Seguridad en redes telemáticas
Correo Electrónico y Servicios Internet

GTA **Grupo de Usuarios de Telecomunicaciones en la Administración**

SSITAD **Comité Técnico de Seguridad de los Sistemas de Información y Tratamiento Automatizado de Datos Personales**

SEGURIDAD EN REDES TELEMÁTICAS
CORREO ELECTRÓNICO Y SERVICIOS INTERNET

Índice

Madrid, 8 de julio de 1996

INTRODUCCIÓN

Con la realización de este trabajo se ha tratado de reunir en un documento de carácter sintético una descripción suficientemente comprensiva de la problemática de seguridad del correo electrónico y de los servicios Internet. Dicho documento se estructura de la siguiente manera:

Resumen ejecutivo
1. Servicios de seguridad
2. Tecnología. Descripción de las normas X.400 y de Internet
3. Estándares y referenciales para seguridad en correo electrónico X.400 e Internet
4. Productos de seguridad
5. Aspectos legales
6. Políticas y administración de seguridad del correo electrónico e Internet
7. Glosario de seguridad
8. Bibliografía

El Resumen Ejecutivo proporciona una panorámica rápida del estudio respondiendo de forma concisa y breve a las cuestiones clave de la seguridad en el correo electrónico y en los servicios Internet.

El capítulo 1 "**Servicios de seguridad**" se inspira en el análisis de riesgos para responder a cuestiones tales como ¿por qué es necesaria la seguridad?, ¿qué servicios de seguridad se deben proporcionar?, ¿cómo se deben implementar?. Así, recorre el camino que va desde la determinación de las *amenazas* a las que se encuentran expuestos el correo electrónico y los servicios Internet, teniendo en cuenta cuáles son los requerimientos de proveedores, organizaciones y usuarios finales, pasando por la identificación de los *servicios de seguridad* que satisfacen los requerimientos de seguridad y dan respuesta a las potenciales amenazas, hasta llegar a la descripción de las *técnicas o mecanismos* más importantes para implementar los servicios de seguridad identificados.

El capítulo 2 "**Tecnología. Descripción de las normas X.400 y de Internet**" responde a la cuestión de hasta dónde llegan los estándares de jure y de facto. Incluye en primer lugar y de una forma más profunda la descripción de los aspectos básicos del correo electrónico X.400 y de Internet. En segundo lugar se describen los demás servicios que Internet proporciona aparte del de correo electrónico. El capítulo se orienta a la presentación de los conceptos fundamentales al objeto de que se puedan entender y relacionar con las cuestiones relativas a la seguridad.

El capítulo 3 "**Estándares y referenciales para seguridad en correo electrónico X.400 e Internet**" describe el marco de estándares y referenciales a considerar para implementar la seguridad en el correo electrónico y en Internet. En el caso del correo electrónico *X.400* el referencial básico que se ha seguido es el Manual EPHOS, y más concretamente su módulo referente a los Servicios de Seguridad. En el caso de *Internet* los referenciales son el Privacy Enhanced Mail (RFCs 1421-1424), el Secure Sockets Layer Protocol (SSL) y el Secure HyperText Transfer Protocol (HTTP). Las referencias tanto a Internet como a X.400 se apoyan grandemente en la misma fuente que no es otra que la norma "ISO 7498-2 Information Processing Systems-Open Systems Interconnection Basic Reference Model- Part 2: Security Architecture".

El capítulo 4 "**Productos de seguridad**" describe los *productos* que permiten la implementación

real de las medidas de seguridad a los escenarios de uso del correo electrónico y de los servicios Internet con que se encuentre cada organización. Se trata de ver cómo a través de diversos productos se pueden implementar los servicios, técnicas y mecanismos de seguridad. No es una labor sencilla teniendo en cuenta que se trata de un mercado en constante ebullición en el que a lo largo del período del estudio se han producido enormes cambios. Por otra parte, se hubiera deseado incluir, además, un conjunto de consideraciones coste-beneficio; si bien no ha sido posible debido a que el factor coste se ha considerado, en este caso, como un factor poco orientativo, ya que los diversos proveedores contactados coinciden en la circunstancia de que los precios están sujetos a importantes variaciones según sea el entorno en el que se vayan a implantar sus productos. En consecuencia la prospección de productos de seguridad para correo electrónico y servicios Internet, se ha centrado en identificar la naturaleza de los mismos, bien como productos de correo electrónico, de servicios Internet con funcionalidades de seguridad, o bien como productos exclusivamente de seguridad. Por otra parte, el hecho de que la relación de productos no pueda ser exhaustiva, lo cual requeriría un esfuerzo adicional, y de que no todos los proveedores que han aportado información hayan adjuntado el dato coste, reduce el valor añadido que el citado dato coste pudiera aportar.

El capítulo 5 "**Aspectos legales**" señala en primer lugar el marco legal a considerar en lo relativo a las garantías y derechos de los ciudadanos y a la protección de los datos atendiendo a la legislación existente en este sentido tanto a nivel nacional como a nivel de la Unión Europea. En segundo lugar se incluye una reflexión sobre los aspectos de carácter legal a considerar para la *realización de comercio electrónico*, entendiendo por comercio electrónico la realización de actos y negocios jurídicos mediante transacciones electrónicas basadas en el correo electrónico o en Internet; estos aspectos legales se refieren a la contratación, a la identificación de las partes, a la seguridad y a la confidencialidad y a la seguridad procesal. Se incluye además como anexo el Modelo Europeo de Contrato EDI. En tercer lugar y conforme se cita en la Ley Orgánica 10/1995 de 23 Noviembre, en relación con la aprobación del nuevo *Código Penal* en vigor desde el 23 Mayo 1996, se tipifican delitos y faltas que puedan cometerse utilizando métodos informáticos, concretamente los que se refieren a la Intimidad, Patrimonio y socioeconómicos, y Propiedad Intelectual. Entre otros se penaliza con prisión y multa, al que se apodere de mensajes de correo electrónico, documentos electrónicos y soportes informáticos para la vulneración de secretos de empresa o datos reservados de carácter personal y coincidiendo con la LORTAD, los datos especialmente protegidos.

El capítulo 6 "**Políticas y administración de seguridad del correo electrónico y servicios Internet**" se centra en la problemática de organizar, implantar, gestionar y administrar el correo electrónico y los servicios Internet en condiciones de seguridad de forma integrada con la estrategia general de seguridad de la organización. Se tratan los elementos del programa de protección de la información, las responsabilidades de la seguridad, las directrices de privacidad, la clasificación de la información y la administración y gestión de la seguridad con un enfoque orientado a las técnicas de interés en este análisis.

El capítulo 7 "**Glosario de seguridad en correo electrónico e Internet**" ofrece un glosario básico de conceptos relacionados con la seguridad en el correo electrónico e Internet.

El capítulo 8 "**Bibliografía**" muestra las referencias básicas de las que se ha partido para elaborar el presente documento.

La coordinación del desarrollo de este documento ha corrido a cargo de:

- Francisco López Crespo, Jefe de Área de Sistemas Telemáticos,
  C.E.: X.400:C=ES;A=400NET;P=MAP;OU1=DGOPTI;OU2=SGCI;S=LOPEZCRESPO;
  G=FRANCISCO
  Internet: francisco.lopez-crespo@sgci.dgopti.map.es

- Miguel Ángel AmutioGómez, Técnico Superior de Tecnologías de la Información
  C.E.: X.400:C=ES;A=400NET;P=MAP;OU1=DGOPTI;OU2=SGCI;S=AMUTIO;
  G=MIGUEL
  Internet: miguel.amutio@sgci.dgopti.map.es

de la Subdirección General de Coordinación Informática, del Ministerio de Administraciones Públicas.

La realización del estudio ha contado con la colaboración de:

- D. Aurelio Hermoso Baños, Iberia Líneas Aéreas de España
- D. Javier Rebollo Martínez, Telefónica de España, S.A.
- D. José Javier Galián, Telefónica de España, S.A.
- Dª. Mª Victoria Ibarra, Banco Bilbao Vizcaya
- D. Tomás Arroyo Salido, Banco Bilbao Vizcaya
- D. Víctor Manuel Jiménez Castellano, Banco Bilbao Vizcaya
- D. Atilano Hernández, El Corte Inglés
- D. Roberto Navarro, El Corte Inglés
- Dª Patricia Corral, Teneo, S.A.

Se han recibido aportaciones de
- D. Juan Manuel Manzano, Renfe
- D. Santiago del Pino Casado, Indra SSI

RESUMEN EJECUTIVO

Correo electrónico y servicios Internet

Correo electrónico
Un sistema de correo electrónico o mensajería proporciona al usuario los medios para transferir pequeñas cantidades de información (mensajes) a uno o más destinatarios en ubicaciones locales o remotas. Los destinatarios no tienen necesidad de estar conectados a la red al mismo tiempo que se envía el mensaje y el remitente puede estar conectado directamente o no al receptor.

El servicio de correo electrónico puede ser proporcionado por sistemas de mensajería diferentes como puedan ser los basados en *X.400* o en *Internet*.

Internet
Internet es una red de redes, no jerarquizada y ninguna parte implicada la controla.
Además del *correo electrónico* puede proporcionar otros servicios:

Herramientas de búsqueda y visualización de información. Con el fin de facilitar la búsqueda de información en la red se han desarrollado herramientas que se han extendido de tal manera que suponen un estándar de facto en cuanto a navegación por la red, extracción de información o transferencia de ficheros. Destaca el *World Wide Web* (*WWW)* que maneja información gráfica con estructura hipertextual.

Los grupos de discusión (USENET-NEWS). Se puede considerar como un servicio ligado al correco electrónico en el que los usuarios publican información que se hace pública a modo de tablón de anuncios. Su orientación principal es la de crear foros de dicusión.

Transferencia de ficheros (FTP). A lo largo de toda la red se encuentran miles de programas, ficheros de imágenes, ficheros de sonido, catálogos de bibliotecas, y bases de datos de todo tipo, ubicados en servidores. Esta información puede ser de libre acceso o de pago (requiriéndose por lo general una suscripción a un servicio de un servidor o de un conjunto de servidores). Hay diversos protocolos que permiten la realización de la transferencia de ficheros. El más extendido es el FTP (File Transfer Protocol) que emplea comandos de navegación parecidos a los proporcionados por UNIX. Existe una variante del FTP, denominada FTP anónimo, que permite la distribución de información, y se emplea por ejemplo para realizar distribución electrónica de software.

Conexión remota (TELNET) es un servicio que permite la conexión remota con cualquier ordenador de la red, simulando un teminal local de la máquina accedida. Se pueden realizar varias conexiones TELNET simultáneas. Necesita por lo general de distintos controles de acceso, por motivos de seguridad del proveedor del servicio. Este servicio se puede emplear para montar una red corporativa de ámbito nacional o internacional, que de otra forma resultaría más compleja o más cara.

Uso del correo electrónico y de los servicios Internet

1. Comercio electrónico.

El uso del correo electrónico ya sea Internet o X.400 y de los demás servicios que proporciona Internet abre nuevas posibilidades de actividad para las organizaciones.

Permiten que una organización pueda estructurarse de forma distribuida con independencia de la lejanía y de la ubicación geográfica a nivel mundial, sin necesidad de implantar una costosa red corporativa.

Todas éstas técnicas constituyen un nuevo medio de relación bidireccional entre las organizaciones y los usuarios de sus productos y servicios, abriendo la posibilidad de realizar comercio electrónico:

- Transacciones comerciales vía EDI sobre la mensajería X.400.
- Comercio electrónico vía el World Wide Web de Internet: venta de productos y servicios, suscripciones, etc.
- Difusión y distribución de información relativa a productos y servicios, de márketing, para 'educar' el mercado, para diferenciación de la competencia, para captación de ciertos colectivos de clientes o usuarios.
- Interacción con el cliente o usuario: información de pre-venta y de post-venta, asistencia técnica, etc.

2. Integración de los Sistemas de Información de la Organización

a) Integración de los sistemas de información por medio del correo electrónico.

Los sistemas de correo electrónico constituyen una infraestructura que facilita la difusión de información a lo largo de la organización, mejoras en los diversos procesos de actividad y en la toma de decisiones. El correo electrónico evolucionará desde su funcionalidad básica para el intercambio de mensajería interpersonal, hacia una infraestructura para el intercambio de información intra e inter organizaciones. En esta evolución el aspecto clave es la implantación de aplicaciones integradas con el sistema de mensajería. Se pueden distinguir diversos grados de integración:

- Integración básica de las aplicaciones con el sistema de mensajería.
- Uso en las aplicaciones de las funcionalidades del sistema de mensajería y aportación de valor añadido con un mínimo desarrollo adicional.
- Aplicaciones dependientes del sistema de mensajería para proporcionar funcionalidades de carácter principal que requieren la transferencia de información, que no tiene por qué ser correspondencia interpersonal, y que dan soporte a la interacción entre entidades y no sólo entre individuos.
- Integración de herramientas de trabajo en grupo, *de Work-Flow*, favoreciendo la productividad de los equipos de trabajo.

b) Integración de los Sistemas de Información mediante el uso de servicios Internet

Los servicios Internet utilizados internamente en una organización, con independencia de que existan o no enlaces con el exterior, formando lo que se denomina INTRANET constituyen el medio ideal para facilitar el trabajo en grupo, el *Work-Flow*, la difusión de información técnica, comercial, de recursos humanos, finaciera, etc a quienes la necesitan, la integración de aplicaciones, la comunicación entre miembros y departamentos de las grandes corporaciones e instituciones, la homogeneización de interfaces, dar respuesta a la exigencia siempre presente de disponer de la información cuándo y dónde se necesita, interna o externa, propia o relativa a la competencia, que permite adoptar las mejores decisiones en cualquier nivel de la organización. Para ello se requieren redes que soporten los protocolos TCP/IP.

3. Acceso a otros recursos

Los servicios Internet facilitan el acceso a otros recursos ya puedan ser otras máquinas mediante los servicios de terminal virtual que permiten el acceso a bases de documentación, aplicaciones y programas, de ejecución de comandos en sistemas remotos o bien de servicios de noticias. .

4. **Intercambio de correspondencia interpersonal**.

La funcionalidad básica tradicional del correo electrónico es el intercambio de correspondencia interpersonal en general: envío de textos, notas, mensajes, etc, constituyéndose en el vehículo ideal para estimular el intercambio de conocimiento y la colaboración entre aquellos conectados al sistema de mensajería.

5. Intercambio de cualquier tipo de ficheros.

Tanto el correo electrónico como los servicios Internet permiten enviar cualquier fichero (gráficos, video, sonido) que pueda manejar el ordenador. Proporcionan una extensión a las herramientas que se utilizan para generar documentos, hojas de cálculo, etc, de lo que se derivan beneficios en productividad personal.

Beneficios del uso del correo electrónico y de los servicios Internet

Correo Electrónico

El correo electrónico es sencillo de utilizar, no requiere la participación simultánea de emisor y receptor en el proceso de la comunicación, y aporta interesantes beneficios como los siguientes:

- Permite *aprovechar los textos transmitidos* pues no es necesario reescribirlos (a diferencia del fax).
- Permite la *integración de textos, gráficos, e incluso multimedia*, en un mismo mensaje, e incluso de *aplicaciones* con el sistema de mensajería.
- Permite *ahorrar tiempo* pues el receptor no tiene que estar disponible para comunicación directa, además el tiempo de entrega de la información es breve y facilita el desarrollo de tareas distribuidas.
- Permite *ahorrar costes de transmisión* por teléfono, fax o por correo postal al ser más económico que ellos.
- Sirve de base como un *servicio de comunicación confiable* (X.400), para la realización del comercio electrónico.
- Permite *enviar mensajes a grupos de personas*, es decir a múltiples destinatarios.

- Permite *disponer de acuse de recibo* (X.400) y distinguir a la manera del correo tradicional entre *sobre*, *mensaje* y *firma*.
- La *distancia no es un problema*.

Servicios Internet

- Permiten la *integración de los sistemas de información* de la organización utilizando servicios Internet formando la denominada *Intranet.*
- Permite *ahorrar costes de infraestructura de comunicaciones.*
- La *distancia no es un problema*.
- Permite el *acceso a un número casi ilimitado de recursos*: sistemas, fuentes de información, bases de datos, ficheros y datos de carácter público, foros de dicusión y de noticias, etc.
- Abre la posibilidad a *nuevas oportunidades de negocio*: comercio electrónico, teletrabajo, difusión y distribución de información, etc.

Requerimientos, amenazas, servicios y técnicas de seguridad

Las organizaciones que utilizan servicios telemáticos como Internet o X.400 deben adoptar medidas que garanticen la *confidencialidad, integridad* y *disponibilidad* de la información. Para ello, dentro de la estrategia de seguridad de los Sistemas de Información de la organización y mediante el Análisis y Gestión de Riesgos deben identificar las *amenazas* a las que están expuestas por el uso de los citados servicios en base a los requerimientos de seguridad de las organizaciones y usuarios finales, identificar los *servicios de seguridad* necesarios para hacer frente a las amenazas potenciales, las *técnicas o mecanismos de seguridad* para implementar los servicios de seguridad y los *productos* que permiten la implantación real de los servicios de seguridad.

Amenazas

Las **amenazas** son los eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos y son la respuesta al *por qué* es necesaria la seguridad. Los servicios X.400 e Internet se encuentran fundamentalmente expuestos a las siguientes amenazas:

- Divulgación no autorizada de la información
- Modificación no autorizada de la información
- Enmascaramiento
- Repudio de origen o del acuse de recibo
- Acceso no autorizado a recursos
- Denegación del servicio

Qué servicios de seguridad se deben implementar

Los **servicios de seguridad** son la respuesta a las amenazas, y responden al *qué* se debe hacer para satisfacer los requerimientos de seguridad de la organización y hacer frente a las amenazas. Los servicios de seguridad necesarios en el ámbito de nuestro interés son los siguientes:

- **Confidencialidad de los datos**. Impide que alguien distinto del receptor pueda leer el contenido de los mensajes.
- **Integridad del mensaje**. Garantiza que el mensaje recibido es exactamente el mismo que se envió.
- **Autenticación de entidades**. Garantiza al receptor la identidad del remitente del mensaje y viceversa. Desde otro punto de vista garantiza la identidad del servidor o del cliente.
- **No repudio - Acuse de recibo**. Protege al emisor/receptor de un documento de las tentativas de la otra parte de negar el envío/recepción de todo o una parte del mismo. Así mismo, pretende dar validez legal a un documento, ya que requiere que una persona se responsabilice del contenido del documento, poniendo su firma digital en él. El acuse de recibo prueba que el contenido de un mensaje fue recibido por el destinatario.
- **Control de acceso**. Tiene por objeto garantizar que sólo acceden a la información y a los recursos los usuarios que tienen permiso para ello. Este servicio es aplicable con carácter general pero adquiere mayor relevancia en el mundo Internet.

Técnicas o mecanismos de seguridad

Las **técnicas y mecanismos** de seguridad constituyen la lógica o algoritmo que implementa un servicio de seguridad particular en hardware o software y responden al *cómo* implementar los servicios de seguridad.

- **Intercambio de autenticaciones**. Corrobora que una entidad, ya sea origen o destino de la información, es la deseada.
- **Criptografía**. Garantiza que la información no es inteligible para individuos, entidades o procesos no autorizados. Se realiza mediante técnicas de cifrado y descifrado.
- **Control de accesos, Cortafuegos**. Son sistemas que controlan el tráfico dentro de las redes utilizando programas de seguridad situados en un servidor u ordenador independiente. Se diseñan para restringir el acceso a las redes de las organizaciones, especialmente desde el exterior. Analizando dónde se originan los paquetes, los dejan pasar o no. Los cortafuegos pueden tener distintas formas: filtrador de paquetes, cortafuegos a nivel de circuitos y a nivel de aplicación.
- **Firma digital**. Se basa en técnicas criptográficas, y cumple las mismas funciones que la firma manual: el receptor debe ser capaz de validar la firma del emisor, no debe ser falsificable y el emisor de un mensaje no debe poder repudiarlo posteriormente.
- **Relleno del tráfico**. Se basa en introducir tráfico espúreo junto con los datos válidos para que no se pueda conocer si se está enviando información o qué cantidad de datos útiles se están enviando.
- **Etiquetas de seguridad.** Permiten que los mensajes sean clasificados para facilitar un correcto control de acceso y la separación de datos según clases de seguridad.

- **Funciones hash.** Son funciones matemáticas sin inversa, que aplicadas a un elemento o dato que se transfiere impiden que este sea descifrado. También sirven para verificar la correcta recepción de los mensajes.
- **Terceras Partes de Confianza (TTP)**. Son entidades cuyos informes se consideran fiables por todos los elementos del domino de seguridad. Pueden tener registros y firmas digitales y emitir certificados dentro del sistema.

Relación entre Amenazas y Servicios de Seguridad

Amenaza	***Servicio de Seguridad***
Divulgación no autorizada de la información	*Confidencialidad de datos*
Modificación no autorizada de la información	*Integridad del mensaje y del contenido*
Enmascaramiento	*Autenticación de entidades*
Repudio del mensaje de origen o del acuse de recibo	*No repudio*
Acceso no autorizado a recursos	*Control de acceso*
Denegación de servicio	*Control de acceso*

Relación entre Servicios de Seguridad y Técnicas o Mecanismos de Seguridad.

Servicio de Seguridad	***Técnica/Mecanismo de Seguridad***
Autenticación de entidad	*Intercambio de autenticaciones*
Autenticación de datos de origen	*Cifrado* *Firma digital* *Función de comprobación criptográfica*
Control de acceso	*Lista de control de acceso* *Cortafuegos*
Confidencialidad orientada a la conexión	*Cifrado* *Etiquetas de seguridad*
Confidencialidad no orientada a la conexión	*Cifrado* *Etiquetas de seguridad*
Confidencialidad del flujo de tráfico	*Cifrado* *Relleno del tráfico* *Etiquetas de seguridad*
Integridad orientada a la conexión	*Función de comprobación criptográfica* *Funciones hash y cifrado*
Integridad no orientada a la conexión	*Función de comprobación criptográfica* *Funciones hash y cifrado* *Firma digital*
No repudio, origen	*Firma digital* *Teceras Partes de Confianza*
No repudio, destino	*Firma digital* *Terceras Partes de Confianza*

Servicios y Mecanismos de Seguridad; soporte proporcionado por X.400 e Internet.

X.400

La versión original de 1.984 del estándar X.400 proporcionaba básicamente servicios de autenticación y de notificaciones de envío correcto e incorrecto y de entrega correcta e incorrecta. En la versión de 1.988 se añadieron nuevos servicios de seguridad basados en su mayoría en las técnicas criptográficas:

- confidencialidad del contenido y del encaminamiento
- integridad del contenido y de la secuencia del mensaje
- autenticación de origen/recepción
- no repudio de origen y destino
- no repudio del contenido del mensaje
- prueba de envío y de entrega
- etiquetas de seguridad en los mensajes.

Estos servicios manejan claves públicas a través de certificados que se obtienen mediante X.500.

Internet

Los servicios de Internet que más atención prestan a la seguridad son el correo electrónico y el World Wide Web. Para los servicios que no tienen características de seguridad específicas la protección se basa en los permisos de lectura y escritura del sistema operativo a las tareas que los implementan.

Correo electrónico

El correo electrónico original de Internet normalizado por los documentos RFC-821 y RFC-822 no incorpora servicios de seguridad, pero hay dos extensiones que sí los tienen, *Private Enhancement Mail* (PEM) y *Pretty Good Privacy* PGP que proporcionan confidencialidad, integridad del mensaje y autenticación del emisor. PEM también da soporte para no repudio en origen.

La principal diferencia está en que PEM necesita entidades centralizadas para los certificados de claves públicas, mientras que mediante PGP los usuarios intercambian certificados unos con otros sin necesidad de utilizar entidades de certificación.

World Wide Web

El *World Wide Web* es un sistema hipermedia distribuido que ha adquirido una gran aceptación en el mundo Internet. Aunque las herramientas de consulta del WWW soportan diversos protocolos preexistentes el *HyperText Transfer Protocol* (HTTP) es el protocolo nativo y principal utilizado entre clientes y servidores WWW. Su facilidad de uso enseguida despertó el interés de su empleo para aplicaciones cliente-servidor. Muchas aplicaciones requieren la autenticación del cliente y el servidor y el intercambio de información confidencial. La especificación original del HTTP proporcionaba un soporte muy modesto para el uso de mecanismos de criptografía apropiados para transacciones comerciales. Así los mecanismos originales de autorización de HTTP requieren que el cliente intente un acceso que a continuación es denegado antes de utilizar el mecanismo de seguridad.

El cortafuegos o *firewall* es un elemento clave de la seguridad en Internet, pero se trata de un mecanismo especialmente orientado a proporcionar el servicio de control de acceso y es preciso complementarlo con otros que permitan proporcionar los demás servicios de seguridad. Esto se debe conseguir mediante el uso de protocolos adicionales que se encuentran en estado de evolución si bien cuentan con implementaciones en el mercado.

Marco de estándares o referenciales de X.400 e Internet

X.400

El manual EPHOS suministra una guía para el uso de estándares para compras públicas de elementos de Tecnologías de la Información y las Comunicaciones en Europa. Da guías sobre el uso de los perfiles y estándares de OSI, apoyo a la elección del estándar correcto y ayuda en la elaboración de los pliegos de prescripciones técnicas.

EPHOS se divide en módulos temáticos, de los cuales *EPHOS 2 bis Topic U Security Service* está dedicado a la seguridad y permite la identificación y selección de servicios de seguridad para correo electrónico y EDI. Para la definición e identificación de amenazas y servicios de seguridad, EPHOS se basa fundamentalmente en la norma ISO-7498-2 (*Information Processing Systems. Open Systems Interconnection. Basic Reference Model. Part 2: Security Architecture*) que constituye el punto de referencia para describir los servicios de seguridad, referenciar las técnicas y mecanismos de seguridad y situar los servicios de seguridad en determinadas capas del modelo OSI.

Dentro del ámbito de nuestro interés proporciona guías para la adquisición de:

- Servicios de seguridad del Sistema de Tratamiento de Mensajes (MHS), bien se trate de mensajería interpersonal o de mensajería estructurada EDI.
- Servicios de seguridad EDI/EDIFACT.

Internet.

PEM (Privacy Enhanced Mail)

Relativo a seguridad en correo electrónico en Internet existe el estándar PEM (Privacy Enhanced Mail), aparece en las propuestas RFC 1421-1424 y como se dijo anteriormente facilita los servicios de:

- confidencialidad
- integridad no orientada a conexión
- autenticación del origen
- soporte para no repudio con prueba de origen

No es obligatorio que los mensajes PEM incorporen todos estos servicios, hay tres niveles de seguridad, según se requiera.

Secure Sockets Layer (SSL)

Se trata de un protocolo abierto y no propietario desarrollado por Netscape y que ha sido puesto a disposición del IETF, concretamente del grupo de trabajo W3C con vistas a su estandarización. Sus especificaciones en versión borrador pueden ser encontradas en la red.

El protocolo SSL proporciona servicios de confidencialidad, integridad, autenticación del servidor y opcionalmente autenticación del cliente en conexiones TCP/IP. SSL se encuentra en un nivel inferior a los protocolos HTTP, Telnet, FTP, Gopher pero por encima del nivel del TCP/IP. Mediante esta estrategia el SSL puede funcionar con independencia de los protocolos Internet y puede proporcionar seguridad a aplicaciones que trabajan con TCP/IP.

Secure Hypertext Transfer Protocol (SHTTP)

Se trata de un desarrollo de Enterprise Integration Technologies (EIT). SHTTP es una versión mejorada con aspectos de seguridad del protocolo HTTP que constituye la base del Web y proporciona servicios básicos de seguridad entre el cliente y el servidor para transacciones electrónicas comerciales tales como confidencialidad, integridad del mensaje, autenticación y no repudio de origen.

SSL y SHTTP no son protocolos excluyentes sino que pueden coexistir disponiendo el SHTTP sobre el SSL. SSL aporta la seguridad bajo protocolos de aplicación como HTTP o Telnet, mientras que SHTTP proporciona seguridad orientada al mensaje según una filosofía similar a la de PEM.

Productos

La oferta de productos para X.400 e Internet se encuentra en una situación de evolución constante y existe entre los fabricantes la concienciación acerca de la necesidad de incluir las funcionalidades de seguridad en los productos sin las cuales no se puede avanzar en el comercio electrónico. El aspecto más destacable es la aparición de soluciones de servidor y de cliente de *World Wide Web* que incorporan los protocolos SSL y Secure HTTP que permiten la realización de transacciones comerciales seguras. También se puede destacar la existencia de productos muy

avanzados que implementan las funcionalidades de cortafuegos. Los productos de interés se pueden clasificar de la forma siguiente:

- de correo electrónico X.400 o Internet que incorporan servicios y mecanismos de seguridad.
- para servicios Internet, especialmente World Wide Web, que incorporan servicios y mecanismos de seguridad.
- genéricos de seguridad, para implementar sobre otros productos y utilizarlos en combinación.
- cortafuegos.

Aspectos legales

El uso del correo electrónico y de los servicios Internet para la realización de actos y negocios jurídicos en relación al marco legal debe contemplar los siguientes aspectos:

a) Garantías y derechos de los ciudadanos y especialmente protección de los datos de carácter personal.

   - La Ley Orgánica 5/1992 de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD).
   - La Ley 30/92 de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.
   - Real Decreto 263/1996, de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado.
   - La Directiva 95/46/CE del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
   - Código Penal; Ley Orgánica 10/1995, de 23 de noviembre, que aprueba el nuevo código penal.

b) Aspectos legales relacionados con el comercio electrónico.

   - El establecimiento de acuerdos de intercambio o contratos-tipo entre las partes en cuestión que den validez a las transacciones o mensajes EDI intercambiados es de especial importancia.
   - Es conveniente que en el intercambio se establezca el sistema de responsabilidades y se incluyan claúsulas relativas al valor probatorio de la información intercambiada en caso de litigio, a la solicitud de confirmación para evitar errores, al almacenamiento y conservación de la información intercambiada, etc.
   - Existen modelos de acuerdos como el Modelo Europeo de Acuerdo EDI.

Políticas de seguridad

La seguridad en el correo electrónico y en los servicios Internet debe contemplarse en el marco de la estrategia general de seguridad de la organización. El programa de seguridad que tendrá uno de sus más fuertes puntos de apoyo en el análisis y gestión de riesgos debe reconocer la importancia del factor humano, basarse en el conocimiento de la organización y debe considerar los siguientes elementos:

   - Establecimiento de un programa de protección de la información que comprenda

políticas, estándares, guías y procedimientos.

- La asignación de las responsabilidades a la Alta Dirección, Administradores de seguridad de sistemas y Usuarios finales.
- Directrices sobre la privacidad de la información o el acceso a recursos.
- La clasificación de la información según su sensibilidad, integridad o criticidad.
- Función de administración y gestión de la seguridad.

1. SERVICIOS DE SEGURIDAD

1.1. INTRODUCCIÓN

Las organizaciones, para utilizar el correo electrónico y los servicios Internet tanto internamente como para relacionarse con el exterior deben tomar medidas que permitan garantizar la confidencialidad, la integridad y la disponibilidad de la información. Para ello deben identificar las **amenazas** a las que se encuentra expuestos los citados servicios, cuáles son los requerimientos de proveedores, organizaciones y usuarios finales, identificar los **servicios de seguridad** que dan respuesta a las amenazas identificadas, las **técnicas o mecanismos de seguridad** necesarios para implementar los servicios de seguridad identificados y finalmente los **productos** que mediante la implementación de las técnicas de seguridad proporcionan los citados servicios.

El análisis que se realiza sobre amenazas, servicios de seguridad, técnicas de seguridad y productos es válido para el correo electrónico X.400 o Internet y para los demás servicios Internet. Se presta en algunos puntos especial atención a estos últimos por presentar mayores debilidades en el ámbito de la seguridad.

Existen ***cuatro conceptos básicos en seguridad*** que son:

INTEGRIDAD	Se define como la característica que previene contra la modificación o destrucción no autorizadas de los activos.
DISPONIBILIDAD	Se define como la característica que previene contra la denegación no autorizada de acceso a los activos.
CONFIDENCIALIDAD	Se define como la característica que previene contra la divulgación no autorizada de los activos.
AUTENTICACIÓN	Se define como la característica de dar y reconocer la autenticidad de los activos (de tipo información) y/o la identidad de los actores y/o la autorización por parte de los autorizadores, así como la verificación de dichas tres cuestiones.

Se entiende por activos a los recuros del sistema de información o relacionados con éste, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección.

Los análisis en materia de Seguridad de los Sistemas de Información, giran alrededor de estos tres conceptos. Evidentemente, para ello debemos identificar primero los posibles riesgos y amenazas, y su repercusión en la organización, para después estudiar las posibles medidas que debemos tomar para evitarlos o disminuirlos, tomando la decisión final después de un estudio coste/beneficio de acuerdo con el nivel de seguridad establecido para lograr los objetivos propuestos en esta materia.

1.2. IDENTIFICACIÓN Y DESCRIPCIÓN DE AMENAZAS

Una *amenaza* es un peligro potencial que puede romper las medidas de seguridad informática que tenemos establecidas. ***Clases de amenazas***:

ACCIDENTALES	No son premeditadas y en ellas podemos incluir los posibles fallos del hardware y software de nuestra instalación.
INTENCIONADAS	Por medio de algo o de alguien se produce un *ataque* a nuestra información para fines distintos de los que fueron creados.

Nos centraremos por razones obvias en las amenazas intencionadas a las que pueden estar expuestos el correo electrónico y los servicios Internet.

Amenaza
Divulgación no autorizada de la información
Modificación no autorizada de la información
Enmascaramiento
Repudio del mensaje, del origen o del acuse de recibo
Acceso no autorizado a recursos
Denegación de servicio

1.2.1. Divulgación no autorizada de la información.

Una de las prácticas habituales consiste en "**disimular**" de alguna manera la información con el fin de que el intruso no pueda entenderla y por lo tanto no le sirva para nada.

Se pueden utilizar diferentes métodos, todos ellos válidos, pero es obligatorio que el receptor y el emisor estén de acuerdo y sean conocedores de las contraseñas.

Esto nos lleva a una implicación organizativa, en la cual una persona o personas son conocedoras de la metodología y otras son conocedoras de la parte descifradora.

En el caso de que el intruso acceda la información "disimulada", se puede dar el siguiente escenario:

Escenario

- **Conoce las claves** o contraseñas utilizadas y puede descifrar la información.
- Puede averiguar las claves **accediendo a los ficheros que las contienen**, o al software utilizado.
- Puede **alterar cualquier parte del fichero o del mensaje** enmascarado transmitido, modificando el contenido y/o las direcciones del remitente o destinatario.
- **Divulgar el contenido de la información** descifrada.
- **Distribución de la información a otros destinatarios**.
- **Divulgación de las contraseñas**.

Consecuencias

1. Los **Procedimientos y ficheros** que contienen las claves **no están suficientemente protegidos**.
2. La **metodología de cifrado usada es fácilmente abordable** desde el exterior. No está suficientemente protegida.
3. **Las claves usadas son sencillas** o fácilmente de localizar por los programas generadores de claves porque no se han utilizado algoritmos matemáticos dificiles de descifrar.
4. **No se ha utilizado la combinación de claves públicas y privadas**, sólo conocidas por el emisor y el receptor.
5. **No se ha utilizado la técnica de la criptografía**, metodología mas moderna y que constituye por si misma una herramienta importante de seguridad de información.

1.2.2. Modificación no autorizada de la información

Una vez superados, por los intrusos y usuarios no autorizados, los controles que estaban establecidos, se puede dar el siguiente escenario:

Escenario

- **Alteración parcial o total** del contenido de la información, con fines destructivos o especulativos.
- **Modificación del destinatario** con el fin de divulgar la información a otros

destinos no previstos.

- **Manipulación de los mensajes y envíos** a otros destinatarios.
- **Modificación de los datos del remitente** con fines delictivos.

Consecuencias

1. Si es un usuario externo, **ha superado las medidas de seguridad** implantadas, descritas anteriormente.
2. Si es un usuario interno, ha accedido a ficheros en los cuales **no se ha restringido el uso por usuarios no autorizados**.
3. **No se hace auditoría** del uso de los sistemas de seguridad para detectar posibles fallos y mal uso de las claves de accesos a recursos protegidos.

1.2.3. Enmascaramiento

Se trata de una suplantación de identidad, mediante la cual el intruso se hace pasar por una entidad diferente.

Escenario

- La **intrusión no autorizada** a cualquier sistema de la red interna.
- **Acceso a cualquier Aplicación** o Servicio de nuestro Sistema.

Consecuencias

1. Los Sistemas más frágiles son aquellos que **no tienen medidas de seguridad de control de accesos implantadas seriamente**.
2. Caso de tener implantadas medidas de seguridad, puede que **sólo sean las funciones básicas**, las cuales suelen ser conocidades normalmente.
3. Existen **claves de acceso demasiado fáciles** por mal elegidas dentro de una sencillez al alcance de cualquier mente lógica.
4. Es muy importante la figura del Administrador de Seguridad en el **control y seguimiento de los accesos a ficheros** por los usuarios.
5. Las propias **aplicaciones no tienen controles** sobre los diferente usuarios y sus niveles de autorización para el manejo de la información.

1.2.4. Repudio del mensaje, del origen o del acuse de recibo

Debemos tener seguridad en la identificación del remitente y destinatario, con lo cual aseguramos que "en el otro lado", está el usuario deseado y reconocido.

Al disponer de claves de acceso y de identificativos únicos por usuario, aseguramos la confidencialidad de los datos que son tratados sólo por quién autoricemos.

Concretamente es, no admitir a quién NO debe entrar, por lo tanto hay que proporcionar pruebas de la identidad y del origen de los datos.

Protegerse de cualquier intento de negación de envío o recepción, en su totalidad o parte del contenido del mismo. A la vez se envía una prueba de la recepción y aceptación del documento enviado.

Escenario

- **Pérdida de servicio**. Se puede perder el servicio tanto por problemas de seguridad como por otras causas no identificadas.
- **Divulgación de la información**. Revelación fortuita o mal intencionada del contenido del mensaje.
- **Acceso no autorizado a la red de comunicaciones**. Acceso a la red por parte de usuarios no autorizados, pudiendo acceder a la información y modificar su contenido.
- **Fraude**. La no confirmación de la identidad tanto del emisor como del receptor, y de la recepción del mensaje, no aseguran que el mensaje haya sido enviado o recibido.

Consecuencias

1. **No está implantado el servicio de confirmación** extremo a extremo que asegura que el servicio no ha sido interrumpido, al mismo tiempo que **no se ha dañado la integridad de los mensajes**.
2. No están implementadas las **pruebas de notificación de confirmación** de la **identidad del emisor, del contenido recibido y del enviado**.
3. Se debe proporcionar al emisor y al receptor, **pruebas irrefutables de que el contenido del mensaje es el mismo que el enviado/recibido**.

1.2.5. Acceso no autorizado a recursos

Dentro de la política de Seguridad Informática está contemplado el control de accesos a los Sistemas Informáticos, bien desde un nivel de seguridad básica para todos los sistemas y usuarios de la organización, hasta disponer de **medidas especiales para usuarios y recursos concretos, controlados y conocidos**.

En el caso de utilizar correo electrónico u otros servicios a través de la red INTERNET, desconocemos el numero de usuarios que podemos tener por lo que el control que implantemos se complica.

Si pensamos que los intrusos sólo van a poder entrar para curiosear estamos siendo muy optimistas, pues la estadística nos dice que siempre existen personas que por lo menos nos utilizarán como puente para acceder a otros sistemas informáticos y de paso ya que están en el nuestro, aparte de utilizarlo como base, intentarán **acceder a los ficheros** y cuanto más difícil se lo pongamos, más empeño pondrán en ello. Luego vendrá la divulgación, la modificación, la destrucción, etc, etc.

La solución ideal consiste en adoptar medidas preventivas, complementadas con otras restrictivas. Si han sido capaces de acceder, todo dependerá del interés del intruso de que sea solo para aprender, acceder a los recursos que contienen la información o lo que es peor que existan motivos de espionaje o económicos.

Nos podemos encontrar con el siguiente escenario:

Escenario

- La **intrusión no autorizada** a cualquier sistema de la red interna.
- **Acceso a cualquier Aplicación** o Servicio de nuestro Sistema.
- **Obtención de la información** y su posterior divulgación.
- La **utilización de un sistema como "puente" para acceder a otros sistemas**, empleando algoritmos rápidos de cálculo de direcciones y de palabras de acceso, hasta encontrar una puerta.

  Normalmente "colocan" en nuestros ficheros programas para hacer los cálculos, buscan cuentas para trabajar con los "username" que han descubierto y obtener los máximos privilegios.
- **Inserción de virus** o programas que se autoreplican provocando sobrecarga en las redes de comunicaciones y en los ordenadores donde están instalados, dejándolos prácticamente inoperativos.
- **Destrucción total o parcial de la información**, directamente o por medio de inclusión de virus.
- La realización de **"pinchazos" en las líneas de comunicaciones**, teniendo la posibilidad de leer y modificar el contenido de los mensajes.
- La **copia, manipulación y destrucción de los ficheros** contenidos en nuestra Base de Datos

Existen ficheros en Bases de Datos a las cuales se accede vía INTERNET, de libre disposición para cualquier usuario, donde se detalla cómo ser un buen "Hacker", los métodos y formas de introducirse en los Sistemas Informáticos e incluso la existencia de programas que pueden ser transferidos fácilmente y con los cuales intentar saltar los sistemas de seguridad conocidos.

Consecuencias

1. Los Sistemas más frágiles son aquellos que **no tienen medidas de seguridad de control de accesos implantadas seriamente**.

2. Caso de tener implantadas medidas de seguridad, puede que **sólo sean las funciones básicas**, las cuales suelen ser conocidades normalmente.
3. Existen **claves de acceso demasiado fáciles** por mal elegidas dentro de una sencillez al alcance de cualquier mente lógica.
4. La protección por "password" o de claves de lectura/escritura de nuestros ficheros **suele ser eficaz si cambiamos los estándares de instalación del fabricante**.
5. **No existen "barreras" que impidan el acceso** de los usuarios a los diferentes Sistemas de la Empresa.
6. Es muy importante la figura del Administrador de Seguridad en el **control y seguimiento de los accesos a ficheros** por los usuarios.
7. Las propias **aplicaciones no tienen controles** sobre los diferente usuarios y sus niveles de autorización para el manejo de la información.

1.2.6. Denegación de servicio

Se trata del impedimento o interrupción de una comunicación, o retraso en su tiempo crítico de operación. Bastará con que alguien nos envíe cientos de mensajes de gran tamaño hasta agotar irremediablemente la capacidad de nuestro disco.

Escenario

- **Pérdida de servicio**. Se puede perder el servicio tanto por problemas de seguridad como por otras causas no identificadas.
- **Destrucción total o parcial de la información**, directamente o por medio de inclusión de virus.
- **Alteración parcial o total** del contenido de la información, con fines destructivos o especulativos.

Consecuencias

1. **No está implantado el servicio de confirmación** extremo a extremo que asegura que el servicio no ha sido interrumpido, al mismo tiempo que **no se ha dañado la integridad de los mensajes**.
2. Nuestro Sistema Informático **no controla el acceso de usuarios** o es fácilmente superable.
3. Si es un usuario externo, **ha superado las medidas de seguridad** implantadas, descritas anteriormente.
4. Si es un usuario interno, ha accedido a ficheros en los cuales **no se ha restringido el uso por usuarios no autorizados**.

1.3. SERVICIOS DE SEGURIDAD

1.3.1. Requerimientos de servicios seguridad

Los servicios de seguridad que implementados van a permitir contrarrestar las amenazas previamente identificadas, son los siguientes:

a) *Confidencialidad de datos.*

b) *Integridad del mensaje y del contenido.*

c) *Autenticación de entidades, firma digital.*

d) *No repudio - acuse de recibo.*

e) *Control de acceso*

En la tabla siguiente se relacionan las amenazas, los servicios de seguridad y el objeto protegido.

Amenaza	***Servicio de Seguridad***
Divulgación no autorizada de la información	*Confidencialidad de datos*
Modificación no autorizada de la información	*Integridad del mensaje y del contenido*
Enmascaramiento	*Autenticación de entidades*
Repudio del mensaje de origen o del acuse de recibo	*No repudio*
Acceso no autorizado a recursos	*Control de acceso*
Denegación de servicio	*Control de acceso*

a) CONFIDENCIALIDAD DE LOS DATOS

Su propósito es impedir que nadie que no sea el receptor pueda leer el contenido de un mensaje y, por lo tanto, tener la disponibilidad de divulgarlo.

Hablando de un sistema de transmisión de mensajes, se trata de impedir que la información transmitida sea interceptada (leida) por persona no autorizada, y por lo tanto conocer su contenido.

Se trata en definitiva de garantizar que la información sólo pueda ser leida por el usuario o

usuarios a los que está dirigida.

La confidencialidad por tanto, se puede aplicar en:

- Información del destinatario.
- Texto completo.
- Parte del texto.

La técnica más moderna existente hoy en día que se puede aplicar como una solución muy eficaz, es la **CRIPTOGRAFÍA**, que mediante algoritmos matemáticos y aplicación de claves o contraseñas, y utilizando medios software o hardware, permite transformar el contenido del texto en un conjunto de caracteres no entendibles.

La seguridad se tiene en que se requiere el conocimiento y acuerdo mutuo entre el receptor del mensaje y el emisor, de las claves y utilizar el mismo medio software o hardware para poder cifrar y descifrar el mensaje. Se puede decir entonces que se ha establecido una comunicación segura.

b) INTEGRIDAD DEL MENSAJE Y DEL CONTENIDO

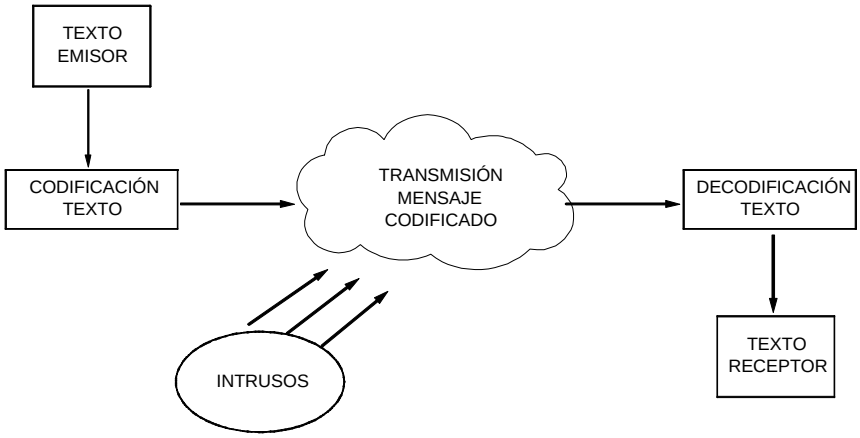
Se garantizará a la entidad receptora que el mensaje o información que está recibiendo es exáctamente el mismo que le envió la entidad origen.

Al mismo tiempo, el receptor tendrá la seguridad de que no ha habido, sobre la información original emitida, ninguna modificación, ni pérdida, ni contenido adicional antes de su recepción.

Para poder lograrlo, nos basamos igualmente en la tecnología de la **CRIPTOGRAFÍA**, pero pudiendo usar esta vez la clave pública y/o la clave privada.

Con la utilización de la clave pública, basta que emisor y receptor la conozcan.

Si utilizamos ambas, la clave pública y privada, deberá existir algún mecanismo adicional que permita a la entidad origen transferir la clave secreta al receptor.



Podemos decir que aparte de una comunicación segura, hemos logrado que no haya manipulacióndel texto en el trayecto emisor - receptor.

c) AUTENTICACION DE ENTIDADES

Garantizará a la entidad receptora que el mensaje que llegó de la entidad emisora, pertenece a quién dice ser. Esto lo podemos realizar mediante lo siguiente:

- **AUTENTICACION DE ENTIDAD SIMPLE**: Puede tratarse de la entidad origen de los datos o de la entidad destino.

  AUTENTICACION DE ENTIDADES MUTUA: Ambas entidades comunicantes se autentican una a la otra.

La autenticación debe de realizarse por medio de mecanismos de cifrado y de **FIRMA DIGITAL**, no por un simple mecanismo de intercambio de 'passwords' o de mensajes cifrados del tipo pregunta / respuesta, que son más vulnerables.

El empleo de este mecanismo de intercambio de autenticación con tecnologías de certificados puede utilizarse para proporcionar una capacidad de autenticación distribuida de modo que sea

posible un tratamiento seguro de la información y una mayor seguridad en la conectividad entre emisor / receptor.

Pueden utilizarse diversos mecanismos conjuntamente, que garanticen la Integridad, Confidencialidad, Autenticación y No Repudio en la transmisión de mensajes vía Correo Electrónico.

d) NO REPUDIO - ACUSE DE RECIBO

Proporcionará al emisor/receptor de un mensaje, una prueba irrefutable de que el contenido recibido fue el mismo que el del mensaje enviado por el emisor, y que por lo tanto no ha habido modificación del mismo desde el emisor, y se aceptará el mensaje.

Para poder proporcionar una confirmación de **NO REPUDIO**, el procedimiento sería el siguiente:

i. El **emisor del mensaje** solicita notificación afirmativa o negativa de la recepción con autenticación no repudiable.

ii. El **receptor del mensaje**, emite notificación afirmativa o negativa con no repudio, utilizando el procedimiento de autenticación.

iii. El **emisor del mensaje**, cuando recibe la notificación, utiliza los procedimientos de verificación para asegurarse que el emisor de la notificación es el deseado.

La presencia de un **CERTIFICADO DE NO REPUDIO**, prueba que el receptor aceptó la notificación de no repudio solicitado por el emisor.

Este servicio protege al emisor/receptor de un documento, de cualquier intento por parte del origen/destino de negar su envío/recepción en su totalidad o en parte del contenido del mismo.

Asimismo pretende **dar una validez legal a un documento**, ya que requiere que una persona se responsabilice de contenido del documento estampando su firma digital en él.

Estos servicios pueden ser de dos clases:

- Con **PRUEBA DE ORIGEN**. El receptor tiene prueba, demostrable ante terceros, del origen de los datos recibidos.
- Con **PRUEBA DE ENTREGA**. El emisor tiene prueba de que los datos han sido entregados al receptor deseado.

Acuse de recibo

Todas las funciones descritas anteriormente, están dentro de la confirmación de entrega extremo a extremo. Su propósito es poder probar que el contenido del mensaje enviado por la entidad origen fué recibido por la entidad destino. Esta función es similar al concepto de **ACUSE DE RECIBO**.

La necesidad del acuse de recibo

La posición del emisor puede resultar difícil ya que el receptor puede alegar que no recibió mensaje alguno o lo que es lo mismo, negar su existencia.

Al emisor sólo le puede quedar la seguridad de que el receptor no le puede alterar el contenido del mensaje.

Para que el emisor esté seguro de que el mensaje ha llegado a su destino, aparece la figura del **ACUSE DE RECIBO**. Este se produce en un mensaje del receptor al emisor, de haberlo recibido.

Para que el ACUSE DE RECIBO sea operativo, se debe establecer un plazo de tiempo mínimo en que se produzca el envío del mismo.

Es en este punto cuando se invierten las posiciones, pues el receptor no puede justificar que envió el acuse de recibo, estaríamos dentro de un círculo cerrado de envíos y contraenvíos de acuses de recibo.

Para solucionar este problema, **se impone la figura de una tercera parte**, siendo a través de su actuación la forma de que se logre que todas las partes tengan prueba plena del origen, contenido y destino de cualquier mensaje que se haya emitido o recibido.

e) CONTROL DE ACCESO

Los servicios de seguridad de control de acceso tienen por objeto garantizar que sólo acceden a la información y a los diversos recursos del sistema aquellos usuarios que tienen los derechos para ello. Los mecanismos a utilizar van desde una adecuada gestión de claves de acceso o *passwords* hasta las más complejas técnicas de cortafuegos o *firewall* como se verá más adelante.

1.3.2. Requerimientos por parte del proveedor de servicios.

- Disponer de personal que **administre la seguridad. Informes seguridad**.
- Efectuar con regularidad **pruebas del sistema de seguridad** implantado.
- Maquinas gestionadas, **operativa 24 h., non-stop**.

- **Seguimiento anuncios del CERT** (Computer Emergency Response Team).
- Conocimiento **soluciones dadas por el Centro Alarmas** de INTERNET.
- **Detección temprana de intentos de ataque**. Seguridad ante la intrusión.
- **Uso de criptografía** para el transporte seguro de datos.
- Asegurar la **privacidad** en:
    - Transacciones comerciales, financieras y comercio electrónico.
    - Transporte seguro de información confidencial. Firma Digital.
    - Confidencialidad en la transferencia de ficheros.
- Asegurar **integración con sistemas** existentes.

1.3.3. Requerimientos por parte del usuario individual o empresas usuarias.

- **Disponer de las herramientas estándar** existentes en el mercado, para las cuales hay productos de seguridad y disponibles en la red INTERNET.

- Implementar Sistemas, programas y protocolos de comunicaciones para que el **administrador de seguridad pueda desarrollar procedimientos** operativos de seguridad de la empresa, para los siguientes servicios:
    - *Correo electrónico*. Utiliza las herramientas estándar del mercado. Utiliza protocolo de comunicaciones TCP/IP estándar.
    - *Transferencia de ficheros*. Permite dentro de un ordenador remoto mirar directorios, seleccionar ficheros y transferirlos por las líneas de comunicación a otro ordenador externo.
    - *Telnet*. Un terminal con un programa de emulación de pantallas, puede establecer sesiones de trabajo con otros ordenadores situados en la red INTERNET. Los usuarios deben facilitar la dirección o el nombre del ordenador remoto a TELNET.
    - *List server*. Directorio automátizado de direcciones que acepta los mensajes enviados a él y los distribuye a sus suscriptores. Este directorio permite ver cada mensaje que le ha sido enviado sólamente a los usuarios suscritos.

1.4. TÉCNICAS Y MECANISMOS DE SEGURIDAD

Los servicios de seguridad constituyen el *qué*, mientras que las técnicas y mecanismos de seguridad constituyen el *cómo* en la implantación de la seguridad. Así una técnica o mecanismo de seguridad es la lógica o algoritmo que implementa un servicio de seguridad particular en hardware y software.

La siguiente tabla expresa la relación entre los servicios de seguridad y las técnicas o mecanismos de seguridad aplicables.

Servicio de Seguridad	***Técnica/Mecanismo de Seguridad***
Autenticación de entidad	*Intercambio de autenticaciones*
Autenticación de datos de origen	*Cifrado* *Firma digital* *Función de comprobación criptográfica*
Control de acceso	*Lista de control de acceso* *Cortafuegos*
Confidencialidad orientada a la conexión	*Cifrado* *Etiquetas de seguridad*
Confidencialidad no orientada a la conexión	*Cifrado* *Etiquetas de seguridad*
Confidencialidad del flujo de tráfico	*Cifrado* *Relleno del tráfico* *Etiquetas de seguridad*
Integridad orientada a la conexión	*Función de comprobación criptográfica* *Funciones hash y cifrado*
Integridad no orientada a la conexión	*Función de comprobación criptográfica* *Funciones hash y cifrado* *Firma digital*
No repudio, origen	*Firma digital* *Teceras Partes de Confianza*
No repudio, destino	*Firma digital* *Terceras Partes de Confianza*

1.4.1. Técnicas de criptografía.

El uso de la criptografía o cifrado puede proporcionar la confidencialidad, tanto de los datos como del flujo/tráfico de información, y puede formar parte o complementar otros mecanismos de seguridad. Aunque la criptografía ha sido utilizada desde muy antiguo desde la aparición de los ordenadores ha adquirido una mayor relevancia, al facilitarse su uso con estas máquinas.

El sistema genérico es el siguiente:

```
--->mensaje original ---> Sistema de Cifrado --->mensaje cifrado ---> (*)
            Clave de cifrado -          |
                                        | ---> Sistema de Descifrado ---> mensaje original
```

Los algoritmos de cifrado pueden ser reversibles o irreversibles. Existen dos clasificaciones generales de algoritmos reversibles:

- *Sistema convencional o simétrico*; donde la clave de cifrado y de descifrado es la misma.
- *Sistema asimétrico o de clave pública*; en el que existen dos claves, una

pública y otra privada. El mensaje se cifra utilizando una y se descifra utilizando la otra y el conocimiento de una de las claves no implica el conocimiento de la otra.

Los algoritmos de cifrado irreversible pueden o no usar una clave. Si usan una clave ésta puede ser pública o secreta.

Cifrado y descifrado

Un método de cifrado, bien sea simétrico o asimétrico, no debe pretender abordar un planteamiento de inviolabilidad absoluta; se busca que el coste de su descifrado 'desleal' a través de un mecanismo externo al proceso de comunicación sea muy costoso, a ser posible en varios ordenes de magnitud, tanto en tiempo como en recursos necesarios.

ALGORITMO DES (Data Encryption Standard). Desarrollado por IBM en 1.977, se basa en un algoritmo que funciona de forma diferente según una palabra clave que se mantiene en secreto, conocida sólo por emisor y receptor.

El mensaje M del emisor es codificado por el algoritmo, al que se le introduce como datos de entrada la palabra clave K y el mensaje M; de esta forma obtenemos:

AlgoritmoE(K,M) -- se genera --> C, que es lo que viaja por la Red.

El receptor usando el algoritmo y los datos que conoce, es decir, la clave K y la información que le llega C, obtiene de nuevo el mensaje en claro M.

AlgoritmoR(K,C) -- obtiene --> M.

Los algoritmos usados se basan en operaciones de permutaciones de bits que se realizan de forma muy rápida en los ordenadores; pero muy difíciles de detectar sin concocer la palabra clave K.

El problema de mantener una protección con este tipo de algoritmos de clave secreta es la necesidad de tener muchas palabras secretas (tantas como usuarios diferentes con los que nos vamos a comunicar), siendo difícil establecer un sistema de cambio de clave o *password* cada vez que sospechemos que ha sido descubierta.

ALGORITMO DE CLAVE PUBLICA (RSA: Rives-Shamir-Adleman, 1.977). Se basa en la teoría matemática de la factorización de grupos finitos. En concreto se selecciona como palabra clave un número producto de dos primos muy grandes, uno de los cuales constituye la clave secreta del usuario, mientras que el otro se puede declarar como público.

Existen algoritmos tales que si se les introduce un mensaje M y la clave pública, generan un dato D cifrado, que puede ser descifrado solo conociendo este dato D y la clave secreta; es decir se sigue el esquema:

M --> KPR(M)=D dato que viaja cifrado por la Red y que sólo puede ser descifrado concociendo la clave privada del receptor R al cual va dirigido el mensaje; el cual actuará usando el algoritmo con datos de entrada D y KSR, con los que obtendrá M:

D ----------> KSR(D)= M o lo que es lo mismo:
KPR(M) --->KSR(KPR(D)) = M.

Este algoritmo permite el proceso inverso ; es decir:

KSE(M) ---> KPE(KSE(M)) = M,
siendo KSE= clave secreta del emisor y KPE = clave pública de emisor.

La validez de este algoritmo se basa en que no existe función o algoritmo tal que conociendo la clave pública pueda descifrar la privada y viceversa.

Gestión de claves

Distinguiremos dos sistemas diferentes de Gestión de Claves:

a) *de Claves Secretas*: Cuando para descifrar un algoritmo sólo es necesario conocer la clave secreta (además del algoritmo en cuestión) es preciso propagar las clave por medios diferentes al camino de comunicación a los que esa clave va a proteger.

b) *de Clave Pública*: Es conveniente enviar la clave pública a una autoridad de certificación (CA), cifrada con la clave pública de esa CA y preferiblemente firmada.

Cada vez que queramos enviar un mensaje a un usuario R, deberemos solicitar de nuestra Autoridad de Certificación (CA), o de la CA correspondiente, una certificación de R. Esta operación se puede omitir sólo si tenemos otra certificación válida del usuario (debemos asegurarnos de que sigue siendo válida, es decir que no ha caducado por haberla modificado el receptor R).

1.4.2. Firma digital

Se basa en el uso de técnicas criptográficas. Se puede implementar tanto con técnicas de cifrado de clave secreta, como con técnicas de cifrado de clave pública.

Para evitar la necesidad de conocimiento de claves secretas, se puede elegir la utilización de claves secretas para cifrar y de claves públicas para descifrar.

La posesión de una clave privada identifica a un usuario ya que ésta es sólo conocida por el propietario y sólo él puede cifrar con ella.

Todo el mundo puede verificar la identidad de un usuario descifrando con la clave pública los datos cifrados con la privada.

Si son iguales la Firma es correcta, en caso contrario se rechaza. Cualquier modificación del documento, de parte de su contenido o de la firma sería detectado automáticamente.

El mecanismo de firma digital define dos procedimientos:

a) Firmar una unidad de datos: Utiliza información privada (p.e. única y confidencial) del emisor. Implica tanto el cifrado de la unidad de datos como el de la producción de ún código de control criptográfico asociado a la unidad de datos, utilizando para ello la información privada del firmante como clave privada.

b) Verificar la firma de una unidad de datos: Utiliza procedimientos e informaciones públicamente disponibles, pero a partir de las cuales no se puede deducir la información privada del firmante. Implica la utilización de procedimientos e informaciones públicas para determinar qué firma se ha generado con la información privada del firmante.

La característica esencial del mecanismo de firma, es que dicha firma sólo puede haber sido generada con la información privada del firmante. Por lo tanto cuando se verifica la firma, se puede probar que sólo el poseedor de la información privada puede haber generado la firma.

1.4.3. Técnicas de seguridad diversas

Intercambio de autenticaciones. Algunas de las técnicas que se pueden utilizar para el intercambio de autenticaciones son:

a) Utilización de información de autenticación, como contraseñas proporcionadas por la entidad emisora y comprobadas por la entidad receptora.
b) Técnicas criptográficas.
c) Utilización de características y privilegios de la entidad.

El mecanismo puede incorporarse en un nivel para proporcionar la autenticación de entidades semejantes. Si el mecanismo no proporciona una autenticación positiva de la entidad, puede producirse un rechazo o la finalización de la conexión, además de una entrada en el programa de auditoría de seguridad y un informe al centro de gestión de la seguridad.

La selección de técnicas de autenticación dependerá de las circunstancias en que deben ser usadas. En la mayoría de los casos se necesitan utilizar con:

a) Marcado de la hora y de relojes sincronizados.
b) 'Handshakes' de dos y tres vías, para autenticación unilateral o autenticación mutua, respectivamente.
c) Servicios de no repudio, conseguidos con firma digital y mecanismos de tercera parte de confianza.

Funciones hash: Son funciones matemáticas sin inversa, que aplicadas a un elemento o dato que se transfiere impiden que este sea descifrado. Se utilizan para comprobar la integridad de los datos según un mecanismo por el cual se cifra una cadena comprimida de los datos a transferir mediante una función hash; este mensaje se envía al receptor junto con los datos ordinarios; el receptor repite la compresión y el cifrado posterior de los datos mediante la aplicación de la función hash y compara el resultado obtenido con el que le llega, para verificar que los datos no han sido modificados.

Relleno del tráfico: Los mecanismos de relleno del tráfico se pueden utilizar para proporcionar diversos niveles de protección contra los análisis del tráfico. Se trata de enviar tráfico espúreo junto con los datos válidos para que el adversario no sepa si se está enviando información o qué cantidad de datos útiles se está transfiriendo. Estos mecanismos sólo pueden ser efectivos si el relleno del tráfico está protegido con un servicio de confidencialidad.

Etiquetas de seguridad: Los recursos, incluyendo los datos, pueden tener asociadas etiquetas de seguridad, por ejemplo para indicar el nivel de sensibilidad. A menudo es necesario que los datos en tránsito lleven una etiqueta de seguridad apropiada. Las etiquetas de seguridad pueden ser los datos adicionales a los datos transferidos, o pueden ser implícitas, por ejemplo, por utilizar una clave específica para cifrar los datos, o por el contexto de los datos, como su origen o la ruta

utilizada. Las etiquetas de seguridad explícitas deben ser claramente identificables, para que puedan ser comprobadas apropiadamente. Además, deben estar limitadas a los datos a los que están asociadas.

1.4.4. Control de accesos

Se trata de proteger los sistemas de informacion, de accesos no permitidos.

Las medidas de seguridad en INTERNET básicamente son:

- **LA SEGURIDAD DE ACCESOS**. Protección del acceso a nuestros sistemas informáticos y aplicaciones por personas no autorizadas.
- **LA CONFIDENCIALIDAD DE LA INFORMACIÓN**. Evitar la divulgación, pérdida o alteración del contenido de nuestros ficheros o durante la transmisión de los mismos.

La implantación de las medidas de control de acceso ha de tener en consideración los siguientes aspectos:

- Necesidades por un alto numero de accesos públicos.
- Restringir el acceso a INTERNET a empleados de la empresa.
- Mantener la seguridad e integridad de la información.

Veamos las principales técnicas de control de accesos:

FIREWALLS o CORTAFUEGOS

La tecnología de *Firewalls* o cortafuegos, es relativamente nueva y se ha potenciado al comprobar que una red abierta como es INTERNET ha incorporado un nuevo tipo de usuario no corporativo, y por tanto mas difícil de controlar por las medidas y reglas implantadas en los propios 'host'.

Estos cortafuegos, fueron diseñados para impedir a los *Hackers* o intrusos que están utilizando INTERNET, el acceso a redes internas de las empresas. Algunos cortafuegos incluso controlan la información que se mueve por dichas redes.

Pueden ayudar asimismo a prevenir la entrada de virus encapsulados en los paquetes transmitidos con destino a la red empresarial. Se utiliza la expresión cortafuegos para designar pasarelas u otras estructuras más complejas, existentes entre la red propia de la empresa e INTERNET, con la finalidad de restringir y filtrar el flujo de información entre ambas.

Podemos definir la **Tecnología de *firewall* o cortafuegos** como el sistema que controla todo el tráfico hacia o desde INTERNET utilizando software de seguridad o programas desarrollados para este fin, que están ubicados en un servidor u ordenador independiente. Este sistema comprueba que cada paquete de datos se encamine a donde debe, desde la red INTERNET a nuestra red privada y viceversa, al mismo tiempo que contiene la política de seguridad especificada por el Administrador del Sistema.

Para prevenir o permitir el tráfico de red, comprueba el *host*, la red y la puerta desde la cual el paquete es originado o destinado.

Para conectar directamente ordenadores de un sistema corporativo en red INTERNET, existe una aplicación que reside en el servidor para permitir un buen acceso a los servicios INTERNET facilitando al mismo tiempo la mayor seguridad que sea posible.
Este servidor **comprueba**:

- El *host* desde el cual se origina la conexión.
- El *host* al cual la conexión es solicitada.
- Los comandos que se producen en la conexión.

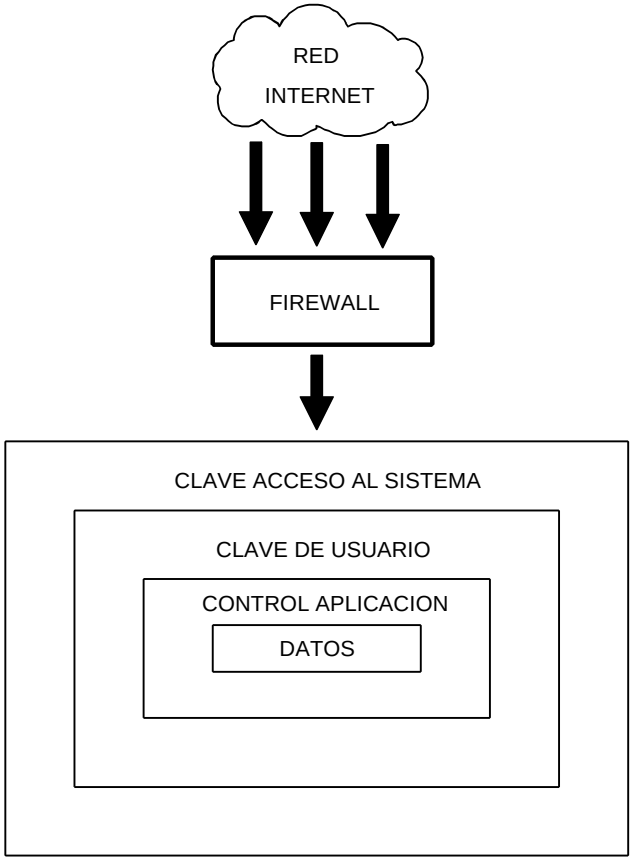
Todo ello puede facilitar al Administrador del Sistema la prevención de todas las conexiones desde *host* especificados o de redes en INTERNET.

Desde esta puerta de entrada, el sistema puede también prevenirse de aquellos usuarios que a través de comandos añaden un factor de riesgo a nuestra seguridad. Se trata de prevenir , por ejemplo, la exportación de información contenida en el cortafuegos o en los servidores hacia el exterior .

Mediante **aplicaciones residentes en el servidor o cortafuegos** el **Administrador del Sistema** puede:

- Definir qué **usuarios tienen palabra clave de acceso** autorizada.
- Configurar las **palabras clave de acceso que deben ser aceptadas por los diferentes hosts** configurados en nuestra red privada.
- **Controlar las cuentas** de aplicación autorizadas.
- **Evitar que la intrusión pueda cambiar la configuración de la aplicación** residente.
- **Controlar los accesos entre la red privada y el servidor** como punto de entrada.
- Llevar un **registro de todas las incidencias** que se produzcan.

BARRERAS DE PROTECCION DE LOS DATOS FRENTE A INTRUSOS INTERNET



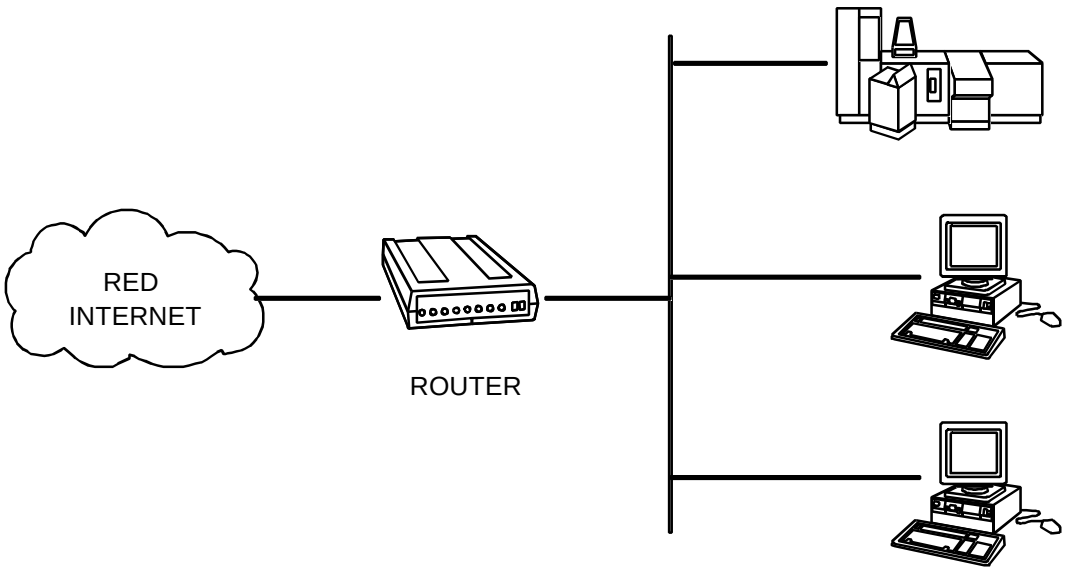
Se entiende por *Firewall* o Cortafuegos cualquiera de los esquemas que se describen a continuación o cualquier combinación de ellas.

a) Cortafuegos filtrador de paquetes. Router.

Un **router o encaminador, es un dispositivo que puede filtrar los paquetes de datos**, tanto los que salen como los entrantes a la red de la empresa, con destino u origen en INTERNET. Es el sistema más sencillo de establecer conexión con INTERNET.

También se pueden configurar los protocolos de filtrado para que permitan la entrada en la red sólo de determinados tipos de transmisiones o de aquellas que tengan su origen en emisores predeterminados. Filtra direcciones de red (IP, X25, 3270,...)

Colocando un router entre la red empresarial e INTERNET se consigue un primer elemento cortafuegos esencial para la seguridad. Siempre desde la base de que sea la única puerta de entrada desde el exterior.



El problema surge cuando además de controlar esa puerta, tiene que filtrar los encamientos a todos o algunos de los hosts y a los distintos tipos de acceso. Por ejemplo, una red interna sólo puede recibir correo electrónico, otra no ser accesible desde Internet, una tercera solo puede facilitar información al exterior, etc.

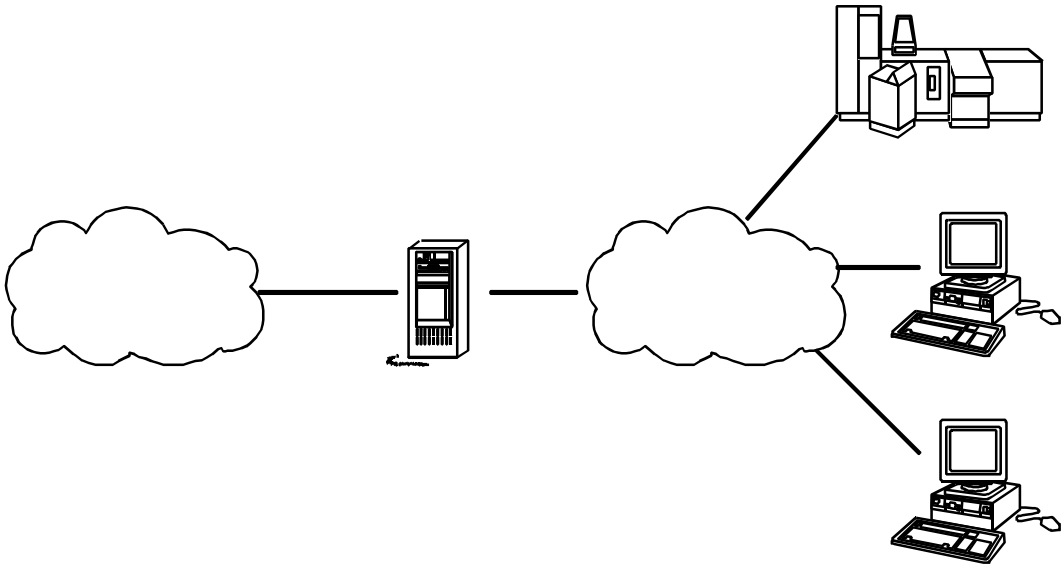
Aunque no pueden facilitar un alto nivel de seguridad, si lo es de forma bastante sencilla y sólida. Es **mucho más asequible** tanto en cuanto a coste, como en relación a la experiencia tecnológica necesaria, que otros sistemas.

Este sistema se debe apoyar o complementar con un mecanismo de seguridad propio de la aplicación que vaya a tratar la información, con el fin de impedir que lleve otro contenido que no sea el solicitado.

B) Cortafuegos a nivel de circuitos.

Cuando **las medidas de seguridad se establecen a nivel de circuitos**, un dispositivo interpuesto transmite las comunicaciones entre las redes internas y externas.

Suele ser un host provisto de dos interfaces operando a modo de pasarela y realiza las tareas de filtrado de paquetes, que en el apartado anterior realizaba el router, pero en este caso **pueden añadirse más funciones de seguridad como las de autenticación mediante el uso de 'password'** o palabras clave asignadas previamente a los usuarios. De esta forma cualquiera que intente acceder a la red interna mediante la técnica de generar dinámicamente 'passwords' aleatorios, se encontrará con un impedimento adicional a las medidas adoptadas, haciendo el acceso mucho más difícil.



c) Cortafuegos a nivel de aplicación

La forma de protección mas completa, además de la más conocida y experimentada, es la utilización de cortafuegos a nivel de aplicación.

Consiste en crear una subred, que constituya una zona de separación entre las redes internas e INTERNET. Por ejemplo mediante un router o encaminador, pero también se puede colocar un cortafuegos de acceso a la red interna.

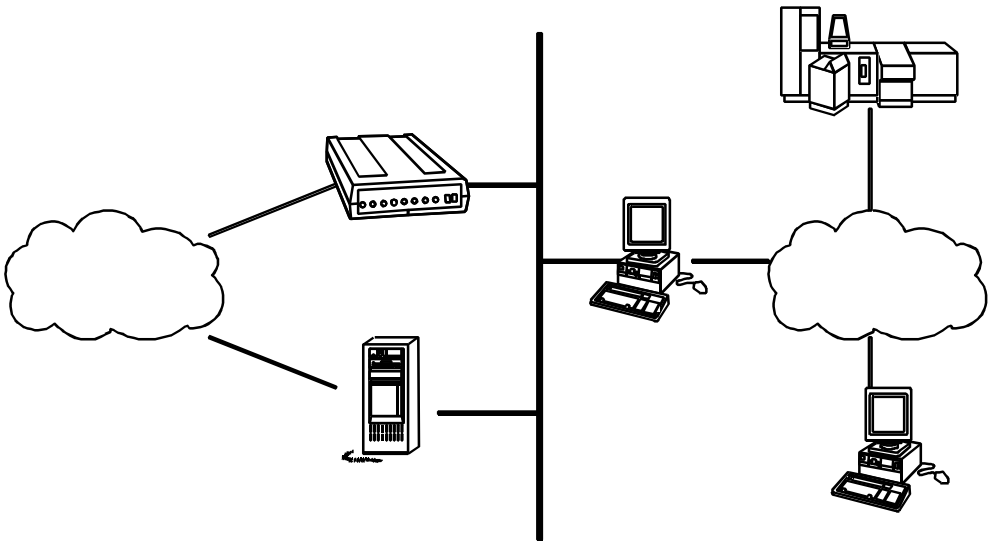
Un segundo dispositivo que debe ser un *host* se situará delante de la red interna. Los usuarios, tanto de entrada como de salida acceden a este *host* mediante una operación *Telnet* (TCP/IP) para trabajar con una determinada aplicación ubicada en el mismo.

Este *Host* gestiona las tareas de autentificación de usuarios, limitación de tráfico de entrada y salida, realiza un seguimiento de todas las actividades manteniendo un registro de incidencias.

Este tipo de cortafuegos debe incorporar código escrito, especialmente para especificar todas y cada una de las aplicaciones para las cuales existe autorización de acceso.

La **ventaja** que aporta este sistema es que el usuario externo nunca tiene acceso a las redes internas de la empresa, por lo tanto nunca podrá realizar ningún tipo de intrusión.

El **inconveniente** es que supone una fuerte inversión en tiempo y dinero para proporcionar un servicio cuyo grado de utilización puede no llegar a ser rentable.



Aplicaciones de los cortafuegos

a) Aplicación al correo electrónico en uso corporativo.

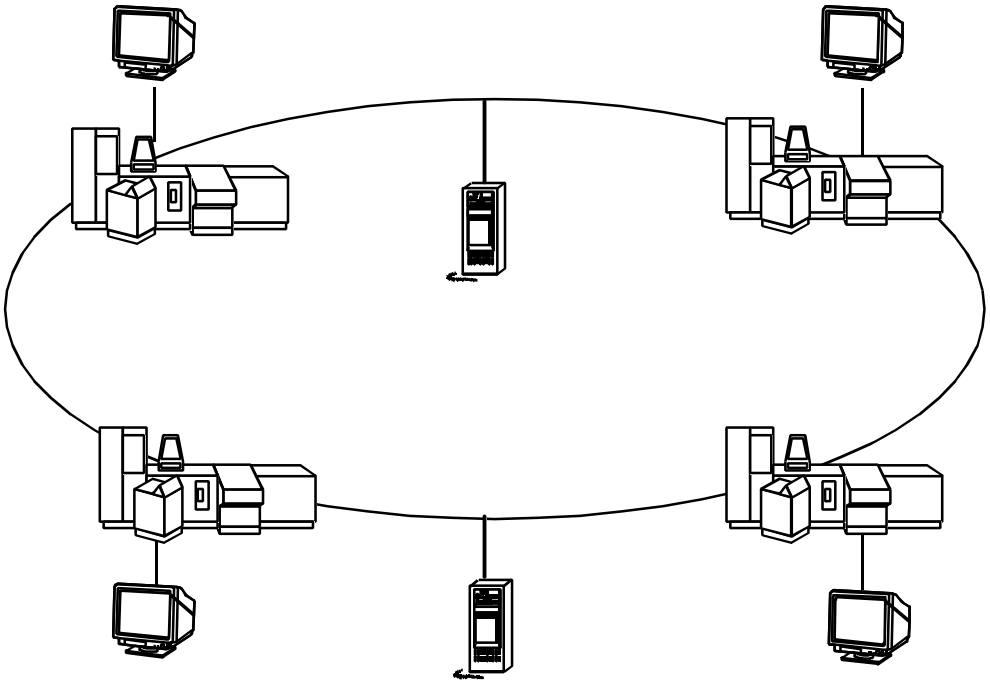
Se puede **crear un Grupo Cerrado que interconecte todos los ordenadores** situados en puntos geográficos distintos incluidos en la red INTERNET, pero que pueden conectarse entre sí para aplicaciones de correo electrónico, transferencia de ficheros y poder conectarse usuarios de otro ordenador incluido en este Grupo, controlados por un sistema de seguridad corporativo.

Cada uno de ellos, a su vez, puede conectarse con otros sistemas informáticos bien por INTERNET o por otros medios de comunicación.

Para evitar intrusiones a través de correo electrónico, se puede **colocar un servidor o punto único de entrada que controle los accesos y salidas del Grupo Cerrado**.

Se le puede **dar funciones de sólo entrada de correo electrónico** pudiendo actuar como cortafuegos, y a cada ordenador del grupo darle funciones de sólo salida.

De esta forma limitaremos los puntos de acceso a uno solo y con un mayor control en todos los sistemas.



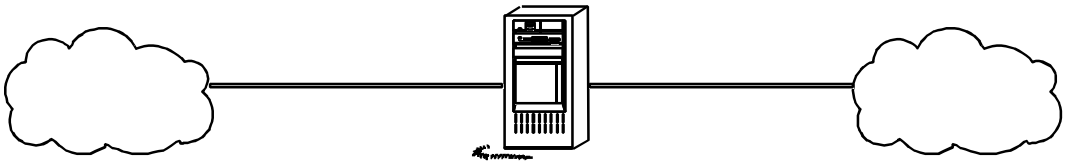
b) Servidor como punto de entrada única a la red interna.

Este tipo de entrada **previene de una conexión directa entre el usuario de INTERNET y la red interna**.

El filtro de acceso a nuestras aplicaciones controla aquellos usuarios que pueden acceder al interior desde el exterior y viceversa.

Sin embargo una aplicación corriendo en este servidor puede establecer conexiones desde el exterior hacia cualquier punto de la red interna.

Un **problema** se nos presenta al ser superada esta barrera, entonces nuestra red está desprotegida.

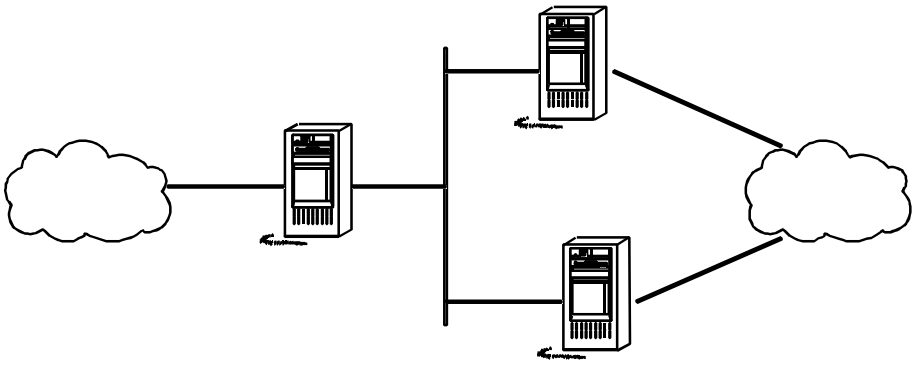


c) Servidor como punto de entrada única a las aplicaciones.

Como complemento del servidor único como punto de entrada única, se pueden colocar **diferentes servidores exclusivos para cada aplicación**.

Nos garantiza que filtrarán todos los accesos, dejando sólo los que corresponden a la aplicación permitida.

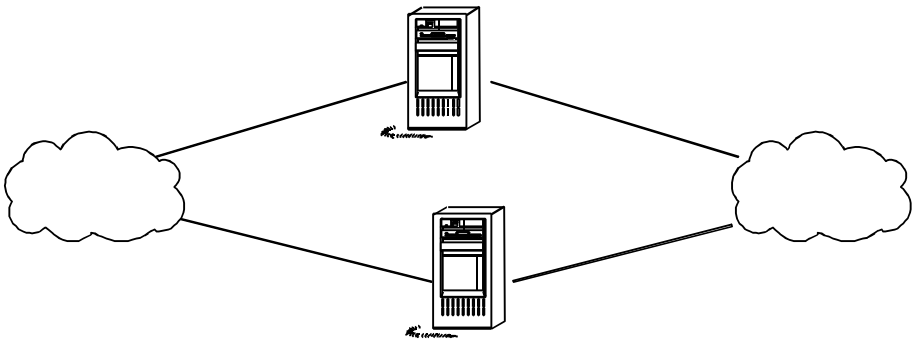
Deben de estar colocados entre INTERNET y el servidor único y pueden contener la lista de usuarios que tienen permitido el acceso al host, y/o aplicaciones.



d) Servidor como punto de entrada único al correo electrónico.

Una puerta de entrada puede ser la colocación de otro **servidor localizado en la red interna**. Distribuye los mensajes del correo electrónico entre los diferentes ordenadores que están en la red privada.

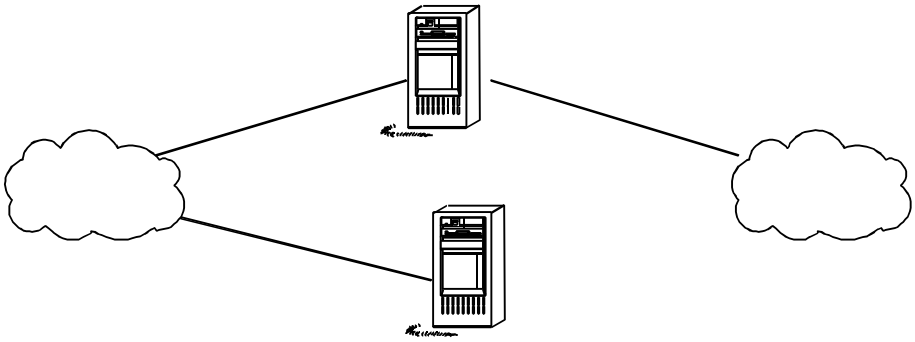
Contiene a su vez la lista de usuarios que pueden recibir mensajes y los que pueden enviar mensajes al exterior. Se puede usar también para el tráfico interior de la red.



e) Servidor sólo para facilitar información.

Cuando nuestro propósito sea permitir únicamente la lectura de información, deberemos de adecuar el control de acceso de usuarios a la **función de lectura** únicamente.

En grandes instalaciones, el ideal sería disponer de otro ordenador único que contenga la información sólamente, de esta manera evitaremos cualquier posibilidad de que se pueda obtener otra información distinta a nuestro propósito debido a tener cortados los accesos a cualquier otro sistema.



1.4.5. Terceras Partes de Confianza (TTPs)

***Las TRUSTED THIRD PARTIES* ó TERCERAS PARTES DE CONFIANZA**, también conocidas por las siglas **TTP**, son entidades con una funcionalidad que basa sus acciones en el arbitrio de situaciones de conflictos por el intercambio de documentos entre interlocutores participantes en comunicaciones seguras, y a requerimiento de una o ambas partes emitiendo de forma automática informe de una resolución.

Como su nombre sugiere, todos los elementos comunicantes pertenecientes al Dominio de Seguridad, consideran fiables y seguros los informes que emita una TTP.

Una atribución de esta entidad es la posesión de firmas digitales de documentos intercambiados, que puedan llevar a litigio a sus interlocutores. Por medio de estas firmas, la TTP podría demostrar la autoría de un documento, pudiendo llegar a dar total validez legal a los documentos intercambiados.

La creacción de un Directorio Público de claves públicas plantea el problema de la autenticidad de los datos del mismo en un marco donde los usuarios desconfían entre si. Esto se soluciona con la creación de un ente Certificador en el sistema, quién de una forma inequívoca, firma o certifica la clave pública y los datos identificatorios de cada usuario.

Esta firma se almacenará en el directorio público junto a los demás datos del usuario, de tal forma que siempre se pueda comprobar la veracidad de los mismos, y con ello asegurarse de que la identidad y parámetros de cualquier interlocutor del sistema son correctos.

El ente Certificador tiene su clave pública conocida por todos los miembros del sistema, y su propia clave privada; esto le permite firmar con la clave privada, y a los usuarios comprobar la firma con la clave pública del ente.

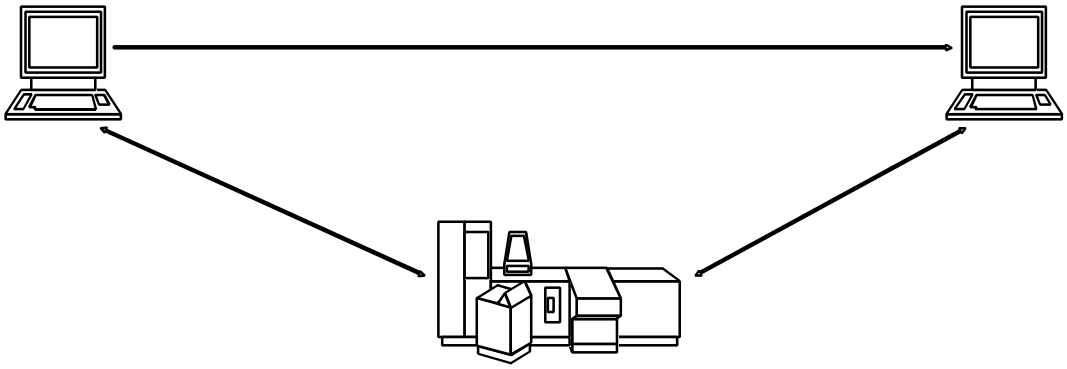
Las firmas digitales, por su parte, dan una nueva dimensión al mundo de la información. Dado que se trata a través de sistemas informáticos, es imprescindible incorporar el concepto de firma que autentifique de una forma inequívoca al autor y la integridad del documento.

Implementar un Sistema Centralizado "TTP". Tiene como finalidad certificar las identidades de los usuarios, receptor y emisor.

- EMISOR. Adquiere garantías de que el receptor es quién dice ser.
- RECEPTOR. Recibe garantías de que el emisor es quién dice ser.
- El sistema **no incluye Control de Acceso**, una vez aceptado el emisor. Dicho control corresponde al sistema informático del receptor.

El sistema TTP, está implementado en una máquina segura, y es depositario de las claves de usuarios.

INCONVENIENTE En caso de un sabotaje al sistema informático del TTP, se podría dejar sin seguridad a toda la red, debido a que se podría acceder a los ficheros que contienen las claves y se perdería toda confidencialidad de la información.



SERVICIOS Y FUNCIONES

Los **servicios de seguridad** para los que resulta más necesario la actuación de las TTPs son:

- **Autenticación** (validez de firmas).
- **Control de accesos** (emisión de credenciales con privilegios de accesos).
- **No repudio**. (emisión de evidencias)

La **función de las TTPs** puede considerarse, según los casos concretos donde actúan, como:

- Entidades que **certifican** la validez de una pieza de información.
- **Monitorización** de los sucesos que se producen.
- **Certificación electrónica**.
- **Jueces que dictaminan** (sólo a efectos internos del Dominio de Seguridad).

TTP al margen de la comunicacion activa

- **No interviene directamente** en el proceso envío-recepción del mensaje.
- Presta servicio a un usuario **cuando es requerido** para ello.
- Es imprescindible que en la comunicación usuario-TTP **existan garantías de la autenticidad de la TTP**.

Casos típicos de utilización pueden ser:

- **Autoridades de Certificación** CA. Emiten información acerca de las claves públicas de los usuarios en un determinado Dominio de Seguridad.
- **Directorio**, DS seguro. Pueden usarse para depositar en él información de seguridad sensible, cuya validez viene garantizada por la seguridad del DS (autenticación, control de acceso e integridad).
- **Verificación de firmas**. Actúa como juez cuando aparece un conflicto entre partes.

TTP diréctamente involucrada en la comunicacion

- En servicios de no repudio de entrega, **es imprescindible la existencia de TTPs** presentes en todas las transacciones que se realicen.
- **Monitorización de todas las actividades** que serán guardadas para ser utilizadas posteriormente, caso necesario, **para la resolución de disputas y litigios**.
- En cuanto a la **validez jurídica**, estará ligada a la fortaleza de la prueba que se presente ante un Tribunal.

Las propiedades de los datos transmitidos entre dos o más entidades, como su integridad, origen, fecha y destino, deben ser asegurados con la utilización de un mecanismo de tercera parte de confianza. La seguridad la proporciona una tercera parte de confianza para las entidades en comunicación, y que debe tener la información necesaria para proporcionar la seguridad requerida. Cada instancia de comunicación debe utilizar mecanismos de firma digital, cifrado e integridad, apropiados para el servicio que va a proporcionar esta tercera parte. Cuando se invoca un mecanismo de este tipo, los datos se transmiten entre las entidades comunicantes vía las instancias de protección de la comunicación y la tercera parte de confianza.

1.4.6. Acciones básicas de seguridad para servicios Internet

a) Correo electrónico

Como queda recogido en el excelente artículo titulado 'Seguridad en Internet' y publicado por Manuel Medina y Ángel Fernández en la revista Novática (jul/ago.1995) existe un conjunto de acciones básicas que se pueden realizar enfocadas a servidores de correo electrónico Internet, basados en SMTP (*Simple Mail Transport Protocol*) funcionando sobre el sistema operativo UNIX:

- Centralizar el servicio de correo en una sola máquina, por la que deberá pasar todo el correo entrante y saliente de nuestro dominio. Esto permite centralizar la gestión, dotar de mecanismos de filtrado de cabeceras al correo en un único punto o manejar un solo fichero de alias.
- Configurar el correo de forma que en las direcciones salientes nunca aparezca el nombre de la máquina desde donde se generó realmente el mensaje, sino únicamente el nombre del dominio. Por ejemplo si la máquina se llama *ejemplo.sale.desde.aqui*, la dirección del mensaje debe ser *loquesea@sale.desde.aqui* .
- Configurar el *Sendmail* para que no sea necesario que se ejecute como el usuario *root*.
- Utilizar un sistema de cifrado de correo electrónico; uno de los más conocidos es PGP (*Pretty Good Privacy*).

- Configurar el correo eletrónico para su uso a través de un sistema de cortafuegos.
- Asegurarse de que el directorio depósito de correo, donde están las carpetas de los usuarios, está protegido de escritura para quien no sea propietario del directorio, y que los usuarios sólo tienen permiso de lectura y escritura para el propio usuario.
- Revisar periódicamente los ficheros de *log* de correo.
- Comprobar que las protecciones del directorio de *spool* (normalmente *usr/spool/queue*) son de lectura/escritura para todo el mundo, excepto para el propietario del proceso de *Sendmail*.
- Comprobar que en el fichero de aliases no existen declaraciones que permitan enviar un *Mail* a un fichero o a un programa. Por ejemplo *decode: '|/usr/bin/uudecode'*.
- Revisar que en el fichero *sendmail.cf* no existen reglas que permitan que un mensaje provoque la ejecución de un comando.
- Si se utiliza correo con soporte MIME (*Multipurpose Internet Mail Extensions*, usado para la transmisión de todo tipo de formatos como imágenes, sonido, etc), verificar que en el fichero *mailcap* o los ficheros *$HOME/.mailcap* de los usuarios no contienen reglas que puedan suponer un riesgo.

  Por ejemplo: activar el visualizador de *PostScript* al procesar un mensaje que en su cabecera diga que contiene un texto *PostScript* puede suponer que se pierdan todos los ficheros pues *PostScript* tiene instrucciones que permiten borrar ficheros.
- Mantener información constante sobre el estado del arte en seguridad sobre correo electrónico. Mantenerse constantemente informado sobre los posibles errores que se hayan encontrado en las versiones de los programas que utilicemos. Un excelente sistema son las comunicaciones del CERT o los grupos de *NEWS* que tratan temas de seguridad. El CERT (*Computer Emergency Response Team*, de la Universidad Carnegie Mellon en Pittsburgh Pensylvania es un organismo subvencionado por el Gobierno Federal que alerta a los usuarios de fallos en la seguridad de Internet. Apoyando los esfuerzos del CERT hay más de 34 CERTs locales que componen lo que se denomina FIRST (*Forum of Incidence and Response Security Teams*). Fuentes con información sobre seguridad accesibles en Internet son las siguientes:
  - TCP Wrapperby Wietse Venema. Disponible por FTP en *ftp.win.tue.nl* (*/pub/security/tcp_wrapper*)
  - Socks. Koblas and koblas, 1992. Disponible por FTP en *ftp.inoc.dl.nec.com* (*pub/security/socks.cstc*)
  - TIS Firewall Toolkit. Avolio and Ranum, 1994. Disponible por FTP en *ftp.tis.com* (*/pub/firewalls/toolkit*)
  - Screend, Mogul 1989. Disponible por FTP en *gatekeeper.dec.com* (*/pub/DEC/Screend/screend.tar.Z*)
  - TAMU, Stafford, 1993. Disponible por FTP en *net.tamu.edu* (*/pub/security/tamu*)
  - COPS, Farmer & Spafford, 1990. Disponible por FTP en *ftp.cert.org* (*/pub/tools/cops*)
  - SATAN. Disponible por FTP en *ftp.win.tue.nl* (*pub/security/satan.tar.Z*)
  - CERT Tools & Advisories. Disponible por FTP en *ftp.cert.org* (*pub/sert_advisories*)
  - Grupo de NEWS. Disponibles vía USENET News. Los grupos *comp.security.** .
  - Servidores WWW con información de seguridad:
    http://www.tis.com
    http://www.csl.sri.com
    http://mls.saic.com
    http://www.cs.purdue.edu/homes/spaf/coast.html

http://www.delmarva.com/raptor/raptor.html
http://www.digital.com/info/key-secure-index.html
http://www.spy.org
http://www.rsa.com

b) WWW (Gopher, wais)

- Configurar el servidor para que el servicio a las conexiones no se ejecute bajo el usuario root.
- Si se disponen servidores de uso exclusivamente interno, utilizar puertos de conexión distintos a los habituales.
- Mantener ciertas precauciones en la forma de trabajar de los clientes. No se debe aceptar ciegamente cualquier orden de un servidor. Se debe comprobar el comportamiento de los clientes mediante sus ficheros de configuración.
- Asegurarse mediante las protecciones del sistema de ficheros que el servidor no puede ofrecer más ficheros que los que se han preparado para ello.
- Evitar que el servidor comparta el árbol de directorios con FTP, sobre todo con los directorios de escritura pública, si los hay.
- No utilizar programas de interrogación a bases de datos o ficheros.
- Revisar periódicamente los ficheros de log.
- Mantenerse informado de las novedades sobre seguridad que afecten a nuestras versiones de clientes y servidores.
- Hacer que cada uno de los servicios implicados en nuestro servidor se ejecute en un entorno aislado, usando chroot.
- Si se desea ofrecer información resultante de realizar consultas a ficheros o bases de datos comprobar que realizan sólo la función que deben, que no son interrumpibles y que no tienen comportamientos anómalos ante la llegada de parámetros inesperados.
- Ofrecer el servicio mediante un sistema de cortafuegos.

2. TECNOLOGÍA. DESCRIPCIÓN DE LAS NORMAS *X.400* Y DE *INTERNET*.

2.1. CORREO ELECTRONICO - X.400

2.1.1. Descripción del correo electrónico X.400

Durante años, el correo fue la manera más popular de enviar mensajes entre personas. Con la llegada del teléfono, el correo fue perdiendo importancia como medio de comunicación interpersonal, ya que el teléfono permite establecer una comunicación casi instantánea entre los dos extremos, mientras que una carta requiere usualmente unos días.

Sin embargo, a pesar de la difusión que tiene el teléfono en la actualidad, el correo no ha desaparecido; éste tiene la ventaja de que no es preciso que ambas partes se encuentren disponibles simultáneamente. Una carta que llega, no precisa ser leída en ese mismo instante.

El correo electrónico ofrece ventajas de ambos medios, al hacer posible el envío de mensajes, como en el correo ordinario, y que éstos sean entregados en unos pocos segundos.

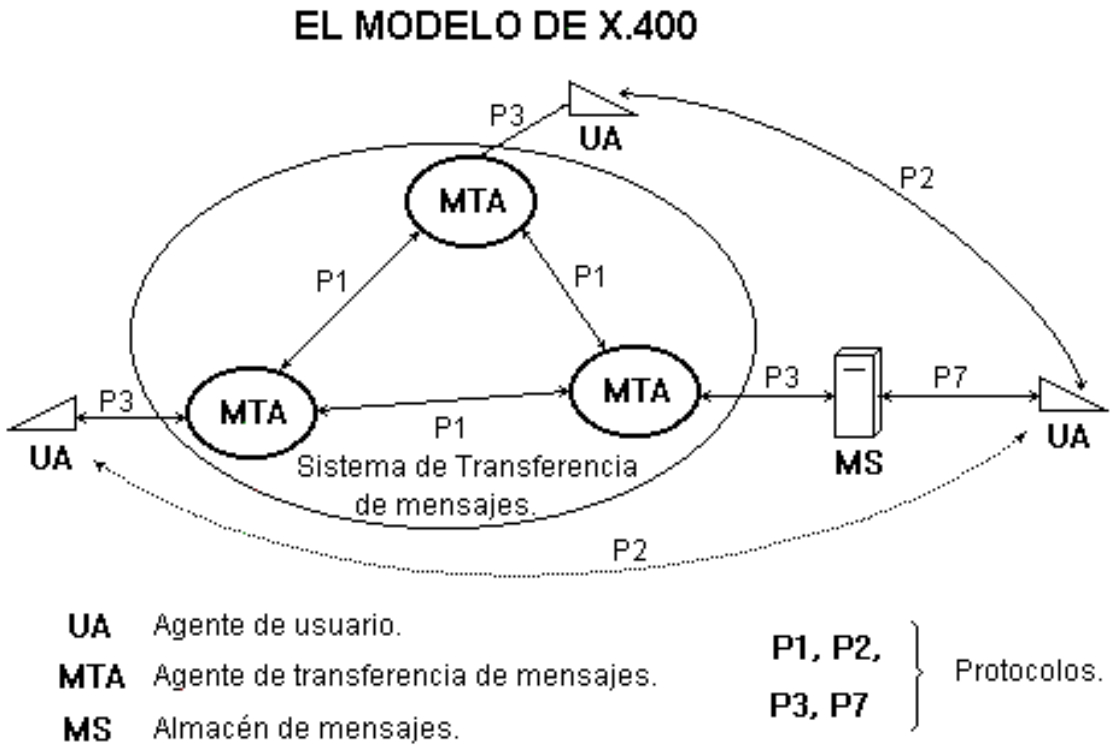
Los primeros sistemas de correo electrónico eran básicamente un sistema de transferencia de ficheros. Para enviar un mensaje, se escribía en un fichero, y se ponía la dirección del destinatario en la primera línea. Este sencillo sistema funcionaba, si bien enseguida se vió la necesidad de incluir facilidades adicionales como la siguientes:

- Posibilidad de transmitir mensajes a grupos de personas.
- Saber si el mensaje llegó o no a su destino, es decir acuse de recibo.
- Necesidad de estructura interna de los mensajes para que sea posible tratarlos de manera automatizada.
- En ausencia de un usuario, poder desviar su correo a otra persona.
- Posibilidad de transmitir mensajes compuestos por una mezcla de texto, dibujos, etc.

Para cubrir estas necesidades se fueron definiendo otros sistemas de correo electrónico más elaborados. Para evitar la aparición de múltiples sistemas incompatibles entre sí, el CCITT presentó en 1.984 la recomendación X.400, la cual sirvió de base para el Sistema de Intercambio de Textos Orientado a Mensajes (MOTIS) de la OSI. En 1.988, el CCITT modificó el X.400 para adaptarlo a MOTIS.

Esta norma ha conseguido un gran éxito en la actualidad debido a tres razones fundamentales:

i. En primer lugar, X.400 proporciona una normativa bastante completa, que hace posible transmitir texto simple, archivos binarios, de voz digitalizada, etc.
ii. En segundo lugar, especifica el modo de conectar equipos heterogéneos, posiblemente de diferentes fabricantes, e independientes entre sí.
iii. Por último, cuenta con el apoyo recibido por parte de empresas y administraciones públicas de todo el mundo.



La figura 1 muestra el esquema básico del sistema de mensajería X.400. Los componentes principales del sistema son los **agentes de usuario** (UA) y los **agentes de transferencia de mensajes** (MTA). Los usuarios interactúan con los agentes de usuario, donde pueden crear, enviar y recibir los mensajes. Los agentes de transferencia de mensajes se encargan de transportar los mensajes hasta el destinatario. Un tercer elemento son los **almacenes de mensajes** (MS), unos buzones donde dejar los mensajes cuando el agente de usuario no está conectado.

Aunque puede haber un agente de usuario y un agente de transferencia de mensajes en una misma máquina, se espera que estén en máquinas distintas. Los agentes de usuario podrían estar en ordenadores personales en el domicilio o en la oficina del usuario, mientras que los agentes de transferencia de mensajes se situarían en ordenadores principales en oficinas de correos, compañías de teléfonos o otras compañías privadas.

Al conjunto de los agentes de transferencia de mensajes se le llama **sistema de transferencia de mensajes** (MTS), que se divide en dominios de gestión, cada uno con uno o varios agentes de transferencia de mensajes, de modo que cada dominio tenga un administrador definido. Cuando el administrador es una compañía operadora o PTT recibe el nombre de *dominio gestionado por la administración* (ADMD), y cuando se gestiona por una compañía privada se le llama *dominio de gestión privada* (RTMD), aunque estos deben quedar bajo la responsabilidad de un ADMD.

X.400 también normaliza la forma en que los elementos del correo electrónico se comunican entre sí. Los agentes de usuario utilizan el protocolo P3 para recibir y entregar mensajes a los agentes de transferencia de mensajes. Los agentes de usuario se comunican con los almacenes de mensajes a través del protocolo de acceso a almacenes de mensajes, P7. El protocolo P1 normaliza la interacción entre agentes de transferencia de mensajes. La comunicación entre dos agentes de usuario está regulada por el protocolo P2, que es un protocolo "virtual", puesto que

dos agentes de usuario no pueden conectarse directamente.

2.1.2. Transferencia de mensajes en X.400

Los mensajes.

Al contrario que los primeros sistemas de correo electrónico, los mensajes de X.400 son estructurados. En particular, se puede distinguir entre el **sobre** y el **mensaje**. El sobre contiene el destinatario del mensaje, así como su dirección, prioridad y datos de seguridad. En la figura 2 se muestra la distinción entre el sobre y el mensaje. A su vez, en el mensaje se diferencian *cabecera* y *cuerpo*.

Nombre: Antonio Gómez. Direccion: C/Julián Camarillo, 8, M-4, P-3. Ciudad: Madrid. Pais: España. Codigo Postal: 28037. Prioridad: Urgente. Encriptacion: Ninguna.		SOBRE
Remite: Jimenez y Cia. Direccion: C/Mayor, 39. Poblacion: Almeria 04009. Fecha: 12-05-95. Asunto: Presentación de Nuevos Productos.	(Cabecera)	MENSAJE
Estimado Sr. Gómez, Tengo el honor de invitar a Ud. a la presentación de nuestros productos que tendrá lugar el próximo día 30 de .... Atentamente, Sr. Jimenez.	(Cuerpo)	

Figura 2. Distinción entre sobre y mensaje.

El protocolo P1 está relacionado con el *sobre* de los mensajes. La figura 3 muestra un resumen de los campos que puede llevar. Entre los campos más evidentes tenemos la dirección de correo electrónico de quien emite el mensaje, la dirección del destinatario y la dirección de un receptor alternativo, pues, si se desea. X.400 da la posibilidad de especificar la prioridad del mensaje, de solicitar confirmación de entrega, y de indicar una fecha en la cual el mensaje deja de ser válido.

Puesto que pueden existir terminales de distintos tipos, en ocasiones es preciso convertir el contenido de un formato a otro. En el sobre se indica el tipo de información que contiene mensaje (p.ej, un texto ASCII, un texto EBCDIC, un fichero binario, etc.). Al usuario se le da la posibilidad de controlar las conversiones, por ejemplo, solicitando un tipo de conversión determinado, o prohibiendo explícitamente que se hagan conversiones.

Dirección del remitente	Dirección de correo del emisor
Dirección del receptor	Dirección de correo del receptor
Receptor alternativo permitido	¿Está permitido entregarlo a otra persona?
Receptor alternativo	Receptor alternativo
Id. del mensaje	Identificativo del mensaje
Prioridad	Baja, normal, urgente
Solicitud de acuse de recibo	Tipo de notificación al emisor
Entrega diferida	Entregar a partir de este momento
Fecha límite de entrega	Plazo máximo para entregar
Solicitud de devolución	Devolver contenido si no se puede entregar
Tipo de información	Texto, fichero binario, facsímil, etc.
Conversión prohibida	No está permitido convertir el contenido
Conversión imprecisa prohibida	Convertir sólo si se puede hacer bien
Conversión explícita	Se indica qué conversión hacer
Identificación de cifrado	Indice en la tabla de claves de cifrado
Comprobación de integridad	Código de redundancia del contenido
Firma del remitente	Firma digital
Etiqueta de seguridad	Clasificado, confidencial, secreto...
Comprobación de entrega	Firma del receptor

Figura 3. Algunos de los campos del sobre.

Algunos otros campos están relacionados con la integridad y confidencialidad de los mensajes. Su finalidad es manejar el envío de mensajes cifrados, incluir firmas digitales del emisor o del receptor para un acuse de recibo, o incluir un códigos de redundancia para descubrir posibles alteraciones de los mensajes.

El agente de usuario.

El agente de usuario debe interactuar con el usuario, con los agentes de transferencia de mensajes y con los almacenes de mensajes. Así, en primer lugar, necesita una interfaz para el usuario. Un programa de correo electrónico suele presentar un menú o un interprete de comandos para ver un resumen de los mensajes que se han recibido, leer un mensaje completo, enviar un mensaje nuevo, contestar a uno que se ha recibido, eliminar mensajes o moverlos de un buzón a otro, etc.

La forma en que se comunican dos agentes de usuario viene dada por el protocolo P2, que en su mayor parte define los campos de cabecera de los mensajes.

La figura 4 muestra algunos de los campos que pueden formar parte de la cabecera de los mensajes. Entre estos tenemos el usuario que envía el mensaje, y quién le autoriza a ello; qué usuario o grupo de usuarios van a recibir el mensaje o copias de él; también hay posibilidad de indicar a quién enviar la respuesta y el plazo para hacerlo. Otros campos traen identificadores de este mensaje y de mensajes que guardan relación. En *asunto* se proporciona un pequeño resumen del contenido, mientras que en *importancia* y *sensibilidad* se indica la urgencia del mensaje y el deseo del emisor de no revelar su contenido.

Remitente Usuarios que autorizan	Nombre de quien expide el mensaje Quienes le autorizan
Receptores principales Receptores con copia Receptores con copia ocultos	A quien va dirigido el mensaje Quienes reciben copia Quienes reciben copia secretamente
Receptores de respuestas Plazo de respuesta	A quien enviar la respuesta Plazo de tiempo para responder
Id. del mensaje En respuesta a Mensajes que anula Mensajes relacionados	Identificador del mensaje A que mensaje se responde A que mensajes anula Mensajes que guardan relación con este
Asunto Importancia Sensibilidad	De que trata el mensaje Prioridad del mensaje Grado de confidencialidad
Válido hasta	Fecha de "caducidad"

Figura 4. Campos de cabecera del protocolo P2.

El agente de transferencia de mensajes.

El agente de transferencia de mensajes se encarga de hacer llegar el mensaje desde del usuario que lo envía hasta el receptor. Su forma de trabajo es mediante almacenamiento y reenvío. Cuando llega un mensaje al agente de transferencia de mensajes se comprueba su validez. Si contiene algún error sintáctico, se devuelve al usuario con una explicación. Si es correcto, se le asigna un identificador de mensaje y a partir de aquí, se procesa igual que un mensaje recibido de otro agente de transferencia de mensajes.

A continuación, se comprueba si el receptor es local. Si lo es, se puede entregar el mensaje o dejarlo en un buzón. Si es preciso, se puede emitir una confirmación de entrega al remitente. Entregar el mensaje a un receptor local puede complicarse si emisor y receptor tienen distintos tipos de aparatos terminales; si el receptor no puede aceptar directamente el tipo de mensaje, el agente de transferencia de mensajes puede intentar convertirlo a otro formato. Algunas conversiones no son posibles.

Primitiva del servicio de transferencia fiable	Descripción	Confirmar
RT-OPEN	Establece asociación	Sí
RT-CLOSE	Libera asociación	Sí
RT-U-ABORT	Aborto debido al usuario	No
RT-P-ABORT	Aborto debido a sistema	No
RT-TRANSFER	Transfiere un mensaje	Sí
RT-TURN-PLEASE	Solicitud del testigo	No
RT-TURN-GIVE	Entrega del testigo	No

Figura 5. Primitivas del servicio de transferencia fiable (RTS).

Si el receptor no es local, el agente de transferencia de mensajes selecciona a quién debe entregar el mensaje, y lo envía mediante el **servicio de transferencia fiable** (RTS) del protocolo P1. El servicio de transferencia fiable trata de evitar la pérdida de mensajes, aunque se produzcan caídas repetidas. Para ello, establece una asociación entre dos agentes de transferencia de mensajes y utiliza un protocolo de "parada y espera" sobre ésta; después de enviar cada mensaje, es preciso confirmarlo para enviar el siguiente.

La figura 5 muestra las primitivas del servicio de transferencia fiable. Las dos primeras (RT-OPEN y RT-CLOSE) permiten establecer y liberar una asociación entre dos agentes de transferencia de mensajes. Las dos siguientes (RT-U-ABORT y RT-P-ABORT) dan cuenta de caídas producidas por el usuario o externas. La primitiva RT-TRANSFER es la empleada para transferir los mensajes. Cuando se produce una caída en la comunicación, se utilizan las facilidades de la capa de sesión para recuperar el sistema sin perder datos. Las primitivas RT-TOKEN-PLEASE y RT-TOKEN-GIVE se utilizan para solicitar y conceder testigos.

2.1.3. Seguridad en correo electrónico X.400

La versión de correo electrónico X.400 de 1988 presenta una larga lista se servicios y mecanismos de seguridad, todos ellos opcionales:

- Confidencialidad del contenido
- Integridad del contenido, del flujo y de la secuencia del mensaje
- Autenticación
- No repudio de origen
- No repudio de destino
- Etiquetas de seguridad
- Prueba de entrega
- Prueba de envío

2.2.CORREO ELECTRONICO - INTERNET

2.2.1. Descripción del correo electrónico Internet

A finales de los años 60 se creó la red Arpanet gracias a un programa del Departamento de Defensa de Estados Unidos dedicado a estudiar las redes de ordenadores. A partir del trabajo de varias universidades y de algunas compañías privadas, en diciembre de 1.969 comenzó a funcionar una red experimental de cuatro nodos. Posteriormente se conectaron a ARPANET dos redes de satélites, y después las redes locales de universidades y contratistas del gobierno norteamericano, formando la red Internet. Actualmente esta red ha alcanzado una gran difusión, y están conectados a ella centenares de hosts de todo el mundo.

Entre los servicios que ofrece Internet se incluyen la transferencia de archivos, correo electrónico y conexión remota. Estos servicios están soportados por los protocolos FTP (protocolo de transferencia de ficheros), SMTP (protocolo simple de transferencia de mensajes) y TELNET (protocolo de conexión remota).

El **correo electrónico** se inició en Internet, y es una de sus aplicaciones más importantes; aproximadamente, el 60% del tráfico de Internet se debe al correo electrónico. Dos documentos

normalizan su funcionamiento: el **RFC-821** y el **RFC-822**. El documento RFC-821 trata sobre el protocolo SMTP que se encarga de la transferencia de mensajes de correo entre hosts. El formato de los mensajes de correo electrónico está recogido en el documento RFC-822, que ha ido incorporando nuevos elementos a lo largo del tiempo.

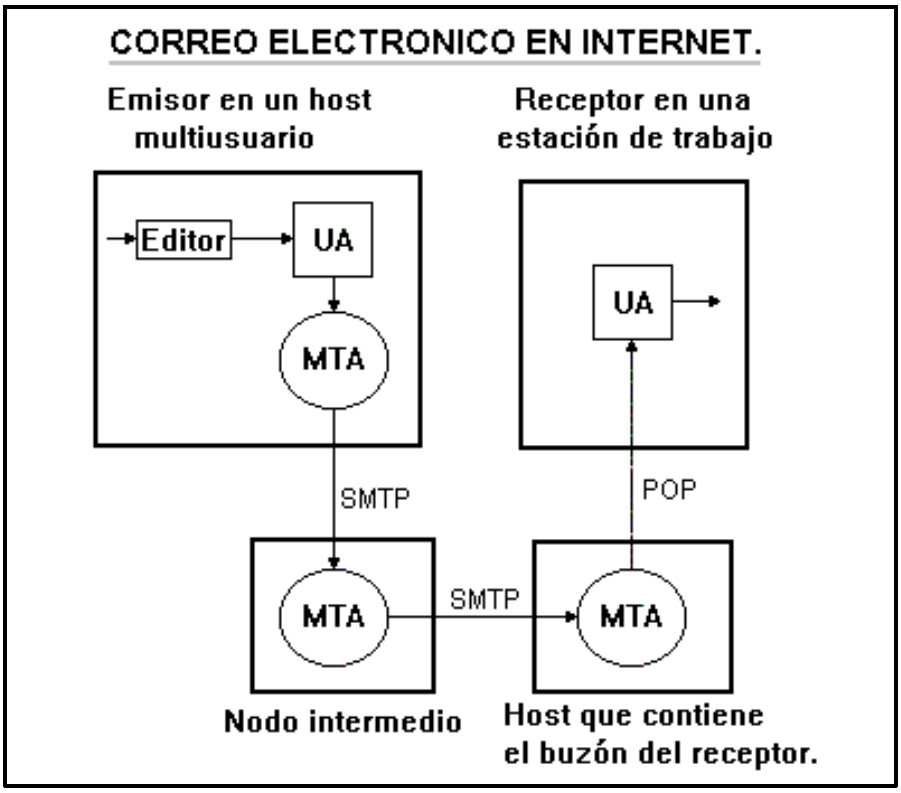


Figura 6. El sistema de correo electrónico de Internet.

En la figura 6 se muestra un *esquema del sistema de correo electrónico en Internet*. Los mensajes son texto ASCII, así que el usuario puede utilizar un editor de texto de propósito general para crear mensajes o bien otro editor orientado a correo electrónico. El host donde trabaja el usuario debe tener un programa que actúe de agente de usuario (UA), el cual trata las cabeceras de los mensajes, los analiza sintácticamente y los transmite al agente de transferencia de mensajes (MTA). Este último se encarga de encaminar los mensajes por la red hasta el host destinatario, y para ello utilizada el protocolo SMTP. Ya en el destino, el mensaje puede ser entregado al agente de usuario del receptor, o bien quedar almacenado en un buzón, donde más tarde, el usuario puede recuperarlo utilizando el protocolo de acceso a buzones (POP).

Los conceptos de "agente de usuario" y "agente de transferencia de mensajes" pertenecen a la terminología de X.400, pero se ajustan bien al modelo de Internet.

2.2.2. Transferencia de mensajes en Internet

El formato de los mensajes.

El correo electrónico definido en el RFC 822 únicamente permite la transferencia de texto ASCII, y aunque existen otras normas para manejar mensajes de otros tipos, no están tan extendidas. Un mensaje RFC 822 es un fichero ASCII con dos partes diferenciadas: la **cabecera** y el **cuerpo**. La

cabecera consta de varias líneas que empiezan por una palabra clave seguida de dos puntos y un valor.

Emisor (sender)	Dirección del emisor
Para (to)	Dirección receptor
Recibido de	De dónde procede el mensaje
Recibido por	Quién recibió el mensaje
Recibido vía	Medio físico por el que llegó
Recibido por medio de	Protocolo que se utilizó
De	Nombre del remitente
Contestar a	Dirección a quien hay que contestar
Con copias	Direcciones a las que enviar copias
Con copias ocultas	Direcciones a las que enviar copias ocultas
En respuesta a	Ident. del mensaje al que responde
Referencias	Otros mensajes relacionados
Asunto	De qué trata el mensaje
Palabras clave	Palabras destacadas del contenido
Fecha	Fecha de envío
Ident. del mensaje	Identificativo del mensaje
Comentarios	Los define el usuario
Cifrado	Indice en la tabla de claves cifradas

Figura 7. Campos de cabecera de RFC-822.

En la figura 7 se muestra un resumen de los posibles campos de cabecera. El primer grupo está relacionado con el *sobre*. Al contrario que en X.400, no se distingue entre sobre y mensaje; lo que constituye el sobre en X.400 se sitúa aquí en los campos de cabecera. Los campos Emisor (sender) y Para (To) son las direcciones del emisor y del receptor. Por ejemplo, un mensaje podría comenzar con las líneas:

to: juan@dep.ejemplo.com (comentarios)
sender: daniel@di.um.es (comentarios)

indicando que el destinatario del mensaje tiene la dirección de correo electrónico "juan@ejemplo.com". El texto entre paréntesis se interpreta como comentarios. A medida que un mensaje circula por la red, cada host por el que pasa le añade unas líneas en la cabecera que indican:

Recibido de = De quién ha recibido el mensaje.
Recibido por = Identificativo del host actual.
Recibido vía = Por qué medio físico llegó (red local, Internet...)
Recibido por medio de = Protocolo utilizado.
Fecha y hora en que se recibió.

Con esta información, es posible seguir el camino que ha recorrido el mensaje y controlar el funcionamiento de la red.

El segundo grupo de campos contiene el nombre del remitente y direcciones a las que enviar la contestación. El siguiente grupo está relacionado con el mensaje. Entre otros campos incluye el asunto del mensaje y las palabras clave del texto. En el último grupo se incluye el campo *cifrado* para especificar el tipo de encriptación que se está empleando. Puesto que solamente es posible cifrar el texto del mensaje, quedarían al descubierto el *asunto* y las *palabras clave*, que pueden dar una información significativa sobre el contenido.

```
  para: martinez@qf.ccs.es
emisor: daniel@di.um.es
   de: Daniel García García
asunto: Comentarios sobre los temas tratados en...
 fecha: 07/07/95
 X-Ref: xyz

 Estimado Sr. Martinez,
    en respuesta a la proposición de incrementar los
 recursos destinados a la investigación en los depar-
 tamentos de...
```

Figura 8. Ejemplo de un mensaje de correo electrónico.

La figura 8 muestra un ejemplo de un fichero de correo electrónico. La cabecera está formada por las seis primeras líneas, que contienen las direcciones de emisor y receptor, nombre del emisor, asunto, fecha y un comentario. Tras la cabecera viene el texto del mensaje. Conforme el mensaje se va desplazando por la red, se le irían añadiendo líneas a la cabecera con información sobre la ruta seguida.

El protocolo SMTP.

Para utilizar el protocolo SMTP el agente de transferencia de mensajes de un host inicia una conexión con otro host, que puede ser el destinatario final o una etapa intermedia. Al iniciar la conexión el host que inicia envía un comando MAIL que identifica al emisor, de modo que el destinatario sepa a quién enviar los mensaje de error. A continuación, se envía un comando RCTP para identificar al receptor del correo. El receptor puede aceptar o rechazar el comando. Si el comando es aceptado, el emisor lanza un comando DATA seguido el texto del mensaje. El mensaje consta de una serie de líneas ASCII y acaba con una línea que sólo contiene un punto (si el mensaje tiene alguna línea de estas características, el agente de transferencia de mensajes emplea caracteres de relleno para no confundirse). Existen otros comandos para verificar direcciones, expandir listas de distribución, enviar notificaciones a un terminal, acabar una conexión, etc.

Solamente los agentes de usuario analizan los mensajes en busca de las direcciones de origen y destino. El protocolo SMTP transmite las direcciones por separado del mensaje.

Direccionamiento en Internet.

El direccionamiento en Internet utiliza el formato nombre@dominio. El dominio identifica al host donde entregar el correo, mientras que el nombre especifica el usuario dentro de dicho host. Los dominios pueden dividirse en subdominios, separados por puntos.

```
juan @ dep . ejemplo . com
---------  ---------------------------
 nombre        dominio
```

Donde:

dep	Subdominio (departamento)
ejemplo	Subdominio (empresa)
com	Dominio de mayor nivel

Los dominios de mayor nivel constan de una abreviatura del país de dos o tres caracteres, excepto para Estados Unidos, donde los dominios de mayor nivel posibles incluyen EDU (instituciones educativas), COM (compañías), GOV (gobierno), MIL (instituciones militares) y ORG (resto de organizaciones).

El nombre del destinatario suele ser el *login* en la máquina receptora del destinatario, aunque hay otras posibilidades. Puede tratarse de un **alias** o de una **lista de distribución**. Un alias es simplemente otro nombre con el que se puede hacer referencia al destinatario. Una lista de distribución contiene direcciones de uno o más usuarios (normalmente, más de uno). Cuando un mensaje va dirigido a una de estas listas, se envía una copia de dicho mensaje a cada una de las direcciones incluidas en ella. Puede suceder que alguna de estas direcciones se refiera a otra lista de distribución.

Aunque a una dirección Internet se le puede dar información sobre el enrutamiento, se aconseja no hacerlo. Muchos sistemas lo soportan por compatibilidad por sistemas antiguos. Una dirección como:

juan@dep.ejemplo.com@host3@host2@host1

indicaría enviar un mensaje a juan@dep.ejemplo.com pasando por el host1, host2 y host3.

2.2.3. Servicios Internet

Herramientas de búsqueda y visualización de la información. World Wide Web

El World Wide Web, también conocido como WWW, W3, o simplemente Web es de los intentos más recientes y a la vez más poderosos de sistematizar y simplificar el acceso a la información en Internet. Los servidores WWW distribuidos por todo el mundo constituyen un entramado mundial. Para acceder a uno de estos servidores es necesario disponer de un programa especial para conectarse con ellos. Estos programas se llaman en la jerga Internet *Browsers* (hojeadores), manejan información hipertexto o hipermedia en la que la navegación se produce mediante hiperenlaces.

El WWW incluye servicios de búsqueda de información como los que proporcionaban GOPHER o WAIS. En él un ordenador cliente se conecta con un servidor al cual envía una referencia a una información; el servidor contestará con un fichero o con una referencia a uno o más servidores donde se puede encontrar la información solicitada.

Con este servicio el usuario no tiene que preocuparse por decodificar la información codificada en los ficheros que recibe, pues WWW comprueba el formato de la información y emplea el programa adecuado para presentarla. WWW utiliza fundamentalmente el protocolo HTTP (HyperText Transfer Protocol). El protocolo HTTP permite presentar 'formularios' que presentan información y permiten la introducción de datos, razón por la que se ha configurado como un medio adecuado para la realización de transacciones comerciales y de otros tipos. Por este motivo se está experimentando una versión segura de HTTP llamada SHTTP (Secure HTTP) que

proporciona confidencialidad en las transacciones, integridad, autenticación y no repudio de origen.

Servicios de noticias o grupos de discusión (NEWS).

Este servicio simula tablones de anuncios sobre diferentes temas donde los usuarios aportan preguntas y respuestas. Los grupos de noticias pueden ser libres o moderados. En un grupo moderado el moderador lee las noticias y decide si publicarlas o no. Los grupos suelen mantener permantentemente listas de 'preguntas frecuentes', con los temas ya tratados en el grupo. Los grupos reecomiendan que se consulten antes de enviar nuevas preguntas.

Transferencia de ficheros (FTP)

El protocolo de transferencia de ficheros FTP (File Transfer Protocol) se utiliza para transferir ficheros de una máquina a otra, teniendo en cuenta las diferencias entre dichas máquinas que pueden obligar a realizar ciertas conversiones durante la transferencia.

El protocolo FTP distingue cuatro tipos de archivos : archivos de imagen, ascii, ebcdic y de octetos lógicos. También reconoce ciertos tipos de estructura de ficheros como no estructurados, de secuencia de registros y de acceso aleatorio.

La transferencia de ficheros se puede hacer en tres modos diferentes que son modo de flujo, para ficheros ordinarios, modo bloque para ficheros estructurados en registros y modo bloque para los ficheros de acceso aleatorio.

FTP soporta gran variedad de comandos,los cuales se ocupan del envío y recepción de ficheros, del manejo de directorios o del establecimiento de parámetros y modos de transferencia.

Una variante es el FTP anónimo, mediante el cual un usuario que no necesita identificarse se conecta para capturar ficheros públicos.

Conexión remota o servicio de terminal virtual (TELNET)

Con el servicio de terminal virtual TELNET es posible conectarse a una máquina distante a través de la red. Es posible conectarse en modo terminal a procesos muy diferentes, como consultas a una base de documentación o a un intérprete de comandos del sistema operativo.

Una sesión de TELNET suele comenzar con un proceso de login para que el usuario se identifique e inicialice la sesión. En este servicio puede ser peligroso que las contraseñas viajen en claro por la red. También hay que cuidar las operaciones transmitidas al usuario remoto.

Si los ordenadores confían mutuamente pueden utilizar un protocolo TELNET seguro que permite cifrar la sesión completa, protegiendo la contraseña y los datos transmitidos.

2.2.4. Seguridad en Internet

Los servicios de Internet que más atención prestan a la seguridad son el correo electrónico y el

World Wide Web. Para los servicios que no tienen características de seguridad específicas la protección se basa en los permisos de lectura y escritura del sistema operativo a las tareas que los implementan.

Uno de los aspectos relativos a la seguridad en INTERNET que más auge está tomando es la relacionada con transacciones comerciales y cifrado de datos. Hasta ahora, el envío de números de tarjeta de crédito, palabras clave e incluso mensajes de correo electrónico, estaban sujetos a la potencial intromisión o uso ilícito de ellos. Este aspecto, clave en el comercio electrónio, está siendo estudiado por todos los fabricantes de software para INTERNET, así como bancos, instituciones financieras y proveedores de tarjetas de crédito como Visa o American Express. El resultado de todos estos esfuerzos se está viendo en la mayoría de los productos que están apareciendo en el mercado como los servidores y visualizadores WWW seguros de NETSCAPE INC. o los protocolos S-HTTP (Secure HTTP) que están siendo introducidos en INTERNET. Así mismo desde los comités de estándares, se ha tomado conciencia de la falta de seguridad en INTERNET y sin ir más lejos, el protocolo que sirve de sustento a INTERNET, TCP/IP está siendo objeto de una revisión (V.6) que tiene como una de sus prioridades acabar con la vulnerabilidad que existe hasta el momento.

a) Seguridad en correo electrónico

El correo electrónico original de Internet normalizado por los documentos RFC-821 y RFC-822 no incorpora servicios de seguridad, pero hay dos extensiones que sí los tienen, PEM y PGP que proporcionan confidencialidad, integridad del mensaje y autenticación del emisor. PEM también da soporte para no repudio de origen.

La principal diferencia está en que PEM necesita entidades centralizadas para los certificados de claves públicas, mientras que mediante PGP los usuarios intercambian certificados unos con otros sin necesidad de utilizar entidades de certificación.

De ellos se dan más detalles en los capítulos 3 y 4.

b) Seguridad en los servicios Internet

- El *World Wide Web* es un sistema hipermedia distribuido que ha adquirido una gran aceptación en el mundo Internet. Aunque las herramientas de consulta del WWW soportan diversos protocolos preexistentes el *HyperText Transfer Protocol* (HTTP) es el protocolo nativo y principal utilizado entre clientes y servidores WWW. Su facilidad de uso enseguida despertó el interés de su empleo para aplicaciones cliente-servidor. Muchas aplicaciones requieren la autenticación del cliente y el servidor y el intercambio de información confidencial. La especificación original del HTTP proporcionaba un soporte muy modesto para el uso de mecanismos de criptografía apropiados para transacciones comerciales. Así los mecanismos originales de autorización de HTTP requieren que el cliente intente un acceso que a continuación es denegado antes de utilizar el mecanismo de seguridad.

- El cortafuegos o *firewall* es un elemento clave de la seguridad en Internet, pero se trata de un mencanismo especialmente orientado a proporcionar el servicio de control de acceso.

- Es preciso complementar el mecanismo de cortafuegos con otros que permitan proporcionar los demás servicios de seguridad. En el caso de Internet esto se debe conseguir mediante el uso de protocolos adicionales. Estos protocolos adicionales se encuentran en estado de evolución si bien cuentan con implementaciones en el mercado.

- Se pueden citar aquí el *Secure Sockets Layer* (SSL), que se encuentra por debajo de los protocolos http, Telnet y Ftp pero por encima del TCP/IP y permite proporcionar los servicios de confidencialidad, integridad y autenticación. Otro protocolo de interés es el *Secure Hypertext Transfer Protocol* que es una versión mejorada con aspectos de seguridad del protocolo base de *World Wide Web*, el http, y está destinado a proporcionar los servicios de confidencialidad, integridad, autenticación y no repudio de origen a transacciones comerciales de propósito general.

3. ESTÁNDARES Y REFERENCIALES PARA SEGURIDAD EN CORREO ELECTRÓNICO X.400 E INTERNET

3.1. CORREO ELECTRÓNICO X.400

3.1.1. El Manual EPHOS, qué es.

El proyecto *EPHOS* arranca de la Decisión del consejo (87/95/CEE) de 22 de diciembre de 1986, relativa a la normalización en el campo de las tecnologías de la información y de las telecomunicaciones, (DOCE 7.2.87) que impone a todos los órganos contratantes a nivel comunitario y dentro de los estados miembros de la UE, la obligación de hacer referencia a las normas y normas previas europeas, a las normas internacionales o a los proyectos de normas internacionales, en todo lo relativo a requisitos de interoperabilidad de los sistemas e intercambio de información y de datos.

El programa *EPHOS* (Manual Europeo para las Compras Públicas de Sistemas Abiertos) está dedicado a la aplicación de las normas internacionales y europeas. Esta inciativa constituye uno de los vectores de integración más importantes del mundo en el campo de las Tecnologías de la Información y las Comunicaciones (TIC). Moviliza el considerable peso de los planificadores y compradores de las administraciones públicas, cuya influencia en la creación de una demanda de sistemas abiertos, que puedan intercomunicarse y que estén basados en especificaciones técnicas normalizadas, está dejándose sentir en el mercado de las TIC.

Aunque se denomine *Manual*, los textos de *EPHOS* constituyen un documento general, fruto de una inversión sustancial de recursos financieros y humanos. Es un vademécum técnico que reune las experiencias más avanzadas de algunos de los profesionales más prestigiosos de las TIC en Europa, y que, por consiguiente, constituye una herramienta indispensable para la armonización de los requisitos ténicos de las administraciones públicas en el campo de las TIC. Teniendo en cuenta que las compras públicas de bienes TIC pueden representar hasta un 15% del total de las compras públicas de la UE, es clara la influencia que *EPHOS* puede llegar a tener. *EPHOS* viene a reforzar el peso del usuario final, lo que tendrá repercusiones inmediatas en el rumbo del mercado mundial de las TIC. Con el tiempo, es probable que se convierta en la herramienta que, aceptada por todos, se incorpore a las orientaciones nacionales relativas a la compra de sistemas abiertos por el sector público de la UE. Se espera asimismo que su influencia se extienda rápidamente a los sectores industrial y comercial de la economía.

EPHOS suministra un conjunto de guías sobre el uso de estándares de TIC para compras con el propósito de uniformar, definir y seleccionar perfiles para todas las compras públicas de TIC en Europa con vistas a soportar en mercado único. Para ello EPHOS da guías sobre el uso de los perfiles y estándares de OSI, suministra apoyo para reducir la complejidad de elegir el estándar correcto o el perfil de una aplicación particular y suministra una fraseología precisa para usar en los pliegos de prescripciones técnicas.

EPHOS está estructurado en torno a los siguientes módulos temáticos:

- Servicios de directorio
- Terminal Virtual
- Servicios de Tratamiento de Mensajes (MHS)
- Transferencia, Acceso y Gestión de Ficheros (FTAM)
- Gestión de redes OSI.
- Intercambio Electrónico de Datos (EDI)

- Formatos de documentos
- Repertorio de caracteres
- Redes de Área Local
- Cableado
- Interconexión de Redes de Área Local (LAN) con Redes de Área Extensa (WAN)
- Sistemas Operativos
- Consulta de Bases de Datos
- Redes de Área Metropolitana (MAN)
- *Seguridad*
- Proceso transaccional
- Extensión de la gestión de redes OSI.

3.1.2. EPHOS 2 bis Topic U: Security Service. Qué es y para qué sirve.

El módulo *EPHOS 2 bis Topic U: Security Service* proporciona un conjunto de recomendaciones para la adquisición de servicios de seguridad. Estas recomendaciones constituyen un soporte adicional a otras posibles recomendaciones de compras recogidas en otros módulos del Manual EPHOS que en nuestro caso serían las recomendaciones incluidas en los módulos *Servicios de Tratamiento de Mensajes (MHS)* e *Intercambio Electrónico de Datos (EDI)*.

Este módulo EPHOS se centra en proporcionar asistencia para la dotación de servicios de seguridad que hagan frente a las posibles amenazas externas que puedan resultar de la existencia de servicios de comunicaciones externos.

Es decir, que EPHOS asume, por un lado, la existencia de un entorno local de seguridad, y, por otro, asume la existencia de servicios externos de comunicaciones cláramente diferenciados del entorno local de seguridad, de forma tal, que los servicios de seguridad recogidos van dirigidos a repeler las amenazas externas.

Una vez acotado el ámbito de seguridad al que se dirige este módulo del EPHOS centraremos nuestro foco de interés en el correo o mensajería electrónica en su más amplio sentido, que podrá abarcar así, tanto mensajería interpersonal, como mensajería estructurada EDI. Queda por tanto fuera del ámbito de nuestro interés la problemática de seguridad asociada a las comunicaciones externas vía X.25 o vía red telefónica conmutada.

En el ámbito de la mensajería estructurada EDI vamos a dedicar especial atención a las normas EDIFACT, que según las define la Comisión Económica para Europa de las Naciones Unidas (CEPE), son las reglas de las Naciones Unidas para el intercambio electrónico de datos en la administración, el comercio y el transporte; constan de una serie de normas, directorios y orientaciones aceptados internacionalmente para el intercambio electrónico de datos estructurados y, en particular, para el intercambio relacionado con el comercio de bienes y servicios entre sistemas de información independientes e informatizados.

Para la definición e identificación de amenazas y servicios de seguridad, EPHOS se basa fundamentalmente en la norma ISO-7498-2 (*Information Processing Systems. Open Systems Interconnection. Basic Reference Model. Part 2: Security Architecture*) que constituye el punto de referencia en el que se apoya EPHOS para:

- Describir los servicios de seguridad
- Referenciar las técnicas y mecanismos de seguridad que se pueden usar para implementar

los servicios de seguridad
- Situar los servicios de seguridad en determinadas capas del modelo OSI.

Otras fuentes claves de referencia para la seguridad como el' Manual de Criterios de evaluación de la seguridad de la tecnología de la información ITSEC (*Information Technology Security Evaluation Criteria*)' también se apoyan en la arquitectura de seguridad OSI definida en la norma ISO-7498-2 cuando recomienda que las funciones -servicios en EPHOS- destinadas a garantizar la seguridad de los datos durante la transmisión se organicen fundamentalmente conforme a los siguientes epígrafes:

- Confidencialidad de los datos
- Integridad de los datos
- Autenticación
- No repudio
- Control de acceso

Determinadas funciones o servicios podrán satisfacer requisitos relacionados tanto con la seguridad informática como con las comunicaciones. El correo electrónico requiere que se garantice la seguridad de los datos durante su transmisión por los canales de comunicación que es lo que se suele denominar como seguridad de las comunicaciones por contraposición a la seguridad informática. Otro aspecto aparte es el relacionado con la seguridad de la información intercambiada mientras esté almacenada en soportes informáticos, como por ejemplo un disco duro de un servidor de correo; este sería un caso de seguridad informática.

Estructura y contenidos del módulo EPHOS 2 bis Topic U: Security Service.
La primera parte del módulo se encuentra estructurada en dos secciones. La sección primera proporciona una introducción a los servicios de seguridad, con indicaciones de cuándo usar servicios de seguridad, cómo establecer los requisitos de seguridad y, finalmente, cómo escoger los servicios de seguridad adecuados. Asimismo se proporciona información para aplicar los servicios de seguridad en conjunción con otros servicios de comunicaciones o de aplicaciones. La sección segunda proporciona una guía para la aplicación de los servicios de seguridad a las comunicaciones OSI, al MHS y al EDI. El soporte para la adquisición de los servicios se proporciona mediante la selección de perfiles y de opciones de seguridad para cada uno de los tres escenarios identificados, junto con sentencias adecuadas para la adquisición de los servicios. También incluye recomendaciones sobre aspectos generales de seguridad.

La segunda parte del módulo incluye explicaciones y detalles técnicos más en profundidad, relacionados con las opciones especificadas en la parte primera y, a su vez, se encuentra estructurada en torno a tres secciones. La primera sección proporciona una explicación sobre el análisis de riesgos y sobre las amenazas más habituales en un escenario comercial; la segunda proporciona información general sobre seguridad; y la tercera incluye información adicional sobre seguridad de intercambio de mensajes y EDI.

3.1.3. Cómo aplicar EPHOS a la seguridad del correo electrónico.

EPHOS proporciona un conjunto de 'sentencias de definición de perfiles y opciones por defecto', que se denominan PODS (*Profile and Options Definition Statements*) e identifican perfiles y opciones que contrarrestan aquellas amenazas y vulnerabilidades más comunes. Estas sentencias se deben escoger de forma que estén lo más relacionadas posible con el servicio a adquirir. En nuestro caso interesan las que se refieren a los siguientes servicios:

- Sistemas de mensajería de propósito general basados en X.400 (*MHS: Message Handling System*)
- Sistemas de mensajería X.400 utilizados para intercambio de mensajes EDI.

Por tanto, EPHOS proporciona una guía para la selección de perfiles y opciones de seguridad para los sistemas anteriormente citados, así como las sentencias de adquisición junto con referencias a aspectos genéricos de seguridad.

Cuando no se precisa atender a requisitos específicos de seguridad se puede recurrir directamente a los mencionados perfiles y opciones de seguridad. Si se precisa atender a requisitos particulares de seguridad se pueden seguir los árboles de decisión que incluye el manual para ir seleccionando las claúsulas de seguridad necesarias para la adquisición de los servicios.

Finalmente hay que señalar que la selección de los mecanismos de seguridad no se produce aisladamente, sino que EPHOS la integra en la política de seguridad de la organización, que, entre otros aspectos, implica, como veremos a continuación, la identificación de requerimientos de seguridad que hay que satisfacer, mediante un análisis de riesgos riguroso que servirá de punto de partida de todo el proceso de implantación de la seguridad.

Política de seguridad de la organización y correo electrónico

La seguridad en la mensajería electrónica se encuentra imbricada en las políticas de seguridad de la organización, de operación general y de interconexión entre entornos informáticos, entendiendo que no todos los entornos necesitan protección para todas las vulnerabilidades. Acerca de políticas de seguridad se habla en el capítulo 5 de este documento.

Análisis de riesgos: Determinación de requerimientos de seguridad específicos para correo electrónico.

EPHOS recomienda realizar siempre como primer paso un análisis de riesgos que permita identificar los requerimientos de seguridad y, en consecuencia, los servicios de seguridad requeridos. Una vez identificados dichos servicios de seguridad, *EPHOS* proporciona el soporte adecuado para la identificación y selección de las claúsulas de compra.

El análisis de riesgos es una actividad esencial que implica la evaluación de las actividades de la organización y la determinación de los requerimientos de seguridad en base al análisis de activos, amenazas, vulnerabilidades, riesgos e impactos. La identificación de los requerimientos de seguridad permitirá definir los servicios y las medidas de seguridad que se deben implementar para proteger un determinado entorno de la organización.

Los requerimientos de seguridad se deben identificar teniendo en cuenta los riesgos, así como otros posibles aspectos del contexto de la organización, y, en cualquier caso, deben estar ubicados en el marco de la política general de seguridad de la organización.

Los aspectos que hay que considerar para identificar los requerimientos de seguridad son los siguientes:

- Análisis de riesgos para identificar amenzas y consiguientemente los servicios de seguridad requeridos.
- Uso de otras medidas de salvaguardia.
- Aspectos legales y normativos nacionales y del ámbito de la Unión Europea, en

relación a la protección de datos de carácter personal, y en relación a posibles restricciones en el uso de técnicas de cifrado.
- Posibles aspectos contractuales, que se puedan derivar de un acuerdo para intercambio de datos via EDI por ejemplo.
- Cualquier política de seguridad que pueda existir en la organización.
- Acuerdos de seguridad con otras partes, con cuyos sistemas pueda interactuar el sistema de la organización.

Estos requisitos de seguridad constituyen el punto de partida para la determinación de los servicios de seguridad -salvaguardas- que les den satisfacción.

Como dice el manual ITSEM (*Information Technology Security Evaluation Manual*):
'Se seleccionará un conjunto de salvaguardias para reducir el riesgo. Estas salvaguardias podrán ser de diversa índole, como físicas, organizativas o técnicas. Las salvaguardias técnicas son aquellas destinadas a reforzar los mecanismos y funciones de seguridad del sistema.
El principal objetivo de seguridad de un sistema informático consiste en reducir los riesgos asociados hasta un nivel aceptable por la organización. La confianza que se puede depositar en la seguridad de un sistema se denomina aseguramiento. Cuanto mayor sea el aseguramiento, mayor será la confianza de que el sistema proteja sus activos contra amenazas con un nivel aceptable de riesgo residual.'

3.1.4. Identificación y selección de servicios de seguridad para correo electrónico.

EPHOS proporciona asistencia para la adquisición de servicios de seguridad mediante claúsulas que proporcionan todos los servicios de seguridad requeridos. Un conjunto de árboles de decisión incluidos en el manual guían al comprador en la tarea de seleccionar las claúsulas de compra de los servicios de seguridad, en nuestro caso para mensajería interpersonal y para mensajería estructurada EDI. El comprador, una vez identificados los servicios de seguridad necesarios, seleccionará aquella claúsula de compra que proporcione al menos todos los servicios de seguridad requeridos.

Se puede conseguir un cierto grado de simplificación pues la implementación de ciertos mecanismos de seguridad proporcionará automáticamente más de un servicio de seguridad, como veremos más adelante.

EPHOS considera a los servicios de seguridad como servicios adjuntos a otros servicios de aplicación o de comunicaciones, destinados a proteger a los activos de posibles amenazas potenciales. *Los servicios de seguridad son proporcionados por servicios de aplicación o de comunicaciones mediante el uso de mecanismos o técnicas de seguridad aplicadas a los activos soportados por dichos servicios.* Como regla general, los servicios de seguridad deben estar respaldados por otras medidas. Así, por ejemplo, el uso de claves de acceso debe estar respaldado por controles de procedimiento.

Finalmente, EPHOS recomienda que, para minimizar los costes de implementación de los servicios de seguridad EDI y MHS, como norma general, se deben utilizar para ambos los mismos algoritmos de criptografiado, mecanismos de gestión de claves, etc.

Seguridad MHS y seguridad EDI

La decisión de usar *seguridad EDI/EDIFACT o seguridad MHS* depende de cuál se considere que sea la protección más adecuada para el sistema en cuestión. Como regla general el uso de ambas opciones proporciona la mejor cobertura de defensa contra las amenazas que se producen en un

entorno comercial.

Los requisitos que debe cumplir un sistema EDI se derivan normalmente de la existencia de un determinado acuerdo entre las partes en cuestión, que entre otros puntos definirá cuáles son los aspectos de seguridad necesarios, así como las circunstacias bajo las que se utilizan dichos aspectos. Un aspecto ténico de EDIFACT a tener en cuenta es que, en su ámbito, los servicios de seguridad se orientan a mensajes EDI individuales dentro de un intercambio. Es decir, que se seleccionan servicios de seguridad EDIFACT para responder a las necesidades genéricas de seguridad cuando se trata de proteger mensajes EDI individuales. Estos servicios pueden ser adicionales a otros posibles que sean necesarios para soportar el intercambio de mensajes EDI por otros medios que no sean MHS.

Los perfiles por defecto soportan el marco de seguridad UN/ECE EDIFACT y las guías de implementación UN/ECE.

A continuación se analizan las recomendaciones de EPHOSacerca de los servicios de seguridad para el Sistema de Tratamiento de Mensajes (MHS) que da soporte a la mensajería interpersonal y para el Intercambio Electrónico de Datos (EDI) que da soporte a la mensajería estructurada.

a) Servicios de Seguridad para el Sistema de Tratamiento de Mensajes (MHS)

Un sistema de mensajería proporciona al usuario los medios para transferir pequeñas cantidades de información, mensajes a uno o más destinatarios en ubicaciones locales o remotas. Los destinatarios no tienen necesidad de estar conectados a la red al mismo tiempo que se envía el mensaje. El remitente puede estar conectado directamente o no al receptor. En el segundo caso el sistema utiliza técnicas de almacenamiento y reenvío para hacer llegar el mensaje.

Un sistema de mensajería puede incluir las siguientes funciones:

- Preparación del mensaje
- Recepción y visualización del mensaje
- Envío del mensaje a uno o más destinatarios
- Gestión del sistema de mensajes
- Administración de usuarios del sistema de mensajería
- *Aspectos de seguridad*
- Archivo, manipulación y recuperación de mensajes
- Acceso a información de direccionamiento

El sistema de mensajería, en adelante MHS, se encuentra definido formalmente en un conjunto de estándares OSI. MHS no estandariza todos los aspectos de un sistema de mensajería, sino que se dirige principalmente a asegurar la interoperabilidad entre sus diferentes partes, que pueden estar localizadas en sistemas informáticos distintos.

El mensaje, como se ha visto anteriormente, se compone de sobre y contenido. La función principal de la información asociada al sobre es asegurar que el mensaje se entrega a los destinatarios correctos, y para ello contendrá una o más direcciones. También identifica la forma del contenido para permitir su adecuado tratamiento por el destinatario.

EL MHS se puede utilizar para diferentes propósitos. Hasta la fecha se ha estandarizado un contenido de mensaje para correo, que se denomina mensaje interpersonal (IPM), y otro contenido para EDI

(EDIM). El usuario final puede ser una persona o bien una aplicación. En consecuencia se han estandarizado dos formas diferentes de intercambio de información asociadas a los dos tipos de contenidos identificados anteriormente, mensajería interpersonal y mensajería EDI.

Los estándares MHS pueden proporcionar varios servicios de seguridad que en su mayor parte se pueden aplicar a todos los tipos de información enviada por MHS. Los servicios de MHS pueden proteger , además de mensajes de correo electrónico, tanto el mensaje EDI estructurado, como también información adicional, como, por ejemplo, un gráfico. Obviamente cuando se utiliza el MHS para soportar mensajería EDI, MHS debe cumplir además los requisitos que se derivan del acuerdo de intercambio entre las partes.

En EPHOS el comprador selecciona las claúsulas comparando los servicios genéricos de seguridad requeridos, con aquellos que proporciona la claúsula de compra.

EPHOS distingue los siguientes servicios de seguridad :

- *Servicios de seguridad comunes*.
- *Servicios de seguridad que son dependientes del contenido*; así contiene recomendaciones para los mensajes EDI de tipo de contenido 35 de EDIMS (Mensajes EDI X.435) y tipo 2 (o 22) para mensajería interpersonal IPMS (Intercambio de mensajes X.420).

Los servicios de seguridad comunes de mensajería se pueden complementar con *servicios de seguridad específicos dependientes del contenido* y según una dinámica de seguridad extremo a extremo. Esto se debe a que mientras que algunos servicios de seguridad de MHS sólo tienen sentido en una dinámica extremo a extremo (Agente de Usuario a Agente de Usuario), otros tienen sentido en Agentes de Transferencia de Mensajes (MTS) o en Almacenes de Mensajes (MS).

Servicios de seguridad dependientes del contenido

El Agente de Usuario (UA) remitente crea el sobre seguro y el receptor valida la seguridad del sobre sellado. Éste además envía los elementos validados al remitente en un nuevo mensaje. Este segundo mensaje se llama notificación y se envía también en un sobre sellado. El remitente valida los aspectos de seguridad dentro de este segundo mensaje.

De esta manera se pueden proporcionar los siguientes servicios de seguridad:

- *Confidencialidad*. Garantiza que la información sólo es accesible a la entidad autorizada.
- *Integridad de contenidos*. Esto asegura que el contenido del mensaje no ha cambiado.
- *Autenticación de origen de mensaje*. Esto asegura quién fue el originador del mensaje.
- *Autenticación de recpeción*. Asegura quién fue el receptor del mensaje.
- *No repudio de origen y destino*. Asegura que tanto el remitente como el receptor no pueden denegar el haber generado y recibido el mensaje y su contenido.
- *No repudio del contenido del mensaje*. Mientras ambas partes mantengan los atributos del sobre sellado, se asegura que tanto el remitente como el receptor no pueden denegar el contenido del mensaje intercambiado.

Servicios comunes de de seguridad

El Agente de Usuario crea un sobre seguro, denominado sobre sellado. El sobre sellado protegerá cualquier información que contenga en su interior. Entonces el UA envía el sobre sellado al sistema de transferencia de mensajes (MTS), que entregará el sobre al destinatario especificado en el mismo.

Finalmente el destinatario valida los aspectos de seguridad en el sobre seguro.

De esta forma los aspectos de seguridad que se pueden proporcionar son los siguientes:
- *Integridad de contenidos*. Esto asegura que el contenido del mensaje no ha sido cambiado.
- *Autenticación de origen de mensaje*. Esto asegura quién fue el originador del mensaje.

Aspectos de seguridad opcionales son los siguientes:
- *No repudio de origen*. Esto asegura que el originador del mensaje no puede denegar ni el haber originado dicho mensaje ni su contenido.

Cuando se requiere alguno de los servicios de seguridad MHS dependientes del contenido, la implementación correspondiente de MHS soportará todos los servicios de seguridad comunes de la mensajería.

El análisis de riesgos o las políticas de seguridad pueden identificar requisitos específicos de seguridad que protejan los diversos tipos de información enviados por el MHS:

a) Autenticación de origen y servicios de seguridad de integridad.
b) Se da lo anterior y además se requieren controles especiales.
c) Se dan los anteriores y además se requiere que el MTS proporcione no repudio controlando las firmas digitales.
d) Se dan los anteriores y además se requieren servicios de confidencialidad extremo a extremo.

Seguridad en los límites del MHS

Además del sobre sellado, se utilizan *etiquetas* que se asocian a cada mensaje y que incluyen un identificativo de política de seguridad que se comprobará en los límites para verificar que el entorno MHS receptor puede soportar la política de seguridad, y, por tanto, manejar correctamente el mensaje. Cuando el control se realiza en los límites de los dominios de seguridad, se denomina *security-context*. *Security-context* es un conjunto de etiquetas que se generan para cada asociación segura basada en las etiquetas que los objetos MHS que se conectan han registrado como capacidades del otro objeto. De esta forma los mensajes sólo se transmiten, entregan o recuperan si el agente de transferencia de mensajes (MTA), MS o UA 'puede manipular' el mensaje.

Los aspectos de seguridad que se puede proporcionar de esta manera son los siguientes:
- Todas las características de los servicios comunes de seguridad extremo a extremo (integridad, autenticación, no repudio) y además el servicio de confidencialidad del contenido deben ser soportadas por la implementación, y se deben utilizar todas las características de seguridad extremo a extremo.

Además se proprocionan las siguientes características:
- Gestión de acceso seguro
- Servicio de seguridad de autenticación de entidad pareja.
- Servicio de seguridad de control de acceso de entidad pareja.
- Etiquetado de seguridad del mensaje
- Gestión de la seguridad

b) Servicios de seguridad para Intercambio Electrónico de Datos (EDI)

EDI es el intercambio de información estructurada, por medios electrónicos, entre sistemas informáticos.

EDI se desarrolla por medio de aplicaciones que pueden intercambiar información estructurada. Por otra parte EDI establece cómo deben estar estructurados los documentos electrónicos para su transmisión y define el significado de cada elemento de información. Finalmente, EDI necesita un servicio de transporte, tal como un sistema de mensajería o un sistema de transferencia de ficheros para hacer llegar la información. EDI tiene lugar entre sistemas informáticos y no se ha previsto su utilización para intercambio de información persona a persona.

EDI respeta, por tanto, la autonomía de las partes implicadas pues no impone restricciones sobre aspectos de procesamiento interno de la información intercambiada, ni sobre los medios de transmisión.

Los estándares EDI proporcionan un conjunto de reglas de sintaxis que permiten definir los documentos estructurados, denominados mensajes EDI, así como un número cada vez mayor de mensajes EDI predefinidos. Las recomendaciones de EPHOS en relación a EDI se basan en un conjunto de estándares y documentos desarrollados por las Naciones Unidas : "*ISO 9735 -Electronic Data Interchange for Administration, Commerce and Transport (EDIFACT) - Application level syntax rules*" (EN 29735). Por razones históricas se han ido desarrollando otros conjuntos de reglas de sintaxis usados en diversos sectores, sin embargo EDIFACT es la única sintaxis estándar.

Como hemos visto, en EDI la información intercambiada se estructura en torno a un conjunto de reglas de sintaxis similares a la gramática de un lenguaje. Estas reglas EDI se aplican sólamente a la información a intercambiar y son independientes de los datos, de los sistemas informáticos y de los mecanismos de comunicaciones utilizados.

Acuerdo de intercambio
Las partes implicadas deben establecer con claridad los deberes y derechos que se derivan del uso del EDI. En consecuencia se precisa la existencia de un acuerdo entre las partes que especifique los aspectos relativos al uso del EDI, tales como mensajes estándar, métodos de comunicación, reglas de procedimiento, aspectos de seguridad, validez legal de los mensajes, etc.
El sistema EDI tiene que satisfacer los requisitos que se derivan del acuerdo de intercambio entre las partes. Este acuerdo puede determinar también qué aspectos de seguridad EDIFACT son necesarios, en cuyo caso especificará las circunstancias bajo las que se van a usar aspectos de seguridad EDIFACT e incluso MHS.

La seguridad es un aspecto muy importante en los entornos abiertos, especialmente cuando los sistemas informáticos dan soporte a comercio electrónico.

Los aspectos de seguridad más relevantes identificados en un escenario EDI son los siguientes:

- confidencialidad del contenido;
- mantenimiento de la privacidad de los mensajes clasificados como confidenciales.
- integridad del contenido;
- integridad de la secuencia del mensaje;
- Autenticación de origen del mensaje;
- no repudio del origen;
- no repudio de recepción;
- prueba de transmisión (*proof of transmission)*;

Desde el punto de vista legal, el aspecto esencial es el acuerdo entre las partes. *Desde el punto de vista técnico, la seguridad EDI no se encuentra completamente soportada por los estándares*

funcionales existentes, encontrándose diferentes soluciones.

Servicios de seguridad EDIFACT

Los requerimientos de seguridad pueden ser soportados a nivel de aplicación, es decir, a nivel de mensaje, y a nivel de comunicaciones.

A *nivel de mensaje,* los servicios de seguridad son soportados por las propias partes involucradas. extremo a extremo, por lo que la seguridad se aplica en el citado nivel, no debiendo implicar cambios en los mensajes individuales. La solución de seguridad por tanto será global y se aplicará de igual forma a todo tipo de mensaje de cualquier aplicación comercial EDI.

A *nivel de comunicaciones* el soporte de los requerimientos de seguridad varía dependiendo del sistema de transferencia utilizado (FTAM, MHS).

Con carácter general son preferibles las soluciones a *nivel de mensaje* cuando las amenazas a los mensajes pueden tener lugar en el proceso de comunicación entre el sistema externo de transferencia y las aplicaciones EDI. En este caso la seguridad debe ser transparente al protocolo de comunicación que se utilice y que no tiene por qué saber si el mensaje EDI lleva o no seguridad, e independiente de los mecanismos de transporte.

EDIFACT contempla los siguientes servicios de seguridad:
- Confidencialidad.
- Integridad del mensaje y del contenido.
- Autentificación del contenido del mensaje.
- No repudio de origen.
- No repudio de recepción.

EDIFACT considera dos formas de aplicar los servicios de seguridad a los mensajes: de forma integrada en los mismos, o bien mediante mensajes separados.
- De forma integrada en el mensaje: Se realiza mediante la introducción de grupos específicos de segmentos de seguridad para proteger el nivel del mensaje: la Cabecera y el Pie de Seguridad. Se pueden incluir en cualquier mensaje EDI y se colocan después de la Cabecera del Mensaje y antes del Pie del Mensaje. Este método actualmente no incluye la posibilidad de aplicar el servicio de Confidencialidad.
- Seguridad separada del mensaje: Se realiza mediante la utilización de mensajes específicos. El mensaje AUTACK de autentificación y acuse de recibo seguro que proporciona seguridad a uno o más mensajes en un solo mensaje separado y además proporciona un acuse de recibo protegido al emisor del mensaje de que éste fue recibido por el receptor al que iba destinado.
  Se encuentran en diversas fases de elaboración otros mensajes para proporcionar confidencialidad o para facilitar la gestión de claves.

El comprador seleccionará las claúsulas de compra que proporcionen al menos todos los servicios de seguridad requeridos.

Las alternativas pueden ser:

- Que la implementación sea capaz de satisfacer todos los servicios de seguridad EDIFACT.
- Que la implementación sea capaz se satisfacer servicios de seguridad EDIFACT individuales según se requiera.

Un aspecto importante a tener en cuenta aquí es que los servicios de seguridad EDIFACT se orientan a la protección de mensajes individuales EDI dentro del intercambio.

En resumen el comprador seleccionará los servicios de seguridad EDIFACT para satisfacer los requisitos de los servicios de seguridad genéricos que se requieren para proteger mensajes EDI individuales.

Una vez identificados los requerimientos de seguridad, tras el análisis de riesgos, los árboles de decisión de EPHOS proporcionan una guía para la selección de las claúsulas de adquisición en base a los cinco perfiles que veremos a continuación.

TODOS LOS SERVICIOS DE SEGURIDAD EDIFACT (EDIFACT SEGURIDAD UNO)

- Se requiere confianza en todos los aspectos de seguridad proporcionados por EDIFACT
- Se requiere confianza en la transacción completa por cada mensaje EDI.
- El marco contractual entre las partes utilizando EDI requerirá que se soporten todos los servicios de seguridad EDIFACT.

Servicio Genérico de Seguridad	*Servicio de Seguridad Específico EDI*
Confidencialidad	Confidencialidad del mensaje EDI individual
Integridad	Integridad del mensaje EDI individual
Autenticación	Autenticación del originador y del receptor del mensaje EDI
No repudio	No repudio del mensaje EDI por el originador y por el receptor

La selección de la claúsula asociada a este perfil equivale a seleccionar al mismo tiempo las correspondientes a EDIFACT DOS, TRES y CUATRO.

EDIFACT NO REPUDIO DE ORIGEN (EDIFACT SEGURIDAD DOS)

Se trata del caso en que se precisa que ninguna de las partes pueda repudiar el origen de la operación. Esto se puede deber a que el análisis de riesgos haya identificado que esta vulnerabilidad presente un riesgo mayor que las otras. En la configuración de un sistema de comercio electrónico automatizado las dos partes en cuestión necesitan tener la confianza de que el comercio electrónico proporciona el marco contractual vinculante en el que poder operar. Así el *no repudio de origen* es un parte esencial del comercio via EDI.

Servicio Genérico de Seguridad	*Servicio de Seguridad Específico EDI*
Integridad	Integridad del mensaje EDI individual
Autenticación	Autenticación del originador del mensaje EDI
No repudio	No repudio del mensaje EDI por el originador

EDIFACT CONFIDENCIALIDAD (EDIFACT SEGURIDAD TRES)
Esta claúsula se debiera utilizar cuando se identifica alguno de los siguientes aspectos:

- La revelación de información dentro de un mensaje EDI se identifica como una amenaza a la seguridad.
- Se precisan aspectos de privacidad extremo a extremo
- Los servicios de *confidencialidad* no son proporcionados por el servicio subyacente

Servicio Genérico de Seguridad	*Servicio de Seguridad Específico EDI*
Confidencialidad	Confidencialidad del mensaje EDI individual

EDIFACT AUTENTICACIÓN DE ORIGEN E INTEGRIDAD (EDIFACT SEGURIDAD CUATRO)
No se requieren servicios completos de no repudio pero sí algo de confianza en que el mensaje sea correcto. Esta claúsula también protege contra las amenazas de enmascaramiento y de modificación.

Servicio Genérico de Seguridad	*Servicio de Seguridad Específico EDI*
Integridad	Integridad del mensaje EDI individual
Autenticación	Autenticación deloriginador del mensaje EDI

EDIFACT NO REPUDIO DE RECEPCION (EDIFACT SEGURIDAD CINCO)
Se requiere *no repudio* para todos los aspectos de la transacción.
Esta claúsula que se aplicará en combinación con EDI 2 o EDI 4 se utiliza para contrarrestar la vulnerabilidad derivada de que el receptor pueda bien denegar la recepción del mensaje o bien alterar su contenido. Para contrarrestar esta vulnerabilidad el receptor debe enviar un mensaje de confirmación del mensaje recibido, denominado AUTACK anteriormente descrito.

Servicio Genérico de Seguridad	*Servicio de Seguridad Específico EDI*
Integridad	Integridad del mensaje EDI individual
Autenticación	Autenticación del receptor del mensaje EDI
No repudio	No repudio del mensaje EDI por el receptor

Otros aspectos

Las técnicas de seguridad de MHS mencionadas hasta ahora se orientan a la interoperabilidad de los sistemas e implican la existencia de ciertos protocolos de seguridad. La satisfacción a otros requerimientos de seguridad puede implicar la existencia de otras técnicas independientes de los protocolos de seguridad, como pueden ser las siguientes:

- Requisitos de aseguramiento
- Requisitos de audit
- Gestión de la seguridad
- Técnicas criptográficas.

3.1.4. Marco referencial de estándares para correo electrónico X.400.

- ISO-7498-2 Information Processing Systems-Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture.
- Internet Privacy Enhanced Mail. Privacy and Security research Group (PRSG), Internet Architecture Board (IAB).
- X.509 The Directory - Authentication Framework.
- EPHOS 2 bis Topic U Security Service
- Green Paper on the Security of Information Systems
- Information Technology Security Evaluation Criteria
- Information Technology Security Evaluation Manual
- The IBAG framework for Information Security
- ISO/IEC/JTC1/SC27 N519 Revised Guide for Open Systems Security
- ISO/IEC/JTC1/SC27 N566 Glossary of IT Security Terminology (Version 2.0)
- ISO/IEC/JTC1/SC27 N720 Guidelines for the Management of IT Security (GMITS) Part 2: Managing and Planning IT Security
- Guía de Seguridad de los Sistemas de Información para Directivos de las Administraciones Públicas.
- Estándares del entorno financiero (Catálogo de servicio estándar TC68)

3.2. INTERNET

Para poder enfocar la problemática de seguridad que se presenta al utilizar los servicios Internet es preciso conocer sus aspectos básicos a fin de comprender las implicaciones que puede implicar su uso.

3.2.1. Marco institucional y estructura de la red Internet.

El Boletín de la red nacional de I+D, RedIRIS, constituye una interesante fuente para conocer la 'arquitectura' y la 'estructura' de la red Internet especialmente el artículo 'A,B,C de Internet' publicado por Miguel A. Sanz Sacristán en el número 28 del citado boletín.
El marco institucional que orienta y coordina la evolución de Internet se denomina *Internet Society* (ISOC) y se trata de una sociedad profesional internacional sin ánimo de lucro, formada por organizaciones e individuos de todos los sectores involucrados de una u otra forma en la construcción de la Internet (usuarios, proveedores, fabricantes de equipos, administradores, etc) cuyo principal objetivo es fomentar el crecimiento de Internet en todos sus aspectos (número de usuarios, nuevas aplicaciones, aplicaciones, mejor infraestructura, etc). También se encarga del desempeño de actividades de importancia crítica como son el desarrollo de estándares, el control de la correcta administración de los recursos de Internet delegada en los NICs (*Network Information Center*), la coordinación en temas de investigación y la cooperación con otros organismos internacionales como la Unión Internacional de Telecomunicaciones (ITU), la Organización Internacional de Estandarización (ISO) y la Organización de las Naciones Unidas (ONU).

La ISOC dispone de una serie de órganos con distintas responsabilidades:

IAB *Internet Architecture Board*, comité encargado de determinar las necesidades técnicas a medio y largo plazo y de la toma de decisiones sobre la orientación tecnológica de la Internet. También aprueba las recomendaciones y estándares de Internet, recogidos en una serie de

documentos denominados RFCs (*Request For Comments*).

IETF *Internet Engineering Task Force* e IRTF (*Internet Research Task Force*), sirven de foros de dicusión y trabajo sobre los diversos aspectos técnicos y de investigación respectivamente. Su principal cualidad es la de estar abiertos a todo aquél que tenga algo que aportar.

IESG *Internet Engineering Steering Group* e IRSG (*Internet Research Steering Group*), coordinan los trabajos de IETF e IRTF respectivamente.

IANA *Internet Assigned Number Authority*, responsable último de los diversos recursos asignables de internet.

Una de las características esenciales de Internet es su descentralización, nadie gobierna la Internet, de forma que cada red conectada conserva su independencia. Sin embargo es preciso tener claro que la conexión a Internet por parte de un usuario, entendiendo por usuario desde una gran organización con toda su red corporativa y multitud de individuos, hasta u simple individuo a título particular, se efectúa siempre por medio de un proveedor del servicio de acceso a Internet.

Cada proveedor del servicio de acceso a Internet dispone de su propia infraestructura de red y de su propio menú de servicios, modalidades de acceso a los mismos y precios. En función de las necesidades del usuario y de la oferta del proveedor las posibilidades de conexión son muy variadas, pudiendo ir desde una conexión permanente mediante una línea dedicada de gran capacidad, hasta un simple acceso esporádico mediante llamada telefónica, pasando por el acceso restringido a determinados servicios o equipos mediante el empleo de pasarelas de aplicación y **cortafuegos**.

A su vez los proveedores de servicio llegan a acuerdos de interconexión entre ellos para el intercambio del tráfico entre sus redes o para permitir su tránsito hacia otros proveedores. La existencia de proveedores con infraestructura de red de diversos tamaños y ámbitos geográficos, da lugar a una cierta jerarquía de redes dentro de Internet en cuyo vértice están las grandes redes troncales o *backbones*.

- En esta categoría se pueden englobar las redes de las agencias federales de los EEUU: NSFNET(la más importante), NSINET(NASA), ESNET (Departamento de Energía), MILNET, conectadas entre sí en los determinados FIX (*Federal Internet Exchange*) y que en la actualidad convergen hacia la NREN (*National Research and Education Network*).
- Las grandes redes de proveedores comerciales: Alternet, PSI, Sprint, CERFnet, etc, interconectadas entre sí en los denominados CIX (*Commercial Internet Exchange*).
- Las grandes redes internacionales como EuropaNET, Ebone, etc que se interconectan con todas las anteriores en el denominado GIX (*Global Internet Exchange*).
- Las grandes redes troncales conectan a su vez a los proveedores intermedios como por ejemplo las denominadas redes regionales en los EEUU o las redes académicas nacionales.
- Por último las redes intermedias dan servicio a las redes de las organizaciones finales como pueden ser la red de una universidad o la red corporativa de una empresa.

Un paquete IP enviado entre dos ordenadores de Internet suele pasar por muchas redes distintas bajo distintas responsabilidades de gestión. Para resolver los problemas de funcionamiento que puedan surgir cada proveedor dispone de su centro de gestión y operación de red, NOC (*Network Operation Center*), existiendo asimismo mecanismos y herramientas de coordinación entre los NOCs de los diferentes proveedores. También existen organismos como el RIPE NCC en Europa que facilitan esta coordinación entre los proveedores de servicios Internet.

De la forma de funcionamiento de Internet se desprende la necesidad de administrar una serie de recursos comunes. Esta especie de servicio público para toda la comunidad Internet la desempeñan los denominados NIC (*Network Information Center*), que se encargan de actividades vitales como

son la asignación de direcciones IP, el registro de nombres de dominio y la gestión del DNS (*Domain Name System*) que consiste en una base de datos distribuida de forma jerárquica por toda la Internet que es consultada por las aplicaciones de usuario para llevar a cabo la traducción entre los nombres y las direcciones numéricas.

Estas tareas se encuentran descentralizadaas por áreas geográficas, así a nivel mundial se encarga el InterNIC, en Europa el RIPE NCC y en España el registro delegado de Internet o ES-NIC , gestionado por Red-IRIS.

3.2.2. Seguridad en correo electrónico Internet.

Correo electrónico seguro en Internet (P.E.M.)

El correo electrónico estándar de Internet está definido en las propuestas RFC 821-822. Este sistema de correo sólo permite la transmisión de documentos de texto en ASCII, así, que han surgido diversas propuestas para adaptarlo a nuevas aplicaciones. Las más conocidas con las normas MIME (correo electrónico multimedia) y PEM (correo electrónico seguro).

El desarrollo de PEM (Internet Privacy Enhanced Mail) se inició en 1.985 por el Grupo de Investigación de Seguridad y Privacidad (PSRG) bajo la dirección de la Internet Architecture Board (IAB). Como resultado han aparecido una serie de recomendaciones, las RFC 1421-1424, que han sido propuestas como estándares Internet.

El objetivo principal en el desarrollo de PEM era proporcionar seguridad en el correo electrónico a los usuarios de Internet. Los servicios que facilita son:

- confidencialidad
- integridad no orientada a conexión
- autenticación del origen,
- soporte para no repudio con prueba de origen.

Estos servicios, definidos en el modelo OSI de seguridad, se dividen en dos grupos: todo el correo PEM incorpora autenticación, integridad y soporte para no repudio, mientras que la confidencialidad es opcional.

Servicios de seguridad.

La ***confidencialidad*** trata de evitar que el contenido del mensaje pueda ser leído por alguien distinto de su destinatario legítimo. Durante el tránsito de los mensajes por la red, los mensajes están expuestos a que alguien pueda "pinchar" las líneas, o que pueda acceder a los discos donde se almacenan mensajes para su reenvío. Los usuarios que acceden a través de una red de área local sufren el peligro añadido de que los administradores u otros usuarios de la red local puedan acceder al contenido de sus mensajes.

La ***autenticación del origen*** consiste en identificar de forma fiable al emisor de un mensaje. De esta forma, al recibir un mensaje, podemos estar seguros de que el emisor es quien dice ser en el mensaje y no otro que se hace pasar por él. Este servicio suele darse junto con el de integridad.

La ***integridad "no orientada a conexión"*** garantiza que no se ha alterado el mensaje durante su transmisión, y por tanto que se ha recibido tal y como se envió. No es difícil comprender la necesidad

de este servicio. Por ejemplo, una compañía emite un correo electrónico a su cajero diciendo: "Páguese 100.000 Pts. al Sr. X"; mientras tanto, alguien cambia el '1' por un '9' mientras viaja por la red, y el cajero recibe una nota que dice: "Páguese 900.000 Pts. al Sr. X". Se llama "sin conexión" porque no se impone ninguna ordenación entre los mensajes recibidos.

Se proporciona soporte para el ***no repudio*** porque el emisor de un mensaje puede enviarlo a una "tercera parte" que podría verificar la identidad del emisor y que el mensaje no ha sido alterado por nadie.

Formato de los mensajes PEM.

Los mensajes PEM se diseñaron para que fueran compatibles con el formato RFC-822. La cabecera es idéntica, con la excepción de que algunos campos "sensibles" pueden incluirse dentro de la parte codificada. Así, un usuario puede decidir que el campo "asunto" no va a ir en la cabecera, sino en la parte codificada.

El usuario da la dirección del receptor y otros campos para la cabecera.		CABECERA Campos de cabecera RFC-822
	BEGIN PRIVACY ENHANCED MESSAGE	
El usuario proporciona la información necesaria para encriptar.	CABECERA ENCAPSULADA: Contiene la información de autenticación, integridad, encriptación (opcional) e información relacionada.	MENSAJE ENCAPSULADO
	LINEA EN BLANCO	
Cabeceras y texto para encriptar	TEXTO ENCAPSULADO: Campos de cabecera y texto del mensaje encriptados.	
	END PRIVACY ENHANCED MESSAGE	

El cuerpo comienza con un delimitador específico (BEGIN PRIVACY ENHANCED MESSAGE). Después viene la cabecera PEM, que contiene las comprobaciones de integridad y autenticación del emisor, junto con otra información sobre el tipo de encriptación utilizada, algoritmos utilizados, y otra información necesaria. A continuación se incluye una línea en blanco que marca el final de esta cabecera y el comienzo del texto (opcionalmente) codificado. El mensaje acaba con el delimitador (END PRIVACY ENHANCED MESSAGE).

PEM proporciona tres tipos de mensajes llamados MIC-CLEAR, MIC-ONLY y ENCRYPTED. El primer tipo está pensado para poder enviar correo electrónico a destinatarios que no tienen implementado PEM. A estos mensajes se les incluye un código criptográfico de integridad del mensaje (MIC) y el mensaje no va codificado. Así, es posible enviar un mensaje a una lista de distribución que contenga usuarios PEM y usuarios no PEM. Todos ellos pueden leer el mensaje, puesto que no va codificado, aunque sólo los usuarios PEM pueden utilizar los servicios de integridad y autenticación.

Los mensajes MIC-ONLY son como los anteriores, pero se les hace una codificación adicional, que ayuda a que puedan atravesar sin modificaciones las pasarelas de correo electrónico. Este paso es conveniente, ya que cualquier pequeña modificación haría fallar la prueba de integridad.

El tipo ENCRYPTED añade la confidencialidad a los servicios de integridad y autenticación. También se realiza la codificación adicional de los mensajes MIC-ONLY, puesto que la salida binaria del proceso de codificación no puede transmitirse tal cual.

SERVICIOS/TIPOS DE MENSAJES	MIC-CLEAR	MIC-ONLY	ENCRYPTED
INTEGRIDAD Y AUTENTICACION	SI	SI	SI
CODIFICACION ADICIONAL	-	SI	SI
MENSAJE ENCRIPTADO	-	-	SI

Tipos de mensajes PEM.

Envío de los mensajes.

Cuando un mensaje se lanza al sistema para su transmisión, se llevan a cabo una serie de pasos:

ENTRADA = Texto en claro.

Paso 1 : Paso a la forma canónica.
Paso 2 : Cálculo del MIC y cifrado.
Paso 3 : Codificación en 6 bits y formateo de las líneas.

SALIDA = Mensaje procesado.

El primer paso consiste en transformar el mensaje a la representación estándar de la red, con el fin de eliminar las diferencias en el formato del texto debidas a las máquinas concretas (p. ej., la manera de señalar el fin de línea o el final de fichero). El formato final se indica en el campo Content-Domain de la cabecera. Además del formato RFC-822 para SMTP hay otras posibilidades, como el ASN.1 para X.400.

En el segundo paso se calcula el MIC del texto. Para ello, se aplica una función *hash*, indicada en la cabecera, al texto en forma estándar. PEM exhorta a utilizar funciones *hash* irreversibles en todos los casos, en especial cuando los mensajes van dirigidos a múltiples destinatarios. Utilizar funciones así evita un tipo de engaño, en el que un usuario A envía un mensaje a los usuarios B y C. Si se utilizara un función *hash* débil para calcular el MIC, B podría capturar el mensaje, modificarlo de manera que tuviera el mismo MIC, y entonces enviarlo a C, quien no notaría la diferencia.
A continuación, el MIC se protege con la clave privada del emisor, obteniéndose una firma digital que garantizará la integridad del mensaje y la autenticación del emisor. Cuando el receptor trate de verificar la firma digital, requerirá la clave pública del emisor. Para que pueda obtenerla fácilmente, se puede incluir el certificado de la clave pública del emisor en la cabecera, e incluso el certificado de la autoridad de certificación (CA's) que lo expidió.

MENSAJE ORIGI-NAL	hash ----->	MIC	RSA ----------> (clave privada)	FIRMA DIGITAL

>> GENERACION DE LA FIRMA DIGITAL POR EL EMISOR.

El cifrado de los mensajes se realiza durante este segundo paso. En la cabecera, el campo DEK-Info indica el algoritmo que se emplea para cifrar, junto con los parámetros que sean necesarios. Lo

más frecuente es cifrar el mensaje con un algoritmo simétrico (p.ej, DES), de modo que es necesario hacer llegar la clave al receptor. Esta tarea se realiza con el campo KEY-Info, que lleva la clave del mensaje cifrada con la clave pública del destinatario[1]. El texto cifrado se coloca después de la cabecera PEM, separado de ella por una línea en blanco.

Esto es suponiendo que para distribuir la clave se utiliza un algoritmo criptográfico asimétrico. Podría emplearse un algoritmo simétrico, pero requiere otra técnica.

Proc-Type	Tipo de mensaje MIC-CLEAR, MIC-ONLY, etc.
Content-Domain	Transformaciones en el paso 1.
MIC-Info	Firma digital y algoritmos utilizados para obtenerla
Originator-Certificate	Certificado del emisor.
Iusser-Certificate	Certificados de la(s) CA's que certifican al emisor
DEK-Info	Datos sobre el cifrado: algoritmo y parámetros.
Recipient-ID-Asymmetric	Destinatario del mensaje.
Key-Info	Clave del mensaje cifrada.

Campos de la cabecera de los mensajes PEM.

Cuando existen múltiples destinatarios, se envía a cada uno el mensaje cifrado con una clave distinta. Como hay que enviar a cada cual la clave con que va cifrado su mensaje, tendremos más de un campo KEY-Info (uno por cada destinatario) con las claves encriptadas. Antes de cada KEY-Info se incluye un campo Recipient-ID-Asymmetric que identifica a qué usuario pertenece el Key-Info que viene después.

El tercer paso no se aplica cuando el mensaje es MIC-CLEAR. Su finalidad es evitar que el mensaje sea modificado, aunque sea muy levemente, durante su transmisión porque fallaría la prueba de integridad. En la mayoría de los sistemas de correo electrónico Internet sólo está permitido enviar textos en código ASCII con caracteres de 7-bits. Por otra parte, al cifrar un mensaje es frecuente obtener códigos binarios de 8-bits. Para solucionar este problema, se toma el resultado del paso 2, se convierte a un código de 6-bits y las líneas se adaptan a unas longitudes máximas. Así, el resultado puede transmitirse sin modificaciones por toda la red.

Recepción de los mensajes.

Cuando un usuario recibe un mensaje PEM, en primer lugar examina su cabecera para determinar si es MIC-CLEAR, MIC-ONLY o ENCRYPTED. Si no es MIC-CLEAR se convierte del código de 6-bits a la forma original.

A continuación, si el mensaje es ENCRYPTED se descifra. El receptor recorre los campos Recipient-ID-Asymmetric, buscando su identificador. Después lee el campo Key-Info que hay justo después, con lo que encuentra la clave del mensaje encriptada, y el algoritmo que encripta dicha clave. En caso de utilizar un algoritmo de clave pública, utilizaría su clave privada para desencriptarla.

Como resultado, obtiene la clave del texto cifrado. Entonces, mirando el campo DEK-Info, consigue saber el algoritmo criptográfico utilizado, y con la clave anterior, lo aplica al mensaje cifrado para obtener el texto en claro.

Ya en este punto se puede verificar la integridad del mensaje, y la identidad del emisor. Para hacerlo se lee el campo MIC-Info, que indica: la función *hash* utilizada para calcular el MIC, el algoritmo

con que se encriptó el MIC, y la firma digital. Entonces, el receptor busca la clave pública del emisor y la utiliza con la firma digital para obtener el MIC. A partir del mensaje puede saberse la clave pública del emisor (si envió su certificado) o de otra fuente fiable (puede tenerse ya, u obtenerse de una CA).

Ahora, aplicando la función *hash* al mensaje que se ha recibido se tiene un valor MIC'. Si MIC y MIC' son iguales, queda verificada la integridad del mensaje y la identidad del emisor.

FIRMA DIGITAL	RSA ---------->(clave pública)	MIC	---------->	¿SON IGUALES? SI: Verificado mensaje y emisor NO: Error detectado en la verificación.
MENSAJE RECIBIDO	hash	MIC'	---------->	

>> COMPROBACION DE LA FIRMA DIGITAL POR EL RECEPTOR.

Una vez recibido y validado el mensaje, se convierte del formato estándar de la red a la representación utilizada por la máquina local, y se presenta al usuario. Si ocurre algún error durante la verificación o el descifrado, se advertiría al usuario, y se tomarían las acciones oportunas.

Finalmente, el usuario puede decidir la forma en que almacena un mensaje PEM. Es posible guardar el texto desencriptado, sin la cabecera PEM, también se puede guardar la cabecera PEM (dejando la firma digital, la identificación del emisor, etc.) o puede almacenarse en la forma cifrada.

3.2.3. Seguridad en servicios Internet

Secure Sockets Layer (SSL)

Se trata de un protocolo abierto y no propietario desarrollado por Netscape y que ha sido puesto a disposición del IETF, concretamente del grupo de trabajo W3C con vistas a su estandarización. Sus especificaciones en versión borrador pueden ser encontradas en la red.

El protocolo SSL proporciona servicios de confidencialidad, integridad, autenticación del servidor y opcionalmente autenticación del cliente en conexiones TCP/IP. SSL se encuentra en un nivel inferior a los protocolos HTTP, Telnet, FTP, Gopher pero por encima del nivel del TCP/IP. Mediante esta estrategia el SSL puede funcionar con independencia de los protocolos Internet y puede proporcionar seguridad a aplicaciones que trabajan con TCP/IP.

SSL proporciona un protocolo de seguridad que se utiliza al establecer una conexión TCP/IP, de forma que el cliente y el servidor pueden acordar el nivel de seguridad a utilizar y responder a los requerimientos de autenticación para establecer la conexión. Después el papel principal del SSL es cifrar y descifrar la corriente de bytes correspondiente al protocolo de aplicación que se utilice. Esto significa que toda la información en la petición HTTP y en la respuesta HTTP está completamente cifrada incluyendo el Universal Resource Locator (URL) que el cliente está solicitando, los contenidos, cualquier información de autorización de acceso como nombres de usuario o palabras de paso, así como toda la información devuelta por el servidor al cliente.

El objetivo básico del protocolo es permitir conexiones seguras en aplicaciones cliente/servidor. Para ello presenta las siguientes características básicas:
- Utiliza algoritmos de clave simétrica como DES o RC4 para el cifrado de los datos.
- Utiliza algoritmos de clave pública como RSA o DSS para la autenticación de entidades.
- Aplica funciones hash seguras como SHA o MD5, que se utilizan para incluir un checksum que se adjunta con el mensaje.

Secure Hypertext Transfer Protocol (SHTTP)

Se trata de un desarrollo de Enterprise Integration Technologies (EIT). SHTTP es una versión mejorada con aspectos de seguridad del protocolo HTTP que constituye la base del Web y proporciona servicios básicos de seguridad entre el cliente y el servidor para transacciones electrónicas comerciales tales como confidencialidad, integridad del mensaje, autenticación y no repudio de origen.

Terisa Systems ha producido una versión comercial del SHTTP.

SSL y SHTTP no son protocolos excluyentes sino que pueden coexistir disponiendo el SHTTP sobre el SSL. SSL aporta la seguridad bajo protocolos de aplicación como HTTP o Telnet, mientras que SHTTP proporciona seguridad orientada al mensaje según una filosofía similar a la de PEM.

Secure HTTP puede incorporar a los clientes y servidores diversos estándares criptográficos, como pueden ser entre otros PKCS-7 y PEM, es compatible con HTTP. Clientes SHTTP pueden comunicarse con servidores HTTP sólo que en este caso no estarán disponibles los servicios de seguridad.

SHTTP soporta modos de operación en base a claves simétricas que permiten la realización de transacciones espontáneas sin necesidad de que los usuarios tengan establecida una clave pública.

SHTTP dispone de gran flexibilidad en cuanto a algoritmos criptográficos, modos de operación y parámetros. Clientes y servidores pueden negociar el modo de las transacciones para acordar aspectos relacionados con el cifrado, la firma digital o la selección de certificados.

4. PRODUCTOS DE SEGURIDAD

Este capítulo ofrece una panorámica de los productos capaces de suministrar los servicios de seguridad para X.400 e Internet. Se referencian desde la óptica proyectada por los fabricantes, indicando los servicios de seguridad que son capaces de aplicar y qué medios utilizan para conseguirlo. Hay que tener en cuenta que Internet, cuyo tamaño se dobla cada año, constituye un vasto mercado por explotar comercialmente, que se está incrementando día a día la oferta de soluciones para la realización de transacciones seguras y que se trata de un mercado en ebullición y en constante desarrollo.

El coste de los productos, es un dato que no ha sido posible incluir en este documento, pues la manifestación de los proveedores es generalizada en cuanto a que los precios se ajustan según el entorno en el que se incorpore el uso del producto. Se ha dado el mismo tratamiento a todos ellos omitiendo el dato coste, al no ser proporcionado por la totalidad de los mismos.

4.1. PRODUCTOS PARA CORREO ELECTRÓNICO

X.400 permite el intercambio de mensajería interpersonal, es decir, correo electrónico y de mensajería EDI. Además, X.400 es ideal para el acceso a redes de valor añadido, que permiten comunicaciones muy eficaces para EDI. Una de las ventajas más destacables de X.400 es que a través de las distintas redes permite el intercambio de mensajes entre diferentes tipos de terminales: PC, fax o videotex.

PRETTY GOOD PRIVACY (PGP)

Pretty Good Privacy (PGP) es un paquete de seguridad originalmente desarrollado por Phil Zimmermann para correo electrónico Internet y que también se puede aplicar a correo electrónico X.400. Combina confidencialidad y firma digital de forma robusta y sencilla de usar.

La primera versión de PGP apareció en 1991. El desarrollo del PGP fue motivado por el intento del FBI de apoyar una ley que podría prohibir ciertos tipos de algoritmos de seguridad y forzar a los fabricantes de ordenadores a implantar ciertas características de seguridad que podrían ser evitadas por las agencias de Gobierno. Zimmermann vio en esto una amenaza para la privacidad y la libertad.

Objetivos.

PGP fue concebido como un paquete susceptible de ser utilizado por un usuario medio con un pequeño sistema y que proporcionara privacidad y autenticación con correo electrónico. En PGP esto se consigue:

- Seleccionando los mejores algoritmos de seguridad.
- Integrando estos algoritmos en una aplicación de propósito general independiente del sistema operativo y del equipo, que se basa en un conjunto de comandos reducido.
- Haciendo el paquete y su documentación, incluido el código fuente, de libre distribución y disponible para todo el mundo.

Firmas digitales. PGP utiliza los algoritmos criptográficos siguientes.

- IDEA (International Data Encryption Algorithm). Utiliza una clave de 128 bits para cifrar bloques de datos de 64 bits. Es un algoritmos simétrico (se emplea una clave secreta para cifrar y descifrar).
- RSA (Rivest-Shamir-Adleman). Es el algoritmo de clave pública más universal. Existen dos claves, una pública, que todo el mundo conoce, y otra privada, en poder del receptor.

Bastaría con el algoritmo RSA para tener un correo electrónico seguro. Cualquiera que quisiera usar PGP podría crear un par de claves (privada y pública) y distribuir la clave pública. Para enviar un mensaje, primero se cifraría con la clave privada del emisor para garantizar la autenticación. Después, se cifraría con la clave pública del receptor para que nadie lo pueda leer.

Este esquema es válido, pero no es práctico. El problema es que RSA, y los demás esquemas de clave pública son muy lentos. Hacer el doble cifrado de los mensajes podría llevar minutos o incluso horas en un ordenador personal.

PGP utiliza la fortaleza de los cifrados convencional o simétrico y de clave pública o asimétrico. Cuando se envía un mensaje, se hacen dos procesos relacionados con la seguridad: firma digital y cifrado.

Para la etapa de cifrado, PGP genera aleatoriamente una clave secreta de 128 bits y utiliza IDEA para cifrar el mensaje y la firma digital. El receptor puede descubrir la clave secreta usando RSA. PGP toma la clave secreta como entrada del RSA, usando la clave pública del receptor, y produce una clave secreta cifrada que se asocia al mensaje. En el extremo receptor, PGP usa la clave privada del receptor para obtener la clave secreta. Entonces, la utiliza con IDEA para recuperar el mensaje en claro y la firma.

Para la firma digital se toma el mensaje y se obtiene un código de 128 bits. El algoritmo que hace esto se llama MD5, y tiene la propiedad de que el código que se obtiene es único para el mensaje. Es muy difícil alterar el mensaje o sustituirlo por otro y obtener el mismo código.

PGP cifra este código usando RSA y la clave secreta del emisor. El resultado es la firma digital, que se añade a continuación del mensaje. Quien recibe el mensaje, puede recalcular el código de 128 bits a partir del mensaje descifrado y descifrar la firma digital con la clave pública del emisor. Si ambos coinciden, la firma digital es válida. Como esta operación sólo implica cifrar y descifrar un bloque de 128 bits, lleva poco tiempo.

OBTENCION DE CLAVES PUBLICAS.

El cifrado de clave pública hace uso de dos claves para cada usuario. Una clave privada conocida sólo por un usuario, y su clave pública correspondiente, dada a conocer a todos los usuarios. Sin embargo, no es suficiente con que los usuarios den a conocer sus claves públicas. Un impostor podría generar un par de claves y darlas a conocer como si fuera otro usuario. Es preciso un intercambio seguro de claves públicas.

La herramienta que permite la obtención segura de las claves es el certificado de clave pública. Este certificado contiene esencialmente la clave pública, un identificador de usuario, compuesto por el nombre y la dirección de correo electrónico, y una o más firmas digitales para los datos anteriores. Las firmas testifican que el identificador de usuario asociado a la clave pública es válido. Si se modifica alguno de los dos, la firma digital deja de ser válida.

Para la obtención de certificados, un enfoque que utilizan modelos como PEM es tener autoridades centrales de certificación (CA). Cuando la autoridad de certificación se asegura de

la identidad del usuario, firma un certificado que asocia al usuario con su clave pública. Como todos los usuarios confían en la autoridad de certificación, los certificados adquiridos de ésta se consideran válidos.

Nada impide que PGP emplee autoridad de certificación. Sin embargo, PGP está concebido como un esquema para las masas. Puede usarse en multitud de entornos formales e informales. De acuerdo con esto, PGP se diseñó para soportar un esquema en que los usuarios se firman unos a otros las claves.

FIABILIDAD DE LAS CLAVES PUBLICAS.

Cada usuario recoge claves firmadas y las almacena en un fichero PGP llamado anillo de claves públicas. En cada entrada se guarda la identidad de un usuario, y su clave pública. Esta última tiene asociado un campo de legitimidad KEYLEGIT, que indica el nivel con que PGP confía que la clave es válida para este usuario; cuanto mayor sea su valor, indica más seguridad en que la clave pública pertenece al usuario. Este campo lo calcula PGP. Además, para cada entrada se mantienen una o más firmas que garantizan la validez del certificado. Otro campo OWNERTRUST señala la confianza en este usuario para firmar certificados.

Si un usuario inserta una nueva clave en su anillo de claves públicas, PGP debe asignar un valor al nivel de confianza en el propietario de la clave. Si es el propio usuario, se le asigna el máximo nivel de confianza. En caso contrario, se pide al usuario que asigne el nivel. Se puede indicar que el propietario es 'desconocido', 'poco fiable', 'medianamente fiable' o 'totalmente fiable'.

Cuando se introduce una clave pública, puede tener asociadas una o más firmas. Después pueden añadirse más firmas. Cuando se introduce una firma, PGP examina el anillo de claves para ver si el autor de la firma es conocido. Si es así, asigna el valor OWNERTRUST del usuario al campo SIGTRUST de la firma. En otro caso, le asigna el valor 'desconocido'.

El valor de la legitimidad de la clave se calcula a partir de las firmas asociadas. Si alguna de las firmas tiene la máxima fiabilidad, automáticamente la clave se considera probada. Si no, PGP hace un cálculo ponderado de los valores de confianza. Se da peso 1/X a las firmas totalmente fiables y peso 1/Y a las firmas medianamente fiables, donde X e Y son valores introducidos por el usuario. Si la suma llega a 1, la asociación usuario/clave se considera probada.

Para mantener la consistencia en el anillo de claves públicas, PGP recalcula periódicamente los valores de confianza.

ISOCOR

ISOCOR es un software de correo electrónico X.400 que proporciona servicios de seguridad sin necesidad de recurrir a otros productos adicionales.
Los servicios de seguridad proporcionados por ISOCOR son:

- Integridad de contenido
- Autentificación de emisor
- Confidencialidad del contenido
- No repudio del contenido por parte del emisor
- No repudio del contenido recibido
- No repudio de notificación EDI

Utiliza los siguientes algoritmos:

- DES ECB y DES CBC para cifrado simétrico
- RSA para cifrado asimétrico
- Funciones hash, simple MDC2, Doble MDC2 y Ripe MD.

Es ofertado en el mercado español por Informática El Corte Inglés.

4.2. PRODUCTOS PARA SERVICIOS INTERNET

La red INTERNET abre un mundo nuevo de oportunidades de negocio y servicio. A través de ella las organizaciones pueden publicitar y ofrecer sus productos o servicios adpatando sus técnicas de marketing al nuevo entorno y a los usuarios del mismo. INTERNET no sólo ofrece nuevas formas para hacer marketing de productos y servicios, sino que provee de nuevas herramientas que pueden revolucionar la forma en que se realizan las transacciones.

INTERNET es cada vez más un lugar idóneo para la actividad comercial, gracias a la simplificación y facilidad deuso que le confieren las nuevas herramientas de acceso como el *World Wide Web*. La disponibilidad de estas nuevas herramientas y a medida que la seguridad en la red va avanzando, hacen que cobre sentido la utilización por parte de las organizaciones tanto públicas como privadas, de una red de ámbito mundial como es INTERNET, en lugar del mantenimiento de redes privadas con unos altos costes y coberturas locales.

Una gran corporación, un organismo público, una pequeña empresa, etc, pueden ofrecer sus productos y servicios por medio de Internet, y todas ellas acceden a un medio común con las misma oportunidades de tal forma que en algunos casos, se puede llegar a minimizar el efecto de economía de escala a la que únicamente pueden acceder grandes organizaciones.

El efecto de INTERNET en los negocios y servicios, no afecta únicamente a la igualdad de oportunidades, sino que ofrece ventajas tales como el acceso a posibles clientes/proveedores en cualquier parte del mundo, lo que para algunas organizaciones podría significar la única oportunidad de vender sus productos o servicios fuera de su ámbito local. La posibilidad de acceso 24 horas al día, 365 días al año, proporciona unas oportunidades de negocio enormes desde cualquier aspecto comercial: Atención al cliente, venta, envío de software, información, etc.

Una de las aplicaciones más comunes en INTERNET es el soporte a clientes. Permite a los usuarios el envío de peticiones o preguntas vía correo electrónico y a las organizaciones ofrecer de hecho un servicio de soporte de 24 horas al día. Un aspecto conocido del soporte a clientes es que las preguntas suelen repetirse y los problemas con los que se encuentran los usuarios acostumbran a ser los mismos. En estos casos el correo INTERNET simplifica ernormemente el proceso de respuesta simplemente enviando los mismos mensajes a los diferentes usuarios. Otra ventaja es la rapidez de la respuesta que se puede obtener con respecto a métodos tradicionales.

Otro servicio muy extendido en INTERNET y que es perfectamente valido para el soporte a clientes son las 'cuestiones más frecuentes' conocidas como FAQ (*Frequent Asked Questions*). Estas preguntas más comunes, están presentes en la mayoría de los servidores WWW y GOPHER, por lo que la comunidad INTERNET está muy acostumbrada a usarlas y son de gran ayuda. En el caso de soporte a clientes, es una forma muy natural en INTERNET poner FAQ con la solución a los problemas más comunes.

La tendencia hacia sistemas distribuidos permitiendo a los usuarios acceder a la información desde cualquier punto de la red, obliga a desarrollar técnicas de seguridad para controlar el acceso a las redes. Las comunicaciones seguras mediante el WWW requieren que tanto el cliente como el servidor soporten los protocolos y las técnicas mediante las cuales se pueden proporcionar los servicios de seguridad.

NETSCAPE COMMERCE SERVER

Netscape Commerce Server es el software de un servidor que soporta comercio electrónico seguro en Internet así como en otras redes basadas en protocolos TCP/IP.
Protege las comunicaciones Internet proporcionando los servicios de confidencialidad, integridad de los datos y autenticación del servidor mediante certificados y firma digital, apoyándose para ello en el protocolo SSL anteriormente descrito.
Permite la publicación de documentos hipermedia utilizando el lenguaje *HyperText Markup Language* (HTML) y distribuirlos por la red Internet o bien por otras redes basadas en TCP/IP mediante el protocolo HTTP.
La comunicación segura requiere además que el cliente utilice un producto sensible al protocolo SSL como el *Netscape Navigator*.
Características:
- Compatible con el estándar HTTP; da servicio a todos los clientes HTTP.
- Seguridad integrada mediante el protocolo SSL que utiliza tecnología criptográfica de clave pública de *RSA Data Security*.
- Opciones avanzadas de autorización tales como autorización de acceso HTTP, control de acceso basado en IP y DNS, palabras de paso, etc.

IBM INTERNET CONNECTION SECURE SERVER

Se trata de un software de servidor Web orientado no sólo a la difusión de información sino también a la realización de transacciones comerciales.
Es el primer servidor Web que soporta los dos protocolos anteriormente comentados, SSL orientado a la protección de los mensajes y *Secure HTTP* orientado a la protección de las transacciones para prorcionar características tales como cifrado de la información, autenticación y gestión de claves.
La realización de transacciones seguras requiere, como es lógico, que el cliente disponga de *un browser* seguro como el *IBM Internet Connection Secure Web Explorer* que también soporta los dos protocolos anteriormente citados.

WEB SECURITY TOOLKITS

Terisa Systems que es una compañía lanzada por *Enterprise Integration Technologies* (EIT) y *RSA Data Security* distribuye un conjunto de herramientas para el desarrollo de aplicaciones WWW seguras (*Web Security Toolkits*). Estas herramientas incluyen una implementación del *Secure HTTP* para asegurar la autenticidad y la confidencialidad de las transacciones realizadas vía WWW e incorpora tecnología criptográfica de clave pública RSA.

4.3. PRODUCTOS GENÉRICOS DE SEGURIDAD

PRODUCTO HARDWARE/SOFTWARE CRYPT SE-500 (PENTA-3)

Proporciona servicios de seguridad tanto a correo electrónio como a EDI.
Puede ser utilizado para X.400 y para INTERNET, tanto si se utiliza PEM como si no.
Es una tarjeta que puede instalarse en cualquier PC que disponga de un slot de ampliación con bus ISA o MCA, pudiendo adaptarse también a otras arquitecturas.
Aplica los siguientes servicios de seguridad para X.400 y PEM:

- Control de acceso
- Autenticación de emisor
- Integridad de contenido
- Confidencialidad de contenido
- No repudio del contenido por parte del emisor
- No repudio del contenido recibido

Estos servicios de seguridad están disponibles por medio de API's escritas en lenguaje C, que permiten integrar el sistema en cualquier aplicación.
El cifrado se lleva a cabo a través de hardware utilizando un chip de alta velocidad de cifrado DES.
El mecanismo de firma digital está basado en el algoritmo standard de cifrado RSA en clave pública, implementando un procesador del tipo DSP, aunque también está disponible el estándar DSA.
El control de acceso de usuario se realiza a través de passwords que se almacenan en memorias de alta seguridad en la tarjeta. Para aquellas aplicaciones que lo requieran, se dispone también de control de accesos a través e tarjetas inteligentes, que llevan implementada la algorítmica RSA para autentificación y firma digital.

Este producto ofrece otras funcionalidades adicionales como:

- Generación aleatoria de claves

  Pueden ser generadas claves RSA de hasta 1024 bits de longitud

- Almacenamiento de claves

  Las claves son almacenadas de forma segura en memorias EEPROM y RAM, que se borran cuando se intentan leer de forma no autorizada.

  Sólo pueden ser leidas por el procesador y nunca podrán ser extraídas.

  Si se utiliza la tecnología de tarjeta inteligente, la clave RSA se almacenará en ellas y desde ellas se realizarán los procesos de firma digital y autenticación.

- Notaría de claves

  Las claves públicas son certificadas por la autoridad y se almacenan en certificados en dominio público, donde todos los usuarios del sistema tendrán acceso libre a ellas.

Este producto es ofertado en el mercado español por Penta-3, que además es su fabricante.

4.4. PRODUCTOS CORTAFUEGOS

Cuando se diseña una red local, que cuenta además con una conexión con el mundo exterior INTERNET, se recomienda que los usuarios de dicha red puedan acceder a la información de fuera, pero que nadie pueda acceder a los datos internos. Para conseguir este objetivo, se desarrollan los *firewalls*. Se puede considerar un *firewall* como un paso intermedio entre la red corporativa y la INTERNET pública.

Configurar un *firewall* conlleva la toma de decisiones aceca del tipo de accesos que mantendrán los usuarios de la red local en INTERNET, así como los accesos que tendrán desde fuera a datos de nuestra red, en el caso de que exista alguno. Esto requiere una planificación que abarca a diversos niveles de la organización.

El primer nivel de *firewall*, apropiado para redes pequeñas o donde un nivel máximo de seguridad no es necesario es un *router*. Estos dispositivos, pueden filtrar paquetes de información en base a unas reglas definidas. El *router* verifica la información de cabecera de los paquetes y decide si debe enviarlos a través de la red corporativa. Este filtro permite evitar que ordenadores fuera de nuestra red puedan enviar comando de control. Por ejemplo, se puede definir que los paquetes SNMP (*Simple Network Management Protocol*) puedan ser enviados exclusivamente por el proveedor de conexión o el administrador local, o que una sesión TELNET pueda ser iniciada por un usuario interno pero no externo, o que un acceso FTP pueda ser realizado desde el exterior pero no desde un puesto local. Un *router* es capaz de efectuar estos tipos de control de acceso, pero a su vez, permitir el paso a la red corporativa de todos los paquetes que cumplan con estas reglas.

Para redes de mayor tamaño y donde se requieran mayores niveles de seguridad, es más recomendable la utilización de un *cortafuegos* dedicado que sea capaz de gestionar todo el tráfico de entrada/salida dela red corporativa. En un sistema de *cortafuegos* dedicado, se puede especificar individualmente los usuarios que pueden accedera a INTERNET y además no permite que nadie desde fuera pueda acceder directamente a la red corporativa, sino que siempre se encuentren primero con el cortafuegos.

Los sistemas de *cortafuegos* dedicados se implementan en el nivel 7 de OSI (nivel de aplicación) de TCP/IP y requiere que se establezca la seguridad para cada aplicación, en consecuencia, para cada nueva aplicación la configuración del *cortafuegos* debe ser actualizada. Los sistemas externos establecen conexión con el *cortafuegos* y hacen sus peticiones de servicio, el *cortafuegos* se encarga de trasladar dichas peticiones al servidor INTERNET de la red.

Los sistemas de *cortafuegos* dedicados son recomendables en redes medias a relativamente grandes, ya que un *cortafuegos* puede ocasionar un cuello de botella en casos de tráfico intensivo en redes muy grandes.

Los servidores públicos de INTERNET, como los WWW pueden ser conectados directamente a la red corporativa o conectados separadamente a INTERNET. Separar los servidores públicos de la red privada ofrece el mayor nivel de seguridad posible, pero puede resultar un inconveniente: que el acceso desde la red privada al servidor público se realice a través de INTERNET en lugar de la conexión en red local.

La utilización de *cortafuegos* no es un substituto de la seguridad interna de la red y se debe tener en cuenta que en muchas ocasiones los problemas de seguridad son provocados desde las redes y usuarios corporativos. Los *cortafuegos* son únicamente buenos complementos a la seguridad ya implantada en la red local.

INTERNET CONNECTION SECURED NETWORK GATEWAY FOR AIX

En líneas generales proporciona los siguientes servicios:

- Proporciona una interfaz segura entre la red privada corporativa y redes externas como Internet.
- Permite prevenir el intercambio de información de forma indiscriminada entre los usuarios internos y el exterior.
- Protege la red de ataques del exterior, especialmente de intrusos provenientes del mundo Internet.
- Permite definir quién tiene acceso a la red desde Internet y quién desde dentro tiene acceso a Internet. También permite controlar qué aplicaciones TCP/IP se pueden utilizar cuando se accede de una red a otra.
- Securiza la información en su paso a través de redes públicas.
- Permite controlar el tráfico según las direcciones IP, los usuarios o los servicios de aplicación dependiendo de cómo se haya diseñado la política de seguridad.

Sus características más destacadas son las siguientes:

- Cifrado: La confidencialidad se asegura en el flujo de información a través de redes públicas entre dos cortafuegos, mediante el cifrado de los paquetes IP que permite crear un *túnel* privado.
- Alarmas: Permite la activación de eventos y la generación de notificaciones en tiempo real al administrador de la red.
- Capacidades de filtro: Los filtros son transparentes a los usuarios y permiten denegar el acceso a puntos específicos de la red corporativa. Se utilizan para controlar el flujo de los paquetes al origen o destino IP, puertos y respuestas TCP, etc.
- *Application gateway proxy*: Por medio de Telnet o de FTP el usuario puede acceder al gateway donde autentica su identidad. Tras este proceso el cortafuegos permite que el usuario lance cualquier aplicación TCP/IP a la que tenga acceso autorizado. Todos los paquetes que fluyen desde el cortafuegos llevan la dirección IP del mismo como dirección de origen de tal forma que el cortafuegos oculta al mundo exterior las direcciones IP de la red interna. También permite conceder derechos en base a usuarios en lugar de basarse en direcciones IP.
- Servidor de dominio: Presenta la red corporativa al mundo Internet como un dominio. El mundo exterior no puede ver la estructura de la red ni los nombres ni direcciones de los hosts internos.
- Servicio de correo electrónico: Permite el envío de correo electrónico a un servidor de correo dentro de la red segura.
- Autenticación: Ofrece diversos mecanismos de autenticación.

5. ASPECTOS LEGALES

5.1. ASPECTOS NORMATIVOS.

5.1.1. La Ley Orgánica 5/1992 de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD)

Los medios informáticos, en el sentido más amplio de la expresión para abarcar técnicas electrónicas, informáticas y telemáticas, constituyen instrumentos idóneos para la generación de actos y negocios jurídicos en masa, facilitando la realización de transacciones comerciales, así como el intercambio de documentos mediante sistemas de comunicación electrónica. La aparición y difusión de las nuevas tecnologías en la convivencia diaria de los ciudadanos, en las relaciones comerciales, con las administraciones, etc, hace que, en muchas ocasiones, los conceptos jurídicos tradicionales resulten poco idóneos para interpretar las nuevas realidades, a la vez que es necesario desde un punto de vista jurídico el reconocimiento formal de estos nuevos medios, de forma que no se produzca una disociación entre normativa y realidad.

El uso del correo electrónio y del EDI como instrumentos para la realización de comercio electrónico plantea numerosos y complejos problemas jurídicos, relacionados con las garantías generales de la utilización de soportes, medios y aplicaciones electrónicas, informáticas y telemáticas, y que se ponen de manifiesto tanto en el plano privado como en el público, en lo que se refiere al negocio jurídico y al documento electrónico, especialmente en relación con la forma y la prueba, así como en relación a la conservación, copias y almacenamiento de los documentos en general.

La globalidad de procesos o aplicaciones informáticas que se llevan a cabo con los datos almacenados y que son susceptibles, si llegan a conectarse entre sí, de configurar el perfil personal que, sin duda, pertenece a la esfera privada de las personas, justifica la necesidad de una nueva frontera para la intimidad y el honor.

Por lo que los aspectos de seguridad aparecen como un factor relevante, tanto durante el proceso de la comunicación, como a posteriori, cuando la información intercambiada, o las transacciones realizadas, quedan almacenadas en algún soporte, como, por ejemplo, un disco duro de un servidor de correo electrónico.

La Ley Orgánica 5/1992 de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD) concibe la seguridad informática como la suma de cuatro conceptos más precisos que son, *confidencialidad,* entendida como el acceso permitido a usuarios autorizados, *veracidad,* referida a datos verídicos y actuales, *integridad* para evitar alteraciones y usos indebidos y finalmente *disponibilidad* para la utilización por los usuarios en el momento en el que estén autorizados. La Ley está animada por la idea de implantar mecanismos cautelares que prevengan las violaciones de la privacidad que pudieran resultar del tratamiento de la información. Por esto define pautas a las que debe atenerse la recogida de datos, pautas encaminadas a garantizar tanto la veracidad de la información contenida en los

datos almacenados, cuanto la congruencia y racionalidad de los datos. Este principio, verdaderamente cardinal, de la congruencia y la racionalidad, garantiza que los datos no puedan ser usados sino cuando lo justifique la finalidad para la que han sido recabados.

Aunque existe una mención al correo electrónico en la consideración Número 6 de la Exposición de Motivos de la Ley que aparece, más bien, como consecuencia de la innovación y de la evolución tecnológica y como objeto de regulación posterior, la LORTAD no incluye una mención específica en su articulado a la seguridad en las comunicaciones, si bien ésta debe considerarse implícitamente contemplada en el contexto general de la ley.

Esta consideración se debe a que la LORTAD introduce *el concepto de tratamiento de datos*, concibiendo los ficheros desde una perspectiva dinámica. No los entiende por tanto como un mero depósito de datos, sino como una globalidad de procesos o aplicaciones informáticas que se llevan a cabo con los datos almacenados y que son susceptibles, si llegasen a conectarse entre sí, de configurar el perfil personal del afectado.

En este sentido, la Ley entiende el tratamiento de datos como el conjunto de operaciones y procedimientos técnicos, de carácter automatizado o no, que permiten la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

En consecuencia, dentro de la globalidad de los procesos y aplicaciones informáticas que se llevan a cabo con los datos almacenados, puede considerarse que se encuentra la transmisión de los mismos por vías telemáticas y, más específicamente, por medio del correo electrónico, o mediante EDI, que por lo que aquí nos interesa se puede apoyar en el correo electrónico. Máxime cuando vía EDI pueden realizarse transacciones de comercio electrónico que entre sus datos incluyan datos de carácter personal.

Ahondando en los aspectos del comercio electrónico son de destacar las disposiciones relativas a la transmisión internacional de datos. Así la Ley transpone la norma del art. 12º del Convenio 108 del Consejo de Europa. La protección de la integridad de la información personal se concilia con el libre flujo de los datos, que constituye una auténtica necesidad de la vida actual, de la que las transferencias bancarias, las reservas de pasajes aéreos o el auxilio judicial internacional son ejemplos de práctica diaria. La condición exigida es la de que el país de destino cuente en su ordenamiento con un sistema de protección equivalente al español, si bien permitiendo la autorización de la Agencia de Protección de Datos cuando tal sistema no exista, pero se ofrezcan garantías suficientes. Con ello se adecúa a instrumentos internacionales como los Acuerdos de Schengen o las futuras normas comunitarias.

Finalmente es de interés recordar aquí el Real Decreto 1332/1994, de 20 de junio por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal.

5.1.2. La Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, Ley 30/92.

En nuestra legislación, la Ley 30/92 de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común constituye una decidida apuesta por la abierta incorporación de las técnicas electrónicas, informáticas y telemáticas a la actividad administrativa y, en especial, a las relaciones entre los ciudadanos y las Administraciones Públicas. Así, el artículo 45 se convierte en la verdadera piedra angular del proceso de incorporación y validación de dichas técnicas en la producción jurídica de la Administración Pública, así como en sus relaciones con los ciudadanos, admitiendo expresamente la validez de los documentos emitidos por medios telemáticos, informáticos o electrónicos y permitiendo la relación de los ciudadanos con la administración mediante los citados medios.

El desarrollo reglamentario del artículo 45º se realiza por medio del Real Decreto 263/1996 de 16 de febrero, BOE 29/02/96, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estadoy pretende delimitar en el ámbito de la citada Administración las garantías, requisitos y supuestos de utilización de las técnicas electrónicas, informáticas y telemáticas, prestando especial atención a recoger las garantías y derechos de los ciudadanos frente a la Administración cuando ésta utiliza dichas técnicas, sin dificultar su implantación y exigiendo cautelas o requisitos adicionales a los que, con carácter general o de forma específica, vienen establecidos en nuestro ordenamiento jurídico.

Esta atención se pone especialmente de manifiesto en el artículo 4º del desarrollo reglamentario por el que se obliga a adoptar las medidas técnicas y de organización necesarias para asegurar la confidencialidad, integridad y disponibilidad de la información. Estas medidas deberán garantizar la restricción de la utilización del acceso a los datos a las personas autorizadas, la prevención de alteraciones o pérdidas de los datos e informaciones y la protección de los procesos informáticos frente a manipulaciones no autorizadas.

5.1.3. Directiva del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

La Directiva 95/46/CE del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, de 24 de octubre de 1995 (DOCE 23/11/95), en su artículo 17, párrafo primero, incluye una referencia expresa a la protección de datos cuando se transmiten por redes de comunicaciones.

Art. 17 Seguridad del tratamiento

1. Los estados miembros dispondrán la obligatoriedad por parte del responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas, necesarias

para la protección contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizado, **en particular cuando el tratamiento incluya la transmisión de datos dentro de una red**, y contra cualquier otro tratamiento ilícito de datos personales.

Dichas medidas deberán garantizar, habida cuenta de los progresos técncicos y del coste de su aplicación, un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse.

2. Los Estados miembros dispondrán que el responsable del tratamiento, en caso de tratamiento por cuenta propia, elija un encargado del tratamiento que reuna garantías suficientes sobre las medidas de seguridad técnica de los tratamientos que deban efectuarse, se asegure de que se cumplen dichas medidas.

3. La realización de tratamientos por cuenta de un encargado deberá estar regulada por un contrato u otro acto jurídico que le vincule con el responsable del tratamiento, y que disponga, en particular:

   - que el encargado del tratamiento actúa sólo siguiendo instrucciones del responsable del tratamiento;
   - que las obligaciones del apartado 1, tal y como las define la legislación del Estrado miembro en el que esté establecido el encargado, incumben también a este.

4. A efectos de conservación de la prueba, las partes del contrato o acto jurídico relativas a la protección de datos y a los requisitos relativos a las medidas a que hace referencia el apartado 1 constarán por escrito o en otra forma equivalente.

Esta directiva constituye un importante paso adelante en las actuaciones de seguridad en el ámbito de la Unión Europea desde que el Consejo de Ministros aprobara el 31 de marzo de 1992 (DOCE 8/5/92) la única hasta la fecha Decisión Europea relativa a la Seguridad de los Sistemas de Información, cuyo preámbulo establece la necesidad de desarrollar estrategias que permitan la libre circulación de la información en el mercado único, pero garantizando al mismo tiempo la seguridad de utilización de los SI en toda la Unión.

Por otra parte, la Unión Europea a través del programa TEDIS (*Trade Electronic Data Interchange Systems*) ha perseguido armonizar las legislaciones de los Estados Miembros para facilitar el intercambio electrónico de documentos comerciales, siendo consciente de la necesidad de cambiar unos sistemas jurídicos que fundan sus medios de prueba, muy especialmente, sobre la escritura.

5.1.4. Legislación civil y mercantil.

En la legislación mercantil se observan ciertos preceptos o usos que sugieren la necesidad de unos procedimientos de seguridad informática. Así, el actual Código de Comercio, la Ley de Sociedades Anónimas y el Reglamento del Registro Mercantil permiten la utilización de procedimientos informáticos para la llevanza de los libros, y establecen la obligatoriedad de conservarlos, junto con su documentación y sus justificantes, durante seis años.

No es por tanto una 'obligatoriedad' de desarrollar sistemas de seguridad informática, pero sí es una 'recomendación tácita', con el fin de poder hacer frente a posibles inspecciones, auditorías o requerimientos judiciales. La desaparición de los archivos puede suponer caer en sanciones pecuniarias por no seguir los preceptos mercantiles.

Los asesores jurídicos recomiendan a las compañías de software que incorporen una claúsula explícita de responsabilidad subsidiaria de la empresa usuaria por hechos ilícitos cometidos por sus empleados.

El 7 de julio de 1.994 fue publicada la Ley reguladora de la responsabilidad civil por los daños causados, que adapta el Derecho Español a la Directiva 85/374/C.E.E., que establece responsabilidades objetivas de los fabricantes e importadores, con multas de hasta diez mil quinientos millones de pesetas; en el mismo sentido se espera la promulgación de una Ley referente a responsabilidades de los prestadores de servicios, en relación con las cuales existe una propuesta de directiva, que motivará un espectacular incremento de los sistemas de seguridad informática en cualquier empresa que preste servicios por medios telemáticos o informáticos.

5.1.5. Código Penal.

La Ley Orgánica 10/1995, de 23 Noviembre, que aprueba el nuevo Código Penal en vigor desde el 23 de Mayo de 1996, tipifica delitos y faltas que puedan cometerse utilizando medios informáticos, concretamente los que se refieren a la Intimidad, Patrimonio y socioeconómicos, y Propiedad Intelectual.

En el Título X, "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", en su Capítulo 1º, Del descubrimiento y revelación de secretos, asigna penas "al que para descubrir secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, **mensajes de correo electrónico** o cualesquiera otros documentos o efectos personales, o **intercepte sus telecomunicaciones**, o utilice **artificios técnicos de escucha, transmisión, grabación o reprodución de sonido o de la imagen**, o de cualquier otra señal de **comunicación**...".

"... al que **sin estar autorizado**, se apodere, utilize o modifique, en perjuicio de terceros, **datos reservados de carácter personal** o familiar de otro que se hallen registrados en ficheros o soportes magnéticos, electrónicos o telemáticos...".

También se penaliza **la difusión, revelación o cesión a terceros de los datos o hechos descubiertos o las imagenes captadas**.

Significativa es la penalización a "... **las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros**".

En concordancia con la LORTAD respecto a los datos especialmente protegidos, se asignan penas **a los que revelen ideología, religión, creencias, salud, origen racial o vida sexual**.

En el Capítulo XI, "De los delitos relativos a la Propiedad Intelectual e Industrial, al mercado y a los consumidores", en la Sección 1ª, De los delitos relativos a la propiedad intelectual, se penaliza a "**También se consideran reos de estafa los que, con animo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consiguen la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero**".

Será objeto de pena "**El que hiciere uso de cualquier equipo terminal de telecomunicación**, sin consentimiento de su titular" ... "**Causar daños mediante la destrucción, inutilización o alteración o cualquier otro modo que dañe los datos, programas o documentos electrónicos ajenos, contenidos en redes, soportes o sistemas informáticos**".

Se tipifica el delito de "**la fabricación, puesta en circulación y tenencia de cualquier medio específicamente destinado a facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger Programas de ordenador**".

En el mismo Capítulo, en la Sección 3ª, De los relativos al mercado y a los consumidores, se castiga "el que **con intención de descubrir un secreto de empresa se apodere por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos**...", como asimismo "el **que encubre, ocultando, alterando o inutilizando el cuerpo, los efectos o los instrumentos de un delito, para impedir su descubrimiento**".

En cuanto a las penas que se imponen al infractor, son las prisión y oscilan entre:

De 1 a 5 años, por interceptación de datos y/o su divulgación.

De 3 a 5 años, si lo delitos son realizados por los responsables de los ficheros.

De 2 a 4 años, si se apoderan y divulgan secretos de la empresa.

Estas penas irán acompañadas de multas de carácter económico basado en el sistema de dias multa, oscilando en un mínimo de 200.- pts/dia y un máximo de 50.000.- pts/dia, siendo los periodos:

De 6 a 12 meses, importe mas bajo (6 m.) de 36.000.- a 72.000.- pts, y el importe mas alto (12 m.) de 9.000.000.- a 18.000.000.- pts.

De 12 a 24 meses, importe mas bajo (12 m.) de 72.000.- a 144.000.- pts, y el importe mas alto (24 m.) de 18.000.000.- a 36.000.000.- pts.

5.2. COMERCIO ELECTRÓNICO

5.2.1. Comercio electrónico y contratación

En el caso de realizarse comercio electrónico vía EDI es necesario establecer 'acuerdos de intercambio' o contratos-tipo entre las partes en cuestión que otorguen valor vinculante a los mensajes EDI, siempre que conste la clave de identificación. Un caso concreto de contrato tipo es el Modelo Europeo de Acuerdo de EDI (DOCE, 28/12/94) que consta de 14 artículos que se refieren a los siguientes aspectos:

1. Objeto y ámbito de aplicación
2. Definiciones
3. Validez y formato del contrato
4. Admisibilidad como prueba de los mensajes de EDI
5. Procesamiento y acuse de recibo de los mendajes de EDI
6. Seguridad de los mensajes de EDI
7. Confidencialidad y protección de los datos personales
8. Registro y almacenamiento de los mensajes de EDI
9. Requisitos para la explotación del EDI
10. Especificaciones y requisitos técnicos
11. Responsabilidad
12. Resolución de litigios
13. Derecho aplicable
14. Efecto, modificaciones, duración y separabilidad.

Un caso particular del comercio electrónico especialmente relevante es la contratación electrónica. Existe un evidente apoyo al desarrollo de los sistemas de contratación electrónica, tanto de las instancias institucionales, Unión Europea, Estado Central, Autonomías, etc, como de las empresas. Por parte de distintos organismos se han creado varios contratos-tipo que prevén los posibles riesgos jurídicos.

El contrato existe desde que hay acuerdo de voluntades. En el contrato en tráfico mercantil la perfección es desde la emisión de la aceptación (art.54 del Código de Comercio para contratos por correspondencia). En la contratación electrónica se suele establecer como momento de perfección de los contratos, el instante de la recepción de la aceptación, por la buena fe mercantil y la velocidad de la transmisión.

Este tipo de transacciones plantean diversos problemas legales que determinan actuaciones de seguridad informática encaminadas a evitar su producción:

- Validez de la forma de celebración
- Comprobación de identidades
- Garantizar la fiabilida de la transmisión y de su contenido.
- Aspectos procesales.

En cuanto a la forma de celebración existe libertad de forma en nuestro ordenamiento jurídico (art. 251 del Código de Comercio y 1.278 y 1.279 del Código Civil), y el Tribunal Supremo admite la obligatoriedad de los contratos con independencia de su forma a excepción de ciertos contratos (la mayoría inmobiliarios) que exigen la forma escrita, e incluso su formalización en escritura pública e inscripción en el Registro.

Es válida la celebración de contratos por medios informáticos con independencia de la existencia de un escrito.

La dificultad reside en la prueba. Deben preverse dichas contingencias en los contratos que celebren las partes, siendo de gran importancia pactar que ambas partes admitirán como documentos válidos los '*outputs*' del sistema, aspectos en los que profundizaremos en el apartado 5.2.3.

Hoy en día puede decirse que ante la carencia de una regulación normativa adecuada, los empresarios europeos han asumido voluntariamente el valor probatorio de las transferencias y los negocios jurídicos concertados por medio del EDI.

5.2.2. Identificación de las partes.

Como premisa general partimos del hecho de que toda persona tiene derecho a firmar cualquier información. Dentro del ámbito más especifico de la realización de operaciones por las cuales se contraen obligaciones y derechos (comercio, contratación) la firma cumple la doble función de ser, por un lado, el signo principal de la voluntad de obligarse y, por otro, de constituir el signo personal de identificación.

En el documento en papel se reconocen fácilmente sus componentes, que son el soporte, es decir la hoja de papel, el texto e imágenes que constituyen la representación física de la información y la información referente al originador, con el fin de comprobar la autenticidad, que normalmente se materializa en una firma. Todos estos componentes son solidarios en virtud del papel que soporta la información , constituyendo una combinación *no modificable* y duradera.

Los documentos en papel, por tanto, reciben normalmente los signos de autenticidad mediante la firma, de forma que el lector puede así confiar en que la información sobre el originador es correcta.

En los documentos electrónicos el soporte, el texto y la firma no están relacionados mutuamente de la misma forma *solidaria* y duradera que en el documento en papel. Además la manipulación de un registro digital se efectúa alterando una configuración de bits, modificación que no deja huella y, por otra parte, el control de autenticidad visual que un individuo efectúa, a menudo de forma inconsciente, sobre un documento en papel no tiene equivalente en el área de los servicios electrónicos de información.

Como sucede con la firma manuscrita, toda persona tiene derecho a utilizar una firma digital. Con el fin de comprobar la firma del originador aparece el concepto de habilitación, que se refiere a la facultad del originador para firmar una determinada información, documento o transacción. El proceso de comprobación de la firma se realizará en dos etapas, que serán la comprobación formal de la firma y la comprobación de la habilitación del remitente, que se puede lograr mediante el uso de un certificado añadido al documento que se firma.

Por tanto, la firma digital es una analogía electrónica de la firma manuscrita y presenta características también análogas:

- El receptor debe ser capaz de validar la firma del transmisor.
- La firma no debe ser falsificable.
- El transmisor de un mensaje firmado no debe poder repudiarlo posteriormente.

En la práctica jurídica los requisitos funcionales y de seguridad de la firma manuscrita varían de forma que esta puede servir para indicar una expresión de voluntad, para indicar que el firmante ha concluido su hilo de pensamiento; en unos caso la autenticidad de la firma puede ser evidente y en otros debe poder demostrarse; hay otros casos en los que se puede exigir un certificado, o se requiere la firma de varias personas o una fe pública.

Así, desde la perspectiva del pensamiento jurídico, para facilitar la transición desde la firma manuscrita a la firma digital, la implantación técnica de esta última debe ajustarse todo lo posible a los requisitos funcionales tradicionales de la primera; es decir todas las funciones de la firma manuscrita deben aplicarse también a la firma digital.

Las nuevas formas de identificación personal tales como la firma digital tienen validez jurídica completa; sin embargo, la validez queda desvirtuada judicialmente ante una negativa del presunto interviniente, que conllevaría pruebas periciales para su identificación.

Puesto que las partes contratantes pueden quedar obligadas por mensajes enviados por personas no autorizadas, es conveniente que se establezca el sistema de responsabilidades en el acuerdo de intercambio, incluyendo, por ejemplo, solicitud de confirmación para evitar

errores, y, por supuesto, establecer sistemas de seguridad físicos y lógicos que impidan tales acciones.

Hay que tener en cuenta que en base a la doctrina de la representación aparente, existe una comunicación con una clave que constituye una manifestación de voluntad, además la buena fe mercantil y la seguridad del tráfico hacen que la negligencia del emisor, como por ejemplo no guardar correctamente la clave o equivocarse, no sea imputable al receptor.

5.2.3. Seguridad, confidencialidad y protección de datos de carácter personal.

El Modelo Europeo de Acuerdo de EDI contempla los aspectos de seguridad de los mensajes EDI, así como los aspectos de confidencialidad y datos personales en los artículos 6º y 7º respectivamente.

En relación a la seguridad de los mensajes EDI, las partes se han de comprometer a aplicar y mantener procedimientos y medidas que se deberán de aplicar de forma obligatoria a todos los mensajes EDI para garantizar la protección de los mismos frente a amenzas tales como, acceso no autorizado, modificación no autorizada, denegación del servicio o demora, destrucción de la información o pérdida de la misma. Este conjunto de procedimientos y medidas de seguridad que han de aplicar las partes del contrato, debe incluir *autenticación* de entidades, *integridad* del mensaje, *no repudio* de origen y destino y la *confidencialidad* de los mensajes de EDI. Además queda abierta la posibilidad de especificar expresamente procedimientos y medidas de seguridad complementarias en un Anexo Técnico del contrato.

En relación a la confidencialidad según este modelo de acuerdo, las partes se han de comprometer a mantener en secreto y a no revelar, ni transmitir a personas no autorizadas, ni a utilizar para fines distintos de los previstos información confidencial, porque así lo haya especificado el remitente o lo hayan acordado mutuamente las partes. La información mantiene el grado de confidencialidad en ulteriores transmisiones. En lo relativo al uso de algún método de cifrado para proteger ciertos mensajes, el modelo se remite a posibles disposiciones relacionadas en los respectivos paises.

En relación a la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, las partes han de acordar como criterio mínimo, respetar lo dispuesto en el Convenio del Consejo de Europa en el intercambio de mensajes EDI que contengan datos personales con paises en los que no exista legislación de protección de datos, y hasta el momento en que se aplique una legislación comunitaria pertinente.

Un aspecto importante es el del valor probatorio de los mensajes EDI en caso de litigio. En este aspecto el Modelo Europeo de Acuerdo de EDI en su artículo 4º se refiere a la admisibilidad como prueba de los mensajes EDI. Así, según este modelo de contrato, en la medida que lo permita la legislación nacional aplicable a las partes, en caso de litigio los registros de los

mensajes EDI que hayan mantenido serán admisibles ante los tribunales y constituirán prueba de los hechos que en ellos figuren salvo que se aporte prueba de lo contrario.

En relación a la validez como prueba de los mensajes EDI, se pueden realizar algunas observaciones. La información en soportes informáticos tiene la validez que se otorga a cualquier otro documento privado que consta en poder de una parte. Por tanto, en general, se admite la validez del soporte informático como medio de prueba, pero sometido a la valoración del juez. Sin embargo, la facilidad para alterar los mensajes, tanto de EDI como de fax, y el encontrarse estos en posesión de una de las partes dificultan la valoración de la prueba.

En relación con esta última observación viene al caso el apartado primero del artículo 8º del modelo de acuerdo, Registro y almacenamiento de mensajes EDI, que dispone que cada una de las partes deberá conservar un registro cronológico completo de todos los mensajes EDI intercambiados en el curso de una transacción comercial, sin modificar y debidamente protegidos, de conformidad con los plazos y especificaciones previstos por las disposiciones legales de su Derecho interno, y en cualquier caso durante un período mínimo que será de tres años si no se especifica otro mayor.

Además y según el apartado segundo del mismo artículo 8º, por un lado el remitente deberá almacenar los mensajes EDI en el formato en el que los haya transmitido, y, por otro lado, el receptor en el formato en el que los haya recibido.

Finalmente cabe destacar los esfuerzos armonizadores y normativos que en este sentido se están llevando a cabo en Europa. Así, la Recomendación R(81) 20 del Consejo de Ministros del Consejo de Europa, intenta armonizar las legislaciones comunitarias respecto a admitir el microfilm y los soportes informáticos como medio de prueba en los procesos judiciales. Por otro lado, en nuestro país, en el campo del derecho público, *la Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, Ley 30/92*, ha reconocido plenamente respecto de los actos de la Administración, su posibilidad de manifestarse y documentarse por medios informáticos teniendo, a todos los efectos valor probatorio (Art. 45).

5.2.4. Seguridad procesal

Existen grandes dificultades para establecer pruebas fiables ante un tribunal. Las partes pueden someterse libremente a la Ley y Tribunales elegidos por ellas mismas, caso de los contratos internacionales. El modelo de acuerdo de EDI al que ya nos hemos referido anteriormente en su artículo 12º, Resolución de litigios, presenta como alternativas una claúsula de arbitraje y una claúsula de jurisdicción. En el caso de esta última, en caso de litigio, las partes se someterán a los tribunales que se hayan especificado en el acuerdo, que serán los únicos competentes.

La armonización internacional de los intercambios informáticos de información, especialmente en el ámbito de la Unión Europea debido a la libre circulación de personas, bienes, servicios y capitales, se plantea como una cuestión esencial para disponer de seguridad jurídica.

5.2.5. Modelo Europeo de Acuerdo de EDI

(Diario Oficial de las Comunidades Europeas, 28 de diciembre de 1994, nº L 338/100 y siguientes.)

6. POLÍTICAS Y ADMINISTRACIÓN DE SEGURIDAD DEL CORREO ELECTRÓNICO

6.1. INTRODUCCIÓN

La protección de la información puede ser definida como un proceso dirigido a preservar la integridad, confidencialidad, y disponibilidad de los sistemas de información. El principal reto debe ser encontrar el punto de equilibrio entre los riesgos posibles, la probabilidad de que sucedan y los elevados costes de su prevención. Para ello el Análisis y la Gestión de Riesgos permiten cuantificar y priorizar los requerimientos de seguridad.

Sería utópico pensar que el proceso se reduce a instalar productos de seguridad e implantar procedimientos. El **factor humano** es el elemento decisivo en el éxito o fracaso de una política de seguridad. La mayoría de problemas relacionados con la seguridad provienen de acciones personales, por lo que un perfecto conocimiento de la organización debe ser el objetivo más importante en cualquier programa de seguridad.

Por ello, entre el abanico de posibilidades que se le brindan a una compañía para salvaguardar su información, quizá la más importante sea crear una atmósfera que promueva la lealtad, la ética y la satisfacción laboral. Los empleados deben ser conscientes de la necesidad de preservar la información y de las consecuencias que acciones inapropiadas en este sentido pueden ocasionar a la compañía.

Las empresas cada vez más identifican la información y los sistemas de proceso de la información como puntos críticos de la organización. Esto lleva a proteger esta información de pérdidas, modificaciones, difusión no autorizada y falta de disponibilidad.

6.2. ASPECTOS ORGANIZATIVOS

6.2.1. Aspectos previos

En muchas compañías, la necesidad de realizar un programa de seguridad únicamente aparece después de verse afectadas sus instalaciones por algún incidente. Además, la primera y única respuesta consiste en asignar a una persona la tarea de implementar seguridad en el sistema, habitualmente en forma de control de acceso a los recursos.

Lógicamente, esta persona se encuentra muy pronto en serias dificultades: necesita saber qué información proteger, qué grado de protección debe dar a esa información, quién puede acceder a esa información, quién puede cambiar esa información, etc... Mientras se deciden

estas cuestiones, la implementación de la seguridad puede llevar varios años. Incluso, en el peor de los casos, algunas organizaciones creen que han protegido su información en el momento en que han instalado un software de seguridad.

Si se busca el éxito en un programa de protección de la información, no se debe buscar implantar soluciones hasta que no se hayan acordado unos objetivos en materia de seguridad, se identifiquen las necesidades propias del negocio y se asignen las responsabilidades en la gestión de la seguridad. Esta gestión de la seguridad debe quedar recogida formalmente en una política a seguir, sustentada en unos requerimientos mínimos (estándares) que identifiquen los valores corporativos de la información. El conjunto de políticas y estándares son la base fundamental de un programa efectivo de protección de la información.

La apertura y la protección son requerimientos parcialmente contradictorios, que necesitan ser reconciliados dependiendo de las circunstancias específicas. Sólo después de haber alcanzado un acuerdo global y una aceptación general por los usuarios estaremos en disposición de decidir la opción tecnológica mas conveniente.

6.2.2. Elementos de un programa de protección de la información

En cualquier organización, un programa de protección de la información debe contemplar los siguientes elementos:

- **Políticas.** Contemplan una descripción de objetivos y estrategias.

- **Estándares.** Recogen requerimientos más específicos para la consecución de los objetivos marcados. Deben ser suficientemente generales para su amplia aplicación, pero lo suficientemente concretos para poder ser contrastados y evaluados.

- **Guías.** Incluyen recomendaciones sobre cómo sintonizar con los estándares establecidos.

- **Procedimientos.** Detallan paso a paso formas de conseguir un resultado final. Los procedimientos son a menudo establecidos con el fin de satisfacer requerimientos de control y deben ser seguidos cuidadosamente para proporcionar el nivel de control requerido.

Las guías y procedimientos son frecuentemente implementaciones específicas de las políticas y estándares. Son necesarios cuando varían los equipos, el software y el entorno proporciona diferentes vías para satisfacer los requerimientos de control. Las guías contemplan sugerencias y no son estrictas. Por el contrario, los procedimientos deben ser seguidos escrupulosamente y estar sujetos a permanente revisión por parte de la dirección.

Hasta este punto, se ha mantenido en un segundo plano el enfoque técnico. Indudablemente, cualquier planificación enfocada a la protección de la información finalmente desemboca en la gestión y administración de mecanismos de seguridad tales como contraseñas, control de accesos y recursos, cifrado de datos, alarmas y notificaciones a los administradores, etc... No obstante, la información y no la tecnología debe ser el punto central de trabajo.

La solución técnica adoptada es un hecho puntual, mientras que la naturaleza y velocidad de los cambios tecnológicos y organizacionales nos llevan irremediablemente a una protección de la información dinámica y flexible. Las características y objetivos deben ser revisados y modificados tan pronto como los cambios lo requieran.

6.2.3. Responsabilidades de la seguridad

Para la gestión adecuada de todos estos recursos, de forma que se garantice la seguridad del sistema, es necesario disponer de una estructura funcional, en base a la asignación de responsabilidades, que podemos estructurar en:

- **Alta Dirección**. Establece y mantiene los presupuestos, personal y procedimientos para asegurar el cumplimiento de la política y su adecuación a los costes.

- **Administradores de seguridad de sistemas**. Implementan estándares y aseguran su cumplimiento para cada sistema sobre el que tienen asignada responsabilidad.

- **Usuarios finales**. Comprende a todas las personas que tienen acceso a los sistemas corporativos y son requeridos en el cumplimiento de los procedimientos recogidos en la política de seguridad.

6.3. PRIVACIDAD DE LA INFORMACIÓN

6.3.1. Privacidad de la información

La mayoría de las personas tiene una idea intuitiva de lo que la privacidad viene a significar, pero puede ser contemplada desde dos vertientes:

- Un derecho a permanecer invulnerable a los intrusos.
- Un derecho a decidir qué información personal debe ser comunicada y a quién.

Sin embargo, todos estamos de acuerdo en que una compañía debe velar por sus intereses. Alguien puede necesitar, por ejemplo, recuperar la correspondencia de sus empleados en ciertos casos legítimos:

- Localizar mensajes perdidos.
- Asistir a los empleados, a petición suya o con su consentimiento, en el desarrollo de sus tareas cuando se encuentran fuera del puesto de trabajo.
- Analizar la efectividad del sistema de correo electrónico.
- Iniciar una investigación.
- Asegurar que los recursos están siendo utilizados con fines laborales y no con fines personales.

Aquí cabe preguntarse si la privacidad en un correo electrónico puede equipararse a un correo ordinario. Sinceramente creemos que no. Cada organización debe establecer sus propios límites, de acuerdo con sus objetivos y estrategias.

6.3.2. Directrices de privacidad

En materia de privacidad podemos citar las siguientes directrices:

- El correo electrónico se presenta de una manera explícita como un recurso de la compañía para el uso empresarial, no para uso personal.

- Se deja patente la posibilidad de sanción por el uso indebido, y se establece un estamento organizativo responsable de controlar el uso correcto.

- Se apela al sentido común de los empleados para que comprendan que cuando usan un recurso de la compañía, como es el correo electrónico, con un fin empresarial, la privacidad no puede ser plena. Parece lógico que si una comunicación debe ser estrictamente privada, deben canalizar su comunicación a través de correo interno marcándolo como personal y confidencial, antes que usar un ordenador de la compañía.

- La política de seguridad en el correo electrónico pone gran énfasis en que los administradores adquieren una gran dosis de responsabilidad pareja a sus privilegios. Deben asumir el hecho de no abusar de su autoridad accediendo al correo electrónico sin indicación expresa.

6.4. CLASIFICACIÓN DE LA INFORMACIÓN

6.4.1. Por qué hay que clasificar la información

Clasificar la información proporciona un excelente medio de separar la información en categorías, con diferentes niveles de protección y sus correspondientes requerimientos. Dado que en el fondo subyace un tema económico, el factor decisivo en la clasificación de la información es la justificación económica de su protección. No obstante, en el correo electrónico, la privacidad ocupa un lugar de privilegio.

El mundo de los negocios está marcado por la obtención de beneficios o pérdidas, lo que significa que la seguridad debe estar justificada en sus costes. Las decisiones de clasificación en el sector privado están marcadas por las consecuencias no sólo de la difusión no autorizada, sino de la destrucción, modificación o falta de disponibilidad de la información. Esta protección contra pérdida, cambio o indisponibilidad puede ser más importante que la protección contra su difusión. La información es clasificada basándose en las pérdidas financieras que la organización sufriría si tuviera lugar un ataque, bien sea accidental o intencional.

La Administración Pública, por otra parte, en el ejercicio de las competencias que legalmente tiene atribuidas debe velar por el interés público, así, en consecuencia, la clasificación de la información que maneja vendrá definida por razones de interés público, por intereses de terceros más dignos de protección o cuando así lo disponga la Ley. La protección de la información en la Administración contra pérdida, cambio, indisponibilidad o difusión es de gran transcendencia y no sólo económica, pues un fallo en la misma produciría lesiones en sus derechos a los terceros afectados y podría afectar negativamente a intereses de estado.

6.4.2. Categorías de clasificación de la información

Por todo ello, establecemos la clasificación de la información según tres aspectos fundamentales. Un baremo indica la **sensibilidad a la difusión** (confidencialidad), otro hará referencia a la **manipulación fraudulenta** (integridad) y un último señalará la **criticidad** de la información para la operativa de la organización.

- Tanto el grado de *sensibilidad* como el de *integridad* marcan el nivel requerido de control de accesos.
- El grado de *criticidad* determina los procesos de recuperación y 'backup'.

Una información designada como confidencial y no crítica, por ejemplo, sugiere un control estricto en los accesos pero no así en los procedimientos de recuperación.

Así, podemos establecer unos procedimientos derivados de la clasificación establecida, de forma que:

- Si se requiere total o selectiva confidencialidad, la conexión debe establecerse de la manera apropiada, incluyendo la implementación de claves de trabajo y la negociación de los parámetros de criptografía para la conexión.

- Si la integridad de todos los datos del usuario, con o sin recuperación, o la integridad de parte de ellos es un requerimiento, al igual que en caso anterior, debe procurarse una conexión protegida adecuadamente.

6.5. AMENAZAS Y REQUERIMIENTOS

Ya hemos visto en el capítulo 2 tanto los requerimientos de seguridad como las amenazas a las que está expuesto el correo electrónico. Partiendo de este análisis queremos significar algunos aspectos especialmente relevantes desde el punto de vista de las políticas de seguridad.

Los requerimientos de la política de seguridad derivan de la necesidad de proteger la transferencia de información de un rango de potenciales amenazas que podemos identificar en:

- *Interceptación de la identidad*. Se produce cuando la identidad de uno o más usuarios es observada con fines dudosos.

- *Suplantación de la identidad*. Es la pretensión de un usuario de emular la identidad de otro con el fin de obtener acceso a información o adquirir privilegios adicionales.

- *Repetición*. Registro/grabación de una comunicación y posterior emisión.

- *Interceptación de datos*. Observación de los datos de un usuario durante una comunicación por parte de otro usuario no autorizado.

- *Manipulación*. Cambio, inserción, borrado o alteración de los datos de usuario durante una comunicación par parte de un usuario no autorizado.

- *Repudio*. Negación por parte de un usuario de su participación en una comunicación.

- *Negación de servicio*. Impedimento o interrupción de una comunicación, o retraso en su tiempo crítico de operación.

- *Direccionamiento erróneo* provocado por un usuario.

- *Análisis del tráfico*. Observación de la información referente a las comunicaciones entre usuarios

Hemos identificado una gran variedad de amenazas. A pesar de que algunas de ellas se dan en la práctica a pequeña escala, debemos acordar los requerimientos generales y establecer la disponibilidad para el usuario final. A continuación señalamos los requerimientos más significativos, los cuales serán implementados a través de los mecanismos de seguridad adecuados:

No repudio. El no repudio de origen/destino significa que un usuario particular, llamado emisor/receptor, no puede repudiar (denegar) haber firmado/recibido un documento electrónico particular. Esto no prueba quién ha creado el documento realmente. Tenemos exactamente el mismo problema que en los documentos soportados en papel: el hecho de que alguien ponga su firma en una partitura no significa que él sea el compositor.

Los servicios de no repudio son precisamente los servicios en los cuales las comunicaciones electrónicas pueden cubrir las funcionalidades legales de una firma manual, pero de una manera mucho más segura. La principal diferencia es que la firma digital que soporta el no repudio proporciona una conexión lógica al mensaje.

Certificación de origen. El *copyright* es una servicio importante de seguridad en el manejo electrónico de un documento. Pongamos por ejemplo una aplicación software de dos versiones es difícil decidir cuál es la original. Este problema, por supuesto, no está restringido a los documentos electrónicos únicamente. De hecho, aparecen los mismos problemas que en los documentos soportados en papel.

El servicio requerido es la certificación de origen. Es la contrapartida al no repudio en el sentido que permite al creador probar quién creó el documento, en contraposición al no repudio de origen, que permite a cualquiera probar que alguien ha firmado un documento particular. La diferencia está en que con los servicios de no repudio, el receptor es capaz de probar algo, allí donde la certificación de origen pertenezca al transmisor.

Certificación de propiedad. El objetivo a cubrir aquí es atribuir la propiedad de un documento electrónico en cualquier momento a un usuario particular.

Con los documentos ordinarios en papel, el problema se resuelve dando al documento original atributos físicos que sean difíciles de reproducir. Con esta precaución, tiene sentido hablar del original de un documento, y definir al propietario simplemente como la persona que posee el original.

Los documentos negociables deben ser protegidos contra la reproducción. Debe ser fácil distinguir un original de su copia. Aunque una firma digital protege la integridad del documento firmado, ésta puede, sin embargo, ser copiada fácilmente de tal forma que sea imposible distinguir físicamente la copia del original.

Anonimato. El hecho de que datos personales sean almacenados electrónicamente, introduce la posibilidad de que alguien pueda recopilar esos datos, incluso sin conocimiento de los mismos usuarios.

En su forma más general, el anonimato es un servicio con el objetivo de prevenir la recolección de datos personales. El reto es permitir accesos, llamadas, transacciones, etc... sin revelar la identidad del usuario. Ejemplos donde se requiere el anonimato los tenemos en servicios abiertos a miles de usuarios donde la suscripción al servicio no es gestionada directamente por él, sino por otra compañía.

Sin embargo, esta clase de técnicas no pueden ser usadas cuando a la vez se requiere su auditabilidad. En este caso, donde se hace necesaria la convivencia entre los dos sistemas, sólo puede lograrse mediante la cooperación de auditores diferentes e independientes.

Certificación de fecha y hora. En las comunicaciones se requiere un confirmación digital equivalente a la obtenida en el papel. Si estas certificaciones son simplemente acordadas por el emisor y receptor, en caso de litigio, resultaría difícil establecer si esas fechas eran erróneas o habían sido soslayadas.

6.6. LA ADMINISTRACIÓN DE LA SEGURIDAD

6.6.1. Objetivos

La administración de la seguridad es una función indispensable para el normal funcionamiento de cualquier organización y surge como consecuencia de los aspectos de control de las actividades de gestión.

Las objetivos de esta función son los de asegurar la existencia y el mantenimiento de los niveles de seguridad en:

- Hardware, software.
- Personal.
- Comunicaciones y redes de comunicaciones.
- Entorno físico.

La administración de la seguridad representa un coste no despreciable en una empresa. Asimismo, puede ser interpretado como restricción a las personas en la forma de hacer sus trabajos. Por ello, es un objetivo primordial reconciliar las labores de administración de la seguridad con aquellas propias de la gestión.

6.6.2. Funciones

Entre sus funciones están comprendidas las siguientes:

- Gestión del sistema de seguridad.
    - Gestión de la política de seguridad.
    - Adaptación a las prescripciones legales.
    - Gestión de las tareas de recuperación.

- Gestión de servicios de seguridad.
    - Determinación y asignación de la protección de la seguridad para el servicio.
    - Asignación y mantenimiento de las reglas para la selección de mecanismos específicos de seguridad para proporcionar el servicio de seguridad requerido.
    - Negociación (local y remota) de los mecanismos de seguridad disponibles.

- Gestión de mecanismos de seguridad.
    - Gestión de claves.
    - Gestión de criptografía.
    - Gestión firma digital.
    - Gestión de controles de accesos.
    - Gestión de la integridad de datos.
    - Gestión de la autentificación.
    - Gestión de relaciones con TTPs.

- Gestión de la auditoría de seguridad.
    - Gestión de los eventos a ser registrados.
    - Activación o desactivación de auditorías.
    - Edición de informes.
    - Verificación de adopción de medidas correctoras.
    - Concordancia en la implementación de la tecnología con la política de seguridad adoptada.

En la práctica, estas labores de gestión se materializan en:

- Controles sobre seguridad crítica.
- Control sobre los procesos.
- Conexiones seguras.
- Alarmas en tiempo real para detectar intrusos, allí donde sea apropiado.

6.7. DOMINIOS DE SEGURIDAD

El nivel de seguridad en la información es adaptado dinámicamente a una situación dada. Esto nos introduce en el concepto de Gestión Dinámica de los Sistemas de Información y a la necesidad de ser capaces de establecer dominios, en los cuales la seguridad de la información es aplicada homogéneamente.

Los dominios son agrupaciones de usuarios compartiendo algunas de sus funciones. Para algunas actividades, operan como grupos cerrados virtualmente, pero tiene la posibilidad de interoperar con otros dominios, mediante unos requerimientos mínimos, sin pérdida de seguridad o transparencia en el uso.

La noción de dominio de seguridad es aquí importante por dos razones:

- Es usado para describir la forma en que la seguridad es gestionada y administrada.

- Puede ser usado como un elemento constructivo en el modelo de seguridad, que involucra distintos elementos bajo distintas autorizaciones en seguridad.

Ejemplos de dominios de seguridad son:

- Acceso a elementos
- Operaciones relativas a labores específicas de gestión.
- Enlaces y comunicaciones.

La política de seguridad recoge los siguientes aspectos concernientes a los dominios de seguridad:

- Qué se entiende por seguridad en un dominio.
- Las reglas sobre las cuales se asienta la obtención del dominio.
- Las actividades sobre las que se aplica.
- Las reglas de aplicación en las relaciones con otros dominios generales.
- Las relaciones para su aplicación con otros dominios de seguridad particulares.

Administración de los dominios de seguridad.

La gestión y administración de los dominios de seguridad está basada en las similitudes existentes entre dominios. En cuanto a la gestión de relaciones entre dominios, se establece un acuerdo con el fin de obtener el nivel adecuado de seguridad. Los mecanismos actuales que articulan esta administración recogen los siguientes requerimientos:

- Mecanismos para la gestión, procedimientos y controles entre dominios donde intervenga una TTP.
- Procedimientos para la creación de dominios, su gestión y control.
- Desarrollo de una arquitectura común para el trabajo entre dominios.

6.8. CLAVES DE SEGURIDAD

Las firmas digitales conllevan la implementación de especificaciones relacionadas con las tres fases de una gestión de claves: incorporación de usuarios, distribución y certificación de claves y mantenimiento operacional (revoques, listas negras, destrucción), que debe ser acordada y aceptada.

En la aplicación de seguridad a cualquier proceso o mensaje, son de especial interés los siguientes aspectos:

- Aspectos legales e implicaciones (incluyendo aspectos sociales)
- Definición e identificación del servicio de seguridad a aplicar.
- Los mecanismos que lo soportan.
- Los algoritmos y protocolos.

Servicio de gestión de claves

Los aspectos más generales que se pueden identificar en relación a un servicio de gestión de claves pueden ser:

- *Definición de responsabilidades y obligaciones* para aquellos servicios que proporcionan seguridad en la integridad de comunicaciones y aquellos que proporcionan confidencialidad.
- *Desarrollo de prácticas para la generación, distribución, almacenamiento y destrucción de claves*, con los fines de integridad y confidencialidad, en entornos que poseen diferentes niveles de seguridad.

- '*Escrow Services'*. Algunos de los secretos pueden ser de vital importancia, y pueden requerir ser distribuidos entre partes seguras, de tal manera que ninguna de las partes conozca la totalidad del secreto sino nada más que una mínima parte. Para la completar la totalidad del secreto todas las partes deben aportar su contribución.

- *Mecanismos y criterios de asesoramiento para discernir la conveniencia de los solicitantes de servicios de TTPs*. No todos los potenciales usuarios de una TTP pueden tener las características necesarias (status legal, viabilidad financiera, etc...)

- *Integridad y firma digital.*

- *La relación entre las funciones de gestión de claves, gestión de directorios y certificación* necesita ser clara.

- *Celeridad en la emisión de firma, verificación de veracidad de la firma*, revisión periódica de la veracidad de los signatarios existentes.

- *Eliminación de firmas de la "lista activa" e iniciación de una auditoría para confeccionar una "lista de usos ilegales"*. Esto conlleva una interfase de gestión de claves - gestión de certificaciones.

- *Relaciones de privacidad*.

- *Gestión de los dominios* en los cuales son válidas las claves de confidencialidad. Identificación de los sujetos autorizados en el dominio, distribución de claves a los usuarios autorizados (personas y procesos automáticos).

- *La TTP debe definir dominios por su capacidad de gestionarlos*. Si no pudiera atender su gestión, otra TTP debe soportar la gestión del dominio.

- *Establecimiento del nivel de seguridad del dominio sobre el cual se van a emplear las claves de confidencialidad*. Clasificar desde usuarios vetados al uso, usuarios con acceso físico y lógico controlado hasta usuarios liberados.

7. GLOSARIO DE SEGURIDAD

Amenaza: Acción o acontecimiento que pueda perjudicar la seguridad. (European ITSEC)

Potencial violación de la seguridad del sistema. (ISO 7498-2)

Análisis de Tráfico: Información inferida de la observación del tráfico de datos (presencia, ausencia, dirección y frecuencia). (ISO 7498-2)

Aseguramiento: Confianza que puede tenerse en la seguridad que proporciona un objetivo de evaluación. (European ITSEC)

Autenticación de Entidad: Comprobación de que una entidad es la que se presupone. (ISO/IEC 9798-1)

Autenticación de Origen de Datos: Comprobación de que la fuente de los datos recibidos es la afirmada. (ISO 7498-2)

Certificación: Expedición de una declaración formal que confirma los resultados de una evaluación y el hecho de que los criterios de evaluación han sido correctamente utilizados. (European ITSEC)

Certificado: Claves públicas de un usuario, junto con alguna otra información, infalsificable mediante cifrado con la clave secreta de la autoridad de la certificación que la emite.

Clave: Secuencia de símbolos que controla las operaciones de cifrado y descifrado. (ISO 7498-2)

Confidencialidad: Propiedad de la información que hace que ésta no sea disponible o descubierta a individuos, entidades o procesos no autorizados. (ISO 7498-2)

Prevención de la revelación no autorizada de información. (European ITSEC)

Denegación de servicio: Rechazo de un acceso autorizado a los bienes del sistema p retraso en las operaciones críticas en el tiempo. (ISO 7498-2)

Disponibilidad: Propiedad que requiere que los recursos de un sistema abierto sean accesibles y utilizables a petición de una entidad autorizada. (ISO 7498-2)

Prevención de una negación no autorizada de información o recursos. (European ITSEC)

Etiqueta de Seguridad: Indicador sensible que está permanentemente asociado con datos, procesos y/u otros recursos OSI protegidos, y que puede ser usado para poner en práctica una política de seguridad. (ISO 7498-2)

Firma Digital: Datos añadidos a un conjunto de datos o una transformación de estos que permite al receptor probar el origen e integridad de los datos recibidos, así como protegerlos contra falsificaciones. (ISO 7498-2)

Gestión de claves: Generación, almacenamiento, distribución segura y aplicación, de claves de cifrado de acuerdo con una política de seguridad. (ISO 8732 & CD 11166)

Integridad de datos: Propiedad de los datos que garantiza que éstos no han sido alterados o destruidos de modo no autorizado. (ISO 7498-2)

Prevención de la modificación no autorizada de la información. (European ITSEC)

Mecanismo de Seguridad: La lógica o el algoritmo que implementa una función particular de seguridad tanto en hardware como en software. (European ITSEC)

Notarización: Registro de datos por una tercera parte fiable, que suministra posteriores recursos a los mismos y garantiza la exactitud en lo que respecta a sus características como contenido, origen, tiempo y entrega de los datos. (ISO 7498-2)

Política de Seguridad: El conjunto de reglas para el establecimiento de servicios de seguridad. (ISO 7498-2).

Privacidad: Derecho de reclamar una seguridad adecuada y a definir usuarios autorizados de las informaciones o sistemas. (ISO 7498-2)

Repudio: Denegación, por una de las entidades implicadas en una comunicación, de haber participado en todo o parte de dicha comunicación. (ISO 7498-2)

Servicios de Seguridad: Servicios suministrados por uno o más niveles de sistemas abiertos de comunicación que llevan a cabo la seguridad del sistema y las transferencias de datos. (ISO 7498-2)

Suplantación: Pretensión de una entidad de ser una diferente, para así acceder sin autorización a los recursos. (ISO 7498-2)

Tercera Parte Fiable: Autoridad de seguridad, o agente suyo, fiable para otras entidades con respectos a actividades relativas a su seguridad. En el contexto de esta norma, una tercera parte fiable es de confianza para un demandante y/o verificador a efectos de autenticación.

Vulnerabilidad: Debilidad de la seguridad de un Objetivo de Evaluación, debido a errores en el análisis, diseño, implementación u operación. (European ITSEC)

Referencias para el glosario

- Glosario de ISO-7498-2 Information Processing Systems-Open Systems Interconnection- Basic Reference Model- Part 2: Security Architecture.

- Glosario de EPHOS 2 bis Topic U Security Glossary

- ISO/IEC JTC1/SC27 Glossary of IT Security Terminology (Version 2.0).

- X.509 The Directory - Authentication Framework; Glossary.

- Information Technology Security Evaluation Criteria (ITSEC) Glossary.

- Guía de Seguridad de los Sistemas de Información para directivos; Glosario.

- Otras fuentes: Glosario de terminología de seguridad, de criptología, etc.

8. BIBLIOGRAFÍA

- EPHOS 2 bis Topic U Security Glossary. European Procurement Handbook for Open Systems.
- Libro Verde de la Seguridad de los Sistemas de Información. Comisión Europea.
- ISO-7498-2 Information Processing Systems-Open Systems Interconnection- Basic Reference Model- Part 2: Security Architecture.
- ISO/IEC JTC1/SC27 Glossary of IT Security Terminology (Version 2.0).
- X.509 The Directory - Authentication Framework.
- Information Technology Security Evaluation Criteria (ITSEC).
- MAGERIT, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.
- Guía/Vademécum para la aplicación de la LORTAD a los ficheros de datos de carácter personal de las Administraciones Públicas. MAP, 1995.
- Informática y legalidad. Curso de Auditoría, Máster DISTIC.Pablo Lanza Suárez.
- Guía de Seguridad de los Sistemas de Información para directivos; Cuadernos de la COAXI nº 1.
- Emilio del Peso Navarro, Miguel Ángel Ramos González. Confidencialidad y Seguridad de la Información: La lortad y sus implicaciones socioeconómicas. Díaz de Santos, 1994
- AUERBACH Publications. Data Security Management. Policies for email privacy.
- AUERBACH Publications.William Stallings. E-mail Security Using Pretty Good Privacy.
- GARTNER GROUP. Internet Security: Why Firewalls are not enough.
- The Secure HyperText Transfer Protocol. Web Transaction Security Working Group. E. Rescorla, Alan Schiffman. Enterprise Integration Technologies. July 1995.
- The SSL Protocol. Version 3.0. Netscape Communications. March 1996.
- Stephen T. Kent. Internet Privacy Enhanced Mail. Communications of the ACM. Agosto 1993, Pág. 48
- Mike Hendry. Practical Computer Network Security.Artech House Inc., 1995.
- Andrew S. Tanenbaum. Redes de Ordenadores. Prentice-Hall, 1991.
- 'Internet en la Práctica'. Ediciones Anaya Multimedia, S.A.
- Novática, Monografía Seguridad Informática, Julio-Agosto 1995.
- Miguel A. Sanz Sacristán. A, B, C de Internet. Boletín de la red nacional de I+D, RedIRIS.
- Grupo FRANJA. 400 x 500 ... igual mensajería. Comunicaciones World. Septiembre 1990. Pág. 27.

- Deb Cameron. The Internet, a global business opportunity. Computer Technology Research Report, 1994.
- Jacob Palme, *Electronic Mail*, Artech House, Inc, 1995.
- www.ibm.com
- www.netscape.com