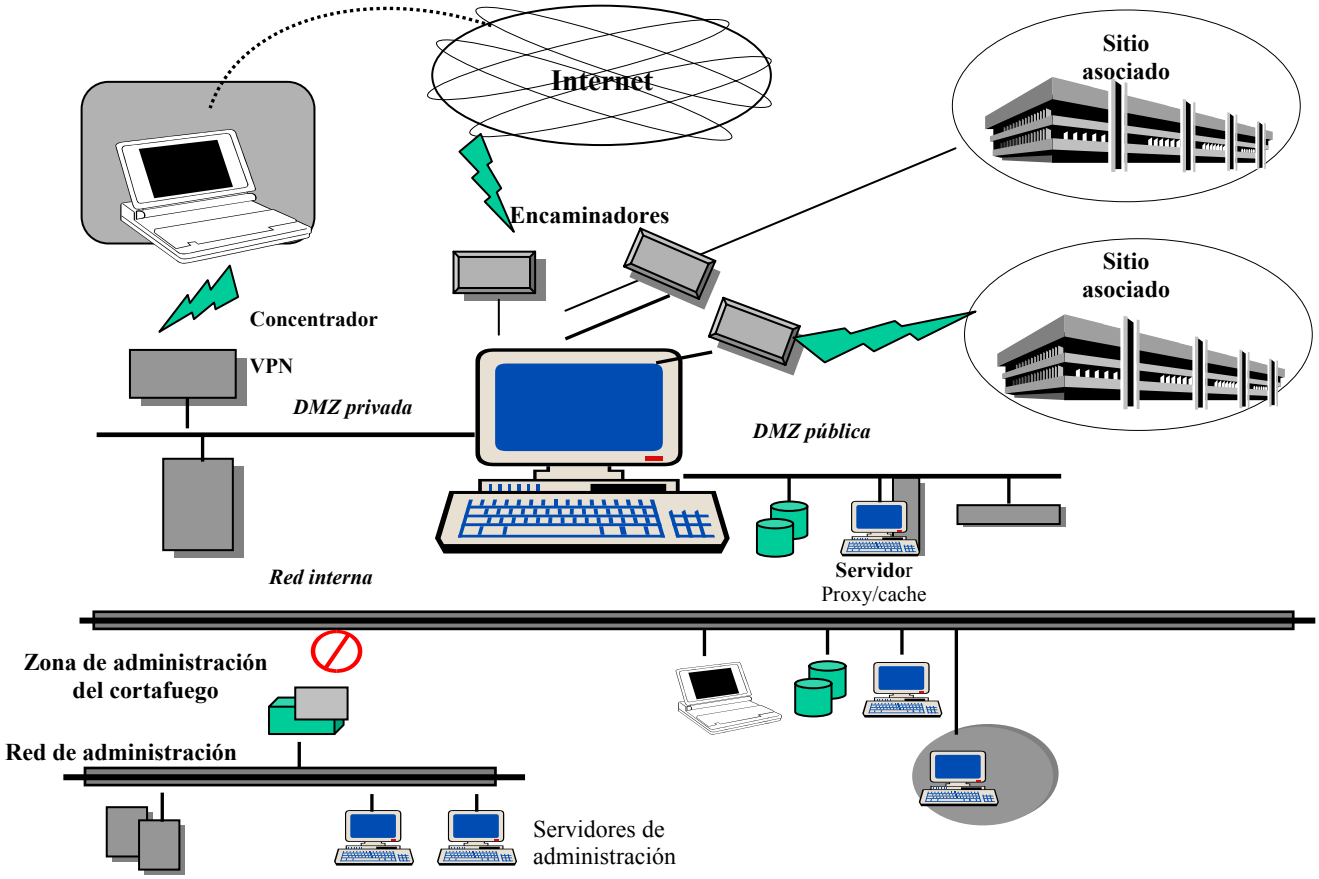



La atención debe centrarse en crear zonas desmilitarizadas (DMZ) o subredes. Estas zonas suelen estar destinadas a dar cabida a equipos más o menos sensibles o que tienen una función muy precisa en la topología de seguridad desplegada, de modo que actúan como «compartimentos» total o parcialmente herméticos. Las diversas partes de la red protegida utilizan planes de direccionamiento determinados según las necesidades de funcionamiento y pueden segmentarse como sigue: la red «proveedora de acceso» de conexión a internet, es decir, la red exterior, la(s) zona(s) denominada(s) desmilitarizada(s), con una o varias DMZ públicas y una DMZ privada, y la red interna.

Es absolutamente indispensable inspeccionar detenidamente los flujos de comunicación, incluso los datos que entran en el perímetro. Esta actividad suelen llevarla a cabo elementos «periféricos» e imprescindibles, para que la inspección sea completa y no quepa duda alguna acerca de la naturaleza del paquete. En este contexto, servidores y equipos utilizados para controlar o alertar en caso de situación anormal complementan la función del cortafuegos. En consecuencia, una red cuyo cortafuegos esté instalado sin complemento alguno puede ser fácilmente vulnerable, puesto que no puede analizar e inspeccionar los paquetes hasta el nivel de los propios datos.

El cortafuegos es el centro de la estrella que forma la red: interfaz, hacia la red interna, el exterior (internet, red pública, otra subred), las zonas desmilitarizadas (DMZ) y subredes particulares. La DMZ acepta las conexiones iniciadas desde la red interna o internet únicamente para los servicios en cuestión, mientras que el servicio interno se mantiene inaccesible desde el exterior o desde esta zona desmilitarizada. A continuación se muestra un ejemplo de conexión de un cortafuegos.

**Figura 2 – Ejemplo de conexión de un cortafuegos**




En resumidas cuentas, la instalación de un cortafuegos debe empezarse forzosamente por su configuración. Al principio, este cortafuegos ha de ajustarse de modo que no deje pasar nada, independientemente del sentido (entrada, salida de la red o acceso hacia o desde la DMZ). En función de las necesidades, poco a poco se añaden redes que permiten el acceso, con objeto de establecer únicamente las conexiones autorizadas en el marco de la política de seguridad.

Ha de tenerse en cuenta otro elemento en la instalación del cortafuegos: el direccionamiento del perímetro de seguridad, que debe ser confidencial. Para ello, se debe activar e iniciar el mecanismo de traslación de las direcciones en el/los cortafuegos y los encaminadores, con el fin de ocultar completamente las direcciones de la red interna. Esta traslación puede ser estática o dinámica, en función de las necesidades. Cabe señalar que, respecto del exterior, todas las comunicaciones IP utilizan en este caso la misma dirección o un número muy limitado de direcciones. Esto no sólo aporta eficacia, permite sobre todo autorizar únicamente a esas direcciones IP a salir a través del encaminador de acceso a internet.

Así pues, en el caso de dos subredes DMZ (una pública y una privada, por ejemplo) y una interfaz hacia la red interna, cada una de las subredes debe estar incluida obligatoriamente en una gama de direcciones única. Se debe poder acceder a los servidores situados en la DMZ pública desde el exterior (internet). En este caso, pueden recibir directamente una dirección pública y encaminable, o una dirección interna y no encaminable en internet. Si se trata de una dirección interna y no encaminable no se puede acceder directamente desde internet a un servidor web situado en una DMZ. Para acceder a los datos, los internautas deben llegar hasta el

cortafuegos que alojará en su interfaz externa la dirección pública del servidor objetivo. Su función consistirá en traducir esta dirección a la dirección interna del servidor web, para permitir el acceso. En este caso, el cortafuegos desempeña la función de jefe de orquesta y puede impedir todo acceso directo hacia dicho equipo. Este principio recibe el nombre de traslación de direcciones.

En el marco de las redes grandes, para las cuales sería grave perder una conexión hacia el exterior, se prevé cierta redundancia de los equipos (utilización paralela de dos cortafuegos, uno de los cuales se considera primario y otro secundario).

También se pueden instalar al menos dos cortafuegos situados en el punto de entrada al que acceden los encaminadores web, que aseguran una distribución del tráfico generado en el punto de acceso. De este modo se pueden constituir conjuntos de cortafuegos, que son autónomos y vuelven transparente para las otras máquinas la configuración y la distribución de la actividad entre sus miembros.

Por supuesto, la administración de estos conjuntos de cortafuegos se realiza siempre de manera centralizada. De hecho, las políticas de seguridad revisten una dimensión «global» para la red y la empresa; a menudo son las mismas para todos los puntos de acceso. Cuando varios sitios geográficos de una misma red empresarial están conectados a internet, es más eficaz y seguro administrar de manera sincronizada las adiciones, modificaciones y revocaciones de las reglas de seguridad. Además, las alertas están dirigidas a una o varias consolas centrales.

**Las reglas de seguridad de los cortafuegos**

La delincuencia informática (ciberdelincuencia) es el resultado del auge de los ordenadores en las telecomunicaciones internacionales. Los delitos han aumentado exponencialmente en los últimos años, según lo confirman varios estudios nacionales e internacionales. En la mayoría de los países no existen datos exactos acerca de la cantidad de incidentes del tipo robo de ordenadores o violación de la seguridad, especialmente los relacionados con las telecomunicaciones internacionales.

En general, las organizaciones y las empresas no disponen de ninguna estructura especializada para tratar los incidentes de seguridad relativos a las redes de la información y la comunicación (RIC), pero sí tienen un grupo para solucionar cualquier tipo de crisis. La definición de «incidente de seguridad» figura en la ISO 17799. Cuando ocurre un incidente de seguridad RIC, quien detecta el problema asume la responsabilidad de resolverlo de la mejor manera posible. En algunas organizaciones, se suele olvidar o disimular los incidentes de seguridad informática, ya que afectan la producción, disponibilidad e ingresos.

En general, la persona que detecta un incidente de seguridad RIC no sabe a quien comunicárselo. Esto significa que el administrador del sistema o de la red tiene que utilizar soluciones alternativas o provisionales, sin contar con las facultades, el tiempo o los conocimientos para corregirlo de forma que no se vuelva a producir. Por ello, es mejor tener un grupo o unidad capacitados para hacer frente a los incidentes de seguridad de forma rápida y correcta. Además, muchos de los problemas pueden aparecer en dominios tan diversos como las relaciones con los medios, o los asuntos jurídicos, de cumplimiento de la ley, de cuota de mercado o financieros.

El uso de clasificaciones diferentes en los informes o en la gestión de los incidentes ocasiona confusión. A su vez, esto da como resultado que el incidente de seguridad RIC no reciba la atención adecuada ni se tomen las medidas oportunas para interrumpirlo, contenerlo e impedir que vuelva a ocurrir. Las consecuencias para la organización afectada (o víctima) pueden ser desastrosas.

Para comunicar y tratar los incidentes con éxito, es necesario entender cómo se los detecta, trata y soluciona. Mediante el establecimiento de un marco general para hacer frente a los incidentes (sean físicos, administrativos, orgánicos o logísticos), es posible conseguir una visión general de la estructura y del flujo de un incidente. Para lograr que todos entiendan las palabras y expresiones, es indispensable contar con un vocabulario uniforme.

La Recomendación E.409 del UIT-T da una visión general y unas bases que sirven de directrices para planificar la organización de los incidentes y del tratamiento de los incidentes de seguridad además de describir su flujo y la forma de tratarlos.

Los cortafuegos en tanto que guardianes, vigilan las redes y controlan el tráfico entre dichas redes e internet. El tráfico no solicitado o sospechoso se bloquea sistemáticamente. Por otra parte los cortafuegos pueden configurarse para garantizar la seguridad de una red en relación con una o varias redes.

Para instalar cortafuegos han de seguirse cinco reglas de seguridad:

*1) Identificar las zonas de confianza*

La primera etapa para lograr la seguridad de una red consiste en definir las zonas de confianza (*trusted zones*) existentes. En su forma más sencilla, la seguridad en las redes aborda las zonas de confianza.

*2) Actualizar las reglas*

Es muy importante que los cortafuegos beneficien de una actualización de las reglas de seguridad. La única forma de comprobar que el cortafuegos sea conforme con la política de seguridad aceptada consiste en cerciorarse de dicha conformidad con un sistema de detección de intrusión (*Intrusion Detection System*) (véase el punto 2.6) o realizar una verificación manual basada en una prueba de intrusiones o encomendar un examen del cortafuegos a un tercero.

*3) Examinar el tráfico*

Para adoptar una política de seguridad del cortafuegos, conviene recordar que es importante consignar las alertas en un boletín de explotación (log). Una de las principales funciones de gestión de los cortafuegos consiste en registrar diariamente el tráfico que circula por ellos. Sin embargo, el registro diario será inútil si no se examinan con regularidad los ficheros de los boletines de explotación. Por ende, este punto debe formar parte de las reglas integradas en la política de seguridad.

*4) Vigilar la estabilidad*

Los cortafuegos se asemejan a cualquier otro elemento de la infraestructura de las redes y deben administrarse como tales. En otros términos, habrá que cerciorarse de que pueden asegurar una duración máxima de funcionamiento. De hecho, si un cortafuegos no es estable, los usuarios investigarán la forma de evitarlo para no hacer frente a un incidente, lo que conlleva evitablemente a una disminución importante del nivel de seguridad. Esta regla debe formar parte también de la política de seguridad.

*5) Documentar la política de seguridad*

La política de seguridad de los cortafuegos debe documentarse constantemente a fin de facilitar un elemento de referencia a los administradores y usuarios del mismo.

Si la política de seguridad se documenta eficazmente, los usuarios pueden trabajar con normalidad, y conforme a la política de seguridad establecida, por lo cual tenderán a reaccionar de manera *ad hoc*.

**La importancia de los cortafuegos (ejemplo)**

En agosto de 2003 la propagación del gusano «MSBlast» puso de manifiesto la vulnerabilidad de los usuarios de sistemas de banda ancha conectados a internet. Este programa gusano se introduce en los computadores aprovechando una falla del sistema de explotación; busca las puertas de entrada que han quedado abiertas o los computadores que siguen conectados a internet. Cuando finaliza la búsqueda, «BSBLast» establece una conexión y se telecarga en el computador; a partir de este nuevo huésped, el

gusano explora de nuevo internet en busca de otras puertas de entrada abiertas en otros computadores conectados a internet, por lo cual la propagación se realiza paulatinamente. La particularidad que sorprende de este gusano es que actúa sin interacción alguna por parte de los usuarios. De ahí que, si bien las conexiones de banda de ancha y permanentes a internet, son por su propia índole más vulnerables, este gusano puede afectar a todos los tipos de conexión.

Así es como en pocos días «MSBlast» infectó a 180 000 computadores en todo el mundo; no obstante, quedaron indemnes los que estaban protegidos por cortafuegos, pues éstos redujeron la gravedad de las repercusiones. Este ejemplo pone de manifiesto la importancia que reviste tomar medidas de seguridad como los cortafuegos cuando se utiliza una conexión de banda ancha. Es evidente que los usuarios de banda ancha pueden no hacer nada y aguardar a ser víctimas de un virus antes de protegerse, pero los poderes públicos y los ISP, que desempeñan una importante función pedagógica, deberían tomar medidas concretas; por ejemplo, normalizar los programas de seguridad instalados previamente.

(http://www.msnbc.com/news/951168.asp?cp1=1)

## 2.5 Los antivirus

Existen dos tipos de antivirus cuyas técnicas difieren pero se complementan, a saber:

### 2.5.1 Los de exploración (*scanners*)

Este antivirus compara los ficheros con su cuadro de firmas, que contiene la identidad de cada familia de virus. Esta técnica es eficaz con los virus conocidos a condición de que el cuadro esté actualizado, pero no ofrece protección contra virus desconocidos o antiguos virus cuyo código ha sido modificado.

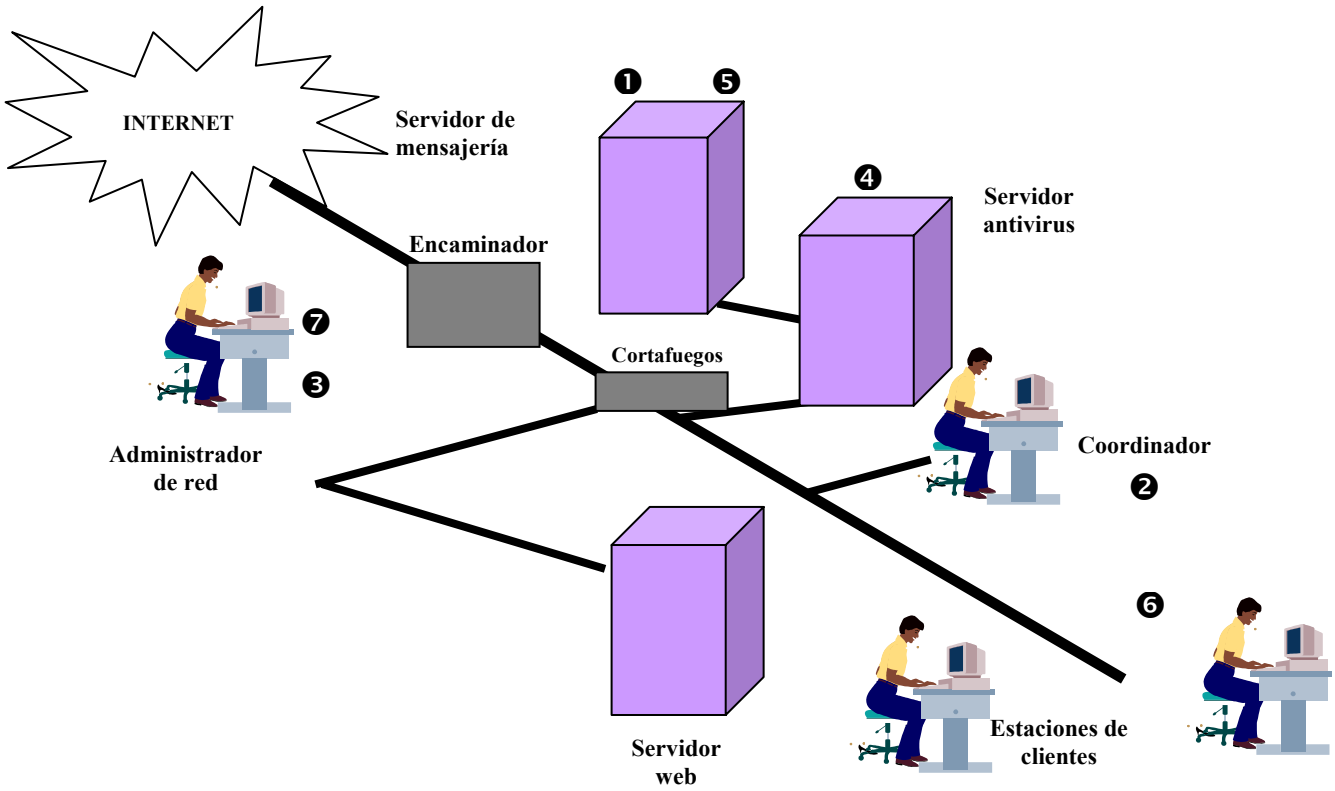
### 2.5.2 Los genéricos

Como parte de la política de seguridad, se utilizan varias técnicas de detección: el método heurístico (búsqueda de estructuras sospechosas en un programa), la verificación de la integridad de los ficheros (detección de las modificaciones), el análisis de comportamiento (sorprender al virus en flagrante) y la emulación del virus en una máquina virtual. Estos métodos son los únicos capaces de interceptar un virus desconocido pero generan numerosas falsas alertas y una carga importante en el sistema. Por este motivo suelen estar asociados a una base de firmas, de modo que el motor heurístico se limita a tratar de interceptar los virus desconocidos más obvios.

Ante los virus, la política de seguridad de la empresa debe centrarse en dos funciones clave: la administración del sistema y la coordinación de la seguridad viral. La primera realiza todos los ajustes de los servidores y puestos de trabajo, que permitirán a las aplicaciones ser lo más herméticas posible ante las infecciones. La segunda es responsable de actualizar periódicamente el parque de antivirus. También debe estar al acecho de las alertas de información sobre los virus para poder darlas a conocer a los usuarios. Avisar sobre los encabezamientos de correos electrónicos que difunden los virus ya constituye una precaución eficaz. Además, el coordinador tiene la responsabilidad de poner en marcha un plan de respuesta rápida a los ataques. Se puede cortar el acceso del usuario final a la red, y tal vez sea necesario interrumpir las aplicaciones afectadas.

A semejanza con los editores de programas antivirus, la empresa debe tener su propio centro de respuesta rápida. Todas las personas implicadas componen la célula de urgencia. La función de cada una queda definida tras realizar un simulacro previo de ataque viral. La rapidez de ejecución del plan es la primera condición del éxito.

**Figura 3 – Plan de acción antiviral**




## 2.6 Sistemas de detección de intrusiones

Los sistemas de detección de intrusiones (SDI) se han convertido en una de las principales preocupaciones de las empresas y los operadores. Numerosos expertos se han concertado para definir de manera satisfactoria el término «intrusión», pero ésta no ha resultado tan fácil como parecía a primera vista. De hecho, ¿se puede considerar una intrusión una simple exploración de puertos? Y, ¿qué hay de los ataques por negación de servicio (Dos) que, desde el punto de vista estrictamente técnico, no tienen por objeto penetrar en un sistema de información, sino simplemente saturarlo?

Así pues, definiremos la intrusión como una actividad inhabitual en el marco de un sistema de información. Esta definición incluye, en particular, las exploraciones de puertos, los ataques directos o indirectos contra un componente del sistema de información, los ataques virales, los ataques por negación de servicio y los abusos relativos a la utilización de la banda de paso. Se deben integrar los SDI en la política de seguridad.

### 2.6.1 Categoría de los sistemas de detección

#### 2.6.1.1 Sistemas de detección de intrusiones basados en la red (NIDS, *network-based intrusion detection systems*)

Los NIDS son probablemente los sistemas más conocidos. Se trata de un componente que actúa como un *sniffer* (husmeador), que captura y descodifica todas las tramas que transitan por el segmento al que está conectado. Sin embargo, a diferencia de un *sniffer*, esta sonda analiza los paquetes IP (protocolo internet) íntegramente, con objeto de localizar firmas de ataque conocidas o anomalías en los encabezamientos de los paquetes.

#### 2.6.1.2 Sistemas de detección de intrusiones basados en el computador primario (HIDS, *host-based intrusion detection systems*)

Los HIDS son el complemento natural de los NIDS. Se trata de agentes informáticos que se instalan en las máquinas que han de protegerse y cuya función es triple:

- detectar ataques contra las aplicaciones instaladas en el sistema protegido;
- verificar la integridad de los ficheros sensibles;
- establecer una relación entre los ficheros históricos procedentes de otros equipos o aplicaciones como encaminadores, cortafuegos o conmutadores.

#### 2.6.1.3 Honeypots (señuelos)

Inspirado en las estrategias militares, el sistema de *honeypots* (señuelo) es, sin duda alguna, un componente menos conocido. Muchas técnicas de ataque utilizan mecanismos de reconocimiento previo (sistema de huella digital) con objeto de determinar la naturaleza de los sistemas de explotación y las aplicaciones escogidos como objetivo. Por ejemplo, el «nmap» es un escáner de puertos relativamente corriente, que permite también tomar la huella de un sistema. Para evitar que se utilicen estos métodos de reconocimientos, los *honeypots* interfieren los escáneres emulando un sistema virtual y generando falsas respuestas para engañar al intruso.

Los sistemas *Honeypots* más utilizados son los siguientes:

1) Back Officer Friendly

El programa gratuito *Back Officer Friendly*, o BOF (www.nfr.com/products/bof), permite emular en un computador que funciona con Windows servicios de http (protocolo de transferencia de hipertexto), ftp (protocolo de transferencia de ficheros), telnet, correo y el programa back office.

Cuando el *honeypot* está activo, la más mínima petición que se realice en la red con destino a uno de los servicios abiertos en el computador basta para activar una alarma de tipo «POP UP» que avisa al usuario. *Back Officer Friendly* es un *honeypot* básico y permite a las personas poco conocedoras del concepto ponerlo en práctica de manera muy simple.

2) Specter

*Specter* (www.specter.com) es un *honeypot* similar que posee la función complementaria de registrar el tráfico efectuado con el atacante o activar respuestas automáticas destinadas al atacante.

Esta función adicional hace que este sistema sea más furtivo que el BOF.

3) Deception Toolkit

*Deception Toolkit*, o DTK (www.all.net/dtk), es una de las primeras realizaciones históricas de *honeypot*.

Esta herramienta, que está disponible en internet, permite simular distintos servicios que abarcan vulnerabilidades conocidas.

4) ManTrap

*ManTrap* (www.recourse.com/product/Man_Trap) es un producto que permite emular varios subsistemas de explotación, además del sistema de explotación básico del computador. El atacante visualiza el *honeypot* como si se tratara de varios servidores con sistemas de explotación distintos. Esta herramienta permite registrar con precisión todas las actividades del *honeypot*.

El principal inconveniente de estas herramientas es que poseen una firma que podría traicionarlos ante un atacante experimentado. Dado que los *honeypots* no deben distinguirse en su entorno, los mejores son los que se parecen tanto a los servidores que los rodean que resulta difícil diferenciarlos (pero que reemplazan los datos sensibles y suprimen las interacciones con los demás servidores).

Un *honeypot* es un sistema de seguridad que complementa la acción de los elementos que ya están instalados. Únicamente las empresas que poseen conocimientos muy avanzados en materia de seguridad pueden permitirse añadir esta nueva herramienta en su arquitectura de red, puesto que un *honeypot* debe utilizarse sólo como complemento de sistemas como los cortafuegos, las sondas de detección de intrusión, el examen periódico de los ficheros de registro, el control permanente de la actividad de la red y los sistemas de los servidores, etc.

### 2.6.2 Técnicas de detección

Se suelen utilizar distintas técnicas para detectar una intrusión, según se centre la atención en el encabezamiento (*header*) de un datagrama o en la parte de datos útiles (*payload*).

#### 2.6.2.1 Análisis de firmas

En la mayoría de los ataques se utilizan cadenas de caracteres conocidas, que se pueden distinguir en el campo de datos: esta cadena constituye la firma de la intrusión. Así pues, el análisis de la firma consiste sencillamente en detectar estas cadenas y generar una alerta en caso de correspondencia con una biblioteca de ataques conocida.

#### 2.6.2.2 Análisis de encabezamientos

Las técnicas de reconocimiento de sistema no suelen estar vinculadas con cadenas de caracteres específicas y, por lo tanto, no se pueden detectar a través del análisis de firmas. En general, estas intrusiones explotan los distintos parámetros de los encabezamientos IP. Cabe citar, por ejemplo:

- los escáneres y los barridos de puertos,
- la explotación del campo «TTL» para determinar la presencia de equipos de tipo cortafuegos o encaminadores,
- la explotación de los campos relacionados con las opciones «TCP» e «IP»,
- la utilización alternativa de las banderas «TCP».

Algunos ataques por negación de servicio son muy sencillos de poner en práctica y aprovechan una mala utilización de los parámetros del encabezamiento. Por ejemplo, cabe citar el ataque «land» que consiste en utilizar la misma dirección IP en el destino y el origen (modificando premeditadamente esta última). La mayoría de los equipos de comunicación no controlan las direcciones de origen y cuando el objetivo recibe una petición, se reenvía paquetes a sí mismo hasta saturar la *stack* IP, lo cual a menudo provoca un bloqueo del sistema. Es pues fundamental completar el análisis de firmas por un análisis de los distintos parámetros del encabezamiento, a fin de detectar este tipo de intrusiones.

#### 2.6.2.3 Análisis del comportamiento

No cabe duda de que el análisis del comportamiento es la evolución más interesante en materia de detección de intrusiones. Se trata de modelizar los comportamientos de los usuarios, a fin de determinar «perfiles tipo» y generar una alerta cuando se detecta un flujo que no corresponde al modelo. Por ejemplo, un empleado de una agencia de viajes realiza periódicamente peticiones a la sede de una compañía aérea para reservar billetes

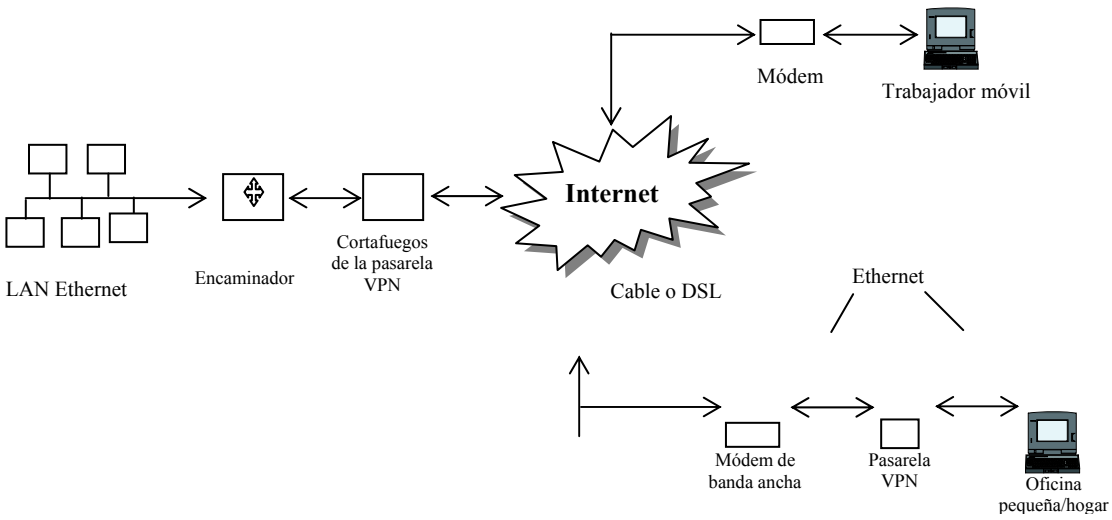
de avión. En general se trata de intercambios de transacciones formadas por secuencias de tramos relativamente cortos. Si los flujos detectados guardan relación con tramos de una longitud próxima al MTU, lo cual no es habitual en este caso, el motor de análisis del comportamiento va a generar una alerta.

Cabe señalar que en este tipo de análisis se utilizan motores de inferencia y técnicas de inteligencia artificial.

## 2.7 La red privada virtual (VPN) y la PKI

El principio fundamental de la VPN es compartir secretos en materia de seguridad para poder crear enlaces seguros entre distintos equipos e incluso entre estaciones de trabajo y equipos. Esta gestión de claves compartidas constituye, por ende, un problema en cuanto se trata de administrar un gran número de equipos o incluso equipos heterogéneos (procedentes de varios proveedores).

**Figura 4 – Ejemplo de arquitectura con VPN**




La nueva generación de VPN ofrece las siguientes perspectivas:

- Comunicaciones mejores y más seguras por internet, puesto que las VPN formalizan la seguridad por medio de la autenticación y el cifrado.
- La seguridad del correo electrónico (actualmente, un ámbito muy inseguro).
- Una mayor eficacia y mejores comunicaciones con las filiales de empresas, terceras partes o usuarios distantes que se conectan.

En las VPN donde se comparten secretos (ejemplos: redes de embajadas), si se pone en peligro uno de los equipos, peligran todos los secretos y, por ende, la propia VPN.

Para evitarlo, es necesario optar por una arquitectura en la que se utilice una clave pública y una privada. (Véase el punto 8.) Entonces es cuando entra en juego la infraestructura de clave pública (PKI), que proporciona una infraestructura encargada de administrar las claves (privadas y públicas). Véase el punto 2.8.

Por consiguiente, la función de la PKI no es sustituir la gestión de los enlaces VPN, sino más bien proporcionar las claves de autenticación de equipo a equipo, con una base de directorio (protocolo ligero de acceso al directorio (LDAP); Recomendación X.509 del UIT-T), común a toda la empresa, accesible a todos los usuarios y que establece un sistema de autenticación estricta, entre cada equipo o de cliente a equipo.

No obstante, como sucede en el mundo real, no poseemos más que una identidad, que puede presentarse en distintas formas; por ejemplo, un certificado de nacimiento, un pasaporte o un permiso de conducir. Asimismo, en el mundo virtual, también puede ser necesario tomar en consideración diferentes infraestructuras de seguridad que den a los usuarios y las aplicaciones forma distintas de identidad, de modo que cada infraestructura existente coexista y se complemente. Las VPN deberían funcionar para una identidad dada que se pueda autenticar.

Algunas tecnologías, como la PKI y KI (*Kerberos Infrastructure*), pueden funcionar en conjunto para dar mejores resultados. La KI surgió del proyecto Athena del MIT (*Massachusetts Institute of Technology*); Microsoft decidió, en 1999, utilizar la Versión 5 de Kerberos en su sistema de explotación Windows 2000 a fin de remplazar el protocolo de propietario de autenticación NTLM.

En una PKI la necesidad de almacenar claves o cualquier dato confidencial para el usuario o la aplicación suele redundar en complejidad para toda la arquitectura de la solución. La solución que suele encontrarse (ya que no existe ninguna otra más segura) consiste en utilizar tarjetas inteligentes, lectores de tarjetas y aparatos de almacenamiento de claves criptográficas en los servidores.

Debido al hecho de que la mayoría de los sistemas existentes utilizan el protocolo Kerberos, los usuarios no están obligados a conservar una tarjeta física o un aparato que contenga datos privados. Así pues, no se suele escoger adecuadamente la utilización de Kerberos en aplicaciones en las que se precisa la funcionalidad de no rechazo o una firma digital. Esto explica que se utilice más a menudo para autenticar una aplicación o un usuario y para prestar servicios de confidencialidad en una red.

Sin embargo, desde el punto de vista de la seguridad, la información privada no debe considerarse tan segura como la PKI en el terminal de usuario. Así pues, en el marco del sistema deseable Kerberos habría que prever el almacenamiento seguro de información privada (por ejemplo, utilizando dispositivos de utilización seguros como tarjetas inteligentes) en el terminal del usuario. Y como el servidor Kerberos (conocido como centro de distribución de clave (KDC)) comparte información privada con todos los terminales de usuario en la mayoría de los sistemas Kerberos, este sistema suele utilizarse en redes privadas.

La introducción del protocolo PKINIT en el juego de las normas de Kerberos permite utilizar la autenticación PKI en un entorno de Kerberos. De este modo puede explotarse plenamente la naturaleza complementaria de ambas infraestructuras ya que juntas pueden resultar muy eficaces, si la situación así lo exige.

## 2.8 Criptografía

La seguridad informática suele empezar por la instalación de un programa antivirus para la protección de los datos y sistemas, un cortafuegos para la protección de las redes y un sistema de autenticación para la protección de los recursos.

La creación de servicios de comercio electrónico, gobernanza electrónica, etc., requiere una mayor protección para crear un espacio de confianza en redes amplias y heterogéneas. Para ello han de utilizarse técnicas de cifrado, autenticación, sellado de autorización, acuse de recibo e indicación de tiempo. El objetivo es que la red sea homogénea, aplicar metodologías comunes, emitidas por una autoridad de confianza, y utilizar protocolos oficiales.

La criptografía es la ciencia que utiliza las matemáticas para cifrar y descifrar datos. Permite garantizar la seguridad de los datos de almacenamiento de informaciones confidenciales o transmitirlos hacia redes abiertas como internet.

El primer tipo de cifrado es el cifrado por clave secreta (o **clave simétrica**). Se utiliza una sola clave para el cifrado y el descifrado. Un remitente y un destinatario que desean comunicarse de manera segura deben ponerse de acuerdo en una clave y no divulgarla. Así pues, la clave no debe transmitirse por el mismo canal que el del mensaje protegido.

La criptografía de clave pública (o **clave asimétrica**) soluciona los problemas de distribución de claves. Para utilizar este procedimiento se necesitan dos claves: una clave pública y una privada. Todo lo que se cifra con una de las claves sólo puede descifrarse con la otra. No se puede deducir una de las claves a partir de la otra. La criptografía de clave pública tiene la ventaja de permitir intercambiar mensajes de manera segura, sin que sea necesario instalar previamente un dispositivo específico. Por este método, el remitente y el destinatario ya no necesitan compartir claves secretas a través de una vía de transmisión segura. En las comunicaciones se utilizan sencillamente claves públicas y ya no se transmiten o comparten claves privadas.

La combinación de estos dos tipos de criptografía permite obtener una seguridad óptima, pero se debe utilizar correctamente para que el usuario no adquiera una falsa sensación de seguridad. Por ejemplo, un agente X desea enviar un mensaje cifrado:

1) X crea un par de claves, una pública y una privada.

2) X conserva la clave privada y envía su clave pública a sus destinatarios.

3) X cifra sus mensajes con la clave privada, que sólo él posee.

4) Los destinatarios descifran los mensajes con la clave pública.

5) A su vez, cifran sus mensajes con la clave pública de X.

6) X recibe los mensajes y los descifra con su clave privada.

La parte más vulnerable es el usuario final.

Además, la criptografía asimétrica ofrece la ventaja de que permite utilizar una nueva funcionalidad: la firma electrónica. Ésta permite al destinatario verificar su autenticidad y origen, y velar por que queden intactas. De este modo, las firmas informáticas garantizan la autenticación e integridad de los datos: al mensaje se le aplica la función *hash* y el resultado se cifra con la clave privada. Las firmas también proporcionan una funcionalidad de no rechazo, a fin de evitar que el remitente haga creer que no ha enviado la información.

Cuando el destinatario recibe el mensaje y la firma (véase la Figura 5):

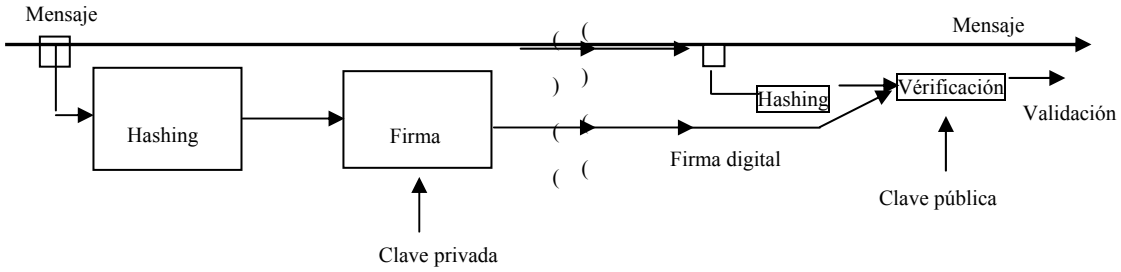
1) Al mensaje se le aplica la función *hash*. El *hashing* es un algoritmo matemático y no es objetivo, es decir, no puede deducirse el mensaje original una vez aplicada la función *hash*.

2) La firma se descifra con la clave pública.

3) Se comparan ambos resultados de la función *hash*.

Una persona malintencionada puede transmitir su clave pública haciéndose pasar por otro. En consecuencia, es necesario establecer un vínculo entre la clave y su usuario; los certificados electrónicos tienen esta función. Un certificado electrónico es un fichero que permite demostrar un vínculo entre un individuo y su clave pública. Así pues, suele ser necesario instalar sistemas que aplican mecanismos de seguridad, almacenamiento e intercambio. Éstos pueden presentarse en forma de sistemas de almacenamiento (servidores de certificados) o de sistemas estructurados (infraestructura de clave pública – PKI) que ofrecen las funciones de almacenamiento y gestión (emisión, revocación, recuperación, almacenamiento) de los certificados.

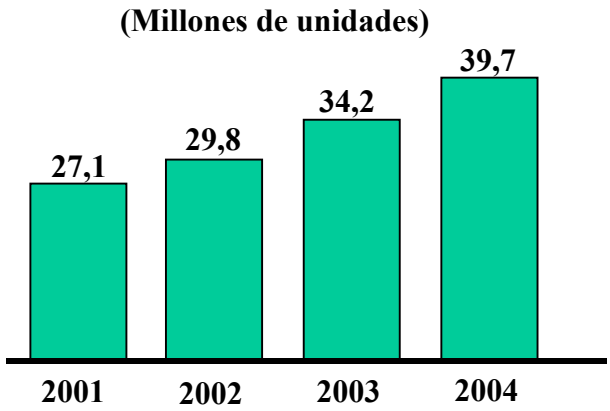
**Figura 5 – Principio general de la firma electrónica**




## 2.9 Redes inalámbricas (WLAN)

Según los datos de que se dispone, se prevé que la industria mundial de las redes inalámbricas (WLAN) experimentará un crecimiento medio anual de un 30% hasta 2006. (www.telecoms.com). Asimismo, se calcula que en 2002 los ingresos ascendieron a 1 970 millones de euros. Este crecimiento va aparejado a la utilización intensiva de computadores portátiles, tanto por las empresas como por los particulares. En 2002, la venta de computadores se distribuyó así: 76,7% de computadores fijos y 23,3% de computadores portátiles.

**Figura 6 – Ventas mundiales de computadores portátiles**




(*Fuente*: Gartner Dataquest)

Los administradores de redes inalámbricas son muy conscientes de los daños que se pueden provocar si no se domina la cobertura radioeléctrica. Todos los productos del mercado pueden transportar tramas Ethernet y las topologías utilizadas se parecen a las del mundo alámbrico: ya sea una conexión punto a punto (Modo ad hoc) o un modelo en estrella que gravita alrededor de un punto de acceso (AP) encargado de encaminar las tramas radioeléctricas (Modo Arquitectura).

Ante las amenazas, las redes pequeñas (número de abonados inferior a 10) se pueden proteger contra las intrusiones utilizando una red privada virtual (VPN). En cuanto la WLAN comienza a extenderse, la situación se complica, y se hace necesaria una interfaz de gestión flexible capaz de gestionar un verdadero control de acceso entre varias subredes. Este tipo de equipos, denominados pasarelas de seguridad WLAN, están concebidos para funcionar con puntos de acceso (AP), tratar los problemas de permanencia o en

restitución de la contraseña durante los cambios de célula y, sobre todo, obtener su información de acceso en un anuario central. Este enfoque facilita la definición de grupos específicos que tienen derecho a explotar los tramos WLAN, y evita el espinoso problema de la aceptación de estaciones invitadas o temporales.

**La seguridad de las WLAN**

Las empresas que utilizan redes locales (LAN – red de área local) inalámbricas (*wireless*) sin tomar medidas de seguridad adecuadas se exponen a los métodos de piratería más sencillos. De hecho, una falla en la seguridad de una red, por ínfima que ésta sea, constituye un problema para cualquier empresa. Una vez introducidos por una brecha, los piratas (*hackers*) pueden acceder a las contraseñas de la empresa, conectarse a los servidores, robar información confidencial, pasar a controlar el sitio web e incluso desactivar toda la red.

La utilización de una WLAN inalámbrica implica que las empresas deben tomar medidas de seguridad adecuadas.

El nivel más elemental de seguridad de las WLAN sigue siento la *Wired Equivalent Privacy* (WEP).

La WEP, elaborada por el *Institute of Electrical and Electronics Engineers* (IEEE), se ideó para garantizar una seguridad elemental a), la escucha de red causal b), proteger la red criptando todos los datos enviados por el sistema inalámbrico, mediante un algoritmo RC4 (*Ron's Code 4*) basado en una clave de criptación compartida en 40 bits.

En teoría, las claves WEP, que constituyen ladrillos básicos, son sobre todo contraseñas de secreto compartido que permiten a los usuarios descifrar los datos encriptados que transitan por una red inalámbrica. En la práctica, el pirata puede acceder a las claves de criptación simplemente permaneciendo delante del edificio de la empresa interceptando el flujo de datos encriptados con un computador portátil y descifrándolos con un programa especial que se descarga fácilmente desde internet. Este proceso, que consiste en una suerte de decodificación al revés, permite al pirata conocer la clave y le da acceso a la red de la empresa.

Las claves de criptación del algoritmo no constituyen un defecto por sí solas, pese a que una mala gestión de las mismas puede hacerlas vulnerables ante la piratería. Los administradores de los sistemas no suelen asignar más que una clave a toda la empresa, lo que significa que una vez que el pirata se apropia de ella puede tener acceso a toda la información de la empresa y a los recursos de la red. En caso de que el administrador proporcionara una clave distinta a cada usuario, bloquearía el sistema, si no la modificase en algún momento. En cualquier caso, una vez que se ha introducido el pirata, puede tener constantemente acceso no autorizado, si el entorno cuenta con un sistema de clave estática y compartida. La gestión de la clave manual puede resultar sencilla en redes más pequeñas y administradas rigurosamente. No obstante, la tarea puede ser considerable y pesada a medida que el número de usuarios de la red inalámbrica aumenta, lo que se traduce, en la mayoría de los casos, en negligencias del administrador del sistema.

En los sistemas de seguridad de las redes locales más extendidas se recurre a especificaciones más especializadas, como el cambio automático de claves, pero también deben aplicarse más allá de las propias redes, debido al gran número de usuarios y a las complejas exigencias de seguridad. Habitualmente, las grandes instalaciones requieren una tecnología de administración de claves de criptación robusta, mecanismos de autenticación y una gestión centralizada de los usuarios a través de la infraestructura de la red, que no puede almacenarse en la memoria limitada de un punto de acceso de una LAN inalámbrica.

Si bien la seguridad de la WEP, a pesar de las vulnerabilidades de la seguridad, está localizada –administrada en el marco de los puntos de acceso de la LAN inalámbrica (WLAN)– un sistema más amplio debe encargarse de acoger miles de usuarios y procedimientos de criptación y autenticación de vanguardia, lo que requiere en general una solución de seguridad administrada desde un punto central. Habitualmente la administración de estos sistemas corre a cargo de una infraestructura RADIUS (*Remote Authenticated Dial-In User Service*), que autoriza la gestión centralizada y la administración de un gran número de usuarios autorizados a acceder a los recursos de la red.

El hecho de que RADIUS soporte la aplicación 802.1x, que es la norma de conexión de red en el marco de una red Ethernet filial y una red inalámbrica 802.11, mejora considerablemente la capacidad de autenticación del usuario en la red inalámbrica de las empresas. Habida cuenta de la naturaleza mixta de la plataforma de infraestructura de las redes actuales y la diversidad de los sistemas de explotación Windows en las empresas, la posibilidad de emular una aplicación 802.1x aporta un conjunto de medios de seguridad inalámbricos de calidad superior y evolutiva. Entre las actuales funcionalidades técnicas, cabe distinguir las siguientes:

- un apoyo de conexión de red 802.1x para los sistemas Windows existentes;
- un certificado de cliente universal que permite la autenticación mutua basada en un certificado;
- una administración protegida con claves, con un apoyo para los protocolos RADIUS-EAP-TLS (*Extensible Authentification Protocol – Transport Layer Security*);
- una integración en los entornos RADIUS existentes que respaldan el protocolo MD-5 (*Message Digest 5*);
- un respaldo para múltiples esquemas de autenticación con el protocolo EAP.

**Solución técnica para Wi-Fi**

En lo que respecta a la experiencia de hacer viable y fiable la explotación de las redes inalámbricas Wi-Fi en las empresas, en la actualidad se aplica una solución técnica denominada «Commutation Wireless». Esta solución innovadora consiste en incorporar el conjunto de las funcionalidades administrativas de la red (parámetros radioeléctricos, seguridad, conectividad a una red de cable) en un conmutador o *switch* creado expresamente, a fin de «aligerar» los puntos de acceso y centralizar la gestión de la infraestructura Wi-Fi.

A diferencia de un conmutador Ethernet tradicional, un *switch* Wi-Fi gestiona por sí solo el tráfico IEEE 802.11 proveniente de los puntos de acceso conectados a él (en realidad, se trata sencillamente de puentes Wi-Fi/Ethernet), lo cual le permite controlar totalmente la red inalámbrica.

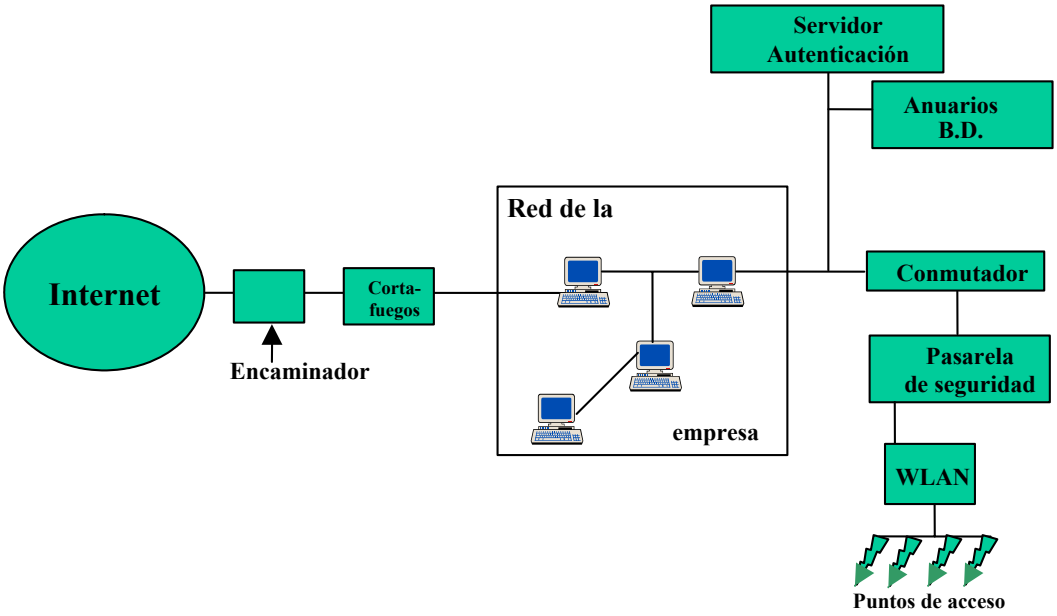
Según este modelo, los administradores de red tienen acceso a una interfaz de configuración única que les facilita una visibilidad global de la red y sus usuarios, y pueden gestionarla del mismo modo que por la red de cable existente en la empresa: autenticación en el marco de un servicio RADIUS, LDAP o, incluso, Active Directory (lo cual permite reutilizar las cuentas de usuarios de los dominios Windows para controlar el acceso a la red), seguimiento del consumo de la banda de paso por parte del usuario, configuración de la red dinámica DHCP (Protocolo de configuración dinámica del ordenador principal), etc.

Gracias a esta solución, el equipo de administración puede protegerse eficazmente contra los riesgos específicos que plantean las redes inalámbricas:

– intrusión de Access Point (desactivación por defecto, es decir, envío de instrucciones que impiden a los usuarios autenticarse en el terminal): detección automática y envío de paquetes de desconexión al conjunto de los clientes a fin de garantizar su protección;
– negación de servicio (*flood*): control de la frecuencia de las operaciones de gestión de red;
– usurpación de identidad (*man in the middle*): detección de la usurpación de una dirección Wi-Fi;
– escucha pasiva (*sniffers*): el material utilizado registra los datos de los dispositivos de escucha pasiva y los expulsa de la red.

Independientemente del nivel y el alcance de seguridad del sistema inalámbrico que se necesiten en la infraestructura de red, se puede idear una solución por capas y a medida para atender a las exigencias particulares de la seguridad de los sistemas inalámbricos. Las soluciones de seguridad inalámbricas pueden puede abarcar desde la WEP elemental, basada en normas, a la seguridad administrada en el punto de acceso de la seguridad robusta y evolutiva administrada de forma centralizada, y desde la infraestructura filial a la inalámbrica.

**Figura 7 – Red de seguridad WLAN**

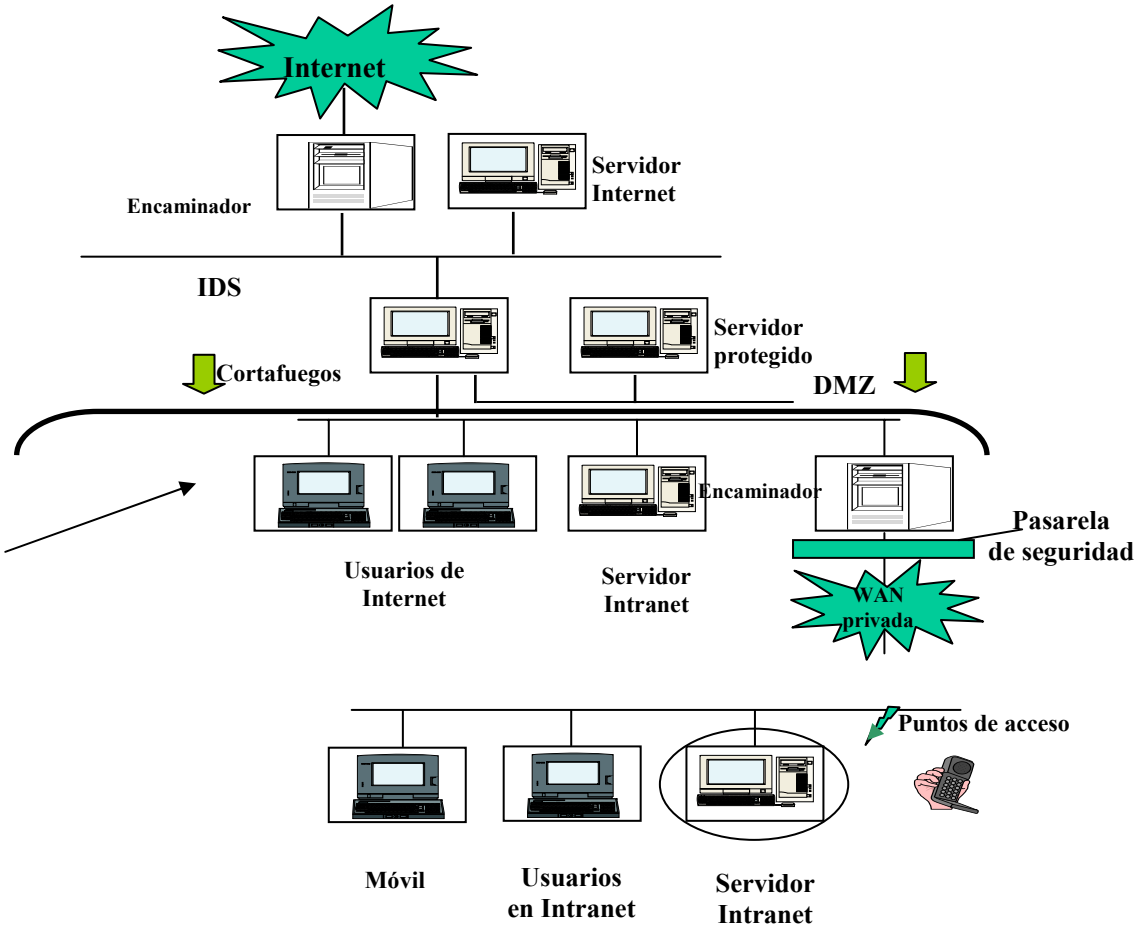



NOTA – En lo que se refiere al almacenamiento, actualmente numerosos portátiles utilizan una clave USB (*Universal Serial Bus*), es decir, una memoria flash que funciona como un disco duro extraíble (32 Mo a 512 Mo). Muchos fabricantes de equipos facilitan claves USB con un programa de privatización, lo que permite proteger los datos de la clave con una contraseña en caso de pérdida o robo. Existen sistemas más sofisticados que ofrecen la posibilidad de protegerse mediante huellas digitales (biometría).

## 2.10 Resumen

En los párrafos anteriores, se han descrito los principales medios para garantizar la seguridad de la red de comunicación e información. Se ha presentado un planteamiento de la seguridad orientado especialmente a la prevención de los riesgos asociados a las nuevas tecnologías de la información y la comunicación (NTIC). A continuación, la seguridad de la red se ilustra con un ejemplo general.

**Figura 8 – Ejemplo de esquema general de organización de la seguridad de una red**




## 3 Intrusiones/ataques automatizados

Los equipos y programas informáticos descritos en el Capítulo 2 son los guardianes de las redes de comunicación y telecomunicaciones que son vulnerables debido a su conexión a internet. Estos equipos tratan cada mensaje electrónico y cada fichero que circula por la red. A continuación se presentan los instrumentos y técnicas que suelen utilizar los piratas informáticos para atacar las redes.

### 3.1 Virus

Los virus, en sentido propio, son partes del código informático destinadas a integrarse en un programa normal. La ejecución del programa infectado activa el virus, que puede entonces propagarse o actuar de forma más o menos grave sobre la estabilidad del ordenador. Un virus puede destruir la totalidad de los datos almacenados en un ordenador o puede limitarse simplemente a mostrar en pantalla un texto hostil, por ejemplo. Distintos tipos de virus –virus ejecutables, macrovirus, virus de scripts y gusanos sofisticados– aprovechan los fallos de seguridad de los sistemas de explotación para extenderse por la red (véase la Figura 9).

En términos generales, un virus informático es un programa autorreproductor, es decir, un programa que realiza copias de sí mismo en ficheros existentes.

Los virus se caracterizan por sus mecanismos de reproducción e infección de un computador -en la zona de arranque, los ficheros de aplicaciones o incluso los ejecutables- y no por sus efectos. Los daños son múltiples: mensaje simple, borrado de ficheros, formatación del disco, modificación de la memoria CMOS, por no mencionar la instalación en el computador de un caballo de Troya (programa instalado en un computador para abrir en él una brecha de seguridad: bomba de relojería, puertas ocultas, programa espía, etc.). Se trata de una función maliciosa oculta en un fichero en apariencia no contaminado.

Los primeros virus conocidos datan de fines de los años 80. En esa época, se instalaban en la zona de arranque de los disquetes y discos duros y contaminaban todo nuevo disquete manipulado. Enseguida aparecieron otros virus que infectaron los PC contaminando los ficheros ejecutables. Por aquel entonces, un mismo programa era contaminado varias veces y así su fichero se incrementaba sin cesar. Posteriormente, los programadores se inspiraron en un virus existente para crear una versión más eficaz. Así surgió la segunda generación de virus ejecutables, más perfeccionada que la anterior, que no volvía a infectar los ficheros ya contaminados.

La proliferación de los virus depende de la seguridad de los sistemas de explotación. En los sistemas Windows, por ejemplo, cualquier usuario puede modificar los ficheros del sistema, incluidos los ejecutables, sin el menor control. Incluso los sistemas de explotación recientes para uso profesional, como Windows NT o 2000 sólo aplican una verdadera política de seguridad con respecto a los ficheros cuando utilizan el formato NTFS (*new technology file system*), que permite definir atributos para cada fichero. No hay que olvidar que un gran número de usuarios se conecta en modo administrador, facilitando así la creación de una brecha. En este tipo de sistema, la difusión de un virus ejecutable resulta bastante sencilla contrariamente a lo que ocurre en los ficheros del sistema. No obstante, existen ataques concretos para Unix, con gusanos para Linus, o para Solaris. Estos programas aprovechan brechas específicas de seguridad de las redes para acceder a la cuenta root (raíz) y contaminar el sistema.

### 3.1.1 Virus multipartito y polimorfo

En 1996 surge una nueva generación de virus, los macrovirus, que al principio servían para automatizar una serie de tareas. Existen incluso virus multipartitos, que pasan de una aplicación Office a otra. Por su parte los virus polimorfos son aquellos que incluyen un código especial que vuelve cada infección diferente de la anterior. Este tipo de virus lleva un código específico que modifica su firma para que no sea posible localizarlo y puede adoptar millones de formas distintas.

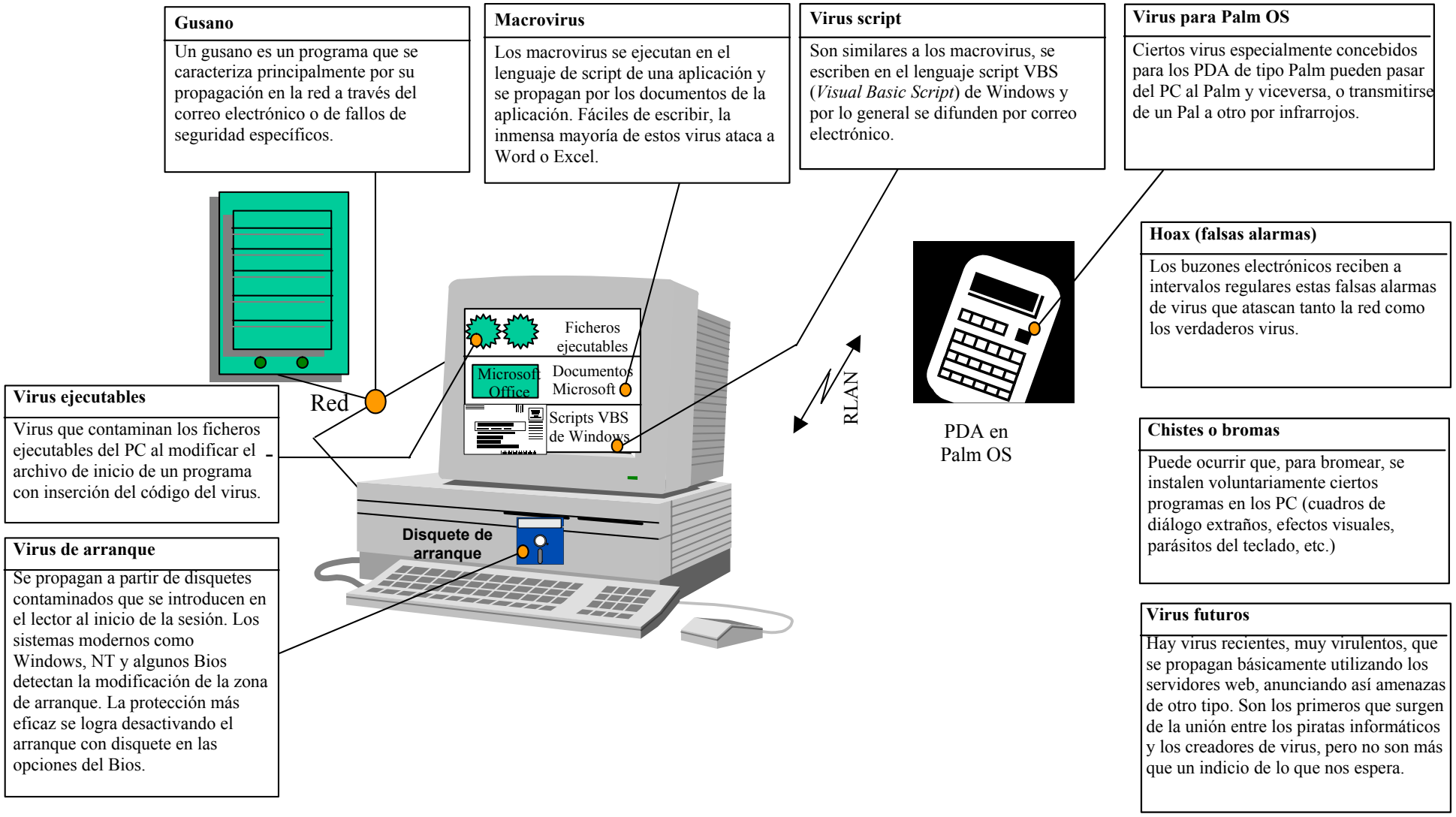
Antes de que aparecieran los macrovirus, sólo los especialistas en programación en lenguaje máquina eran capaces de crear virus. Programar un macrovirus en un lenguaje evolucionado es sencillo si se comprenden los principios básicos, y resulta muy fácil crear una variante (o mutante) de un virus existente a partir de una muestra. (MUTANTE: nueva variante de un virus ya conocido. Un virus no muta nunca por sí solo, toda mutación requiere un programador.) Actualmente, los macrovirus representan más del 95% de los virus en circulación. Aprovechan las facilidades de acceso a la red y al correo electrónico de las aplicaciones Office.

En otoño de 2000 se propagó otro tipo de microorganismo informático: el virus script, escrito únicamente en VBS (*visual basic script*), lo que lo diferencia de los macrovirus. Otro rasgo distintivo es que afecta a los ficheros de sistema Windows.

Desde 2001, los virus ejecutables han reaparecido con fuerzas renovadas. Los mutantes recientes se han convertido en programas muy complejos que utilizan las técnicas de los piratas para penetrar en los sistemas y propagarse.

En el Figura 9 se presentan los distintos tipos de virus que pueden afectar a una red de comunicaciones.

**Figura 9 – Los distintos tipos de virus**



### 3.1.2 Los virus informáticos del mañana (soporte lógico malicioso)

La aceleración del desarrollo de las infraestructuras de comunicaciones, la generalización de las grandes velocidades y la vulgarización de las transacciones en internet, son factores que han hecho que desaparezca prácticamente el límite impuesto al tamaño de los mensajes electrónicos, así como de sus anexos, sus ficheros telecargados, etc.

Esta situación ha hecho que se transforme esencialmente el conjunto de virus informáticos (virus, gusanos, caballos de Troya y otros códigos maliciosos) que, en algunos años, se han convertido en auténticos programas informáticos dotados de una panoplia de funcionalidades específicas.

Esta nueva generación de virus, que conviene bautizar ya con el nombre de «soporte lógico malicioso» (*malware*), ha avanzado tecnológicamente de tal modo que plantea hoy en día y suscitará en un próximo futuro una amenaza inédita, si se compara con las que han prevalecido hasta el momento.

**Funcionalidades virales utilizadas**

Para comprender lo que ocurre, conviene describir algunas funcionalidades virales cada vez más frecuentes:

- Telecarga e implantación de herramientas de pirateo automatizadas. El soporte lógico malicioso «*HackTool/Scansql.A»* permite, por ejemplo, ejecutar en el computador infectado una herramienta legal y conocida para realizar una búsqueda de contraseñas que autorizan el acceso a servidores MS SQL (*Microsoft structured query language*, lenguaje de búsqueda estructurado Microsoft) utilizando un simple texto de fichero como lista de prueba de contraseñas.

  Si, como ocurre en el 80% de los casos, las contraseñas consisten en nombres o sustantivos comunes corrientes, los resultados de esta búsqueda quedan disponibles automáticamente para el gusano siguiente, un pirata, o un utilizador malintencionado.

- Toma de control a distancia.

  Los caballos de Troya del tipo «*W32.Sobig»,* permiten apoderarse a distancia del control de un computador y teleejecutar cualquier programa u operación.

- Recuperación y envío automático de memorias tampón de teclado mediante SMTP (protocolo de transferencia de correo simple) o FTP (protocolo de transferencia de ficheros).

  Los gusanos y/o caballos de Troya del tipo «*W32/lovgate»* son muy significativos, debido a su evolución técnica y a la multiplicidad de procesos que desencadenan.

  En efecto, este tipo de virus reagrupa por primera vez todas las funcionalidades descritas anteriormente, que se combinan, además, con la apertura de una puerta trasera (*backdoor*), lo cual permite volver a contaminar el computador atacado después de que se erradique el virus. Asimismo, el modo de compresión de este tipo de virus hace posible ejecutarlo directamente incluso en el momento de la previsualización en el programa de mensajería y ello sin necesidad de decompresión previa.

- Creación de un servidor SMTP específico, especializado en la difusión viral a partir de cada computador contaminado.

- Creación continua de dominios en servidores distantes.

- Recuperación del conjunto de direcciones de correo electrónico en un computador, a fin de alimentar al propio servidor SMTP.

- Ataque por denegación de servicio de los servidores de mensajería y explotación prácticamente instantánea de los fallos de seguridad existentes.

- Recuperación de direcciones IP (protocolo internet) de los computadores, conectándose al proveedor de acceso a través de direcciones de mensajería.

- Modificación de la firma automática en el programa de mensajería, con el fin de garantizar su difusión en el momento de enviar un correo electrónico, instalar desvíos en la lista de favoritos del navegador de internet, añadir botones en la barra de herramientas o modificar la página de arranque, con el fin de proceder a ejecutar automáticamente una vez abierto el navegador.

Entre otros gusanos el «*Js/Fortnight*» utiliza este método para propagarse y sobre todo para volver a contaminar automáticamente los computadores, gracias a la telecarga de su código durante el acceso a internet.

Este carácter cada vez más complejo de las amenazas y de su alcance hace necesario utilizar herramientas de gestión complicadas, por ejemplo, bases SQL, con el propósito exclusivo de gestionar las alertas generadas por los virus.

Se asiste igualmente a un problema sumamente inquietante, que es el hecho de que los sistemas de explotación sean cada vez más conocidos y que la «comunidad agresora» descubre incesantemente nuevos fallos, que explota inmediatamente obedeciendo a sus propios motivos.

**Conclusiones**

La seguridad de las empresas ante los virus informáticos es un problema urgente y cada vez más crucial, habida cuenta de la evolución de la velocidad de propagación de los virus que, obedece, a su vez, a la evolución de su naturaleza desde los años 90.

A principios del decenio de 1990 el tiempo de reacción frente a un virus de fichero se medía en meses, mientras que a fines de esa década era cuestión de horas y hoy de minutos. Huelga decir que en un futuro próximo, cuando aparezcan las amenazas instantáneas, los códigos maliciosos causarán sus efectos deletéreos en unos cuantos segundos.

Es posible prever medidas destructoras como la reprogramación automática de la *bios* durante el cierre de una sesión, el desplazamiento de los sectores de arranque de los discos duros, el formateo automático, la transformación generalizada en virus de todos los programas ejecutables mediante sobregrabación, o el cambio generalizado de los perfiles de usuario en redes, etc.

Estas posibilidades técnicas ya existen, pero con los actuales lenguajes de programación resulta fácil detectarlas en el momento de su implantación. Asimismo, hay que pensar en la amenaza que supondría la elaboración de un lenguaje específico y de su compilador asociado, puesto que dicha elaboración ya es posible.

La gestión del riesgo viral es cada vez más compleja y los nuevos virus informáticos hacen necesario proceder a protecciones sucesivas y cada vez más numerosas, incluso en el plano del sistema de explotación, que deberá autoprotegerse. El hecho de que Windows XP disponga hoy de su propio cortafuegos al nivel de puesto de trabajo es sintomático de la tendencia mencionada.

Garantizar la seguridad mundial de las redes y las empresas ante los virus informáticos de todo tipo seguirá siendo de la incumbencia de auténticos especialistas, debido a la necesidad de seguir paso a paso las «novedades», a la evolución técnica constante de los programas maliciosos y a la imaginación extraordinaria de los autores de los programas maliciosos.

## 3.2 Técnicas de evasión y de inserción

Cuanto más se generalizan los sistemas de detección de intrusos (SDI), más ingenio desarrollan los piratas para crear nuevos métodos que permitan detectar los detectores. Estas técnicas, utilizadas para evitar que los SDI (véase el punto 2.6) lancen una señal de alarma, se pueden clasificar en dos categorías.

### 3.2.1 Técnicas de evasión

Su objetivo es disimular la cadena de ataque, de forma que sea interpretada correctamente por el sistema atacado, pero no por los SDI.

El servidor web atacado suprime automáticamente los caracteres sobrantes, mientras que el SDI percibe una secuencia diferente y no «hace sonar» la alarma. Algunos SDI pueden detectar este tipo de técnica de evasión, pero no lo hacen de forma sistemática, por lo que constituye un criterio a verificar cuando se realiza una validación técnica.

Hay técnicas de evasión más avanzadas que requieren códigos polimorfos.

### 3.2.2 Técnicas de inserción

A diferencia de los métodos de evasión, estas técnicas consisten en incorporar a la firma secuencias de caracteres que serán descodificadas por el SDI, pero no por el sistema atacado. Un método frecuente consiste en recortar la firma e insertar en ella otros fragmentos que contengan un error a nivel de la suma de control del encabezamiento TCP.

Son pocos los SDI disponibles en el mercado que realizan controles en este campo, principalmente por motivos de rendimiento, por lo que la secuencia parásita se integrará a la cadena de ataque. Por el contrario, en lo que respecta al objetivo, el fragmento integrado será automáticamente suprimido por la pila TCP/IP, que efectúa los controles necesarios de las sumas de control.

## 3.3 Denegación de servicio

### 3.3.1 Denial of service (DoS)

El ataque de denegación de servicio (DoS) constituye una preocupación corriente y recurrente para la infraestructura de seguridad del mundo de las redes. Al impedir los accesos entrantes y salientes de internet, estos ataques pueden sembrar el caos en la capacidad de una empresa para realizar sus operaciones en línea, y en sus relaciones con sus clientes y accionistas. Un simple paro de unas horas de los sistemas de información puede provocar daños incalculables para la reputación de una empresa y minar la fidelidad de sus clientes.

Los ataques DoS tradicionales tienen como propósito acabar con un computador o una red, saturándolos con un volumen elevado de flujo de la red, mediante los paquetes de datos TPC (*transmission control protocol*), UDP (*user datagram protocol*) o ICMP (*internet control message protocol*).

En sí, estos paquetes parecen inofensivos, lo que facilita aún más su paso subrepticio por los cortafuegos y encaminadores de una empresa. Además, no son objeto de los controles necesarios que sigue normalmente cada paquete al pasar camuflados en tráfico lícito o bien procedente del proveedor de equipos.

### 3.3.2 Distributed denial of service (DDoS)

Los ataques DDoS, que constituyen una versión perfeccionada del ataque DoS, son cada vez más utilizados por los piratas.

El DDoS usa numerosas máquinas conectadas a internet y una serie impresionante de sistemas coordinados que lanzan un torrente de ataques distribuidos sobre un único objetivo. Esta operación se realiza cargando un programa informático en máquinas coordinadas situadas en distintas redes de empresas o instituciones públicas.

Los piratas prefieren las redes de universidades para lanzar ataques DDoS, ya que en estos sitios las aplicaciones están considerablemente repartidas. Una vez que el programa informático se halla instalado en cientos de máquinas, el atacante puede activarlas a distancia.

# 4 Principio de seguridad de las redes

## 4.1 Organización

En una administración/empresa, la seguridad debe estar repartida entre el servicio del RSSI (Responsable de la Seguridad de los Sistemas de Información) y el servicio de seguridad de la producción o SOC (*security operation centre*).

El servicio del RSSI debe depender de una dirección general y definir una política de seguridad adaptada a las necesidades, las tareas y los objetivos de la empresa/administración.

El RSSI debe hacer que el tema de las redes inalámbricas sea parte de las actividades de sensibilización de los usuarios respecto a la seguridad, para explicarles el peligro que representan las redes inalámbricas, a fin de que notifiquen como incidente al servicio de seguridad toda conexión inalámbrica realizada sin autenticación.

En general, debe introducir la problemática de las redes inalámbricas a su política de seguridad y procedimientos. Cabe señalar que la Norma ISO 17799 hace caso omiso de la existencia de las redes inalámbricas. (Véase el Capítulo 5.)

El servicio de seguridad de la producción (SOC) debe situarse en el marco de la dirección informática, del mismo modo que el servicio informático, que gestiona los servidores centrales, o el servicio ofimático, que gestiona los microcomputadores y los servidores ofimáticos.

El SOC, por una parte, gestiona los elementos del sistema de información, cuyo objetivo principal es garantizar la seguridad y, por otra, aporta la visión global de la seguridad en el conjunto del sistema de información (el terminal de acceso inalámbrico siempre se sitúa en el perímetro de la red; en consecuencia, el SOC debe gestionarlo, al igual que todos los periféricos situados en el perímetro de la red). Estas funciones centralizadas derivan sobre todo del análisis y la relación entre el registro diario de los acontecimientos y la detección de intrusiones.

Estos elementos del sistema de información, cuyo objetivo básico es garantizar la seguridad, están integrados ante todo por todos los medios de interconexión con el exterior, que se sitúan en el perímetro de la empresa/administración con acceso a internet, la VPN (*virtual private network*) para los accesos a distancia, Extranet, plataformas de comercio electrónico, etc. Ha de existir un servicio especializado y orientado a la seguridad que se encargue de gestionar estos equipos de manera operacional. Lo mismo sucede en el caso de la autenticación de usuarios, por ejemplo, en el marco de los accesos a distancia o a internet.

## 4.2 Búsqueda de la fuente de un incidente de seguridad

El control del funcionamiento (*monitoring*) del conjunto de los elementos que constituyen el sistema de información reviste esencial importancia en todas las fases de la búsqueda de un incidente. Este seguimiento tiene por objeto vigilar la actividad (no sólo en la red, sino también en los elementos del sistema de información) que realiza una persona malintencionada, averiguar si otras personas malintencionadas se sirven de los mismos puntos vulnerables y llegar a una visión de conjunto del perímetro de los incidentes.

Los elementos que han de vigilarse son los intercambios efectuados en las redes (fecha y hora de las actividades, volumen de datos intercambiados, direcciones de origen y de destino) y el funcionamiento de los elementos del sistema de información (carga CPU y/o carga de memoria en el servidor, modificación de un programa binario, incorporación y/o destrucción de datos en un servidor, etc.).

Los elementos de control de la red (*network monitoring*) deben instalarse en lugares prefijados dentro de la red. Se da por sentado que estos elementos no se han visto amenazados, sobre todo en lo que concierne a la integridad de los ficheros de grabación. Los elementos de control del funcionamiento de un determinado elemento se basan principalmente en programas de control de la carga (Patrol, HP Open View, etc.) o en ficheros de grabación (ficheros de registros cronológicos).

En esta fase, es esencial que los relojes de los elementos del sistema de información estén sincronizados a fin de facilitar la tarea de correlación entre los acontecimientos. Una técnica de control del sistema de información consiste en efectuar un amplio control para identificar el perímetro que ha de cubrirse y, a continuación, precisar el control de los elementos que guardan realmente relación con el incidente considerado (análisis de un determinado servicio o una cuenta de usuario específica, etc.).

**Reconstitución del sistema de información**

El objetivo de esta fase es reconstruir el sistema de información a fin de poner fin al incidente e impedir que se reproduzca. Esta fase no puede iniciarse hasta que no se haya analizado completamente el incidente: identificación de las personas malintencionadas, así como de su modus operandi (caballos de Troya, cuentas de usuarios, etc.).

En función del nivel de privilegio que haya obtenido la persona malintencionada, será posible deducir sus maniobras. Además, en función de la ubicación del elemento que se haya puesto en peligro en la red (lugar no sólo en la topología de la red, sino también en el ámbito de confianza en los elementos), puede determinarse qué otros elementos deberán tenerse en cuenta en el perímetro de reconstrucción.

Una vez identificados el modus operandi, la reconstrucción de los elementos se basa únicamente en las vulnerabilidades que han explotado las personas malintencionadas. En caso que subsistan dudas, se recomienda reconstituir los elementos a partir de los soportes de origen (CD-ROM del editor). No siempre resulta recomendable utilizar copias de seguridad. De hecho, es preciso estar seguro de que el incidente haya tenido lugar después de haberse efectuado la copia de seguridad utilizada, puesto que, en caso contrario, se reproduciría el caballo de Troya o la misma vulnerabilidad. Una vez reconstruidos los elementos, es preciso reforzar la seguridad del elemento que se haya puesto en peligro (*hardening*) y corregir los puntos vulnerables.

Es evidente que el procedimiento para poner de nuevo en servicio los elementos afectados no se lleva a cabo directamente en la red. Hasta que no reconstituya íntegramente el elemento, no podrá reactivarse y conectarse a la red interna de la empresa. Numerosas empresas aumentan su nivel de seguridad para responder a acontecimientos que consideran importantes y puedan producirse. En esta fase es posible adaptar nuevos métodos de seguridad; por ejemplo, modificar la topología de la red e instalar listas de control de acceso, reforzar los controles de integridad, actualizar la base de usuarios, definir una política de seguridad y sensibilizar a los usuarios. Si bien es evidente que estas medidas no deben adoptarse en los días que sigan al incidente, es esencial que el RSSI formalice un plan de medidas para varios meses e incluso años.

**La formalización**

Las medidas que se han llevado a cabo en el marco del proceso de respuesta en caso de incidente deben formalizarse y recogerse en un informe que permita efectuar ulteriormente un análisis. Esta documentación permite rehacer con más calma, las mismas pruebas, determinar si se han podido borrar pruebas técnicas por parte de los investigadores en caso de manipulación incorrecta, formular de nuevo posibles conclusiones y aportar las pruebas técnicas del incidente (e incluso del sospechoso) si se entabla un procedimiento de sanción (judicial o administrativa). Estos casos pueden durar incluso meses y resulta muy difícil recordar todas las acciones si éstas no se han formalizado desde el principio, de ahí que la fase de formalización revista suma importancia.

Es preciso tener presente en todo momento que el atacante puede haber infectado la red con numerosos elementos e instalado varios detectores para determinar si su actividad ha sido identificada. Los intercambios electrónicos, las pruebas técnicas recopiladas, los informes sobre los incidentes, etc., deben registrarse fuera del sistema de información. De hecho, no es inhabitual que el atacante se mantenga informado gracias a estos elementos de información y modifique ciertos datos o destruya determinadas pruebas técnicas, pero a largo plazo estas informaciones permiten proponer nuevas medidas de seguridad en lo que respecta al sistema de información y aumentar el nivel de seguridad global de la empresa.

**Conclusión**

La búsqueda de pruebas técnicas de un incidente no es tarea fácil. Únicamente las acciones precisas, llevadas a cabo siguiendo una metodología como la descrita anteriormente, hacen posible iniciar un procedimiento riguroso cuyo objeto es que el atacante, desestabilizado por el efecto de sorpresa inicial, no siga sorprendiendo y que los incidentes de seguridad dejen de representar una amenaza de catástrofe.

## 4.3 Soluciones integradas para proteger el ciberespacio

La seguridad es un requisito indispensable en todos los ámbitos de la sociedad de la información y las nuevas tecnologías. Cualquier actor de la cadena de la información debe ser consciente del problema que suscita la seguridad y participar en la aplicación de **soluciones integradas**.

En las soluciones mundiales encaminadas a proteger el ciberespacio (sociedad de la información) habrá que tomar en consideración todos los aspectos del análisis global de riesgos, con el fin de integrar al menor costo posible soluciones optimizadas y sistemas evolucionados para garantizar la seguridad:


**1) Analizar: asesoramiento y prestaciones en materia de gestión de riesgos de seguridad**

- Análisis y evaluación de riesgos (informáticos, jurídicos, sociales, etc.).
- Auditorías técnicas y funcionales de seguridad (ISO, UIT, etc.).
- Pruebas de vulnerabilidad e intrusión/identificación de fallos.
- Organización de la gestión de la seguridad.
- Política de seguridad y planes directivos, incluida el método tradicional que constituye la seguridad activa.
- Formación y sensibilización en materia de seguridad.
- Ayuda informática, seguimiento de actividades y gestión de crisis.

**2) Seleccionar y desplegar: establecimiento y despliegue de la seguridad**

Seleccionar: Validar la arquitectura, evaluar los controladores, seleccionar las tecnologías, proporcionar las soluciones.

Desplegar: Establecer, integrar soluciones, garantizar la gestión del proyecto, poner en funcionamiento.

En resumen:

- Proporcionar soluciones integradas y/o adaptadas para:
  - garantizar la seguridad de las redes e infraestructuras desplegadas;
  - garantizar la conectividad con seguridad de los accesos nómadas;
  - garantizar la seguridad de la gestión de las identidades y los datos esenciales;
  - garantizar la confianza digital en lo que concierne a las transacciones.
- Construir arquitecturas permanentes y evolutivas aseguradas.
- Garantizar un control y una gestión rigurosos de proyectos.
- Desplegar los sistemas de seguridad desde el punto de vista técnico y humano.

**3) Controlar y garantizar la permanencia: administración global de la seguridad**

Controlar: administrar, supervisar, explotar, intervenir, modificar los sistemas desplegados (incorporación de nuevas tecnologías).

Garantizar la permanencia: mantener, controlar y garantizar la vigilancia activa y poner al día y adaptar la política de seguridad.

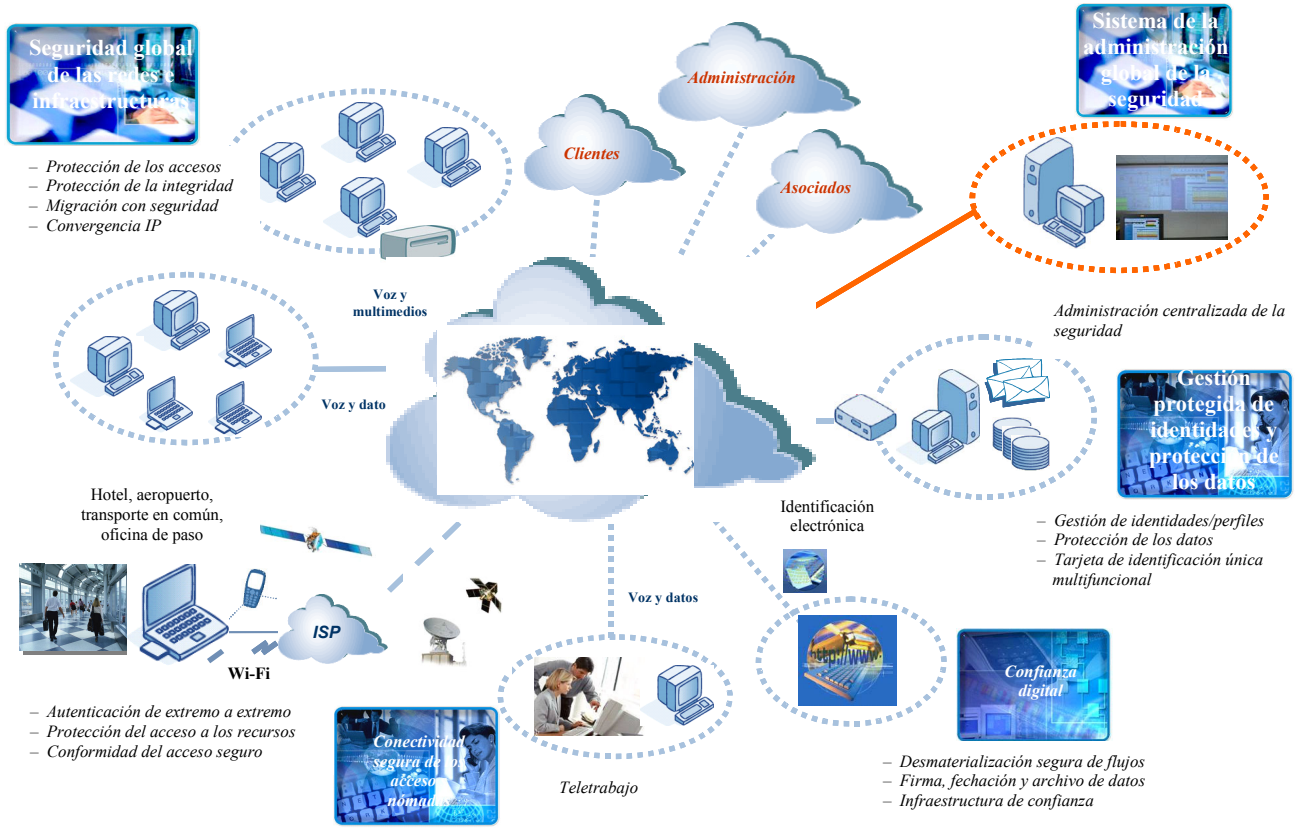
En resumen: una asistencia/respaldo y supervisión activos y permanentes

- Teleadministración
  - Soluciones de seguridad (IATS) y teleadministración protegida.

- Polo de lucha contra virus
  - Vigilancia proactiva y acciones de aplicación preventivas/reactivas.
- Gestión de la seguridad de los puestos de trabajo fijos o nómadas
  - Gestión de los derechos de acceso y control de la conformidad del nivel de seguridad.
- Albergue asegurado
  - Estructura y fechación
  - Infraestructuras de confianza (IGC).

En la siguiente figura se señalan de manera no exhaustiva los diferentes componentes de las soluciones de seguridad integradas.

**Figura 10 – Soluciones integradas de seguridad**




## 5 Aspectos jurídicos

Los rápidos avances de las técnicas de la información tienen repercusiones directas en todos los sectores de la sociedad moderna. Al permitir el almacenamiento y la transmisión de todo tipo de datos, independientemente de la distancia, la integración de los sistemas de telecomunicaciones e información abre un amplísimo horizonte de nuevas posibilidades. Estos avances fueron impulsados por la aparición de las redes informáticas y las autopistas de la información, sobre todo de internet, que han permitido a prácticamente cualquier persona acceder a la totalidad de los servicios de información electrónica desde cualquier lugar del planeta. Cuando se conectan a los servicios de comunicación e información, los usuarios crean una suerte de espacio común, denominado ciberespacio, que puede ser utilizado para fines legítimos pero que también puede dar lugar a abusos. Cuando se comete una infracción en este ciberespacio, lo que se vulnera es la

integridad, la disponibilidad y la confidencialidad de los sistemas informáticos y redes de telecomunicaciones, a no ser que se trate de la utilización de estas redes y sus servicios con el fin de cometer infracciones clásicas. El carácter internacional de estas infracciones –por ejemplo, las cometidas a través de internet– choca con la territorialidad de las instituciones de represión nacionales. Los delincuentes están cada vez más alejados de los lugares que sufren las consecuencias de sus actos. Ahora bien, por lo general, las leyes internas sólo se aplican a un territorio determinado. Por otro lado, las soluciones a los problemas que se plantean son competencia del derecho internacional, lo que exige la adopción de instrumentos jurídicos internacionales adecuados. Por consiguiente, el derecho penal debe seguir el ritmo de estas evoluciones técnicas, que ofrecen medios extremadamente perfeccionados para hacer uso indebido de los servicios del ciberespacio, y perjudican a intereses legítimos. Puesto que las redes informáticas no tienen en cuenta las fronteras, es necesario que se realice un esfuerzo internacional concertado para hacer frente a tales abusos.

Por el contrario, en ciertos sectores de las actividades humanas, se intenta «proteger» los lugares públicos contra perturbaciones ocasionadas por la utilización de las TIC.

Así por ejemplo, en Francia se votó una ley en julio de 2001 para autorizar la interferencia de las comunicaciones móviles en salas de espectáculo, cines y prisiones. Por motivos de seguridad, esta ley comenzó a aplicarse en las prisiones a partir de 2003. En octubre de 2004 el Ministro de Telecomunicaciones firmó un decreto en virtud del cual se autorizaba la adopción de esta medida en las salas de espectáculo y cines.

En este sentido, es posible recurrir a tres tecnologías: En efecto, cabe la posibilidad de aplicar tres soluciones para bloquear las comunicaciones móviles y la más radical está representada por los dispositivos denominados «interferentes», que son emisores que utilizan constantemente las frecuencias de las conexiones telefónicas. La menos agresiva de estas tecnologías utiliza «repetidores» y permite hacer una llamada de urgencia a partir de un teléfono móvil pero hace imposible la llegada de llamadas entrantes. Esta solución es la que debe de utilizarse en principio en el caso de los cines y las salas de espectáculo.

Entre ambos extremos, hay que mencionar los dispositivos interferentes propiamente dichos. Estos sistemas bloquean la comunicación entre un teléfono móvil y los relés del operador, gracias a la emisión de una señal parásita, con independencia del sentido de la comunicación, pero ello únicamente cuando se detecta la correspondiente llamada (estos sistemas son aquellos con los cuales se han equipado las prisiones).

## 5.1 Directrices de las Naciones Unidas y la OCDE

Las Naciones Unidas muestran interés por el problema de la delincuencia informática desde 1994, año en que publicó un Manual sobre la prevención y el control informáticos en lo que concierne a este tipo de delito. Este Manual fue actualizado en 1997. Desde entonces, la Asamblea de las Naciones Unidas, al igual que la OCDE, ha adoptado guías sobre la seguridad de los sistemas de información y comunicación. Los principios establecidos son los siguientes:

1) Concienciación

   Las partes interesadas deben ser conscientes de la necesidad de contar con sistemas de información y redes seguros, y de qué pueden hacer para la seguridad.

2) Responsabilidad

   Las partes interesadas son responsables de la seguridad de los sistemas y redes de información.

3) Respuesta

   Las partes interesadas deben actuar de manera oportuna y cooperativa para prevenir, detectar y responder a incidentes que afecten a la seguridad.

4) Ética

   Las partes interesadas deben respetar los intereses legítimos de las demás partes interesadas.

5) Democracia

La seguridad de los sistemas y redes de información debe ser compatible con los valores esenciales de una sociedad democrática.

6) Evaluación de los riesgos

Las partes interesadas deben llevar a cabo evaluaciones de los riesgos.

7) Diseño e implementación de la seguridad

Las partes interesadas deben incorporar la seguridad como un elemento esencial de los sistemas y redes de información.

8) Gestión de la seguridad

Las partes interesadas deben adoptar una visión integral de la gestión de la seguridad.

9) Reevaluación

Las partes interesadas deben revisar y reevaluar la seguridad de sus sistemas y redes de información y hacer las modificaciones pertinentes en sus políticas, prácticas, medidas y procedimientos de seguridad.

En agosto de 2002, la OCDE publicó un Informe titulado «Directrices de la OCDE sobre la seguridad de los sistemas y las redes de información hacia una cultura de la seguridad». En las directrices de 2002, que atañen a todos los actores de la sociedad de la información, se indica que es preciso comprender mejor los problemas de seguridad, e incluso desarrollar una «cultura de la seguridad». Estas directrices, al dirigirse a todas las partes integrantes de la nueva sociedad de la información, muestran que es necesario tomar mayor conciencia y comprender mejor las cuestiones relativas a la seguridad; el objetivo es desarrollar una «cultura de la seguridad». De hecho, la seguridad debería ocupar un lugar central en el desarrollo de los sistemas y las redes. Es preciso adoptar nuevas formas de pensamiento y comportamiento en cuanto a la utilización de sistemas y redes de información, y en el marco de los intercambios que se producen. En estas directrices se fundan los esfuerzos destinados a instaurar una cultura de la seguridad en el conjunto de la sociedad.

Con motivo del «Foro Mundial de la OCDE» sobre la seguridad de los sistemas de información y las redes, que se celebró los días 13 y 14 de octubre de 2003 en Oslo (Noruega), se hizo un balance del primer año de aplicación de las directrices de la OCDE publicadas en 2002.

En noviembre de 2003, la OCDE publicó otro Informe, titulado «Directrices sobre la protección de la vida privada y las mejores prácticas», que abarca todos los trabajos realizados con objeto de garantizar una política eficaz de protección del usuario privado en línea.

La credibilidad del comercio electrónico depende de la fiabilidad de las infraestructuras y los servicios, de la seguridad y la confidencialidad de las operaciones, así como de la protección de la información confidencial. El Grupo de Trabajo de la OCDE sobre la seguridad de la información y la vida privada promueve la adopción de un enfoque mundial y coordinado en la elaboración de políticas destinadas a crear una cultura de seguridad en línea. Este Informe ofrece un conjunto de métodos de reglamentación y autorregulación que incluyen soluciones jurídicas, técnicas y educativas en función del contexto cultural y social del entorno. Este Informe, que pone de relieve la necesidad de que todos los actores de este ámbito cooperen estrechamente entre sí, está estructurado de la siguiente manera:

**Parte I**

Resumen de la labor realizada por el Grupo de Trabajo sobre la seguridad de la información y la protección de la vida privada de la OCDE.

**Parte II**

Se muestran las directrices basadas en la labor descrita en la Parte I.

**Parte III**

En ella se incluyen todos los documentos presentados en la Parte I, y más precisamente:

- las directrices sobre la protección de la vida privada y la información acerca de los flujos transfronterizos;
- la declaración ministerial sobre la protección de la vida privada en las redes mundiales;

el inventario de los instrumentos y mecanismos que contribuyen a implantar y aplicar las directrices de la OCDE sobre la vida privada en el marco de las redes mundiales.
(www.oecd.org/documentprint/0,2744.fr_2649_34255_19216241_1_1_1_1_,00.html)

El 1 de diciembre de 2003, la OCDE creó un sitio web titulado «Cultura de la Seguridad» encaminado a «luchar» contra los ataques que afectan a la seguridad de las redes y los sistemas de información. (Véase: www.oecd.org/department/0,2688, en_2649_34255_1_1_1_1,00.html)

NOTA 1 – Todos los documentos de la OCDE anteriormente mencionados pueden consultarse en la siguiente dirección: www.oecd.org/COMNET/STI/IccpSecu.nst?OpenDatabase

NOTA 2 – La 26ª. Conferencia Internacional sobre la protección de la información y la vida privada se celebrará del 14 al 16 de septiembre de 2004 en Varsovia (Polonia).

NOTA 3 – El 22/10/2004 se estableció un grupo especial sobre la lucha contra el correo basura en el que participaban los 30 Estados Miembros de la OCDE, así como representantes de la empresa privada, la sociedad civil y las organizaciones internacionales, incluida la UIT. Los trabajos de este grupo durarán dos años.

## 5.2 Consejo de Europa

El Consejo de Europa se ha propuesto aceptar el desafío planteado teniendo en cuenta la necesidad de hacer respetar los derechos humanos en la nueva sociedad de la información, fijando los principios de una cooperación internacional con arreglo a los instrumentos internacionales pertinentes en materia penal, a acuerdos basados en legislaciones uniformes o recíprocas en la mayor medida posible con fines de investigación o de procedimientos relativos a infracciones penales vinculadas a sistemas y datos informáticos o para recabar pruebas de una infracción penal por medios electrónicos. Esta investigación ha dado lugar a la firma internacional de un Convenio sobre la Ciberdelincuencia.

*Convenio sobre la Ciberdelincuencia (Consejo de Europa)*

En noviembre de 1996, el Comité Europeo de Problemas Penales decidió constituir un comité de expertos. Como resultado de las tareas de este órgano, se redactó un Convenio sobre la Ciberdelincuencia, que fue sometido a aprobación durante la Conferencia Internacional sobre la Ciberdelincuencia, celebrada el 23 de noviembre de 2001 en Budapest. Este Convenio mundial fue firmado por la mayoría de los países europeos, incluidos algunos países de Europa del Este y de la CEI, así como otros Estados del mundo (Estados Unidos, Japón, Sudáfrica y Canadá).

Básicamente, los objetivos de este Convenio son los siguientes:

1) Armonizar los aspectos de las infracciones que guardan relación con el derecho penal material de cada país y las disposiciones comerciales en materia de ciberdelincuencia.
2) Conferir al derecho penal procesal de cada país los poderes necesarios para la instrucción y persecución de infracciones de esta índole, así como de otras infracciones cometidas mediante un sistema informático o en cuyo marco las pruebas existentes se encuentren en formato electrónico.
3) Establecer un régimen rápido y eficaz de colaboración internacional.

Los principales asuntos que se tratan en este Convenio son:

- Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos:
  - Acceso ilícito
  - Interceptación ilícita
  - Interferencia en los datos y en el sistema

  - Abuso de los dispositivos.
- Delitos informáticos:
  - Falsificación informática
  - Fraude informático.
- Delitos relacionados con el contenido
- Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines
- Otras formas de responsabilidad y de sanciones:
  - Tentativa y complicidad
  - Responsabilidad de las personas jurídicas
  - Sanciones y medidas.

El Convenio consta de los siguientes capítulos:

- Derecho procesal (derecho penal material, derecho procesal y competencias)
- Cooperación internacional:
  - Principios generales relativos a la cooperación internacional, a la extradición y a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables
  - Disposiciones especiales.

El Consejo de Europa tiene presente que la mundialización entraña riesgos que pueden conducir a la exclusión y el aumento de las desigualdades, sobre todo por motivos raciales y étnicos. Mientras que los avances tecnológicos, económicos y comerciales acercan a los pueblos del mundo entero, la discriminación racial, la xenofobia y otras formas de intolerancia siguen presentes en nuestras sociedades.

Por ello, el 7 de noviembre de 2002, el Consejo de Europa adoptó un Protocolo Adicional al Convenio sobre la Ciberdelincuencia relativo a la incriminación de actos de carácter racista y xenófobo cometidos por medio de sistemas informáticos.

Los textos de los dos documentos citados se pueden consultar en los sitios:
http://conventions.coe.int/Treaty/FR/Reports/html/185.htm y
http://conventions.coe.int/Treaty/FR/Reports/html/189.htm

## 5.3 Unión Europea

En la reunión del Consejo de la Unión Europea (UE) celebrada en Lisboa en junio de 2000 se adoptó un Plan de Acción denominado e-Europe 2002, cuyo principal objetivo era lograr la conectividad de todos a internet con el fin de que en los Estados Miembros se produjera un crecimiento económico considerable.

Los principales resultados de la aplicación de e-Europe 2002 son los siguientes:

- la penetración de internet en los hogares se ha doblado;
- se ha establecido un marco de trabajo europeo para las telecomunicaciones;
- se ha reducido el precio del acceso a internet (http://europa.eu-int/e-europe).

En vista de los resultados de e-Europe 2002, el «Barcelona European Council» pidió a la UE que pusiera en marcha un nuevo Plan: e-Europe 2005. Este Plan de Acción incluye cuatro prioridades, a saber:

- modernizar los servicios públicos en línea: gobierno electrónico, cibereducación y cibersalud;
- crear un entorno dinámico para el negocio electrónico;
- ofrecer acceso de banda ancha a precios de competencia;
- establecer una infraestructura de información segura.

Para garantizar la seguridad de la información, la UE ha aplicado una estrategia basada en la seguridad de las redes de comunicaciones [Network Information Society COM/2001 398 del 6 de junio de 2001], que ha sido objeto de la Resolución del 28 de enero del 2002 (http://register.consillium.eu.int/pdf/en/01/st15/1512enI.pdf) y, más recientemente, la Comisión ha propuesto una decisión marco general en la que se contemplan los ataques contra los sistemas de información (http://europa.eu.int/comm/dgs/justice-home/index-en.htm), COM(2002)173 final de 19 de abril de 2002.

Se proponen las siguientes medidas.

- **Cyber security task force (CSTF)**. El CSTF debería empezar a realizar actividades a fines de 2003. Sobre la base de las propuestas de la Comisión Europea (CE), el Consejo y el Parlamento habrán de adoptar lo antes posible una base jurídica en la que se tome en consideración el carácter «cruzado» de las redes y de la seguridad de la información. El CSTF habrá de convertirse en un centro de competencia sobre cuestiones de seguridad. Asimismo, los Estados Miembros habrán de idear, en colaboración con la CE un sistema de alerta europea en materia de informática.
- **Cultura de la seguridad**. A finales de 2005 deberá instaurarse una «cultura de la seguridad» en lo que respecta tanto al desarrollo como a la implantación de productos de la información y la comunicación (informe intermedio previsto para finales de 2003).
- **Comunicaciones seguras entre los distintos servicios públicos**. A finales de 2003 la Comisión y los Estados Miembros deberán estudiar la posibilidad de establecer un entorno seguro para las comunicaciones, que permita intercambiar informaciones gubernamentales confidenciales.

**e-Europe 2005**

En la reunión del Consejo Europeo celebrada en Barcelona en 2002 se invitó a la Comisión a que elaborara un Plan de Acción e-Europe basado en: «la implantación y la utilización generalizada en la Unión a partir de 2005 de una red de banda ancha, así como la definición del protocolo internet IPv6 [----], relativo a la **seguridad de las redes y las informaciones** [----] y el comercio electrónico».

En el punto 3.1.3 del documento de la UE titulado «e-Europe 2005: Una sociedad de la información para todos» se aborda el tema de la infraestructura segura de la información.

La Unión Europea ha adoptado ya una estrategia global que se basa en las comunicaciones y tiene que ver con la seguridad de las redes[1], la ciberdelincuencia[2] y la directiva actual[3] y futura relativa a la protección de datos en el marco de las comunicaciones electrónicas. La estrategia propuesta fue aprobada y desarrollada mediante la Resolución del Consejo del 28 de enero de 2002[4] y la reciente propuesta de decisión marco del Consejo relativa a los ataques destinados a los sistemas de información[5], presentada por la Comisión.

Las actividades de investigación comunitaria en el ámbito de la seguridad seguirán realizándose durante el sexto programa marco. Las prioridades serán las infraestructuras de red y de información fiables, en las que se prestará especial atención a las tecnologías incipientes (por ejemplo, las arquitecturas inalámbricas, las de banda ancha, la inteligencia ambiente, etc.) y a la identificación de las vulnerabilidades y las interdependencias en las infraestructuras. La investigación comunitaria debería respaldar la normalización para fomentar la utilización de normas abiertas y programas abiertos. Asimismo en las actividades de investigación sobre seguridad debería tenerse en cuenta el «factor humano», por ejemplo en el marco de las normas de seguridad básica y la facilidad de utilización de los sistemas.

---

1 Seguridad de las redes y la información: Propuesta para un enfoque político europeo, COM(2001) 298, de 6 de junio de 2001.

2 Creación de una sociedad de la información más segura, mediante la mejora de la seguridad de las infraestructuras de información y la lucha contra los delitos informáticos – e-Europe 2002, COM(2000) 890, de 22 de enero de 2001.

3 Directiva 97/66/EC del Parlamento Europeo y del Consejo de 15 de diciembre de 1997 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (DA L 24 del 30 de enero de 1998).

4 Véase: http://register.consilium.eu.int/pdf/en/01/st15/15152en1.pdf

5 COM(2002) 173 final del 19 de abril de 2002. Véase: http://europa.eu.int/comm/dgs/justice_home/index_en.htm

Las acciones propuestas para cumplir este mandato son las siguientes:

1) Grupo Especial para la ciberseguridad

   El Consejo y el Parlamento podrán adoptar la base jurídica necesaria en breve plazo, tomando en consideración la dimensión «transpilar» de la seguridad de las redes y la información. Sería necesario que los Estados Miembros y el sector privado respalden las actividades del Grupo Especial, que debería constituir un centro de competencias sobre cuestiones de seguridad, por ejemplo, para perfeccionar junto con los Estados Miembros el plan de un sistema europeo de alerta informática, facilitar las discusiones «transpilares» y mejorar la cooperación transfronteriza.

2) Cultura de seguridad

   A finales de 2005 habría de quedar instaurada una «cultura de seguridad» en el ámbito de la concepción y la aplicación de productos de información y comunicación. El sector privado debería elaborar un manual de buenas prácticas y normas, y promover su aplicación coherente. La Comisión prevé respaldar proyectos y velará por que los usuarios conozcan mejor los riegos para la seguridad. A finales de 2003 se publicará un Informe intermedio sobre los progresos realizados y, a fines de 2005, se publicará una evaluación final.

3) Comunicaciones seguras entre los servicios públicos

   Para finales de 2003, la Comisión y los Estados Miembros habrán estudiado la posibilidad de crear un entorno de comunicación seguro para intercambiar informaciones confidenciales del sector público.

NOTA – En 2004 la Comisión Europea estableció la Agencia Europea de Seguridad de las Redes y de la Información (**ENISA**). La ENISA es un Centro de Excelencia europeo en materia de seguridad y el núcleo de un «diálogo» entre los asociados públicos y las empresas privadas que tiene por objeto definir en la Unión Europea las directrices y las mejores prácticas en lo que concierne a la seguridad.

## 5.4 Estrategia nacional para garantizar la seguridad del ciberespacio (Estados Unidos)

Tras la realización de una serie de estudios encargados por la Casa Blanca sobre la protección contra perturbaciones del funcionamiento de los sistemas de información y la protección de la población, la economía y la seguridad nacionales de Estados Unidos, se publicaron los correspondientes Informes en febrero de 2003.

La Estrategia nacional para garantizar la seguridad del ciberespacio es parte del esfuerzo global para proteger a los Estados Unidos a este respecto. Esta Estrategia es un componente de aplicación de la Estrategia nacional de seguridad interna, que complementa la Estrategia nacional de protección física de infraestructuras esenciales y activos clave. El propósito de este documento es alentar y facultar a los estadounidenses para garantizar la seguridad de las partes del ciberespacio que poseen, explotan o controlan, o con las cuales interactúan. La ciberseguridad es una difícil tarea estratégica que hace necesario que toda la sociedad, el gobierno federal, los gobiernos estatales y locales, el sector privado y la población estadounidense desplieguen esfuerzos coordinados y concentrados.

- Objetivos estratégicos

  De conformidad con la Estrategia nacional de seguridad interna (el 25 de noviembre de 2002 se creó el Departamento de Seguridad Interna (DHS)), los objetivos estratégicos de la Estrategia nacional para garantizar la seguridad del ciberespacio son los siguientes:

  – combatir los ataques cibernéticos contra infraestructuras esenciales de Estados Unidos;
  – reducir la vulnerabilidad del país ante los ciberataques;
  – reducir a un mínimo los daños producidos por los ciberataques y los correspondientes plazos de recuperación.

En el Informe sobre la estrategia precitada y tras un capítulo sobre amenazas y vulnerabilidad se expone la política nacional y los principios de orientación. La protección de los sistemas cibernéticos resulta indispensable en cada sector de la economía y la concepción y aplicación de la directiva referente al programa federal que se aprobó en octubre de 2001 se han basado en los siguientes principios:

1) Esfuerzo nacional
2) Protección de la privacidad y las libertades civiles
3) Reglamentación y fuerzas del mercado
4) Rendición de cuentas y responsabilidades
5) Garantía de la flexibilidad
6) Planificación multianual

**Prioridades esenciales respecto a la seguridad del ciberespacio**

La Estrategia nacional para garantizar la seguridad del ciberespacio se basa en cinco prioridades nacionales:

I) Un sistema nacional de respuesta para garantizar la seguridad del ciberespacio
II) Un programa nacional de reducción de amenazas y factores de vulnerabilidad en lo que atañe a la seguridad del ciberespacio
III) Un programa nacional de capacitación y sensibilización en materia de seguridad del ciberespacio
IV) Garantizar la seguridad del ciberespacio gubernamental
V) Cooperación en materia de seguridad nacional y seguridad internacional del ciberespacio

La primera de estas prioridades se centra en mejorar la respuesta de los Estados Unidos ante los ciberincidentes y reducir los daños potenciales de tales eventos. La segunda, tercera y cuarta de las prioridades mencionadas tienen por objeto reducir las amenazas de un ciberataque y la vulnerabilidad de Estados Unidos ante este tipo de ataques. La quinta prioridad consiste en prepararse contra los ciberataques que podrían afectar adversamente a los activos de seguridad nacionales, así como mejorar la gestión internacional de dichos ataques y la respuesta a los mismos.

Para cada prioridad nacional se indican **Acciones y Recomendaciones** y el Apéndice del Informe incluye un resumen de las mismas.

## 5.5 Medidas de seguridad adoptadas por los editores de programas informáticos

Los editores de soporte lógico han dado acceso al «código de fuente» de algunos de sus programas informáticos para reforzar la seguridad a solicitud de las organizaciones gubernamentales o públicas, que solicitan cada vez más «transparencia».

a) Tras el lanzamiento de Windows en 2001, Microsoft decidió en septiembre de 2004 dar acceso a los diferentes programas que constituían su paquete ofimático Office 2003 (tratamiento de texto Word, la hoja de cálculo Excel y la mensajería Outlook) para consultar estos programas. Gracias a esta iniciativa, las organizaciones públicas y gubernamentales podrán informarse más adecuadamente acerca de los mecanismos de almacenamiento de los ficheros y dialogar e intercambiar información en paralelo con los ingenieros de Microsoft: *las administraciones deben atender a una serie de obligaciones jurídicas de archivo a largo plazo*.

   En septiembre de 2004:

   - Una treintena de países, entre los cuales cabe citar China, Australia y España, concluyeron un acuerdo sobre Windows; el Reino Unido fue el primer país en concertar un acuerdo para acceder al código de fuente de Office.
   - En Francia, 30 organizaciones (la mayoría de ellas establecimientos de enseñanza superior) concertaron un acuerdo con Microsoft en el marco del programa de difusión de los códigos de fuente de Windows y Office.

b) Algunos editores de programas informáticos decidieron dar acceso libre y gratuito a los códigos de fuente de sus programas informáticos, una vez comercializados éstos. Éste es el caso de Linux en lo que concierne a su sistema de explotación, así como de otros editores tratándose de ámbitos distintos, por ejemplo, el de servidores de aplicación, portales y paquetes ofimáticos.

# 6 Normas ISO

Más conocida por el nombre de «criterios comunes» la Norma ISO/CEI 15408, que desde 1996 permite certificar los niveles de defensa que facilitan los dispositivos de seguridad de los sistemas de información, «criterios comunes», fue el fruto de la convergencia progresiva entre los TCSEC (*Trusted Computer Systems Evaluation Criteria*) o «Libro Naranja» y los ITSEC (*Information Technology Security Evaluation Criteria*), los cuales a su vez proceden de la fusión de distintos criterios nacionales.

En diciembre de 2000, la ISO/CEI (*International Organization for Standardization*) adoptó la Norma británica BS 7799-1 con la referencia ISO/CEI 17799.

En la Norma ISO/CEI 17799 se considera que numerosos sistemas de información no se diseñan para ser seguros, por lo que la aplicación de medios técnicos de protección tiene efectos limitados y debe recibir el respaldo de una organización apropiada y sus procedimientos.

Por consiguiente, en esta norma se propone un conjunto de reglas o recomendaciones, en las cuales se describen en un sentido muy amplio las mejores prácticas en materia de seguridad de la información. No se trata en modo alguno de limitar el alcance de dicha norma a los dispositivos informáticos, sino más bien de tener en cuenta la información en todas sus formas, como verdadero patrimonio de un organismo.

Estas reglas se engloban en diez temas:

1) **Política de seguridad**. En este capítulo el objetivo consiste en definir las características del documento en el que se exponga la política de seguridad de un organismo, en cuanto a responsabilidad, aprobación, revisión y adaptación.

2) **Organización de la seguridad**. Las reglas de este capítulo abordan la función de los actores de la política de seguridad y, en particular, del comité que se ocupe de un organismo de la estrategia aplicable en este ámbito. Designado directamente por la dirección general, este comité se encarga de definir y llevar un seguimiento de la política de seguridad; su «cerebro» es el RSSI. Los aspectos contractuales relacionados con la seguridad del acceso de terceros al sistema de información se estudian también en este capítulo.

3) **Clasificación y control de los activos**. El objetivo es mantener un nivel de protección adaptado a cada activo del sistema de información, mediante su identificación, clasificación y ubicación a cargo de un «propietario» designado.

4) **Seguridad de los recursos humanos**. Las reglas referentes a este tema están destinadas a reducir el riesgo de error, robo, fraude o utilización inadecuada de los recursos informáticos, mediante la sensibilización de los usuarios sobre los riesgos y las amenazas a que puedan estar expuestas las informaciones.

5) **Seguridad física y seguridad del entorno**. El objetivo de este tema es prevenir los accesos no autorizados, los daños y las interferencias que afectan a las informaciones, en los locales de la empresa.

6) **Explotación y redes**. En este capítulo la finalidad consiste en minimizar los riesgos de avería y sus repercusiones mediante una explotación correcta y segura de los medios de tratamiento, lo que garantiza la integridad y disponibilidad de las informaciones, el procesamiento y las comunicaciones.

7) **Control de acceso**. Las reglas relativas a este tema tienen por finalidad gestionar y controlar los accesos lógicos a las informaciones, garantizar la protección de los sistemas de red y detectar las actividades no autorizadas.

8) **Desarrollo y mantenimiento de los sistemas**. Sobre la base del principio consistente en tener en cuenta la seguridad ya en la fase de redacción del pliego de condiciones, en este capítulo se proponen reglas destinadas a prevenir la pérdida, la modificación o la utilización inadecuada de las informaciones en los sistemas de explotación y los programas informáticos.

9) **Continuidad de servicio**. El objetivo de este tema es incrementar la capacidad del organismo para responder rápidamente a la interrupción de sus actividades fundamentales por causa de averías, incidentes, siniestros o catástrofes.

10) **Conformidad**. En este tema la idea es velar por el respeto de las leyes, las reglamentaciones y los procedimientos establecidos en relación con la política de seguridad, a fin de alcanzar los objetivos que fije la dirección general, y la eficacia de los dispositivos de localización y seguimiento de los procedimientos en vigor, en especial, los boletines de actividades, las auditorias y los registros de las transacciones.

Si bien la Norma ISO/CEI 17799 permitió dar a conocer la Norma BS 7799-1, que se reproduce fielmente, la segunda parte de la norma, cuya referencia es BS 7799-2, se conoce menos, ya que no se ha propuesto aún a la ISO. Ahora bien, se trata de un documento muy interesante, cuya lectura es indispensable para conocer perfectamente el mecanismo destinado a definir la estrategia de la ISO en materia de gestión de la seguridad de la información. En la última versión de la Norma BS 7799-2, que data de septiembre de 2002, se propone armonizar las Normas ISO 9001:2000 (Gestión y garantía de la calidad) e ISO 14001 (Gestión del entorno ambiental), y con arreglo a los principios de la OCDE (véase el Capítulo 4.1). Por ende, se trata de una verdadera referencia de certificación que se utiliza mucho en numerosos países, entre los que cabe señalar Gran Bretaña, Australia, Noruega, Brasil y Japón.

# 7 Cumbre Mundial sobre la Sociedad de la Información (CMSI)

Organizada por la UIT, la primera fase de la CMSI se celebró en Ginebra del 10 al 12 de diciembre de 2003 bajo los auspicios de la ONU. Esta Cumbre congregó a Jefes de Estado y de Gobierno, Directores de las Secretarías de los organismos especializados de las Naciones Unidas y representantes del sector privado, de los medios de comunicación y de la sociedad civil para coordinar la instauración armoniosa de la sociedad de la información en el mundo. En esta reunión, se examinó un documento de trabajo relativo a una lista de temas preparada con propósitos de referencia, a saber:

1) Infraestructura de la información y la comunicación: financiación e inversión, accesibilidad económica, desarrollo y durabilidad.
2) Acceso a la información y al saber.
3) La función de los Estados, el sector privado y la sociedad civil en la promoción de las TIC en favor del desarrollo.
4) Fortalecimiento de capacidades: desarrollo de los recursos humanos, educación y formación.
5) Seguridad.
6) Crear un entorno propicio.
7) Promover las aplicaciones favorables al desarrollo de las TIC para todos, por ejemplo, el cibergobierno, la empresa electrónica, la teleeducación y la cibersalud.
8) Diversidad cultural y lingüística, contenido local y desarrollo de los medios de comunicación.
9) Cómo superar los obstáculos que impiden instaurar una sociedad de la información con dimensión humana.

La CMSI dio lugar a la adopción de una **Declaración de Principios** y un **Plan de Acción** el 12 de diciembre de 2003.

A continuación se muestran los aspectos de seguridad del ciberespacio que figuran en ambos documentos adoptados.

## 7.1 Declaración de Principios

**Construir la sociedad de la información: un desafío global para el nuevo milenio**

*A Nuestra visión común de la sociedad de la información*

Nosotros, los representantes de los pueblos del mundo, reunidos en Ginebra del 10 al 12 de diciembre de 2003 con motivo de la primera fase de la Cumbre Mundial sobre la Sociedad de la Información,

declaramos nuestro deseo y compromiso comunes de construir una sociedad de la información centrada en la persona, integradora y orientada al desarrollo, en que todos puedan crear, consultar, utilizar y compartir la información y el conocimiento, para que las personas, las comunidades y los pueblos puedan emplear plenamente sus posibilidades en la promoción de su desarrollo sostenible y en la mejora de su calidad de vida, sobre la base de los propósitos y principios de la Carta de las Naciones Unidas y respetando plenamente y defendiendo la Declaración Universal de Derechos Humanos.

*B Una sociedad de la información para todos: principios fundamentales*

**5 Fomento de la confianza y seguridad en la utilización de las TIC**

35. El fomento de un clima de confianza, incluso en la seguridad de la información y la seguridad de las redes, la autenticación, la privacidad y la protección de los consumidores, es requisito previo para que se desarrolle la sociedad de la información y para promover la confianza entre los usuarios de las TIC. Se debe fomentar, desarrollar y poner en práctica una cultura global de ciberseguridad, en cooperación con todas las partes interesadas y los organismos internacionales especializados. Se deberían respaldar dichos esfuerzos con una mayor cooperación internacional. Dentro de esta cultura global de ciberseguridad, es importante mejorar la seguridad y garantizar la protección de los datos y la privacidad, al mismo tiempo que se amplía el acceso y el comercio. Por otra parte, es necesario tener en cuenta el nivel de desarrollo social y económico de cada país, y respetar los aspectos de la sociedad de la información orientados al desarrollo.

36. Si bien se reconocen los principios de acceso universal y sin discriminación a las TIC para todas las naciones, apoyamos las actividades de las Naciones Unidas encaminadas a impedir que se utilicen estas tecnologías con fines incompatibles con el mantenimiento de la estabilidad y seguridad internacionales, y que podrían menoscabar la integridad de las infraestructuras nacionales, en detrimento de su seguridad. Es necesario evitar que las tecnologías y los recursos de la información se utilicen para fines criminales o terroristas, respetando siempre los derechos humanos.

37. El envío masivo de mensajes electrónicos no solicitados («spam») es un problema considerable y creciente para los usuarios, las redes e internet en general. Conviene abordar los problemas de la ciberseguridad y «spam» en los planos nacional e internacional, según proceda.

48. Internet se ha convertido en un recurso global disponible para el público, y su gestión debe ser una de las cuestiones esenciales del programa de la sociedad de la información. La gestión internacional de internet debe ser multilateral, transparente y democrática, y contar con la plena participación de los gobiernos, el sector privado, la sociedad civil y las organizaciones internacionales. Esta gestión debería garantizar la distribución equitativa de recursos, facilitar el acceso a todos y garantizar un funcionamiento estable y seguro de internet, teniendo en cuenta el plurilingüismo.

**7 Aplicaciones de las TIC: ventajas en todos los aspectos de la vida**

51.h Definir mecanismos seguros para el almacenamiento y el archivo de documentos y otras informaciones en soporte electrónico.

51.i Los Estados y las partes interesadas deberían promover activamente la formación y la concienciación de los usuarios respecto a la privacidad en línea y la protección de la misma.

Invitar a las partes interesadas a garantizar que las prácticas encaminadas a facilitar el comercio electrónico permitan también que los consumidores puedan optar por utilizar o no medios electrónicos de comunicación.

**C7 Aplicaciones de las TIC: ventajas en todos los aspectos de la vida**

**15 Cibergobierno**

a) Implementar estrategias de cibergobierno basadas en las aplicaciones y encaminadas a la innovación y a promover la transparencia en las administraciones públicas y los procesos democráticos, a mejorar la eficacia y a fortalecer las relaciones con los ciudadanos.

b) Concebir, en todos los niveles, iniciativas y servicios nacionales en materia de cibergobierno que se adapten a las necesidades de los ciudadanos y las empresas, con el fin de lograr una distribución más eficaz de los recursos y los bienes públicos.

**10 Dimensiones éticas de la sociedad de la información**

58. El uso de las TIC y la creación de contenidos debería respetar los derechos humanos y las libertades fundamentales de otros, lo que incluye la privacidad personal y el derecho a la libertad de opinión, conciencia y religión de conformidad con los instrumentos internacionales relevantes.

64. Las competencias básicas de la Unión Internacional de Telecomunicaciones (UIT) en el campo de las TIC, a saber, la asistencia para colmar la brecha digital, la cooperación regional e internacional, la gestión del espectro radioeléctrico, la elaboración de normas y la difusión de información, revisten crucial importancia en la construcción de la sociedad de la información.

## 7.2 Plan de Acción

**A Introducción**

2) La sociedad de la información es un concepto en plena evolución, que ha alcanzado en el mundo diferentes niveles, como reflejo de diferentes etapas de desarrollo. Los cambios tecnológicos y de otro tipo están transformando rápidamente el entorno en que se desarrolla la sociedad de la Información. El Plan de Acción constituye, pues, una plataforma dinámica para promover la sociedad de la información en los planos nacional, regional e internacional. La estructura peculiar de la Cumbre Mundial sobre la Sociedad de la Información (CMSI), en dos fases, permite recoger esta evolución.

**B Objetivos y metas**

5) Se establecerán, según proceda, objetivos concretos de la sociedad de la información en el plano nacional, en el marco de las ciberestrategias nacionales y de conformidad con las políticas de desarrollo nacionales, teniendo en cuenta las circunstancias de cada país. Dichos objetivos pueden servir de puntos de referencia útiles para las actividades y la evaluación de los progresos realizados en la consecución de los objetivos globales de la sociedad de la información.

**C Líneas de acción**

**C1 Papel de los gobiernos y de todas las partes interesadas en la promoción de las TIC para el desarrollo**

8.1 La participación efectiva de los gobiernos y de todas las partes interesadas es indispensable para el desarrollo de la sociedad de la información, que requiere la cooperación y asociación entre todos ellos.

a) Se debe alentar a la formulación, antes de 2005, de ciberestrategias nacionales, que incluyan la creación de las capacidades humanas necesarias, teniendo en cuenta las circunstancias peculiares de cada país.

## C5 Creación de confianza y seguridad en la utilización de las TIC

### 12 La confianza y la seguridad son unos de los pilares más importantes de la sociedad de la información

a) Propiciar la cooperación entre los gobiernos dentro de las Naciones Unidas, y con todas las partes interesadas en otros foros apropiados, para aumentar la confianza del usuario y proteger los datos y la integridad de la red; considerar los riesgos actuales y potenciales para las TIC, y abordar otras cuestiones de seguridad de la información y de las redes.

b) Los gobiernos, en cooperación con el sector privado, deben prevenir, detectar, y responder a la ciberdelincuencia y el uso indebido de las TIC, definiendo directrices que tengan en cuenta los esfuerzos existentes en estos ámbitos; estudiando una legislación que permita investigar y juzgar efectivamente la utilización indebida; promoviendo esfuerzos efectivos de asistencia mutua; reforzando el apoyo institucional a nivel internacional para la prevención, detección y recuperación de estos incidentes; y alentando la educación y la sensibilización.

c) Los gobiernos y otras partes interesadas deben fomentar activamente la educación y la sensibilización de los usuarios sobre la privacidad en línea y los medios de protección de la privacidad.

d) Tomar medidas apropiadas contra el envío masivo de mensajes electrónicos no solicitados («*spam*») a nivel nacional e internacional.

e) Alentar una evaluación interna de la legislación nacional con miras a superar cualquier obstáculo al uso efectivo de documentos y transacciones electrónicas, incluido los medios electrónicos de autenticación.

) Seguir fortaleciendo el marco de confianza y seguridad con iniciativas complementarias y de apoyo mutuo en los ámbitos de la seguridad en el uso de las TIC, con iniciativas o directrices sobre el derecho a la privacidad y la protección de los datos y de los consumidores.

g) Compartir prácticas óptimas en el ámbito de la seguridad de la información y la seguridad de las redes, y propiciar su utilización por todas las partes interesadas.

h) Invitar a los países interesados a establecer puntos de contacto para intervenir y resolver incidentes en tiempo real, y desarrollar una red cooperativa entre estos puntos de contacto de forma que se comparta información y tecnologías para intervenir en caso de estos incidentes.

i) Alentar el desarrollo de nuevas aplicaciones seguras y fiables que faciliten las transacciones en línea.

j) Alentar a los países interesados a que contribuyan activamente en las actividades en curso de las Naciones Unidas tendentes a crear confianza y seguridad en la utilización de las TIC.

## C6 Entorno habilitador

13) Para maximizar los beneficios sociales, económicos y medioambientales de la sociedad de la información, los gobiernos deben crear un entorno jurídico, reglamentario y político fiable, transparente y no discriminatorio. Entre las medidas que pueden adoptarse figuran las siguientes:

e) Los gobiernos deberían seguir actualizando su legislación nacional de protección del consumidor para responder a las nuevas necesidades de la sociedad de la información.

c) Apoyar las iniciativas de cooperación internacionales en la esfera del cibergobierno, con el fin de mejorar la transparencia, responsabilidad y eficacia en todos los niveles de gobierno.

**C11 Cooperación internacional y regional**

26) La cooperación internacional entre todas las partes interesadas es fundamental para aplicar el presente Plan de Acción y ha de reforzarse con miras a promover el acceso universal y colmar la brecha digital, entre otras cosas, definiendo modalidades de aplicación.

**D Agenda de Solidaridad Digital**

27) La Agenda de Solidaridad Digital tiene por objeto fijar las condiciones necesarias para movilizar los recursos humanos, financieros y tecnológicos que permitan incluir a todos los hombres y mujeres en la sociedad de la información emergente. En la aplicación de esta agenda es vital una estrecha cooperación nacional, regional e internacional entre todas las partes interesadas. Para superar la brecha digital, necesitamos utilizar más eficientemente los enfoques y mecanismos existentes y analizar a fondo otros nuevos, con el fin de proporcionar fondos para financiar el desarrollo de infraestructuras y equipos, así como la creación de capacidad y contenidos, factores que son esenciales para la participación en la sociedad de la información.

**E Seguimiento y evaluación**

28) Se debe elaborar un plan realista de evaluación de resultados y establecimiento de referencias (tanto cualitativas como cuantitativas) en el plano internacional, a través de indicadores estadísticos comparables y resultados de investigación, para dar seguimiento a la aplicación de los objetivos y metas del presente Plan de Acción, teniendo en cuenta las circunstancias de cada país.

e) Crear y poner en funcionamiento un sitio web sobre prácticas óptimas y proyectos con resultados satisfactorios, basado en una recopilación de las contribuciones de todas las partes interesadas, con un formato conciso, accesible y atrayente, acorde con las normas internacionalmente aceptadas de accesibilidad a la web. Ese sitio web podría actualizarse periódicamente y convertirse en un mecanismo permanente de intercambio de experiencias.

**Túnez 2005: segunda fase**

La segunda fase de la Cumbre Mundial, que acogerá el Gobierno tunecino, se celebrará en Túnez del 16 al 18 de noviembre de 2005. En ella se examinarán fundamentalmente temas relativos al desarrollo, se evaluarán los avances logrados y se adoptará un Plan de Acción, si es necesario.

En conclusión, podemos citar una serie de grandes líneas directrices de la CMSI:

**Garantizar la confianza y la seguridad en la utilización de las TIC**

• Autenticación • establecimiento de la confianza y la seguridad • proteger al consumidor • lucha contra la utilización abusiva de las TIC • lucha contra el correo basura • ciberdelito • ciberseguridad • protección de los datos • seguridad de la información y seguridad de las redes • integridad de las redes • seguridad de las transacciones en línea • protección de la vida privada • gestión y procesamiento en tiempo real de incidentes • aplicaciones seguras y fiables.

NOTA – Sitio web para consultar información: www.itu.int/wsis, así como www.un.otg/milleniumgoals/, sitio de las Naciones Unidas en el que se exponen los Objetivos de Desarrollo del Milenio, metas éstas que resultan análogas a las de la CMSI.

# 8 Trabajos de la UIT

## 8.1 Resoluciones sobre seguridad de la AMNT-04

Durante la Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), celebrada en Brasil del 5 al 14 de octubre de 2004, se adoptaron y aprobaron nuevas Resoluciones sobre seguridad, las primeras en su género que haya adoptado una Conferencia de alto nivel de la UIT tras la Resolución 130 de la PP-02:

- **Resolución 50: Ciberseguridad**

Reconociendo las actividades y el interés suscitados por la preparación de normas y Recomendaciones de seguridad en el seno de la UIT, especialmente en la CE 17, la AMNT decidió:

1 que la UIT-T evalúe las Recomendaciones existentes y en curso de elaboración, y especialmente las Recomendaciones sobre señalización y protocolos de comunicaciones, con respecto a la robustez de su diseño y a su potencial para ser explotadas por grupos malintencionados con el fin de interferir destructivamente en su despliegue de la infraestructura mundial de la información y las comunicaciones;

2 que el UIT-T continúe fomentando conciencia, en su esfera de acción e influencia, acerca de la necesidad de defender los sistemas de información y comunicaciones contra la amenaza de ataques cibernéticos, y siga fomentando la cooperación entre las entidades correspondientes a efectos de aumentar el intercambio de información técnica en el campo de la seguridad de las redes de información y comunicaciones,

*encarga al Director de la Oficina de Normalización de las Telecomunicaciones*

que elabore, en consulta con el Presidente del GANT y con los Presidentes de las Comisiones de Estudio que correspondan, un plan para emprender la mencionada evaluación de Recomendaciones pertinentes lo antes posible, teniendo en cuenta los recursos disponibles y otras prioridades, informando regularmente sobre el progreso alcanzado al GANT,

*encarga también al Director de la TSB*

1 que incluya en el Informe anual al Consejo, especificado en la Resolución 130 (Marrakech, 2002) de la Conferencia de Plenipotenciarios, el progreso en las evaluaciones indicadas en el *resuelve supra*;

2 que continúe adoptando las medidas adecuadas para divulgar la necesidad de defender las redes de información y comunicación contra la amenaza de ataques cibernéticos y de cooperar con otras entidades pertinentes en estos esfuerzos;

3 que se coordine con otras entidades activas en este campo, por ejemplo, la Organización Internacional de Normalización (ISO) y el IETF (Internet Engineering Task Force),

*invita a los Estados Miembros, los Miembros del Sector y los Asociados, según corresponda*

a participar activamente en la implementación de esta Resolución y de las medidas asociadas.

- **Resolución 51: Lucha contra el correo basura (spam)**

Tras sus «*reconociendo*», referentes a la CMSI, la Asamblea Mundial de Normalización de las Telecomunicaciones (Florianópolis, 2004),

*considerando*

a) las disposiciones pertinentes de los instrumentos básicos de la UIT;

b) que la adopción de medidas acordadas para combatir el correo basura (envío masivo de mensajes electrónicos no solicitados o *spam*) están en consonancia con la Meta 4 del Plan Estratégico de la Unión para el periodo 2004-2007 (Cláusula 3 de la Parte I) de la Resolución 71 (Rev.Marrakech, 2002) de la Conferencia de Plenipotenciarios;

c) la Resolución 52 sobre medios técnicos contra el correo basura;

d) el Informe del Presidente de la reunión temática de la CMSI de la UIT contra el correo basura, que propugnaba un enfoque global para compartirlo con:

   i) una legislación estricta;

   ii) el desarrollo de medidas técnicas;

iii) el establecimiento de asociaciones en la industria;

iv) la educación;

v) la cooperación internacional,

*encarga al Director de la Oficina de Normalización de las Telecomunicaciones, en cooperación con los Directores de las otras Oficinas y el Secretario General*

que prepare urgentemente un Informe al Consejo sobre las iniciativas de la UIT y otras iniciativas internacionales para combatir el correo basura y que proponga las posibles medidas de seguimiento para que las examine el Consejo,

*invita*

a los Estados Miembros a contribuir a estos trabajos,

*invita además*

a los Estados Miembros (a los Miembros de Sector) a tomar las medidas adecuadas dentro de sus marcos jurídicos nacionales para garantizar que se adopten disposiciones adecuadas y eficaces de lucha contra el correo basura.

- **Resolución 52: Medios técnicos contra el correo basura**

Tras los «*considerando*» a) a f)

La Asamblea Mundial de Normalización de las Telecomunicaciones (Florianópolis, 2004),

*reconociendo*

a) las disposiciones pertinentes de los instrumentos básicos de la UIT;

b) que el correo basura crea problemas de seguridad en las redes de telecomunicaciones, incluyendo el de transformar éstas en vehículo para la difusión de virus, gusanos, etc.;

c) que el correo basura constituye un problema mundial que exige la cooperación internacional para hallar soluciones;

d) que el estudio del tema del correo basura tiene carácter urgente,

*encarga a las Comisiones de Estudio competentes*

que, cooperando con el Grupo de Tareas Especiales de Ingeniería en internet (IETF) y otros grupos pertinentes, elaboren con carácter urgente las Recomendaciones técnicas, incluyendo las definiciones necesarias, sobre la lucha contra el correo basura según corresponda, e informe periódicamente al Grupo Asesor de Normalización de las Telecomunicaciones sobre el avance de sus trabajos,

*encarga al Director de la Oficina de Normalización de las Telecomunicaciones*

que facilite toda la asistencia necesaria para acelerar esas actividades, e informe de ello al Consejo.

**En conclusión**, será la CE 17 (véase el punto 8.2.2) la Comisión de Estudio que se encargará básicamente de dar aplicación a estas tres Resoluciones. Además, el Director de la TSB habrá de presentar a la AMNT-(08) un Informe sobre la aplicación de estas tres Resoluciones.

NOTA – Los documentos antes mencionados pueden obtenerse dirigiéndose al sitio del UIT-T (AMNT-04).

## 8.2 Comisiones de Estudio del UIT-T

### 8.2.1 Periodo de estudios 2001-2004

En este punto se exponen las medidas adoptadas por las Comisiones de Estudio del UIT-T con respecto a la seguridad de las redes de información y comunicaciones.

- La Comisión de Estudio 2 del UIT-T prepara proyectos de Recomendaciones sobre las condiciones de seguridad de las redes de telecomunicaciones (E.408) y el tratamiento apropiado de la seguridad y la organización (E.409) (sometidos a aprobación el 18 de mayo de 2004 (Grupo de Trabajo 2/2)).

- La Comisión de Estudio 4 del UIT-T ha redactado varias Recomendaciones que tratan de los aspectos de la seguridad de la red de gestión de las telecomunicaciones (RGT): M.3010, *Principios para una red de gestión de las telecomunicaciones*; M.3210.1, *Servicios de gestión para la red de gestión de las telecomunicaciones, para la seguridad de las IMT-2000* (Telecomunicaciones móviles internacionales 2000); M.3013, *Consideraciones sobre una red de gestión de las telecomunicaciones*; M.3016, *Visión general de la seguridad en la red de gestión de las telecomunicaciones*; M.3210, Servicios de gestión para la red de gestión de las telecomunicaciones, para la seguridad de las IMT-2000 (Telecomunicaciones móviles internacionales 2000); M.3320, *Marco de los requisitos de gestión para la interfaz X de la RGT*; M.3400, *Funciones de gestión de la red de gestión de las telecomunicaciones*; Q.813, *Elemento del servicio de aplicación de transformaciones de seguridad para elementos de servicio de operaciones a distancia (STASE-ROSE)*; Q.815, *Especificación de un modelo de seguridad para la protección del mensaje completo*; Q.817, *Infraestructura de claves públicas de la red de gestión de las telecomunicaciones – Certificados digitales y perfiles de lista de revocación de certificados*. Los Grupos encargados de las Cuestiones, 7, 9, 10 y 18/4 trabajan actualmente en el tema de la seguridad.

- La Comisión de Estudio 9 del UIT-T preparó la Recomendación J.170, *Especificación de seguridad de IPCablecom*, en el contexto de su Proyecto IPCablecom. Trata de los servicios de seguridad para autenticación, control de acceso, señalización e integridad de contenido de medios, confidencialidad y no rechazo.

- La Comisión de Estudio 11 del UIT-T prepara protocolos de red para señalización y control en los que se integran las condiciones de seguridad identificadas por las Comisiones de Estudio encargadas y otros organismos. Estos asuntos son tratados por el Grupo de Trabajo 1/11 (Cuestiones 1, 2, 3, 4, 5/11), el Grupo de Trabajo 2/11 (Cuestión 6/11) y el Grupo de Trabajo 3/11 (Cuestión 11/11).

- La Comisión de Estudio 13 del UIT-T estudia las cuestiones de seguridad de las redes multiprotocolo y de protocolo internet (IP). Estos temas están incluidos en los Proyectos IP y NGN 2004 del UIT-T. En la última reunión de la Comisión de Estudio 13 (29 de octubre a 8 de noviembre de 2002) se acordó añadir una cláusula sobre la seguridad a todos los textos en estudio o que serán publicados. Obsérvese que la Recomendación Y.110 identifica algunos aspectos de seguridad generales de la infraestructura mundial de la información (GII). El Grupo encargado de la Cuestión 1/13 prepara una nueva Recomendación Y.1271, Marco de requisitos y capacidades de red para soportar las comunicaciones de emergencia. También es de señalar el trabajo que realiza el Grupo encargado de la Cuestión 1/13 para una nueva Recomendación Y.140.1, dedicada a distintos atributos de seguridad en las posibles fronteras de interconexión entre operadores de red y proveedores de servicios. La Recomendación Y.140, *Infraestructura mundial de la información: puntos de referencia para el marco de interconexión*, aporta las informaciones generales que han permitido elaborar la Recomendación Y.140.1.

- La Comisión de Estudio 15 del UIT-T contribuye a los trabajos de normalización para la seguridad en los aspectos de la fiabilidad y la seguridad de las comunicaciones.

- El Grupo encargado de la Cuestión 9/15, Equipos de transporte y protección/recuperación de red, se ocupa de la conmutación de protección para la jerarquía digital síncrona (Recomendación G.841, T*ipos y características de las arquitecturas de protección para redes de la jerarquía digital síncrona*, y Recomendación G.842, *Interfuncionamiento de las arquitecturas de protección para redes de la jerarquía digital síncrona*), así como la conmutación de protección para las redes de transporte ópticas (OTN) (proyecto de Recomendaciones G.808.1 y G.808.2, *Conmutación general de protección*, proyecto de Recomendaciones G.873.1 y G.873.2, *Protección de redes de transporte ópticas*). En las Recomendaciones dedicadas a los equipos o los sistemas de recuperación se integrarán los requisitos para la recuperación de redes.

- Cuestión 15/15, Características y métodos de prueba de los cables y fibras ópticas; Cuestión 16/15, Características de los sistemas ópticos en las redes de transporte terrenales; Cuestión 17/15, Características de los componentes y subsistemas ópticos; Cuestión 18/15, Características de los sistemas de cable submarinos de fibra óptica: en todas estas Cuestiones se incluye un estudio de fiabilidad. La Recomendación G.911, *Parámetros y metodología de cálculo de la fiabilidad y la disponibilidad de los sistemas de fibra óptica*, también trata este asunto. Las Cuestiones 15, 16, 17 y 18/15 también incluyen el estudio de la fiabilidad y la disponibilidad de las fibras ópticas y los cables de fibra óptica, los sistemas, subsistemas y componentes ópticos terrenales y submarinos.

  El trabajo sobre la seguridad de la comunicación se ha asignado enteramente a la Cuestión 14/15, Gestión de red para sistemas y equipos de transporte. Las Recomendaciones G.784, *Gestión de la jerarquía digital síncrona*, y G.874, *Aspectos de gestión del elemento de red de transporte óptica*, tratan de las funciones de fallo, configuración, contabilidad, eficiencia de funcionamiento y seguridad (FCAPS) de los elementos de red SDH y OTN. En estas Recomendaciones, el tema de la gestión de seguridad aún está en estudio. En la Recomendación G.7712/Y.1703, *Arquitectura y especificación de una red de comunicación de datos*, se ha incluido el tema de la seguridad de las redes de comunicaciones de gestión (MCN) y las redes de comunicación de señalización (SCN).

- En el marco de la Cuestión G.16 (http://www.itu.int/ITU-T/studygroups/com16/sg16-qg.html), la Comisión de Estudio 16 del UIT-T, ha preparado y sigue adaptando varias Recomendaciones sobre la seguridad de los distintos sistemas y protocolos para conferencias audiovisuales, por ejemplo H.320 sobre RDSI, H.310 sobre RDSI-BA, H.324 sobre RTPC y las redes de sistema móvil de tercera generación (3G), y H.323 sobre redes de paquetes (incluida la transmisión de voz por IP). Las Recomendaciones H.233, *Sistemas con confidencialidad para servicios audiovisuales*, y H.234, *Sistemas de gestión de claves de criptación y autenticación para servicios audiovisuales* (para sistemas H.320), son de aplicación. Las Recomendaciones de la serie H.conjuntos, S*eguridad para los sistemas de telecomunicaciones de urgencia* están en curso de elaboración y recientemente se ha aprobado la versión 3 de la Recomendación H.235, *Seguridad y criptado para terminales multimedios de la serie H* (*terminales H.323 y otros terminales de tipo H.245*). En la Cuestión I/16 se han empezado a estudiar las medidas de seguridad para las situaciones de emergencia y socorro (por ejemplo, prevención de robo de servicios, autorización de usuario, confidencialidad) mediante comunicaciones multimedios, en coordinación con la Cuestión G/16, Seguridad de los sistemas y servicios multimedios, en colaboración con otras Comisiones de Estudio y otras organizaciones de normalización (SDO).

- Se ha designado a la Comisión de Estudio 17 del UIT-T Comisión Rectora en cuanto a los aspectos de seguridad de las telecomunicaciones. En el marco de la Comisión de Estudio 17 estos esfuerzos se están coordinando en relación con la C.4/17, Proyecto de seguridad de los sistemas de comunicaciones. Quien esté interesado en recabar información sobre el particular puede consultar la página web de la Comisión de Estudio 17 incluida en el sitio web de la UIT (http://www.itu.int/ITU-T/studygroups/com17/tel-security.html).

  La Comisión de Estudio 17 ha preparado un catálogo de Recomendaciones UIT que tratan de la seguridad de los sistemas de comunicaciones y un resumen de definiciones de seguridad tomadas de Recomendaciones del UIT-T aprobadas: estos dos documentos se pueden consultar en la página de la Comisión de Estudio 17 en el sitio web de la UIT (véase http://www.itu.int/ITU-T/studygroups/com17/cssecurity.html). La Comisión de Estudio 17 ha elaborado también un compendio de definiciones sobre seguridad aprobadas por el UIT-T; dicho documento y su addéndum permiten establecer definiciones comunes de los términos relativos a la seguridad para todos los Grupos de Trabajo y las Comisiones de Estudio del UIT-T. El Grupo encargado de la Cuestión 10/17, Requisitos, modelo y directrices de seguridad para los sistemas y los servicios de comunicación, mantiene compendios actualizados sobre la seguridad de sistemas de comunicaciones y ha empezado a preparar una serie de nuevas Recomendaciones.

La Comisión de Estudio 17 mantiene en estudio una serie de Cuestiones sobre seguridad; a saber:

– C.2/17, Servicios de directorio, sistemas de directorio y clave pública/certificados de atributos. En el marco de esta Cuestión la muy conocida Recomendación X.509, «Marco para los certificados de claves públicas y de atributos», constituye la base de las infraestructuras de clave pública (PKI) y las infraestructuras de gestión de privilegios (PMI), y se espera aprobar en 2005 una edición actualizada de dicha Recomendación.

– C.4/17, Proyecto de seguridad de los sistemas de comunicaciones. En el marco de esta Cuestión se traza un panorama general del trabajo de seguridad y se realizan las correspondientes actividades de coordinación.

– C.5/17, Arquitectura y marco genérico de la seguridad. Un conjunto sustancial de Recomendaciones sobre seguridad es el que figura en la Serie X.800. En 2003 se añadió la importante Recomendación X.805, relativa a la arquitectura de seguridad para el sistema que proporcionan comunicaciones de extremo a extremo.

– C.6/17, Ciberseguridad. Se ha comenzado a estudiar muchos de los aspectos de la seguridad en el ciberespacio.

– C.7/17, Gestión de la seguridad. La Recomendación X.1051 relativa a los requisitos de telecomunicación en los sistemas de gestión de seguridad de la información (ISMS-T) se aprobó en 2004.

– C.8/17, Telebiometría. La Recomendación X.1081, El modelo telebiométrico multimodal – Marco para la especificación de los aspectos de la telebiometría relativos a protección y seguridad, fue aprobada en 2005. En el punto 8.4 puede verse más información sobre el particular.

– C.9/17, Servicios de comunicación seguros – En 2004 se aprobaron dos Recomendaciones sobre seguridad móvil. Éstas son la X.1121, Marco general de tecnología de seguridad para las comunicaciones móviles de datos de extremo a extremo y X.1122, Directrices para la implementación de sistemas móviles seguros basados en la infraestructura de claves públicas.

Las actividades de normalización del UIT-T se administrarán en el marco de un nuevo proyecto del UIT-T sobre seguridad, que fue aprobado en la reunión de la Comisión de Estudio 17 celebrada en noviembre de 2002.

Además, para hacer frente al crecimiento de las actividades relativas a la seguridad, la Comisión de Estudio 17 decidió en marzo de 2004 dividir la Cuestión 10/17 en 6 nuevas Cuestiones, de G a L/17, para el periodo de estudios 2005-2008.

NOTA – La Comisión de Estudio Especial sobre las «IMT-2000 y sistemas posteriores, incluyó la seguridad entre los aspectos fundamentales de sus Recomendaciones de referencia para los miembros de la familia de las IMT-2000 (3G). Entre los asuntos abordados por dichas recomendaciones cabe citar: evaluación de las amenazas percibidas y lista de los imperativos de seguridad para afrontar dichas amenazas, principios y objetivos de seguridad, arquitectura de seguridad adecuadamente definida (es decir, mecanismos y características de seguridad), necesidades en materia de algoritmos criptográficos, condiciones de intercepción legal y función y arquitectura de intercepción legal. Estos estudios se han efectuado en el marco de la Cuestión 3/SSG.

### 8.2.2 Periodo 2005-2008

Para atender a lo solicitado en **la Resolución 2 de la AMNT-04** se establecieron diferentes Comisiones de Estudio (CE) para el periodo 2005-2008.

CE 2 **Aspectos de explotación de la prestación de servicios, redes y calidad de funcionamiento,** Comisión de Estudio Rectora para la definición de servicios, la numeración y el encaminamiento.

CE 3 **Principios de tarificación y contabilidad, incluidos los temas relativos a economía y política de las telecomunicaciones,** Comisión de Estudio encargada de los principios de tarificación, contabilidad y operaciones conexas de política general y economía de las telecomunicaciones.

CE 4 **Gestión de las telecomunicaciones**, Comisión de Estudio Rectora en lo que concierne a la gestión de las telecomunicaciones.

CE 5 **Protección contra los efectos del entorno electromagnético**, Comisión de Estudio encargada de la protección contra los efectos ocasionados por el entorno electromagnético.

CE 6 **Implante exterior e instalaciones interiores correspondientes**, Comisión de Estudio en cuanto a las instalaciones exteriores y a las instalaciones interiores conexas cuyo título podría reflejar un tanto más la función LS4.

CE 9 **Redes de cable integradas de banda ancha y transmisión de televisión y sonido**, Comisión de Estudio Rectora, tratándose de las redes de televisión y cable integradas en banda ancha.

C 11 **Requisitos y protocolo de señalización,** Comisión de Estudio Rectora en lo que respecta a la señalización y los protocolos. Comisión de Estudio Rectora en lo que respecta a las redes inteligentes.

CE 12 **Calidad de funcionamiento y calidad de servicio,** Comisión de Estudio Rectora en lo que atañe a la calidad de servicio y la calidad de funcionamiento.

CE 13 **Redes de próxima generación – Arquitectura, evolución y convergencia**, Comisión de Estudio Rectora encargada de las redes NGN y las cuestiones relativas a los satélites.

CE 15 **Redes de fibra óptica y otras infraestructuras de redes de transporte**, Comisión de Estudio Rectora para el transporte en las redes de acceso, y en lo que concierne a las tecnologías ópticas.

CE 16 **Terminales, sistemas y aplicaciones multimedios**, Comisión de Estudio Rectora en el caso de los terminales, los sistemas y las aplicaciones multimedios. Comisión de Estudio Rectora, tratándose de las aplicaciones ubicuas («todo en línea», por ejemplo la telesalud y el comercio electrónico).

CE 17 **Seguridad, lenguaje y soporte lógico de las telecomunicaciones**, Comisión de Estudio Rectora encargada de la seguridad de las telecomunicaciones. Comisión de Estudio Rectora en lo que respecta a los lenguajes y las técnicas de descripción.

CE 19 **Redes de telecomunicaciones móviles,** Comisión de Estudio Rectora encargada de las redes de telecomunicaciones móviles y la movilidad **(esta Comisión de Estudio se estableció, transformando la Comisión de Estudio Especial sobre las IMT-2000, creada para el periodo 2001-2004).**

Por lo que hace a la nueva distribución del trabajo en el seno de las Comisiones de Estudio del UIT-T hay que señalar lo siguiente:

**Comisión de Estudio 2**, incluye ahora internet, ya que la Comisión de Estudio 2 debe recomendar orientaciones en materia de planificación y dimensionamiento de la ingeniería de tráfico, con miras a establecer y explotar todo tipo de redes y elementos de red.

**Comisión de Estudio 11**

la Comisión de Estudio 11 debe preparar Recomendaciones en relación con los aspectos esenciales de la arquitectura y los protocolos de señalización y mando en redes, incluida la convergencia hacia las redes de próxima generación, en colaboración y coordinación estrechas con las llamadas Comisiones de Estudio encargadas de las Cuestiones referentes a otras redes y a las redes NGN.

Habrá que preparar Recomendaciones sobre las siguientes Cuestiones, habida cuenta de la convergencia de las redes fija y móvil:

- Arquitectura funcional de señalización y de mando de red en los entornos incipientes NGN;
- Especificación y protocolo de mando y de señalización de aplicación;
- Especificaciones y protocolos de mando y de señalización de sesión;
- Especificaciones y protocolos de mando y de señalización de soportes;
- Especificaciones y protocolos de mando y de señalización de recursos;
- Especificaciones y protocolos de señalización y de mando para tener en cuenta la vinculación a entornos NGN.

La Comisión de Estudio 11 será llamada a colaborar para preparar un Manual sobre el establecimiento de redes en modo paquete.

La Comisión deberá reutilizar, en su caso, los protocolos que están definiendo otras organizaciones de normalización, con el fin de aprovechar al máximo las inversiones realizadas en la normalización.

La Comisión de Estudio 11 deberá introducir mejoras en las Recomendaciones vigentes sobre los protocolos de acceso y de señalización interredes del mando BICC del ATM, de la RDSI de banda estrecha y de la RTPC, por ejemplo, el sistema de señalización Nº 7 y los sistemas de DSS 1 y DSS 2. Se trata de satisfacer las necesidades comerciales de las organizaciones miembros que deseen ofrecer nuevas funcionalidades y servicios, además de las redes establecidas, basándose en las Recomendaciones vigentes.

Se alienta a la Comisión de Estudio 11 a que, cada vez que ello sea posible y en el caso de ciertas actividades, celebre reuniones mixtas con las Comisiones de Estudio 13 y 19, según lo decidan los equipos de dirección de las tres Comisiones.

**Comisión de Estudio 17**

Esta Comisión está encargada de los estudios sobre seguridad, aplicación de las telecomunicaciones entre sistemas abiertos, incluido interfuncionamiento y la guía, y los lenguajes técnicos, así como sus métodos de utilización y otras cuestiones conexas vinculadas con los aspectos informáticos de los sistemas de telecomunicación.

En el campo de la seguridad, la Comisión de Estudio 17 se encarga de preparar importantes Recomendaciones sobre seguridad, por ejemplo en relación con la arquitectura y los marcos de seguridad. Además, la Comisión garantiza la coordinación general de las actividades emprendidas por el UIT-T en el ámbito de la seguridad.

Por lo que hace a las comunicaciones entre sistemas abiertos, la Comisión de Estudio 17 se encarga de la preparación de Recomendaciones que versan sobre lo siguiente:

- interconexión de sistemas abiertos (OSI) (Recomendaciones de las series X.200, X.400, X.600, X.800, etc.);
- servicios y sistemas de directorio (Recomendaciones de las series F.500 y X.500);
- procesamiento distribuido abierto (ODP) (Recomendaciones de la serie X.900).

En el campo de los lenguajes, la Comisión de Estudio 17 se encarga de los estudios sobre técnicas de modelado, especificación y descripción. Estos trabajos, que versan sobre diferentes lenguajes (ASN.1, SDL, MSC, eODL, URN y TTCN), se emprenden en función de los requisitos de las Comisiones de Estudio competentes (Comisiones de Estudio 4, 9, 11, 13, 15 y 16) y en colaboración con éstas.

Tratándose de los programas informáticos relacionados con los sistemas de telecomunicación, los trabajos se centrarán esencialmente con los aspectos respecto a las cuales la industria estima útil aplicar Recomendaciones del UIT-T, con el fin de mejorar las tecnologías informáticas y los procesos conexos, así como de estimular el mercado de dichas tecnologías.

Los trabajos de la Comisión de Estudio 17 se sincronizarán con los de otras organizaciones de normalización, por ejemplo, la ISO/CEI JTC 1, el IETF y el ETSI. Para lograr el grado de sinergia más elevado posible en lo que atañe a la elaboración de nuevas Recomendaciones, se tomarán en consideración los trabajos que se efectúen sobre este tema en foros y consorcios como el OMG, el TMF, la SDL Forum Society, el Consorcio ASN.1, OASIS, etc.

**Comisión de Estudio 19**

Esta Comisión de Estudio del UIT-T se encarga muy particularmente de los aspectos de «red» de la movilidad y las redes de comunicaciones móviles, incluidos los sistemas IMT-2000 y posteriores. La Comisión tiene a su cargo:

- las necesidades que plantean la capacidad de servicio y la capacidad de red, así como la arquitectura de redes;
- la gestión de la movilidad;

- la identificación de los sistemas IMT-2000 presentes o en evolución;
- la elaboración de un Manual sobre las IMT-2000;
- la convergencia de las redes IMT-2000 en evolución y de las redes fijas en evolución;
- la definición de un escenario de evolución en cuanto a los aspectos de «red» y la movilidad entre los sistemas IMT-2000 existentes y posteriores;
- la preparación de un plan de orientación general sobre los aspectos de «red» y la movilidad de los sistemas IMT-2000 especificados por el UIT-T y de los organismos exteriores (organizaciones de normalización, proyectos en asociación, el IETF y otros foros exteriores competentes, etc.);
- el estudio de las necesidades y las técnicas de gestión de la movilidad, con miras a garantizar la movilidad mundial entre los sistemas IMT-2000 en evolución y los sistemas ulteriores especificados por organismos exteriores.

Los puntos antes mencionados entrañan el diseño de una arquitectura común a largo plazo de las redes IP, arquitectura que resultaría aplicable a las redes de comunicación móviles, lo que incluye la movilidad en el marco de las redes de próxima generación. Además, habida cuenta de la actual evolución de la infraestructura de redes, estos puntos abarcan los trabajos de interfuncionamiento de redes IP a corto plazo.

Por otra parte, la Comisión de Estudio 19 examinará:

- la armonización de las diferentes normas de la familia IMT-2000 a medida que evolucionen más allá de estos sistemas, especialmente en lo que respecta a la gestión de la movilidad y la convergencia con las redes fijas en evolución, y ello colaborando en la mayor medida posible con las organizaciones competentes;
- los aspectos de «red» de la convergencia de las redes fijas e inalámbricas, para ofrecer a los usuarios servicios de forma transparente y con arreglo a diferentes movilidades de acceso.

A fin de ayudar a los países en desarrollo a aplicar las tecnologías de los sistemas IMT-2000 y otras técnicas inalámbricas afines, habrá que instaurar una coordinación con los representantes del UIT-D, para determinar la forma de realizar lo más eficazmente posible las correspondientes actividades en colaboración con dicho Sector.

La Comisión de Estudio 19 deberá establecer estrechos vínculos de cooperación con las organizaciones de normalización exteriores, así como las asociaciones 3GPP, y preparar un programa complementario. Además, tendrá que alentar de manera proactiva la comunicación con dichas organizaciones exteriores a fin de que las especificaciones de las redes móviles preparadas por dichas organizaciones puedan mencionarse como referencias normativas en los textos de las Recomendaciones del UIT-T.

Se insta a la Comisión de Estudio 19 a que, cada vez que ello sea posible, a organizar, conjuntamente con las Comisiones de Estudio 11 y 13 y tal como lo decidan los equipos de dirección, reuniones en las que se examinen ciertas actividades.

NOTA – En el Anexo C a la Resolución 2 (Florianópolis, 2004) figura la lista de las Recomendaciones correspondientes a cada Comisión de Estudio y el GANT para el periodo de estudios posterior a 2004.

## 8.3 Banda ancha y seguridad de la información (Informe de la UIT)

En el presente Capítulo se resume brevemente el Informe de la UIT titulado «Nacimiento de la banda ancha», que se publicó en septiembre de 2003 (www.itu.int).

La explosión del envío masivo de mensajes electrónicos no deseados (spam), bromas electrónicas y ciberataques pone de manifiesto la gran vulnerabilidad de los usuarios y subraya la necesidad que tienen de tomar medidas para protegerse. Si bien todas las conexiones -telefónicas o de banda ancha- pueden ser objeto de estas violaciones, no cabe duda de que las conexiones de banda ancha permanentes están más expuestas; los ataques y los actos de piratería pueden producirse en todo momento y las 24 horas del día, lo que incrementa considerablemente el riesgo en estas conexiones, si se comparan con un computador que está conectado sólo durante un tiempo reducido. Afortunadamente, existe un gran número de herramientas que permiten que las conexiones de banda ancha sean seguras e interesantes para los posibles usuarios.

- Tomar conciencia del riesgo

  La mayoría de los usuarios de conexiones de banda ancha son particulares poco conscientes del riesgo que corren. Aunque las tecnologías de banda ancha son conocidas por ser muy fáciles de usar para acceder a la información, se corre el riesgo de que se propagase la opinión de que son especialmente vulnerables ante la falta de precauciones o la información suficiente; tanto así que los posibles usuarios podrían plantearse el hecho de pasar al servicio de banda ancha por miedo a las amenazas que pasan sobre sus datos, personales y comerciales.

  Los poderes públicos y los proveedores de servicios de internet (PSI) pueden tomar medidas para sensibilizar a los usuarios de servicios de banda ancha e incrementar la seguridad de los sistemas, mientras que los autores de las normas relativas a estas tecnologías comparten la responsabilidad de garantizar un grado de seguridad aceptable en lo que se refiere a la red.

- Los cortafuegos: guardianes vigilantes

  Los cortafuegos (véase el punto 2.4) son dispositivos aceptables en lo que concierne a prohibir a las personas no autorizadas a acceder a los recursos personales que figuran en computadores con acceso de banda ancha. Se trata de un programa o equipo que obstaculiza toda comunicación con destino al computador (o la red) o procedencia del mismo.

  Son numerosos los proveedores de cortafuegos que proponen versiones gratuitas de sus programas, las cuales pueden telecargarse desde la web, incluso si la configuración de estos productos suele plantear dificultades a los usuarios. Algunos proveedores de acceso de banda ancha han decidido ayudar a los usuarios en materia de seguridad incorporando para ello gratuitamente cortafuegos en los paquetes de programas que proponen para las redes familiares, y colaborando con productores de cortafuegos para normalizar los procedimientos de instalación.

  Algunos fabricantes han creado otras herramientas destinadas a luchar contra uno de los problemas más frecuentes a los que han de hacer frente los usuarios de tecnologías de banda ancha: los programas espías que se introducen de manera subrepticia en los computadores mediante programas telecargados desde internet. Por otra parte, se ha acusado a los programas de compartición de ficheros de introducir programas informáticos espías en el momento de instalar los primeros computadores.

  Afortunadamente, existen programas de utilización libre que permiten buscar ficheros de este tipo y eliminarlos con objeto de liberar al computador de virus.

- Cifrado y criptación

  Aunque los cortafuegos permiten rechazar una comunicación sospechosa, existe una forma, incluso mejor de proteger los datos confidenciales almacenados en un computador o que circulan por internet; se trata del cifrado o la criptación (véase el punto 2.8). En las conexiones de banda ancha se pueden utilizar distintas técnicas de cifrado para que los datos sigan siendo privados y puedan circular por Internet sin ser pirateados; además, estas técnicas permiten que circulen comunicaciones cifradas, que habitualmente requieren una anchura de banda del 10 al 20% superior a la que necesitan las informaciones no criptadas.

- Disposiciones legislativas y reglamentarias

  La instalación de sistemas de seguridad mejorados y la preparación de las correspondientes disposiciones legislativas y reglamentarias revisten crucial importancia para la creación de aplicaciones comerciales y públicas tales como la administración electrónica, la cibersalud o el comercio electrónico. Para poder utilizar estos servicios en línea, los usuarios deben tener la certeza de que sólo las personas autorizadas podrán acceder a sus datos y manipularlos, sus buzones de correo electrónico no recibirán spam y que las informaciones que dan determinados servicios son dignas de confianza.

- Seguridad para los particulares

  La seguridad es una cuestión importante también para los particulares, que no suelen beneficiar de los controles y la asistencia técnica que facilitan las empresas o las administraciones. Dejar un computador conectado a internet 24 horas al día equivale a dejar abierta una ventana, para que cualquiera pueda

entrar. Esto explica que la seguridad sea necesaria para infundir confianza y poder explotar al máximo, entre otras cosas, las tecnologías de banda ancha, lo que, a su vez, contribuirá a crear un entorno propicio para la sociedad mundial de la información.

## 8.4 Manual del UIT-T sobre la seguridad en las telecomunicaciones y las tecnologías de la información

### 8.4.1 Edición de 2003

En diciembre de 2003 el UIT-T publicó un Manual, en inglés, titulado «*Security in Telecommunications and Information Technology*» en el que ofrece un panorama general de los trabajos y los resultados de las Recomendaciones del UIT-T vinculados a la seguridad en las telecomunicaciones, y también de las numerosas Recomendaciones publicadas por el Sector con objeto de permitir a los distintos actores de la sociedad de la información garantizar la seguridad de la infraestructura de las comunicaciones y los servicios conexos.

En este Manual se hace una descripción de las prácticas habituales en materia de seguridad y se muestra el modo de aplicar los distintos aspectos relativos a la seguridad que prescribe el UIT-T (www.itu.int/ITU-T/publications). Está compuesto de una introducción y de distintos capítulos en los que se describe, principalmente, lo siguiente:

- la arquitectura básica de seguridad y sus aplicaciones (Recomendación X.805 del UIT-T);
- el marco de implementación de medidas de seguridad en una red de telecomunicaciones;
- los mecanismos de seguridad para la información confidencial (Recomendación X.509-PKI del UIT-T);
- las aplicaciones, en dos partes:
  1) las aplicaciones para el usuario final
     - voz por IP;
     - documento facsímil;
     - multimedios;
  2) las aplicaciones de red (calidad e integridad de los servicios):
     - gestión de las redes;
     - cibersalud.

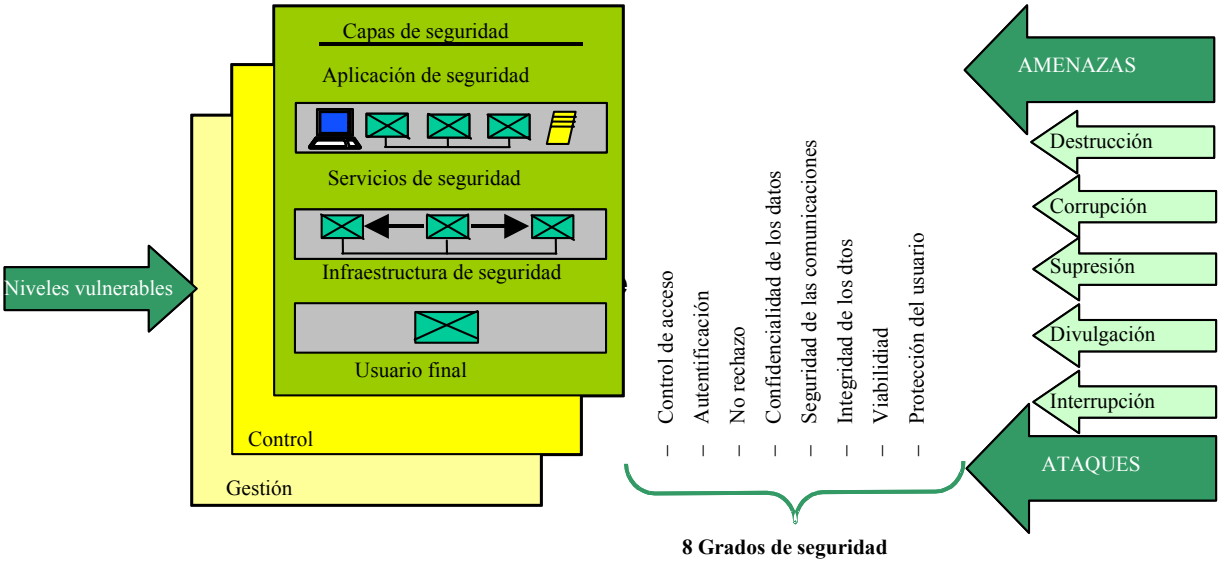
En el Anexo A figura un glosario de la terminología y los acrónimos utilizados en materia de seguridad, y en el Anexo B, un catálogo de las Recomendaciones del UIT-T sobre este tema.

### 8.4.2 Edición de 2004

El Manual ofrece en su edición de 2004 (4 de octubre de 2004) un panorama completo de las numerosas Recomendaciones preparadas por el UIT-T, a veces en colaboración con otros organismos internacionales de normalización, para garantizar la seguridad de la infraestructura de comunicaciones, así como los servicios conexos. Esta segunda edición complementa la publicada a fines de 2003 y abarca los aspectos suplementarios de la seguridad, en particular los relativos a la viabilidad y a los daños que puede ocasionar la ausencia de seguridad en las redes de comunicación. Por otra parte, en el Manual se incluyen los resultados de las actividades de normalización efectuadas desde 2003. Hay que señalar que, por el hecho de tomar en consideración las múltiples facetas de la seguridad, este Manual contribuye a definir un marco de trabajo y una arquitectura que permiten forjarse un lenguaje común para que todos puedan abordar los conceptos definidos.

Después de la introducción que se presenta en el Capítulo 1, en el Capítulo 2 se exponen los elementos y la arquitectura de base en materia de seguridad, tal como éstos se definen en las Recomendaciones del UIT-T. En efecto, se exponen ocho grados de seguridad: protección del usuario, confidencialidad de los datos, no rechazo, control del acceso, seguridad de las comunicaciones y viabilidad. Otros organismos recurren a estos principios generales como fundamentos para preparar normas de seguridad (Recomendaciones de la serie X.800).

**Figura 11 – Elementos de seguridad basados en la Recomendación X.805**




En el Capítulo 3 se exponen los conceptos fundamentales de la seguridad frente a amenazas, vulnerabilidad y riesgos y se explican las relaciones entre dichos conceptos y las normas establecidas por los organismos de normalización sobre el particular.

En el Capítulo 4 se proporciona información para establecer medios de seguridad en favor de las redes de telecomunicaciones.

Concretamente, en esta sección se abordan los objetivos que deben plantearse los encargados de la seguridad de las redes y los servicios asociados, que habrá que tomar en consideración para atender a dichos objetivos.

En el Capítulo 5 se exponen los conceptos de «claves públicas», nociones que revisten gran importancia, así como las infraestructuras que permiten realizar una gestión optimizada. Estas infraestructuras revisten particular importancia como soporte de los servicios de autorización y autenticación.

El UIT-T ha realizado numerosos trabajos sobre seguridad en relación con diferentes sistemas y servicios, lo que ha redundado en la preparación de Recomendaciones. Uno de los principales objetivos del Manual mencionado es la aplicación de estas Recomendaciones y dicha meta se analiza en el Capítulo 6, que versa sobre las aplicaciones vocales y de multimedia con IP (H.323 e IPCablecom), la protección de la salud de los usuarios y el facsímil. Estas aplicaciones se describen en términos de arquitectura de despliegue, así como señalando la forma en que los protocolos se han definido con el fin de atender a las necesidades que suscita

la seguridad. Además, y con el fin de proporcionar información sobre las modalidades de aplicación de la seguridad, se señalan las necesidades que suscitan la seguridad de las infraestructuras de red y la gestión de los servicios de red, y se dan ejemplos al respecto.

El Capítulo 7 aborda la viabilidad que corresponde a los diferentes grados de seguridad y a la infraestructura. Ambos conceptos constituyen el principal tema de los trabajos del UIT-T. Se proporciona información sobre el cálculo de viabilidad y la manera de obtener dicha viabilidad en una red de transporte. En el Capítulo precitado se proporciona orientación para garantizar la seguridad de las redes de transporte.

En el Capítulo 8 se destacan las líneas directrices recientemente aprobadas por el UIT-T en relación con la incidencia de la organización y las medidas que deben adoptarse para afrontar los incidentes de seguridad.

Se admite por lo general que dichos conceptos son indispensables si se desea garantizar la seguridad ante las amenazas que pueden afectar a las infraestructuras de los sistemas de telecomunicaciones y de información.

Por último, en los Anexos del Manual se incluye:

- la lista de Recomendaciones del UIT-T vigentes sobre los aspectos de seguridad;
- la lista de acrónimos y definiciones referentes a la seguridad que se utilizan en el Manual, las Recomendaciones del UIT-T y otros servicios, por ejemplo, la base de datos SANCHO del UIT-T y el compendio de definiciones de seguridad aprobadas del UIT-T, preparado por la Comisión de Estudio 17 del UIT-T;
- la lista de Comisiones de Estudio de la UIT y los trabajos en curso de dichas Comisiones (Cuestiones) en materia de seguridad.

En conclusión, el UIT-T es un elemento esencial para responder a las necesidades de seguridad no sólo en lo que concierne a las tecnologías basadas en el IP, sino también a un gran número de esferas donde las exigencias de seguridad son muy variadas.

El Manual indica de qué forma responden a las necesidades de seguridad las soluciones basadas en las Recomendaciones del UIT-T, tanto desde el punto de vista general (contexto de trabajo y arquitectura) como específico (sistemas y aplicaciones); normalmente, son los operadores de servicios y de redes los que adoptan y aplican estas soluciones.

Estos Informes pueden consultarse en el sitio:

http://www.itu.int/ITU-T/edh/files/security-manual.pdf e itu.int/indoc/itu.t/85097.pdf

## 8.5 Simposio del UIT-T sobre ciberseguridad (octubre de 2004)

En el plano nacional, regional e internacional es cada vez más necesario preparar, aplicar y promover políticas, normas, directivas técnicas y procedimientos que permitan garantizar que los sistemas y las redes TIC resulten menos vulnerables ante diversas amenazas y proteger las informaciones que se memorizan e intercambian en dichos sistemas.

En el marco de los esfuerzos que despliega para contribuir a solucionar estos problemas, la Unión Internacional de Telecomunicaciones celebró el 4 de octubre de 2004, esto es, en vísperas de celebrar su Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT-04) en Florianópolis (Brasil), un Simposio sobre ciberseguridad al que asistieron representantes de alto nivel de un gran número de administraciones, equipos de rápida intervención del sector informático, operadores de redes y fabricantes de equipo, los cuales hicieron balance de la situación en el ámbito de la seguridad y discutieron los enfoques aplicables para garantizar la seguridad del ciberespacio.

Este Simposio de un día de duración giró en torno a los cuatro temas siguientes:

a) los problemas fundamentales que suscitan las amenazas para la ciberseguridad;

b) experiencias y respuestas registradas al hacer frente a estas amenazas;

c) normas, políticas y aspectos reglamentarios y jurídicos;

d) lecciones, experiencias y futura actuación: prácticas óptimas, enfoques e iniciativas que podrían garantizar en mayor medida la seguridad en el ciberespacio.

Cabe resumir como sigue las principales conclusiones a que se llegó en el Simposio sobre ciberseguridad:

1) **La insuficiente seguridad de las redes, en particular de la internet, plantea problemas cada vez más graves**. Por otra parte, estos problemas afectan a esferas más amplias que el mundo de las telecomunicaciones, ya que la informática influye en prácticamente todos los aspectos de nuestras vidas, al ser omnipresentes las redes de información. Y cuando toda la infraestructura sea infraestructura IP, estos problemas se agudizarán. En ausencia de una seguridad adecuada, la internet podría llegar a ser inutilizable en algunos años, especialmente como base estructural de las relaciones económicas mundiales. Además, debido al hecho de que el teléfono móvil está reemplazando al computador personal en cuanto al desempeño de un número creciente de funciones, las redes móviles se verán sometidas en medida creciente a ataques maliciosos.

2) **La seguridad debe integrarse y no añadirse**. La seguridad debe preverse desde el comienzo en el sistema y no organizarse una vez establecido éste. De este principio fundamental se deduce que todas las Recomendaciones y normas han de constar de una sección consagrada a las arquitecturas y protocolos de comunicación, y que dicha sección revestirá siempre importancia.

3) **Los operadores de las redes y los proveedores de servicios internet deben hacer lo que se espera de ellos y combatir la ciberagresión aplicando las mejores prácticas y manteniendo una actitud de vigilancia.** Los operadores, que no pueden depender únicamente de los fabricantes a efectos preventivos, habrán de establecer planes de urgencia, vigilar las actividades realizadas en la red y establecer mecanismos de rápida alerta. La seguridad de las comunicaciones no debe constituir un problema para el usuario sino, por el contrario, ser un elemento intrínseco de las redes.

4) **Es preciso sensibilizar y educar a las partes interesadas (particulares, fabricantes, operadores, empresas y gobiernos).** Resulta necesario conceder particular atención a los problemas de seguridad que se producen en los países en desarrollo. Hoy en día la seguridad preocupa necesariamente a todos, dada la importancia que han adquirido los computadores y las redes en nuestras vidas. Ahora bien, la seguridad es una cadena cuya resistencia es la que tenga el eslabón más débil y hay que disponer de un lenguaje común para llegar a una definición común y constructiva de los diferentes aspectos jurídicos, técnicos, políticos y normativos de la ciberseguridad.

5) **Las diferentes partes interesadas deberían intercambiar la información de que disponen.** Habrá que alentar la constitución de equipos de seguridad/intervención rápida en el sector informático. Los Manuales que versan sobre seguridad (por ejemplo, el Manual sobre seguridad en las telecomunicaciones y las tecnologías de la información en el que se traza un panorama de los aspectos y la aplicación de las Recomendaciones vigentes del UIT-T en materia de telecomunicaciones seguras, octubre de 2004 (110 páginas), www.itu.int/itudoc/itu-t/85097.pdf) y las directivas existentes sobre las «mejores prácticas» y el código de prácticas de gestión para proteger la información (ISO/CEI 17799:2000) constituyen un buen punto de partida. Hoy en día reviste crucial importancia disponer de una norma sobre los sistemas de gestión de seguridad de la información que sea reconocida en el plano internacional y el trabajo de preparación de dicha norma está en curso (se han cubierto ya algunos aspectos relativos a las telecomunicaciones, por ejemplo, en la Recomendación UIT-T X.1051, que se aprobó recientemente).

6) **Es necesario reforzar la cooperación, la colaboración y la asociación internacional en el campo de las políticas de normalización y los marcos jurídicos sobre ciberseguridad.** En todo el mundo se están emprendiendo ya diversas iniciativas en cuanto a este punto, iniciativas que convendría reagrupar.

7) **Los países en desarrollo piden a la UIT que asuma un cometido rector en la esfera de la seguridad, con el fin de que puedan participar en mayor medida en los esfuerzos que permitirán garantizar la seguridad del ciberespacio.**

8) **Huelga decir que la normalización es un componente esencial del enfoque mundial respecto a la ciberseguridad.** En la preparación de normas la seguridad debe ocupar en todo momento un lugar destacado.

   - Hay que acelerar la preparación de normas sobre seguridad, especialmente en lo que respecta a las redes de próxima generación (NGN). Convendría que la UIT mostrase el camino que ha de seguirse en sus esfuerzos de normalización respecto a las NGN (en este sentido, es necesario señalar que uno de los siete Grupos de Trabajo del Grupo Temático de la UIT sobre las redes de próxima generación se encarga precisamente de los asuntos de seguridad).

   - Los organismos y foros de normalización se multiplican y el gran número de normas relativas a la ciberseguridad ya disponibles o en curso de preparación se traducen en problemas de compatibilidad. La UIT podría centralizar los esfuerzos que se emprendan sobre el particular.

   - Los operadores, que se han interesado en cierto modo de las actividades de normalización, deberían colaborar una vez más en estos esfuerzos, ya que el mercado de telecomunicaciones se está reestableciendo después de una crisis sin precedentes.

9) **Es necesario «patrocinar» actividades sobre ciberseguridad en los países que hasta el momento no cuentan con estrategias ni programas en esta esfera.** Convendría explotar en un primer momento varios mecanismos: grupos de discusión en los medios universitarios, asociaciones de consumidores y asociaciones profesionales. Estas actividades iniciales poco onerosas podrían desembocar a su debido tiempo en una colaboración y asociaciones en el plano regional e internacional, y sería posible incluso prever el establecimiento de un sistema de contraataque genuinamente eficaz.

10) **Los gobiernos deberían velar por el establecimiento de un marco jurídico sólido en favor de la ciberseguridad.** Las leyes y políticas deben ser las adecuadas y su aplicación eficaz.

11) **La seguridad es un objetivo y no un derecho adquirido.** En vista de que los problemas de la seguridad se plantean prácticamente siempre antes de los asuntos de organización, huelga decir que habría que revisar en todo momento las políticas, medidas y procedimientos para ajustarlos a los nuevos problemas de inseguridad que puedan plantearse en el mundo informático de la red, de las redes y de los equipos de comunicación.

Para mayor información, consultar: www.itu.int/ITU-T/worksen/cybersecurity/

Se prevé celebrar un segundo Simposio del UIT-T sobre ciberseguridad en marzo de 2005 en Moscú.

## 8.6 Telebiometría

### 8.6.1 Introducción

La biometría humana (del griego antiguo: *tele*: a distancia, *bio*: vida y *metron*: medida o medición) mide parámetros relativos a la fisiología humana, es decir a sistemas naturales.

La biometría se denomina telebiometría cuando sus resultados sirven para la identificación a distancia, sin que sea necesaria la presencia de una persona destinataria de la comunicación. Las señales únicas que representan un individuo y permiten evitar robos y otros fraudes cometidos por identificadores codificados son recopiladas por máquinas normalizadas.

Al ser más difíciles de reparar en caso de avería, los sistemas de datos que utilizan las redes de telecomunicaciones requieren una normalización de los dispositivos de recopilación de registros biométricos coherente con los sistemas de medición normalizados.

### 8.6.2 Trabajos en el ámbito mundial

La Oficina Internacional de Pesos y Medidas (Sistema Internacional de Unidades) creó las bases que se describen en las normas ISO 31 y CEI 60027. El Grupo de Trabajo Técnico 12 (ISO/TC12), encargado de las cantidades y las unidades (www.iso.ch.), y el Grupo de Trabajo Técnico 25 (CEI/TC25), encargado de las cantidades, las unidades y su símbolo alfabético (www.iec.ch), incorporaron la lista de magnitudes y unidades de medida en un directorio internacional válido, habida cuenta de la solidez de los acuerdos que engloban el conjunto de las ciencias. ISO/IEC JTC 1/SC 37 Biometrics está elaborando nuevas normas sobre las tecnologías de biometría genética relativas al cuerpo humano para garantizar el interfuncionamiento y el intercambio de datos entre aplicaciones y sistemas.

La seguridad de los usuarios de los dispositivos de identificación biométrica para el caso de las telecomunicaciones requiere el examen ordenado de esferas de conocimiento en el marco del proceso de concepción de la normalización de la seguridad. Las ciencias fisiológicas y del comportamiento se han organizado ya en subcomités para obtener las especificaciones que requieren los fabricantes de equipos de la industria telebiométrica, con el fin de comercializar productos basados en los conocimientos científicos disponibles que permitan salvaguardar íntegramente los parámetros de los seres vivientes y extraer y encriptar los datos biométricos recogidos.

Actualmente, la ISO y la CEI colaboran con miras a la publicación de una nueva serie de normas ISO/CEI 80.000. Además, la CEI trabaja sobre una nueva propuesta de trabajo (NWP 277) sobre unidades fisiológicas.

Entre otras organizaciones internacionales de normalización que se han interesado en la telebiometría, hay que señalar:

– El Grupo Temático sobre Biometría del ETSI (www.etsi.org).
– Grupo Especial de Ingeniería de internet (IETF) www.ietsi.org.
– La Organización para el Fomento de Normas Estructuradas de Información (OASIS) www.oasis.open.org.

### 8.6.3 Trabajos del UIT-T

Durante el periodo de estudios 2001-2004, y en el marco de la Cuestión 10/17, Imperativos de modelos de seguridad y directrices para los sistemas de telecomunicaciones de la Comisión de Estudios 17 del UIT-T, se examinó un gran número de documentos relativos a la próxima comercialización de soluciones de seguridad basadas en un dispositivo material (equipos) y que contienen uno o dos parámetros biométricos.

Se ha tomado en consideración la necesidad de examinar la esfera de privacidad personal (PPS), que tiene 2 metros de diámetro (el Hombre Perfecto, según Leonardo Da Vinci). Cuando se propone una solución para efectuar una identificación y autenticación normalizadas del usuario de dispositivos biométricos, hay que dar a éste definiciones de la seguridad que se le ofrece a todos los niveles de interacción entre los datos biométricos únicos (e irreemplazables) y la entrada automatizada en las redes de telecomunicación. Por otra parte, la identificación y autentificación voluntarias, que se han visto reforzadas por una seguridad del consentimiento mediante firma digital fundada en la propia fisiología del usuario, ofrece una serie de informaciones utilizables con fines de seguridad y tarificación, que aprecian los operadores de las redes. Se ha obtenido consenso en relación con el modelo marco de la telebiometría multimodal, gracias a la multifuncionalidad de estas taxonomías, con el fin de eliminar toda tendencia a la tecnofobia por parte de los usuarios y responder a las preocupaciones de los operadores de redes.

La Recomendación marco X.1081 del UIT-T aborda la taxonomía multimodal de las operaciones telebiométricas. Tras cuatro años de trabajo, esta Recomendación, publicada a principios de 2004, ha dado paso a numerosos productos que pertenecerán a los nuevos terminales protegidos de telefonía y semafonía. El modelo marco telebiométrico multimodal (TMMF) que se define en la Recomendación X.1081 del UIT-T permite, además, crear un mercado equitativo para los usuarios de redes: el ciudadano libre proporciona una garantía basada en las ciencias biométricas a su proveedor de servicios de telecomunicaciones a cambio de una garantía, basada en los conocimientos actuales, de la total inocuidad de los terminales telebiométricos

según los parámetros de la persona que los utiliza. Los integradores de soluciones telebiométricas ofrecerán en fecha próxima dispositivos de telefonía, semafonía con un sensor biométrico y capacidades de codificación capaces de dar al terminal de quien reciba la comunicación pruebas suficientes que le permitan identificar a quién la origina para atender satisfactoriamente a los objetivos de una política de seguridad óptima, denominada Salvaguarda y seguridad óptima, concepto fundamental del modelo marco de la telebiometría multimodal.

De este modo, se dará a los fabricantes de equipo una importante ventaja para combatir a los impostores adaptando la norma internacional mencionada. Por otra parte, se ha justificado adecuadamente las especificaciones relativas de las características de los terminales telebiométricos de telecomunicaciones. Las soluciones tecnológicas evitan que el derecho consagre las pretensiones infundadas de lo científico, así como distinguir entre los problemas reales que plantean la seguridad y las invenciones psicopáticas o sociopáticas (fobias tecnológicas).

Después de marzo de 2004, la Cuestión 10/17 se dividió en 6 nuevas Cuestiones para el periodo de estudios 2005-2008, entre las que cabe señalar la Cuestión K/17 en cuyo marco se examina la «Telebiometría segura».

Se prevé proporcionar un conjunto de adecuadas soluciones tecnológicas al especificar los sensores telebiométricos. En el marco de la Cuestión 8/17 se ha considerado necesario tomar las siguientes medidas:

1) para autenticar la identidad de cada ciudadano, habrá que acopiar los datos biométricos con sensores inocuos y seguros. La Recomendación UIT-T X.1081 en la que se define un modelo marco de telebiometría multimodal (TMMF), habrá de completarse mediante la creación de una base de datos telebiométrica sobre salvaguarda y seguridad óptimas;
2) la transmisión y el almacenamiento seguros de estos datos personales biométricos confidenciales es un asunto que plantea considerables riesgos y se examina en una Recomendación sobre el procedimiento de protección telebiométrica (TPP) que está en curso de preparación;
3) para resolver este problema de seguridad y privacidad, se ha propuesto un sistema X.509 en una Recomendación sobre el mecanismo de sistema telebiométrico (TSM) basado en PKI, que se encuentra en curso de preparación;
4) habrá que examinar los sensores biométricos y el equipo de procesamiento que permite comparar los datos biométricos almacenados con los medidos en el marco de cualquier proceso de autenticación. Habrá que clasificar jerárquicamente dispositivos de seguridad para atender a las peticiones formuladas expresamente en este sentido por los países en desarrollo, lo que entraña la necesidad de definir equipo a prueba de manipulación indebida.

**Conclusiones**

El modelo cuadro de telebiometría multimodal permite garantizar de manera hasta cierto punto óptima la identidad de un usuario de redes de telecomunicación, respetando al mismo tiempo las libertades civiles elementales y la salvaguarda de los datos únicos conferidos por la naturaleza y, a menudo, irreemplazables para el usuario.

Asimismo, la entrada en una red de telecomunicaciones de un agente inteligente incorporado que autorice identificación telebiométrica y de ser posible que compartan responsabilidades entre el operador que puede garantizar la seguridad de los datos (codificación) y el usuario que está en condiciones de garantizar la seguridad de su terminal con una función telebiométrica.

### 8.6.4 Estudio de caso: Estados Unidos

Para promover la protección de sus ciudadanos, Estados Unidos estableció controles biométricos en los puntos de entrada a su territorio. En efecto, en septiembre de 2004, 115 aeropuertos internacionales, 14 zonas portuarias y una cincuentena de puntos de paso en las fronteras se dotaron de sistemas que toman sistemáticamente la fotografía y las huellas digitales de los viajeros internacionales y unos 40 millones de personas deberán someterse anualmente a este proceso biométrico cuando presenten sus pasaportes a los funcionarios de emigración.

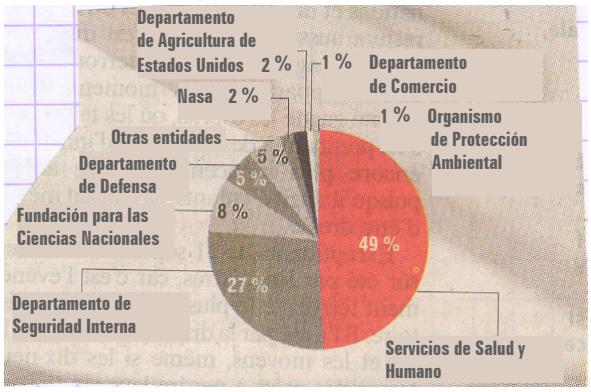
Una vez digitalizados, estos datos se centralizarán y compararán a los que contiene la base de datos del sistema de preselección de pasajeros asistido por computador (CAPPS), que determinará si los funcionarios de inmigración deben considerar sospechoso a un pasajero.

Esta base se alimenta también mediante los datos proporcionados por ciertas compañías de aviación estadounidenses y los dos principales sistemas de reserva aérea (Sabre y Galileo), los cuales han aceptado transmitir parte de su información a la Administración de Seguridad en el Transporte (TSA), dependencia que administra el sistema. Otras entidades se han rehusado a ello y actualmente todas las partes interesadas participan en negociaciones para determinar la índole exacta de las informaciones que los transportistas deberán comunicar obligatoriamente.

Este sistema de control retarda en gran medida las formalidades de entrada en el país y para combatir un embotellamiento que podría ser imposible de resolver, las autoridades estadounidenses acaban de lanzar un programa piloto denominado «Registered Traveller», que concierne a más de 10 000 grandes viajeros (octubre de 2004), que podrán pasar prácticamente sin detenerse durante los controles fronterizos, por ejemplo ejecutivos que viajan al extranjero por motivos profesionales. Provistos de una tarjeta inteligente a la que se hayan incorporado sus datos biométricos, sólo estos pasajeros deberán detenerse unos cuantos segundos ante una cámara que tomará una fotografía de la persona que se trate y la comparará con los datos almacenados.

Gracias a este dispositivo muy informatizado, que entraña la interconexión de bases de datos administradas por organismos públicos y privados el Gobierno de Estados Unidos espera aumentar la seguridad y acelerar el proceso de paso por los controles de inmigración. Además, las informaciones que queden contenidas en el sistema «Registered Traveler» se utilizarán únicamente con propósitos de seguridad.

**Figura 12 – Financiación e investigación sobre seguridad en Estados Unidos**




(En porcentaje durante 2004); total: 3 400 millones USD
Fuente: (AAAS) Les «Echos»

## 8.7 Compendio de seguridad

En el marco de la Cuestión 4/17, Proyecto de seguridad de los sistemas de comunicaciones, la Comisión de Estudio 17 ha preparado y actualiza periódicamente un compendio de seguridad de sistemas de comunicación, que se divide en tres partes:

– un catálogo de Recomendaciones aprobadas del UIT-T sobre seguridad;
– un extracto de definiciones de seguridad extraído de Recomendaciones aprobadas del UIT-T y de otras normas;
– una lista de Cuestiones del UIT-T relacionadas con la seguridad.

Es posible consultar el compendio en la página web de la Comisión de Estudio 17 perteneciente al sitio web de la UIT (http://www.itu.int/ITU-T/studygroups/com17/tel-security.html). El compendio de definiciones de seguridad permite darse una idea global de la terminología de seguridad utilizada por las diferentes Comisiones de Estudio del UIT-T.

# 9 Centro de Control y Capacitación de Transmisiones de Datos, incluido el IP

## 9.1 Introducción

En el presente Capítulo se describe un sistema de control de transmisiones de datos, incluidas las que utiliza el IP, denominado Centro de Control y Capacitación de Transmisiones de Datos (CCATD) destinado al regulador nacional de telecomunicaciones para garantizar la seguridad y el control de las comunicaciones en el ejercicio de sus funciones de salvaguarda de la soberanía nacional contra «piratas informáticos intencionales o accidentales». Este sistema es conforme con las Recomendaciones de la UIT así como con el Capítulo 5 del Manual UIT-R «Control Técnico del Espectro Radioeléctrico».

El CCATD permite el tratamiento de los datos interceptados en las diferentes redes de telecomunicaciones, independientemente de que sean inteligibles y estén codificados, comprimidos o protegidos. Reconoce los distintos formatos de datos transmitidos (tipo de módem, niveles de protocolo IP) y hace posible demodular y decodificar de manera fiable los formatos conocidos y reconocidos, que convierten clara y comprensiblemente, sobre todo cuando se trata de protocolos utilizados en la red Internet.

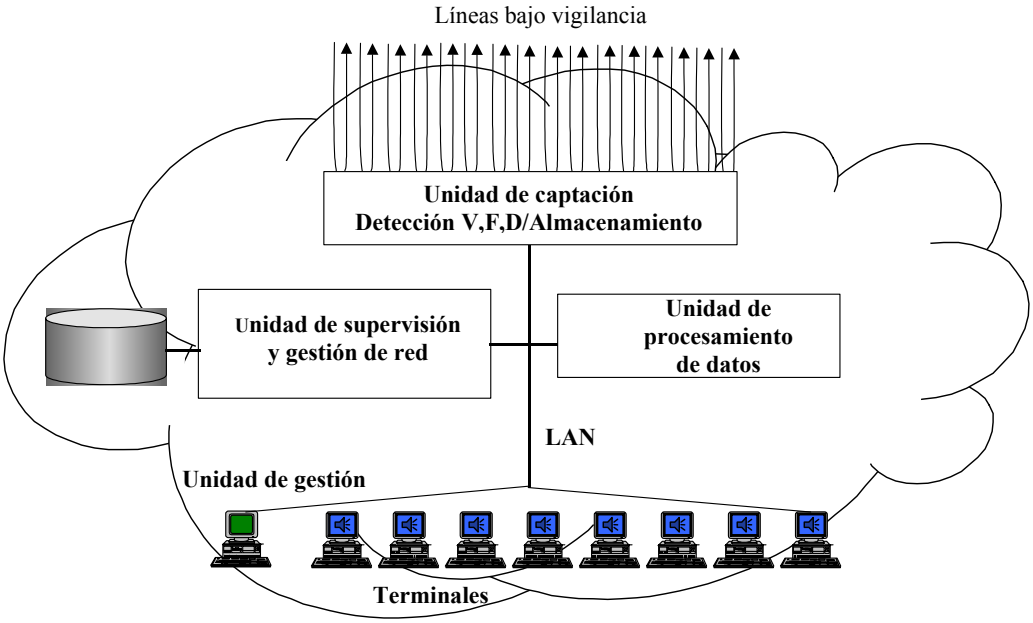
El CCATD es un sistema abierto, flexible y fácil de utilizar, que incluye tres unidades funcionales principales (véase la Figura 13).

- Unidad de captación: intercepta las comunicaciones encaminadas al CCATD y que proceden de los operadores de telecomunicación (telefonía fija, móvil, cable o canal a alta velocidad), extrae el contenido y formateado de muestras de señalización de las comunicaciones y clasifica informaciones claras (separación de la voz, facsímil, datos) y de informaciones poco claras.

- Unidad de supervisión: supervisa la utilización de las intercepciones en el CCATD, encamina hacia los centros que no dependen del CCATD y supervisa el sistema (estado de los módulos de adquisición, registro diario de los acontecimientos, administración de los perfiles del usuario, estadísticas sobre el sistema, etc.).

- Unidad de tratamiento: accede al contenido demodulando o decodificando y formateando los ficheros producidos.

**Figura 13 – Diagrama del Centro de Control y Captación de Transmisiones de Datos**




Las capacidades de «procesamiento» de las intercepciones (demodulación, localización de los protocolos internet, etc.) se integran como módulos de programas informáticos que intervienen a través de un servidor de procesamiento. De este modo, las capacidades del sistema en cuanto a potencia de cálculo (incorporación de servidores físicos, repartición de los tratamientos) e (incorporación de un nuevo procesamiento en el servidor), pueden aumentarse sin dificultad.

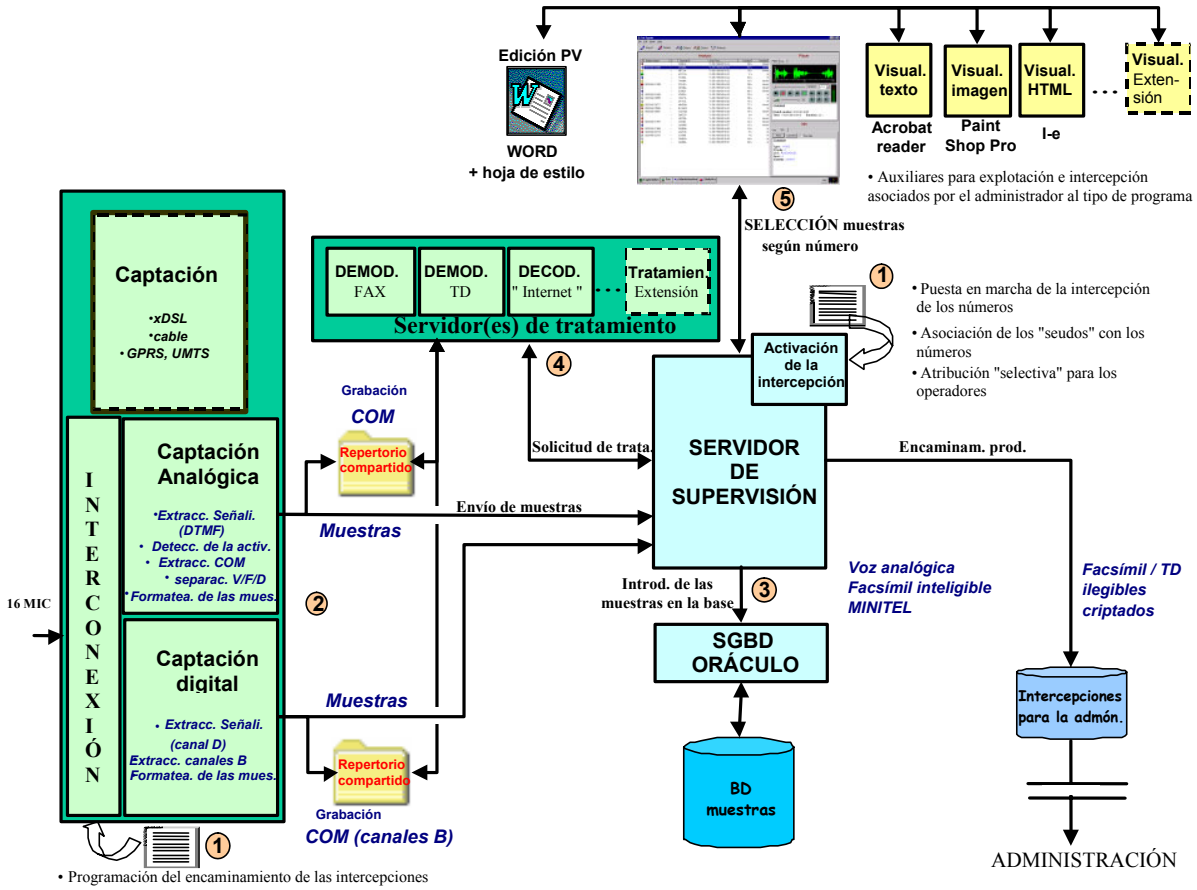
## 9.2 Descripción y arquitectura del CCATD

Las principales funciones del sistema CCATD son las siguientes:

- captación de las comunicaciones en enlaces específicos;
- extracción de la señalización formateada en una muestra;
- detección del tipo de transmisión: facsímil/datos;
- demodulación de las principales normas de transmisión de datos;
- decodificación de los protocolos y formatos de las principales normas de transmisión de datos;
- detección de las transmisiones claras/encriptadas;
- utilización local de las grabaciones;
- encaminamiento de las transmisiones encriptadas hacia una entidad externa.

A continuación en la Figura 14 se presenta la arquitectura del CCATD.

**Figura 14 – Arquitectura del sistema CCATD**




1 El centro del sistema es un servidor de supervisión que gestiona todos los intercambios entre los diferentes componentes internos al sistema (adquisición => procesamiento => explotación) y los componentes exteriores. En el arranque operacional del sistema hay una primera etapa, que es la de configuración de las intercepciones y está a cargo del jefe del CCATD. Éste dispone de las atribuciones de administración necesarias para introducir en el nivel del servidor de supervisión, los números objeto de intercepción y los seudónimos asociados, para cada canal de adquisición. Además, programa la interconexión de las comunicaciones interceptadas que ha transmitido el operador de telecomunicaciones para reagruparlas en un canal de adquisición.

Para finalizar esta etapa de configuración, el jefe del CCATD asocia los números objeto de intecepción en pequeños grupos que se distribuyen a los diferentes usuarios según su finalidad.

2 La captación se ajusta a medios de comunicación que poseen sus propias capacidades de almacenamiento. Cada módulo de captación selecciona previamente las intercepciones, análizando la señalización y el contenido de las comunicaciones (selección con respecto al número y a la detección de voz/datos). Además, almacena el contenido de las comunicaciones, y crea una muestra de intercepción destinada al servidor de superivisión con las informaciones necesarias para la selección y la ubicación de la comunicación correspondiente.

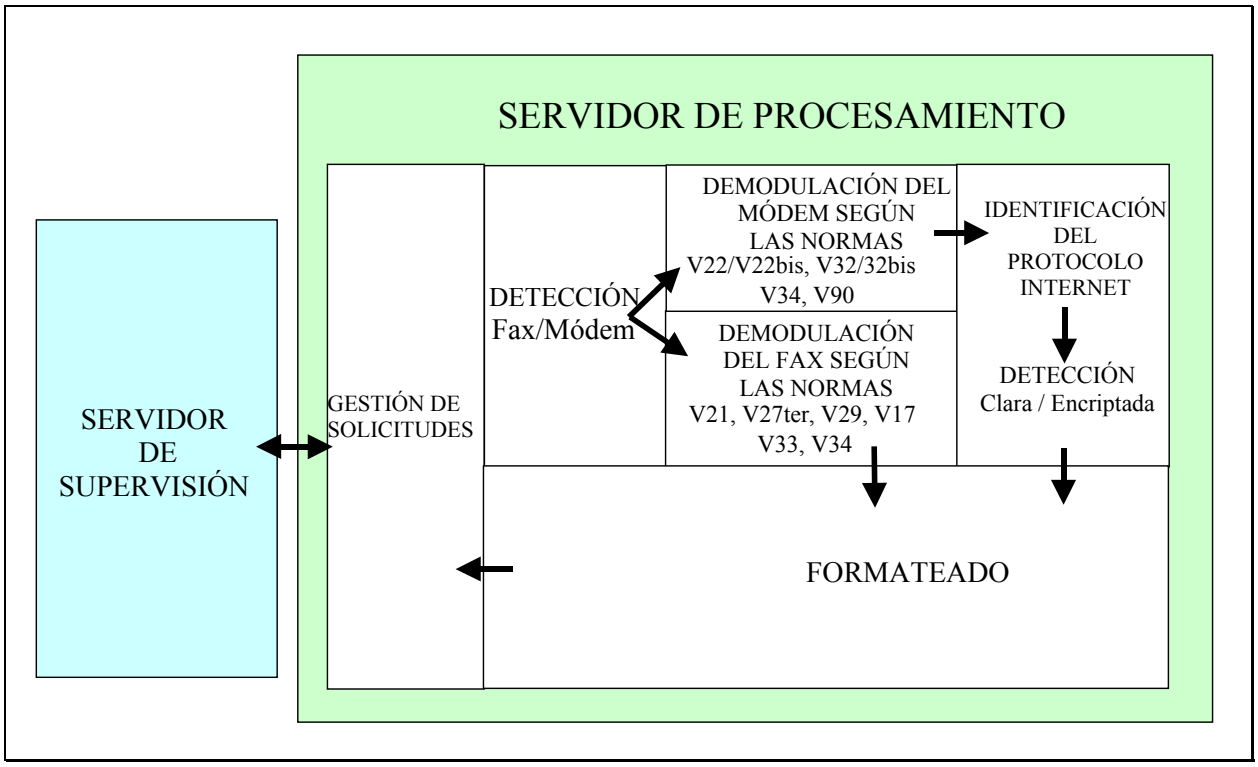
③ El servidor de supervisión introduce la muestra en la base de datos de la intercepción. Si la grabación requiere procesamiento para acceder al contenido (en el caso de la transmisión de datos), el módulo de supervisión llama automáticamente al servidor de procesamiento y le suministra todas las informaciones útiles de la muestra (tipo de comunicación, ubicación de la comunicación, etc.).

El servidor de procesamiento recupera los datos brutos digitalizados de la comunicación en el nivel del módulo de adquisición diseñado para este fin, planifica por secuencias los tratamientos y envía los datos resultantes al nivel del módulo de adquisición. Informa al servidor supervisión sobre el estado del tratamiento.

④ El servidor de procesamiento (véase la Figura 15) da acceso a los siguientes tratamientos:

- demodulación,
- decodificación de los protocolos y formatos asociados,
- detección de las transmisiones de datos criptadas.

**Figura 15 – Funciones del módulo de tratamiento del CCATD**




⑤ De este modo el operador puede utilizar los ficheros en cuestión a partir de la lista de intercepciones a las que tiene acceso.

En esta arquitectura distribuida cada módulo de captación (actual y futuro) dispone de sus propios medios de almacenamiento. La repartición de la carga de almacenamiento en los módulos de captación permite al servidor de supervisión evitar que se saturen sus medios de comunicación y sus capacidades de almacenamiento en caso de que aumente la variedad y la cantidad de módulos de captación.

Esta elección en cuanto a la arquitectura compartida no sólo permite optimizar la utilización del computador y los recursos de la red, sino también facilitar el desarrollo del sistema.

La arquitectura del CCATD facilita la evolución de las capacidades de rendimiento por su diseño:

- utilización sistemática de interfaces y formatos ordinarios o normalizados (ejemplo: página HTML, .htm, sonido .wav, etc.),
- adopción de lenguajes normalizados y un diseño orientado hacia los objetivos,
- conservación de las capacidades de extensión tecnológica,
- utilización del computador personal para realizar los tratamientos y de esta manera facilitar la evolución y la actualización (taller de programación de alto nivel, competencias informáticas comunes) y de aparatos y equipos informáticos normalizados.

La adopción de estas medidas en lo que respecta a la arquitectura facilita la integración de aportes ulteriores sin tener que recurrir sistemáticamente al proveedor del sistema.

La elección de este tipo de arquitectura distribuida permite optimizar la utilización de los recursos informáticos y de red y que el sistema evolucione con mayor facilidad.

# 10 Estudios de caso

## 10.1 UIT

En el marco de las actividades del UIT-T, en mayo de 2002 se celebró en Corea un taller sobre la seguridad de las redes y, principalmente, sobre los aspectos técnicos que permiten la seguridad de las redes de comunicaciones. Se introdujo el concepto de «infraestructura crítica» (*critical infrastructure*). Según la UIT, las infraestructuras de redes son las redes públicas o privadas capaces de transportar grandes volúmenes de datos más allá de las fronteras nacionales. Las «redes críticas» son las que transmiten información relacionada con la seguridad nacional o financiera con gran valor añadido. Los países siguientes han presentado estudios de caso sobre la seguridad de las redes y sus reglamentaciones: Brasil, Canadá, Corea y Países Bajos.

Toda esta información figura en el sitio: http://www.itu.int/org/spu/ni/ipdc/index.html

La UIT tiene previsto volver a celebrar un taller del mismo tipo en octubre de 2005.

## 10.2 Seguridad de las redes en el mundo

A fines de 2002, el Gobierno francés publicó un documento (www.cfce.fr/ntic) en el que se describe la situación de la seguridad de los sistemas y redes de comunicaciones a nivel mundial. Éste es el resumen de dicho estudio:

**África del Norte y Oriente Próximo**

Habida cuenta del bajo índice de penetración de internet y el comercio electrónico en la mayoría de los países de la región, el problema de la seguridad de las redes se plantea a menor escala y el marco reglamentario es prácticamente inexistente.

**África Subsahariana**

En el plano reglamentario, la seguridad de las redes no es todavía una preocupación de primer orden para las autoridades locales, que se hallan más concentradas en la instalación de dichas redes que en su protección.

El cifrado y la encripción de los datos se practican todavía poco, por lo que las autoridades ejercen un control restringido.

**América del Norte**

Esta zona se caracteriza por la ausencia de restricciones con respecto a la criptografía y la confidencialidad de las comunicaciones. Se trata de una situación que responde a la voluntad de no obstaculizar el desarrollo de los intercambios electrónicos y de la industria de las NTIC en general, favoreciendo en contrapartida una autorregulación del sector. Sin embargo, los gobiernos intervienen de manera mucho más activa en el campo de la seguridad nacional. En el plano de la oferta, cabe señalar el avance comercial de las técnicas de biometría o de los sistemas que utilizan tarjetas inteligentes. Las últimas soluciones de seguridad que se están diseñando actualmente en América del Norte corresponden a las VPN y las redes inalámbricas WLAN.

**América Latina**

La seguridad de las redes de comunicaciones es una preocupación secundaria en la mayoría de los países de esta zona. La norma internacional ISO/CEI 17799, en la que se etiquetan los procedimientos de seguridad de la información, ya ha sido adoptada por algunos órganos encargados de la normalización, aunque su difusión en la región sigue siendo limitada. En lo que se refiere al cifrado, América Latina se caracteriza por un vacío jurídico que permite la libre utilización de estas tecnologías.

**Asia**

Primeramente, los países de Asia se caracterizan por la ausencia de un marco legislativo sobre la seguridad de las redes. Consumidores y empresas tienen libertad para optar por las soluciones de seguridad que juzguen apropiadas. Con frecuencia, los gobiernos sientan ejemplo utilizando sistemas de tipo PKI.

El mercado de la seguridad ha experimentado un verdadero auge en los dos últimos años. Cabe destacar que últimamente la demanda en la India se ha orientado hacia sistemas más sofisticados, tales como los servicios de detección de intrusos, la gestión del contenido, la identificación, el filtrado URL, los servicios de asesoramiento en materia de seguridad, los sistemas de criptografía que comprenden las PKI (*public key infrastructure*) y redes privadas virtuales.

**Europa**

La mayoría de los gobiernos europeos han tomado conciencia de la importancia que reviste la seguridad de las infraestructuras de telecomunicaciones. La disponibilidad e integridad de las redes están básicamente garantizadas por las normas impuestas a los operadores de telecomunicaciones en el marco de las licencias concedidas. Son muchos los países que han instalado o están instalando redes privadas destinadas a las fuerzas de policía y protección civil. Los Estados Miembros de la Unión Europea ya utilizan habitualmente la criptografía. Los principales desafíos son la seguridad de las comunicaciones móviles y el paso al protocolo IPv6.

**Oriente Medio**

El uso de los sistemas de cifrado sigue siendo relativamente libre en Oriente Medio. Los operadores nacionales de telecomunicaciones, a menudo en régimen de monopolio, administran las comunicaciones electrónicas por un sistema de filtrado.

Aunque las últimas tecnologías en materia de seguridad de redes se encuentran disponibles, todavía no se utilizan en las empresas locales, la mayor parte de las cuales están satisfechas con sistemas simples. Las empresas apenas están comenzando a tomar conciencia de la importancia de la seguridad de sus comunicaciones en un momento en que el comercio electrónico hace su aparición en Oriente Medio.

**Síntesis mundial**

En una sociedad de la información cada vez más interconectada, las amenazas de actos terroristas que se han venido produciendo desde fines de 2002 han puesto de relieve la importancia de la seguridad de las redes de comunicaciones. La toma de conciencia con respecto a estos desafíos, principalmente económicos, varía de un país a otro en función de su nivel de desarrollo. Así, los países más desfavorecidos muestran mayor interés en la instalación de las redes que en su protección, mientras que los países más desarrollados se centran sobre todo en la seguridad de las comunicaciones del sector público.

## 10.3 La lucha contra el spam

Nos hemos adentrado en la era del correo electrónico y los mensajes instantáneos. Desafortunadamente, el hecho de que el correo electrónico sea tan barato y fácil de utilizar constituye la fuente de nuevos problemas, entre los que cabe señalar el spam (envío masivo de correo electrónico no solicitado), también denominado spam-ming o correo electrónico basura.

### 10.3.1 Origen y definición

El spam es el correo electrónico que se envía a personas que no lo han solicitado. Cualquiera puede enviar spam, ya que resulta muy fácil y no es costoso. Sin embargo, pocas son las personas que aprecian recibir estos mensajes y menos aún las que saben ponerles coto. El spam no sólo contribuye a perder tiempo. Cada año los proveedores de acceso a internet y los operadores de servicios móviles invierten millones USD en almacenar, transmitir y controlar el spam. Estos costos se cobran a su vez a los clientes finales. Además, el spam repercute negativamente en la productividad de las empresas. Las administraciones y las empresas ya han reconocido que el correo electrónico es esencial, si desean realizar de manera óptima sus actividades. Dado que sus empleados lo utilizan cada vez más, aumentar la eficacia de este instrumento de trabajo se ha convertido en una prioridad y filtrar el spam, en una necesidad.

### 10.3.2 Spam: Fenómeno social y técnico

El spam es un fenómeno social y técnico. Su aspecto social, esto es, que hayan sido seres humanos y no computadores quienes han creado el spam, hace que este fenómeno sea algo no sólo mecánico sino también orgánico. La lucha contra el spam no se limita únicamente a una lucha contra un programa o un computador. Se combate contra un ejército de individuos que piensan, respiran y despliegan un arsenal de armas contra la humanidad. Su arma más potente es el cambio, es decir, la posibilidad de modificar constantemente su comportamiento.

El spam está en continua mutación. Los autores de mensajes spam cambian constantemente sus tácticas para eludir los filtros que se instalan. Por ejemplo, suelen modificar los encabezados de los mensajes, que incluyen información detallada como la dirección IP de la fuente, y cambian con frecuencia el nombre de sus sitios en internet.

Así pues, para ser realmente eficaces, los filtros deben poder adaptarse constantemente con el fin de enfrentarse a hábiles adversarios.

Como los autores de mensajes spam modifican sin cesar sus técnicas de ataque y mensajería, no es eficaz utilizar un sistema de filtrado centrado en una única variable (dirección IP o contenido del mensaje, por ejemplo). Una solución eficaz para luchar contra el spam debe ser lo suficientemente compleja como para incorporar simultáneamente varias variables.

### 10.3.3 Criterios fundamentales en la lucha contra el spam

Cuatro criterios son capitales, a saber: eficacia, previsión, facilidad de adopción y resultados.

- El criterio más importante que ha de seguirse para encontrar una solución contra el spam es la eficacia: el número de spam que puede bloquear un filtro.

- Otro factor muy importante es la precisión: la solución que se adopte no debe bloquear los mensajes legítimos. Para que la mayoría de los posibles usuarios acepte una solución contra el spam, es preciso distinguir claramente los mensajes spam de los legítimos.
- La siguiente prioridad es la facilidad de adopción, que está directamente relacionada con la facilidad de instalación y utilización. ¿La solución adoptada ha de exigir a los usuarios crear sus propios filtros? ¿Los propios usuarios finales habrán de encargarse de su actualización? ¿Es en esencia transparente para los usuarios? Si la solución no es fácil de utilizar, probablemente se utilizará mal o no se utilizará en modo alguno.
- Por último, los resultados o la rapidez del filtrado son también factores importantes. ¿La solución contribuirá a frenar la entrega de correo electrónico? Este aspecto puede ser decisivo, en particular para los grandes proveedores de acceso, los cuales controlan y deben transmitir un gran volumen de mensajes.

### 10.3.4 Soluciones técnicas de la lucha contra el spam

Las principales soluciones contra el spam guardan relación con las siguientes metodologías:

a) Bloqueo de direcciones IP

El «Mail Abuse Prevention System Realtime Blackhole List (MAPS RBL)» consiste en una «lista negra», actualizada en tiempo real, por la que se informa sobre los dominios identificados como «favorables o al menos neutros» a los autores de mensajes spam. El sistema MAPS RBL permite a los administradores de mensajería actualizar inmediatamente sus listas de dominios bloqueados y direcciones IP, y realizar dichas actualizaciones de manera automática desde los servidores.

Sin embargo, el sistema bloquea indiscriminadamente dominios enteros. Por lo tanto, el sistema MAPS RBL actúa con prudencia cuando añade nombres a su lista negra. La decisión de bloquear un dominio exige una minuciosa tarea de investigación, que, por tanto puede ser larga. Finalmente cuando se añade un dominio a la lista negra, el número de spam se reduce ostensiblemente.

En resumen, el sistema MAPS RBL no constituye, por sí solo una solución viable para luchar contra el spam y suele combinarse con otras técnicas, pese a su tendencia a bloquear correos electrónicos legítimos.

b) Filtrado del contenido

Desde el punto de vista de la eficacia, hay que señalar que el filtrado del contenido suele provocar problemas parecidos a los que ocasiona la técnica del bloqueo de direcciones IP.

Algunas soluciones de filtrado combinan el filtrado del contenido y el bloqueo de direcciones IP. Estas soluciones incluyen generalmente varios filtros estáticos y permiten a los administradores de redes definir sus propios filtros. Estos filtros de contenido no suelen actualizarse sistemáticamente a partir de una base central. En el mejor de los casos, dichas actualizaciones se realizan mensualmente. Estas soluciones permiten filtrar no sólo el contenido del cuerpo o el tema del mensaje, sino también, en ocasiones, al remitente, así como los mensajes a nivel del servidor, por lo que son fáciles de utilizar. Sin embargo, no permiten detener sistemáticamente el spam puesto que se bloquea del orden del 0 al 2,21% del correo electrónico legítimo.

c) Utilización de firmas contra el spam

La utilización de firmas específicas contra el spam se basa en el modelo implantado por los editores de programas antivirus, los cuales vigilan y detectan la aparición de nuevas amenazas y elaboran reglas que permiten actualizar los filtros, para proteger así la integridad y la seguridad de los sistemas. Puede aplicarse el mismo método al correo electrónico. Los operadores especializados y/o los fabricantes de computadores establecen reglas de filtrado que determinan si los mensajes son efectivamente los deseados o no.

Un aspecto decisivo sigue siendo la capacidad de vigilar en tiempo real la actividad de los autores de mensajes spam. Una red de direcciones de correo electrónico que actúan como señuelo, situada en internet, en lugares que se conocen por ser favorables, contribuye a atraer mensajes spam; acto

seguido, se envían automáticamente a un centro de operaciones que funciona 24 horas al día. Inmediatamente se definen reglas sobre la base de los spam más recientes y estas reglas se transmiten a los programas de filtrado instalados en los servidores de mensajería de los clientes.

Esta solución es viable, ya que las reglas de filtrado pueden activarse o desactivarse según se quiera y en función de su grado de utilidad en un momento dado.

### 10.3.5 Trabajos de la OCDE sobre el spam

La OCDE organizó un taller de trabajo los días 2 y 3 de febrero de 2004 en Bruselas, en colaboración con la Comisión Europea (Dirección de la Empresa y la Sociedad de la Información sobre el spam). El programa y las presentaciones realizadas pueden consultarse en el sitio web de la OCDE.

Cabe señalar los siguientes puntos importantes:

*Sesión 1*

Los gobiernos, los usuarios y los representantes de la industria han de identificar las características del spam para poder elaborar un Informe sobre este problema y solucionarlo. Además, han de establecerse principios destinados a evaluar los esfuerzos que han de desplegarse para suprimir el spam y su expansión; es preciso determinar las medidas que se han de adoptar para luchar contra el spam.

*Sesión 2*

Las repercusiones nefastas del spam son comunes para todas las categorías de usuarios de internet, tanto los particulares como las personas que se ocupan de asuntos comerciales, los gobiernos, las administraciones encargadas de los servicios de gestión y los proveedores de dichos servicios. La erradicación del spam implica importantes costos, económicos y también sociales, para todos ellos. En esta sesión se examinaron todos los costos asociados al spam, teniendo en cuenta el principio de la protección de los usuarios, la confidencialidad de los mensajes y la seguridad de las redes en relación con las líneas directrices de la OCDE a este respecto.

*Sesión 3*

En esta sesión se examinaron los mecanismos, las nuevas tecnologías y los modelos de spam, y se plantearon las siguientes preguntas:

- ¿cómo obtienen los autores de mensajes spam las direcciones de correo-e?;
- ¿cómo es posible que no puedan detectarse los autores de estos mensajes?;
- ¿cómo se puede sacar provecho económico del envío de mensajes spam?;
- ¿cómo se pueden modificar las tecnologías para evitar ofrecer nuevas posibilidades a los autores de mensajes spam (por ejemplo, el envío de spam a través de SMS o mensajería instantánea)?;
- ¿cómo se puede erradicar y detener el fenómeno spam y aumentar el crecimiento del volumen de mensajes de correo-e con ayuda de nuevas tecnologías y una nueva legislación?

*Sesión 4*

Se estudiaron los distintos mecanismos técnicos existentes para luchar contra los ataques spam tanto en el ámbito comercial como en lo que respecta a los proveedores de servicios de internet (PSI).

*Sesión 5*

En esta reunión se examinaron distintas leyes en vigor en los países miembros de la OCDE destinadas a regular el spam.

*Sesión 6*

El spam es un problema de orden mundial y requiere una solución mundial. Aunque resultaría complicado elaborar una ley internacional eficaz contra el spam, sería posible hacerlo si se tomaran como base las leyes nacionales existentes. Para ello han de desplegarse esfuerzos de cooperación.

*Sesión 7*

En ella se estudiaron las mejores prácticas destinadas a minimizar los efectos del spam en las comunicaciones electrónicas.

*Sesión 8*

Para erradicar el spam es necesario adoptar un enfoque multidimensional.

*Sesión 9*

Se determinaron en esta sesión las próximas medidas que han de adoptarse en el ámbito internacional para luchar contra el spam.

(Véase http://www.oecd.org/document/47/0,2340,en_2649_2255297_26514927_1_1_1_1,00.html)

### 10.3.6 Seminario de la UIT sobre el spam

En el punto 37 de la Declaración de Principios adoptada en la Cumbre Mundial sobre la Sociedad de la Información (CMSI), celebrada en Ginebra en diciembre de 2003, los participantes en ella reconocen que *el envío masivo de mensajes electrónicos no solicitados (spam) es un problema considerable y creciente para los usuarios, las redes e internet en general*. Además, en el punto C5 d) del Plan de Acción de la CMSI adoptado en la misma reunión se menciona que, para reforzar la confianza de los usuarios y mejorar la seguridad de la utilización de las TIC, es necesario «tomar medidas apropiadas contra el envío masivo de mensajes electrónicos no solicitados («*spam*») a nivel nacional e internacional».

A raíz de las medidas adoptadas por la CMSI, el Secretario General de la UIT convocó una reunión internacional en Ginebra, del 7 al 9 de julio de 2004, titulada «Reunión temática UIT-CMSI para contrarrestar el spam» (documentos disponibles en la dirección: www.itu.int/spam/).

### 10.3.7 Simposio Mundial para Organismos Reguladores (UIT)

Durante el quinto Simposio Mundial para Organismos Reguladores que tuvo lugar en Ginebra del 8 al 10 de diciembre de 2004, se consagró medio día a examinar el tema de «¿Cómo luchar contra el correo basura (spam)?»

Tras recordar todas las medidas adoptadas por la UIT y las organizaciones internacionales, así como las tareas de la CMSI (véanse algunos capítulos anteriores), la Asamblea aprobó las siguientes líneas directrices con el fin de combatir activamente el correo basura:

1) Legislación nacional

   Se señaló que sólo en pocos países se habían promulgado leyes eficaces al respecto y definido jurídicamente con claridad el correo basura en función de su naturaleza, y que las soluciones administrativas podían ser más rápidas que las penales. Se agregó que no habría que olvidar la coordinación en el plano nacional de todos los actores interesados y que este tipo de legislación debería aplicarse mediante medios técnicos de control.

2) Conocimiento de los efectos del correo basura

   Resulta indispensable realizar encuestas, sondeos y consultas públicas, así como desplegar otros esfuerzos, para determinar en qué plano actúan los autores del correo basura (nacional o internacional) y en qué medida es posible identificarlos (promoción de soluciones técnicas).

3) Cooperación internacional

Esta cooperación es esencial, especialmente para los países en desarrollo. Las infraestructuras de telecomunicaciones de estos países siguen siendo fragmentarias y, en consecuencia, el número de autores de correos basura es reducido o nulo.

Como la fuente del correo basura está fuera de los territorios nacionales, es indispensable cooperar a nivel internacional, basándose en las legislaciones nacionales.

El informe y las conclusiones del simposio mencionado pueden consultarse en el sitio de la UIT.

NOTA – Programa de Intercambio Mundial de Reguladores (G-REX).

Lanzado en mayo de 2001 por la UIT, el G-REX es un foro en línea en que los reguladores y los formuladores de políticas intercambian opiniones y comparten experiencias. En el sitio www.itu.int/ITU-D/treg aparecen informaciones por país y región, por ejemplo sobre la naturaleza de los organismos de reglamentación y la **legislación contra el correo basura**.

**Conclusiones**

Resulta sumamente difícil combatir eficazmente el correo basura y el éxito depende de que se adopten enfoques polivalentes, tanto en el plano técnico como de organización, y de que las soluciones se actualicen rápidamente.

De las tres metodologías a las que se les ha pasado revista en el presente Capítulo, sólo el enfoque que utiliza firmas específicas contra el correo basura se ha mostrado eficaz contra este tipo de correo.

## 10.4 Captura de datos bancarios (phishing)

La Comisión Federal de Comercio de Estados Unidos define este tipo de captura como sigue: la captura de datos bancarios, igualmente denominada piratería de tarjetas bancarias, es una estafa de alto nivel tecnológico en la que se utiliza el correo basura para engañar a los consumidores y forzarlos de este modo a revelar los números de sus tarjetas de crédito, cuentas bancarias, seguridad social, contraseñas y otras informaciones de carácter confidencial[1].

En la práctica, se usurpa la identidad de los bancos mediante correo electrónico encubierto, utilizando el lenguaje HTML para recrear fraudulentamente el logotipo y dirección del establecimiento bancario remitente, tal como esta información figura en mensajes auténticos. Estos correos electrónicos dirigen a los clientes a sitios web falsos que disponen de identificadores de recursos uniformes (URL) semejantes a los de los sitios oficiales y en los cuales se alienta a éstos a volver a registrar sus datos personales y financieros, lo que permite a los piratas utilizarlos ulteriormente para cometer fraudes.La eficacia del correo electrónico y las comunicaciones en línea, hace de estos medios herramientas muy interesantes para el correo electrónico legítimo, pero también instrumentos atractivos para los autores de correos basura y los ciberdelincuentes.

Las empresas que deseen preservar la eficacia y el valor del correo electrónico para comunicar con sus clientes, deberán pensar en cómo proteger estos canales de comunicación contra los delincuentes atraídos por las posibilidades financieras del mundo en línea. Para combatirlos habrá que utilizar una mensajería segura, esto es servirse de cifras y firmas digitales diseñadas para proteger la información y demostrar la autenticidad de los mensajes y los remitentes.

Habrá que aplicar soluciones de mensajería seguras y que no exijan ninguna medida por parte del usuario final. Dichas soluciones harían innecesaria la carga que supone el cifrado y descifrado, así como la firma y la verificación de los mensajes, y el descubrimiento y memorización de las claves necesarias, con el fin de que

---

[1] FTC Consumer Alert, «How Not to Get Hooked by a 'Phishing' Scam»,

<http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.htm>

los sistemas automatizados trabajen de manera invisible en el plano de la red. Sin embargo, si se desea garantizar automáticamente la seguridad de la mensajería electrónica, con el fin de que pueda utilizarse eficazmente y en gran medida por las empresas, esta mensajería debería basarse en normas abiertas y permitir parametrizar y mantener conexiones seguras con los destinatarios que no hayan establecido mensajerías seguras y/o que no puedan ser formados para utilizarlas.

Esta solución debería no sólo resultar invisible para los remitentes sino también, una vez autenticados los destinatarios, deberían permitir automatizar la verificación y el desciframiento de los mensajes electrónicos, garantizando la firma de cualquier respuesta. Para responder a esta necesidad se han desarrollado sistemas que funcionan de modo transparente en una capa determinada en la red y utiliza pequeñas «huellas» sustitutivas al término de los mensajes electrónicos recibidos. Estos sistemas pueden garantizar de manera bilateral y automatizada la seguridad de los mensajes electrónicos y proceder a la autenticación de los dos usuarios (remitente y destinatario de un mensaje electrónico) sin que deban formarse para ello.

Una vez instalados tales sistemas, el correo electrónico y las comunicaciones en línea podrían pasar de ser una meta para los ciberdelincuentes a convertirse en un medio seguro de comunicaciones con clientes y asociados, y reducir significativamente las posibilidades de usurpación de identidad.

Tratándose de los Estados Unidos y Australia, sírvase visitar, respectivamente, los siguientes sitios: www.ftc.gv/bcp/conline/pubs/alorts/phishingalrt.htm y www.data.gov.au/spam

NOTA – En agosto de 2004 una empresa estadounidense especializada en filtros contra el correo basura interceptó en cinco horas más de 125 000 correos fraudulentos con el membrete de un importante banco de este país. Durante estos ataques, que se realizan a escala mundial, los bancos establecen cada vez más filtros contra el correo basura: acceso aleatorio de utilización única, tarjetas con rejilla que cambiar en cada cesión, calculadoras que cambian cada minuto (sistema generalizado en Suiza a partir de mediados de 2004). Hay ataques más refinados que pueden permitir a un pirata (cliquear un URL de un sitio en construcción) implantar un caballo de Troya; solución: correo electrónico a la «basura».

## 10.5 Convergencia de sistemas de información, bienes y personas: la videovigilancia con IP

La actual tendencia en los mercados de seguridad es la convergencia de recursos y la utilización de los sistemas desplegados (tanto físicos como informáticos), se trate de la seguridad de edificios, personas o sistemas de información. En el pasado los sistemas de seguridad (videovigilancia, control de acceso, sistema de información, etc.) eran independientes y autónomos, y funcionaban en circuito especializado y cerrado. Hoy en día con la explosión de internet, la interconexión IP resulta indispensable y permite integrar los sistemas de seguridad en los sistemas de información. Esta convergencia de infraestructura física/lógica responde también a la creciente necesidad de compartir los flujos de información en todo momento y lugar.

A la vista de las nuevas tendencias, tales como la desreglamentación de las telecomunicaciones, la multiplicación de sitios, la movilidad de colaboradores y el seguimiento en tiempo real, las empresas han entrado en una fase de optimización de la inversión, lo que se traduce en los siguientes fenómenos:

– la consolidación y la convergencia de infraestructuras,

– la normalización y la evolución de las tecnologías (protocolo, compresión, etc.),

– la necesidad de realizar economías sustanciales,

– el aumento de la productividad al menor costo posible.

Ahora bien, la problemática de la seguridad es un elemento que habrá que tomar cada vez más en consideración, si se desea mantener un nivel adecuado de seguridad en un sistema interconectado (tanto en el plano de cada uno de los sistemas integrantes como de los datos y su transferencia). Este elemento se plantea:

– en el plano estratégico (tratándose de las direcciones generales),

– en el plano operacional (tratándose de las direcciones funcionales y las profesiones),

– en el plano tecnológico (tratándose de los encargados del sistema).

Una de las aplicaciones que ejemplifican concretamente la convergencia de la informática y el vídeo es la videovigilancia con IP.

Gracias a las grandes velocidades y el desarrollo de las redes, se ha facilitado el acceso a nuevas aplicaciones crecientemente evolucionadas, por ejemplo, el vídeo. Así pues, es cada vez más frecuente que los sistemas de videovigilancia se conecten con los de información para optimizar las infraestructuras.

El mercado de la videovigilancia se encuentra en plena transformación, ya que se está pasando del mundo analógico a un universo íntegramente digital. En 2003, la videovigilancia con IP representaba el 10% del mercado europeo, esto es unos 65 millones EUR y se caracterizaba por un rápido crecimiento (un 100% anual). Hoy en día en Francia una de cada cinco empresas dispone de cámaras de videovigilancia y se registran cada año 600 000 nuevas conexiones.

Antaño reservada a los sitios denominados «sensibles», la vigilancia se ha establecido en nuevos ámbitos (laboratorios, turismo, servicios, gestión de proyectos, etc.) que sobrepasan con mucho la esfera de la seguridad, ya que se aplica, entre otras cosas, a dar mayor fluidez a las colas y analizar comportamientos de compra, lo que entraña, por otra parte, una creciente exigencia por parte de los usuarios en el sentido de que se garantice la seguridad de la vigilancia.

La videovigilancia permite el seguimiento a distancia, la gestión de múltiples sitios, el registro numérico centralizado y una televigilancia que venga acompañada del control del acceso y alarmas. En consecuencia, cualquier encargado de la seguridad deberá estar en condiciones de acceder en tiempo real a su sistema de videovigilancia, siempre y cuando se garantice:

– la vigilancia fuera de los sitios, por ejemplo, a partir de un simple navegador web,
– la disponibilidad del sistema y la gestión de la banda de paso,
– el buen desempeño, la fiabilidad y la calidad del servicio suministrado en tiempo real,
– el interfuncionamiento con otros sistemas, por ejemplo el de control de acceso y el biométrico,
– la transparencia, la facilidad de instalación y la flexibilidad de utilización para el usuario.

Ahora bien, interconectar el sistema de videovigilancia con el de información con IP, es algo que debe analizarse minuciosamente, para determinar los riesgos a que pueda hacer frente:

– riesgos respecto a los protocolos utilizados (H323, SIP, etc.), por ejemplo, ataques a la implementación del correspondiente protocolo mediante equipo desplegado o ataques mediante usurpación de identidad;
– riesgos vinculados a la utilización del sistema de información, por ejemplo la escucha y la intercepción de comunicaciones, o los ataques mediante denegación de servicio para paralizar el sistema.

De ahí que un enfoque de seguridad resulte indispensable:

– para sensibilizar en cuanto a los riesgos existentes y probar intrusiones o probar el aprovechamiento de factores de vulnerabilidad (física o lógica);
– para realizar auditorías técnicas en las infraestructuras instaladas;
– para implementar protecciones técnicas, tales como:
    • la aplicación de parches correctivos en función de los equipos desplegados para garantizar una vigilancia activa;
    • la utilización del protocolo SIP contra la usurpación de identidad;
    • la utilización del protocolo de transporte seguro en tiempo real (SRTP) contra la intercepción;
    • la utilización de sistemas de prevención de intrusión (IPS) contra la denegación de servicio (aunque habrá que estar atento al rendimiento y a los errores de diagnóstico).

Está aumentando la necesidad de contar con videovigilancia con IP en los estacionamientos de las grandes aglomeraciones, las instalaciones públicas (estadios, centros deportivos, etc.), los transportes públicos, las oficinas, los bancos, etc. Asimismo, es cada vez mayor el número de empresas que intentan integrar en sus redes su tráfico de videovigilancia, así como las señales y alarmas de control de acceso.

Impreso en Suiza
Ginebra, 2006