

GUIA TECNOPYME. Fase II.

3. SEGURIDAD EN INTERNET

CAP3.INF

Autor: _____
Raquel Jorge

Revisado: _____
Laura Martínez

Aprobado: _____
Ana Bonilla

Copia de: _____

Versión: 1

Revisión: 0

Zamudio, marzo 2003

GUÍA TECNOPYME

3- SEGURIDAD EN INTERNET

ÍNDICE

1. INTRODUCCIÓN	1
2. HERRAMIENTAS Y ELEMENTOS DE SEGURIDAD	1
2.1. Criptografía.....	2
2.1.1. Firmas digitales.....	3
2.1.2. Certificados digitales.....	4
2.1.3. Autoridades certificadoras.....	7
2.1.4. Ejemplo práctico	8
2.2. Firewalls.....	9
2.3. Sistemas de back-up.....	9
2.4. Sistemas antivirus	10
2.4.1. Tipos de Sistemas de Antivirus	10
2.4.2. Tipos de virus.....	11
3. NORMATIVA VIGENTE.....	12
3.1. LOPD	12
3.2. LSSICE	15
4. POLÍTICA DE SEGURIDAD	17
4.1. Plan de seguridad	17
4.2. Plan de contingencia	18
5. CONCLUSIONES	20
6. REFERENCIAS	21

1. INTRODUCCIÓN

Internet nace en 1968 como un proyecto del departamento de Defensa Americano, para conectar universidades y centros de investigación que colaboran con las Fuerzas Armadas Norteamericanas. En un principio, la información circulaba libremente y no existía preocupación por la privacidad de los datos ni por los mecanismos de seguridad.

Actualmente, la conexión a Internet en todos los ámbitos, bien sea en el laboral como en el de educación, se produce a un ritmo acelerado. Se ha incrementado la variedad y cantidad de usuarios que usan la red para el aprendizaje, la docencia, la investigación, el trabajo, la cooperación o el juego.

La complejidad de la red es una dificultad más a la hora de detectar los problemas de seguridad. Los responsables de la administración y seguridad de la red deben realizar tareas de vigilancia continua y sistemática.

2. HERRAMIENTAS Y ELEMENTOS DE SEGURIDAD

La seguridad es uno de los elementos clave en el desarrollo positivo de las redes de información mundial y particularmente en el comercio electrónico. Ésta genera confianza y hace que los usuarios depositen sus datos en la red, con la seguridad de que no serán alterados ni desviados a usuarios no autorizados.

Todo esto hoy es posible gracias a la utilización de métodos criptográficos, los cuales se usan para codificar los mensajes que circulan por la red y cuyo objetivo es garantizar la seguridad en la difusión de dichos mensajes.

Las empresas han adoptado una configuración en red de sus recursos informáticos utilizando redes de ordenadores para el soporte y distribución de la información, y acceso a las aplicaciones y herramientas de gestión. Por ello, es necesario garantizar:

- **Confidencialidad:** los datos que se envían a través de la red no pueden ser interceptados por personas no autorizadas, lo cual se consigue mediante la *encriptación* de mensajes. De la misma forma se aseguran los datos almacenados en discos duros y otros sistemas de almacenamiento.
- **Integridad:** garantiza que los datos no sean modificados a lo largo de su trayecto por la red. Esto se logra mediante el uso de *firmas digitales*.
- **Autenticación:** garantiza la identidad de la persona que accede a la red. Esto se consigue con la emisión de *certificados digitales*.
- **Control de acceso:** permite restringir las operaciones y acceso a diferentes recursos dependiendo de la identidad del usuario. Se logra mediante grupos de *usuarios y roles*.
- **Disponibilidad:** deben existir medidas de seguridad para soportar fallos de todo tipo: pérdidas en la corriente eléctrica, pérdidas de datos en los discos duros, virus, etc. El sistema debe estar siempre a disposición de sus usuarios.

A continuación, veremos las diferentes herramientas que se utilizan para cumplir las diferentes propiedades que se han descrito anteriormente. Para ello, se utilizan técnicas de criptografía, firmas digitales, firewalls, copias de seguridad y sistemas antivirus. De todo esto hablaremos en los siguientes apartados.

2.1. Criptografía

La *criptografía*, o escritura en clave, se ha utilizado para proteger los secretos de la humanidad desde los tiempos en que el hombre empezó a escribir.

La palabra *criptografía* deriva de las palabras griegas *kryptus*, que significa oculto y *gráphein*, que significa escritura, y su definición es: “Arte de escribir con clave secreta o de modo enigmático”. Obviamente la criptografía hace años que dejó de ser un arte para convertirse en una técnica, o más bien en conglomerado de técnicas, que tratan sobre la protección de la información frente a observadores no autorizados.

Uno de los primeros practicantes más famosos de la criptografía fue Julio Cesar, que desarrolló una clave conocida como “cifra del Cesar”, que estaba basada en la rotación fija de las letras del alfabeto. La figura 1 ilustra el funcionamiento de esta

clave (cipher). Asigna cada letra del alfabeto a otra letra que está separada un número fijo de letras (el nivel de rotación). Por ejemplo, con una rotación de 1, A se asigna a B, B se asigna a C, ..., Y a Z y Z a A (Las letras finales del alfabeto se asignan de un modo circular a las que están al comienzo). Con una rotación de 13, A se asigna a N, B a O, ..., Y a L y Z a M.

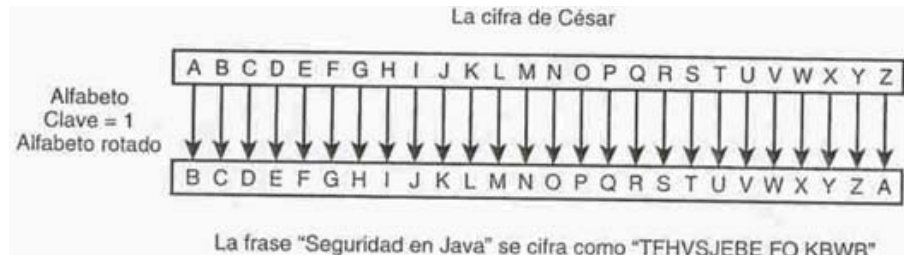


Fig. 1: Ejemplo de criptografía.

En cuanto a la seguridad informática, la criptografía es un sistema o método de transformación de cualquier tipo de mensaje de datos para volverlo ilegible y, poder más tarde, recuperar el formato original. Su finalidad es que solamente las personas que posean las claves correspondientes puedan tener acceso a la información.

2.1.1. Firmas digitales

Una firma digital es una cadena de datos creada a partir de un mensaje, o parte de un mensaje, de forma que:

- Imposibilita el rechazo del mensaje: el que escribe o envía el mensaje no puede renegar de él ya que está firmado con su firma digital, única para cada persona.
- El receptor del mensaje puede asegurar que quién dice que lo ha enviado es realmente quien lo ha enviado.

➤ Aplicaciones

A continuación se enumeran varias aplicaciones en las que se podría usar la firma digital:

- Firma y cifrado de e-mail
- Firma y cifrado de documentos
- Identificación de personas: perfiles de usuario, sin necesidad de registro de datos
- Identificación de sistemas ante usuarios: ¿Cómo sé que es el sistema que dice ser?
- Auditoría de transacciones
- Seguridad al operar comercialmente: transacciones bancarias, operaciones con tarjeta de crédito, etc.
- Identificación de componentes de una red: ordenadores, routers, etc.

2.1.2. Certificados digitales

El certificado digital es como un “pasaporte electrónico” que se usa para identificarse. Sirven para asegurar la veracidad de la clave pública perteneciente al propietario del certificado. Con la clave pública se firman digitalmente documentos que puedan proporcionar las más absolutas garantías de seguridad respecto a cuatro elementos fundamentales:

- **Autenticación** del usuario/entidad (es quien asegura ser)
- **Confidencialidad** del mensaje (que solo lo podrá leer el destinatario)
- **Integridad** del documento (nadie los ha modificado)
- **No repudio** (el mensaje no puede ser rechazado por el emisor).

Un certificado electrónico contiene una **clave pública**, y una **firma digital**. Además, para su correcto funcionamiento, los certificados contienen la siguiente información:

- Un identificador del propietario del certificado, que consta de su nombre, sus apellidos, su dirección e-mail, datos de su empresa como el nombre de la organización, departamento, localidad, provincia y país, etc.

- Otro identificador de quién asegura su validez, que será una Autoridad de Certificación.
- Dos fechas, una de inicio y otra de fin del período de validez del certificado, es decir, cuándo un certificado empieza a ser válido y cuándo deja de serlo, fecha a partir de la cual la clave pública que se incluye en él, no debe utilizarse para cifrar o firmar.
- Un identificador del certificado o número de serie, que será único para cada certificado emitido por una misma Autoridad de Certificación. Esto es, identificará inequívocamente a un certificado frente a todos los certificados de esa Autoridad de Certificación.
- Firma de la Autoridad de Certificación de todos los campos del certificado.

Veamos un ejemplo de un certificado en la Figura 2:

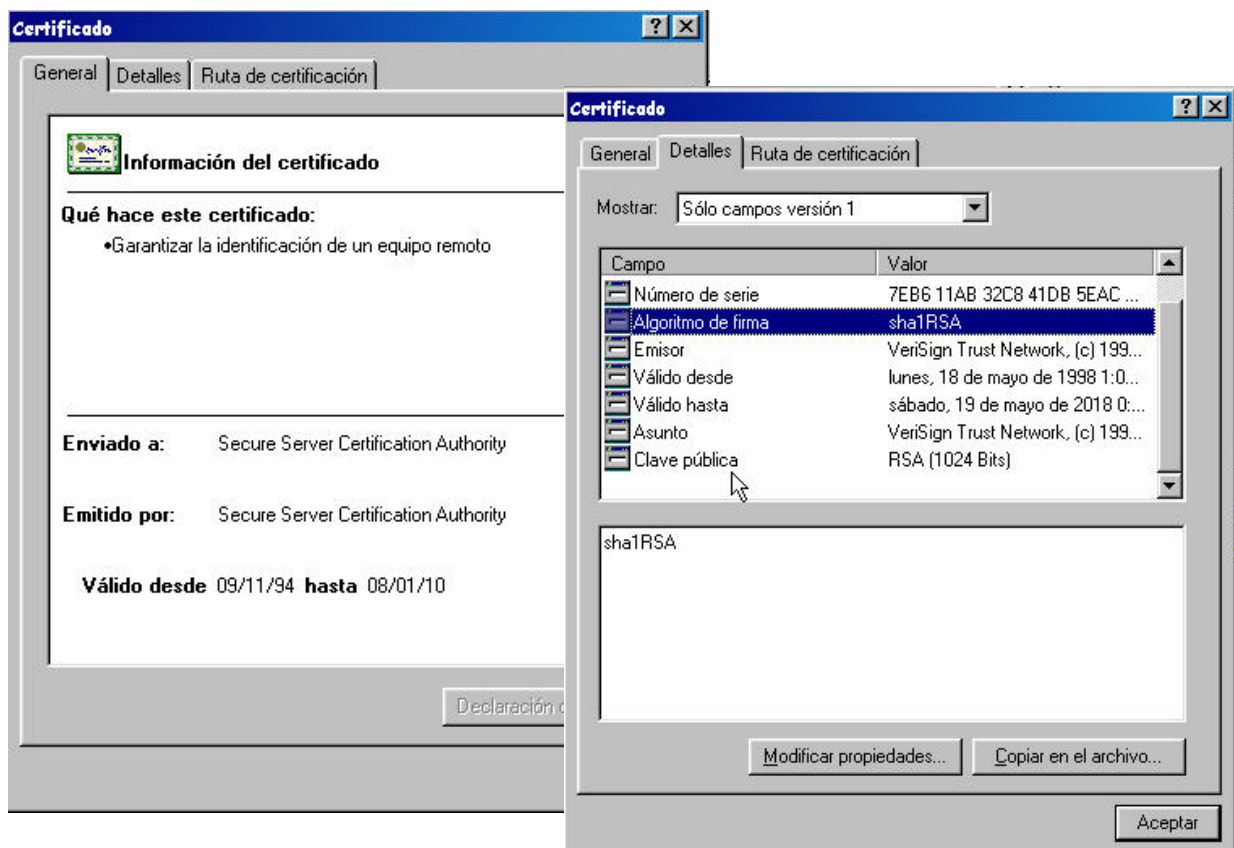


Fig. 2: Ejemplo de certificado

➤ ¿Para qué sirve un certificado digital?

Además de servir como mecanismo confiable y seguro de identificación en la red, un certificado de identidad digital permite disfrutar de otra serie de beneficios:

- Permite enviar y recibir información confidencial, asegurando que sólo el remitente pueda leer el mensaje enviado.
- Permite acceder a sitios Web de manera segura con su firma digital, sin tener que usar el peligroso mecanismo de passwords.
- Permite firmar digitalmente documentos garantizando:
 1. La integridad del contenido y autoría del documento y todas aquellas aplicaciones en que se necesiten mecanismos seguros para garantizar la identidad de las partes.
 2. La confidencialidad e integridad de la información intercambiada en procesos como comercio electrónico, declaración de impuestos, pagos provisionales, uso en la banca, etc.

➤ Tipos de certificados

- *Certificados personales*: expedidos por usuarios e identifican personas. Se usan para autenticar usuarios y enviar correo seguro.
- *Certificados de servidor*: expedidos a servidores para que unas máquinas se comuniquen con otras de forma segura.
- *Certificados de fabricante*: se utilizan para firmar el software que circula por Internet.
- *Certificados de entidades emisoras*: certificados de certificadores que identifican a las entidades que emiten los certificados y que se usan para emitir otros certificados.

➤ Aplicaciones

Algunas aplicaciones en la que se suele usar certificados digitales son:

- Transacciones electrónicas: recibos de pago, facturas electrónicas, cheques electrónicos

- Invitaciones, promociones
- Contratos, solicitudes de adhesión
- E-mails: circulares, confirmaciones, reservas o turnos para talleres, médicos, hoteles, etc.
- Contratos, convenios, acuerdos.
- Relaciones entre empresas.

2.1.3. Autoridades certificadoras

➤ Autoridades de Certificación

La *Autoridad de Certificación (CA)*, es quien firma digitalmente los certificados, asegurando su integridad y certificando la relación existente entre la Clave Pública contenida y la identidad del propietario. La firma de la CA es la que garantiza la validez de los certificados. Algunas CA conocidas son: Verisign Commercial Software Publishers CA o Microsoft Authenticode Root Authority.

Las autoridades de certificación pueden realizar las siguientes tareas:

- Emisión de los certificados de usuarios registrados y validados por *la Autoridad de Registro (RA)*, que se verán en el siguiente punto.
- Revocación de los certificados que ya no sean válidos. Un certificado puede ser revocado porque los datos han dejado de ser válidos, la clave privada ha sido desvelada (alguien la ha publicado) o el certificado ha dejado de tener validez (se ha caducado) dentro del contexto para el que había sido emitido.
- Renovación de certificados.
- Publicación de certificados.

➤ Autoridad de Registro

La *Autoridad de Registro (RA)* es la entidad encargada de identificar de manera inequívoca a los usuarios que solicitan un certificado a la Autoridad de Certificación (CA), así como de gestionar los certificados.

Las autoridades de registro realizan las siguientes tareas:

- Validar solicitudes de certificado en base a determinados procedimientos de identificación, apropiados a los niveles de seguridad que ofrece cada categoría de certificado (políticas de seguridad).
- Mandar las peticiones de generación de certificados a la Autoridad de Certificación (CA), para que ésta los firme con su clave privada.
- Recibir los certificados solicitados a la Autoridad de Certificación (CA).
- Entregar físicamente los certificados a los solicitantes, por cualquier medio.
- Informar a los usuarios de la necesidad de la renovación de su certificado.
- Petición de revocación de un certificado (también puede solicitarlo el propio usuario).

Por último, señalar que la tecnología de certificados digitales ya viene incorporada en aplicaciones como el correo electrónico y navegadores. Microsoft Outlook 2000 permite enviar e-mails firmados y encriptados. De la misma forma, los navegadores Internet Explorer o Netscape Navigator manejan certificados digitales.

2.1.4. Ejemplo práctico

Por ejemplo, se puede realizar la **declaración de la renta por Internet** utilizando la tecnología de firma digital, en la Web www.aeat.es

En primer lugar se necesitan unos programas que se consiguen desde la propia Web, www.aeat.es. Además, hay que pedir un certificado digital de usuario, obligatorio para realizar la operación a través de Internet. En España, la **Autoridad de Certificación** es la FNMT (Fábrica Nacional de Moneda y Timbre), que es quien concede los certificados. Todo se realiza desde la Web.

El procedimiento es el siguiente: el usuario se conecta a la Web de la Consejería de Economía y Hacienda y baja el formulario, se rellena y se firma para luego ser enviado "telemáticamente" a la Administración. Tras este paso, la Administración le devolverá un justificante de dicha declaración.

2.2. Firewalls

Un *firewall* o cortafuegos es un sistema o grupo de sistemas utilizados para separar, en cuanto a seguridad se refiere, una máquina o subred del resto de la red, protegiéndola así de servicios y protocolos que desde el exterior puedan suponer una amenaza a la seguridad. El espacio protegido, denominado **perímetro de seguridad**, suele ser propiedad de la misma organización, y la protección se realiza contra una red externa no fiable llamada **zona de riesgo**.

Las partes que constituyen un cortafuegos son:

- **Máquina o host bastión** (también se denominan **gates**): sistema especialmente asegurado, pero en principio vulnerable a todo tipo de ataques por estar abierto a Internet, que tiene como función ser el punto de contacto de los usuarios de la red interna de una organización con otro tipo de redes. El *host bastión* filtra tráfico de entrada y salida, y también esconde la configuración de
- **Filtrado de paquetes**: acción de denegar o no la circulación de mensajes entre dos redes (por ejemplo la interna, protegida con el *firewall*, y el resto de Internet) de acuerdo a unas normas predefinidas.
- **Proxy**: programa que permite o niega el acceso a una aplicación determinada entre dos redes.

Los *firewalls* son cada vez más necesarios en nuestras redes, pero todos los expertos recomiendan que no se usen **en lugar de** otras herramientas, sino **junto a ellas**.

2.3. Sistemas de back-up

Una correcta política de copias de seguridad permite recuperar los datos vitales ante una situación catastrófica. Por este motivo, dependiendo de los datos necesarios para el funcionamiento de la organización, será conveniente realizar copias de seguridad con una periodicidad horaria, diaria o semanal.

Para realizar las copias se emplean dispositivos con formato de cinta, por tratarse de un soporte que permite realizar un número elevado de operaciones de grabación

de datos, con una alta capacidad de almacenamiento y un reducido tamaño. Estas cintas deberán estar protegidas, siendo altamente recomendable guardarlas en una caja de seguridad ignífuga.

Por otra parte, también es recomendable disponer de un sistema de replicación de datos entre los servidores de las distintas delegaciones de la organización, para que de este modo sea posible recuperar la actividad si alguna de las instalaciones de la organización sufre una catástrofe.

2.4. Sistemas antivirus

Un software antivirus es un conjunto de herramientas que permiten analizar un sistema informático y detectar la presencia de algún tipo de virus. Un virus es un programa que puede infectar otros programas modificándolos para incluir una copia de sí mismo y seguir infectando.

Existe en el mercado una amplia gama de productos, pero se pueden clasificar en dos grandes categorías: *Sistemas de Prevención* y *Sistemas de Detección*.

2.4.1. Tipos de Sistemas de Antivirus

2.4.1.1. Sistemas de Prevención

Estos sistemas intentan detener el avance del virus en tiempo real, esto es, están constantemente pensando los posibles puntos de entrada de virus al sistema e intentan detectar algún tipo de funcionamiento anormal del mismo. Este tipo de programas se instalan en el disco duro e interceptan todas las llamadas especiales del mismo como por ejemplo: *cargar programa, escribir en el disco, borrar archivo*, etc.

2.4.1.2. Sistemas de Detección

Los programas de detección analizan los archivos ejecutables antes de que se ejecuten, buscando en ellos indicios específicos que hagan suponer la presencia de algún tipo de virus. Para realizar esta tarea utilizan complicados cálculos que permiten aislar "características" de varios virus conocidos que son detectables por el antivirus. Los antivirus más especializados buscan también la presencia de indicios tales como mensajes o instrucciones de borrado masivo que hagan suponer la presencia de algún tipo de virus no conocido por la versión actual del programa.

2.4.2. Tipos de virus

Los virus se pueden clasificar por forma de infección y por peligrosidad.

Clasificación	Tipo	Descripción
Por Infección	Virus de sector de arranque	Residen en discos duros o disquetes. Se produce mediante el intercambio de disquetes.
	Parásitos	Se unen a los ficheros ejecutables y se ejecutan antes que el programa.
	Multipartitos	Combinan las capacidades de los dos anteriores.
	Acompañantes	No modifican los ficheros, crean uno nuevo con el mismo nombre engañando al sistema operativo.
	Virus de vínculos	Modifican la forma en que el Sistema Operativo encuentra los programas para que primero ejecute el virus.
	Virus de ficheros de datos o de macro	Infectan programas con macros, y pueden abrir y manipular los ficheros de datos
	Gusano	Se transmiten a través del correo y se activan al abrir el fichero adjunto.
Por peligrosidad	Residentes	Se mantienen activos en memoria e infectan todos los programas que se vayan ejecutando.
	De sobreescritura	Eliminan el fichero infectado y sobreescriben el código del virus.
	Stealth	Se ocultan para luego infectar y reproducirse. Pueden detectar el tipo de antivirus.
	De encriptación	No permiten que el antivirus acceda a su código. Permanece en estado latente.
	Polimorfismo	Evolucionan a la vez que se replican. Cambian de tamaño y de forma.
	Caballos de troya	Ocultan su verdadera identidad haciéndose pasar por aplicaciones inofensivas facilitando el acceso a terceras personas a los recursos del sistema.

Tabla 1: Clasificación de virus

3. NORMATIVA VIGENTE

3.1. LOPD

La *Ley Orgánica de Protección de Datos de Carácter Personal 15/1999*, 13 de Diciembre (LOPD) y el *Real Decreto 994/1999 de 11/VI (RD)* son las dos disposiciones básicas de obligado cumplimiento para todas las empresas y profesionales que traten datos de carácter personal.

La LOPD impone obligaciones relativas a la recogida de datos, consentimiento, almacenaje, conservación uso, datos especialmente protegidos, comunicación o cesión de datos, acceso, rectificación, creación de ficheros, alta en la Agencia de Protección de Datos, etc.

De la misma forma el *R.D* establece la obligación de las empresas de poner en marcha medidas destinadas a la protección de datos, afectando a sistemas informáticos, ficheros de soporte de almacenamiento, personal, etc.

La ley establece tres niveles de seguridad, con diferentes tipos de datos personales, para los cuales se adoptarán distintas medidas de seguridad, como se observa en la Tabla 2. Para las medidas de *nivel medio y alto* es necesario y de obligado cumplimiento la **Auditoría de Protección de Datos**, que como mínimo deberá realizarse cada dos años, pudiendo ser interna o externa.

También se establecen una serie de sanciones para los encargados del tratamiento de ficheros que contengan datos de carácter personal. Éstas se clasifican en tres grupos, dependiendo del tipo de infracción, como puede verse en la Tabla 3.

Los plazos para implantar las medidas de seguridad desde su entrada en vigor son:

- Para las de nivel básico => un plazo de seis meses.
- Para las de nivel medio => un plazo de un año.
- Para las de nivel alto => un plazo de dos años.

Se contará con un plazo **máximo de tres años** si los sistemas de información que se encuentren en funcionamiento no permiten tecnológicamente la implantación.

Nivel-Datos	Medidas de seguridad
Básico Datos de carácter personal	➤ Documento de seguridad. ➤ Funciones y obligaciones del personal. ➤ Registro de incidencias. ➤ Identificación y autenticación. ➤ Relación actualizada de usuarios con acceso autorizado. ➤ Procedimiento de asignación, distribución y almacenamiento de contraseñas que garantice su confidencialidad e integridad. ➤ Contraseñas cambiadas con periodicidad y almacenadas codificadas y encriptadas. ➤ Control de acceso. ➤ Gestión de soportes. ➤ Copias de respaldo y recuperación al menos semanalmente.
Medio - Comisión de infracciones administrativas o penales. - Hacienda Pública. - Servicios financieros. - Prestación de servicios de información sobre solvencia patrimonial y crédito. - Suficiencia para la evaluación de la personalidad del individuo.	➤ <i>Medidas del nivel básico</i> ➤ Documento de seguridad que deberá contener: ▪ La identificación del responsable o responsables de seguridad. ▪ Los controles periódicos a realizar para verificar el cumplimiento del documento. ▪ Medidas a adoptar al desechar o reutilizar un soporte. ➤ Responsable de seguridad. ➤ Auditoría bianual. ➤ Control de acceso físico.
Alto - Ideología. - Religión. - Creencias. - Origen racial o étnico. - Salud. - Vida sexual - Datos policiales recabados sin consentimiento de las personas afectadas.	➤ <i>Medidas del nivel básico y medio</i> ➤ Distribución de soportes. ➤ Registro de accesos: ▪ El período mínimo de conservación de los datos registrados será de dos años. ▪ El responsable de seguridad deberá revisar periódicamente la información y elaborar mensualmente un informe con las revisiones y problemas. ➤ Medidas adicionales de copias de respaldo. ➤ Cifrado de Telecomunicaciones.

Tabla 2: Niveles de seguridad.

Tipo	Descripción	Prescripción de la sanción	Sanción
Leves	- No atender la solicitud del interesado de rectificación o cancelación de los datos personales. - No proporcionar la información que solicite la Agencia de Protección de Datos. - No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos. - Proceder a la recogida de datos de carácter personal de los afectados sin informarles de sus derechos. - Incumplir el deber de secreto.	1 año	601,01€ a 60.101,21 €
Graves	- Creación de ficheros públicos o recoger datos sin autorización publicada en el "BOE". - Creación de ficheros privados o recoger datos con finalidades distintas a las de la empresa o entidad. - Recogida de datos sin el consentimiento de los afectados. - Tratar los datos o utilizarlos incumpliendo los principios de la propia LOPD. - Impedir u obstaculizar el ejercicio de los derechos de acceso y oposición, y la negativa a facilitar la información solicitada. - Mantener datos inexactos o no efectuar las rectificaciones o cancelaciones de los mismos. - Vulnerar el deber de guardar secreto sobre ficheros de nivel de seguridad medio. - Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones y medidas de seguridad. - No remitir a la Agencia de Protección de Datos las notificaciones e información requeridos. - Obstruir la inspección y auditorías. - No inscribir el fichero de datos de carácter personal en el Registro General de Protección de Datos.	2 años	60.101,21 € a 300.506,05 €
Muy graves	- La recogida de datos de forma engañosa y fraudulenta. - La comunicación o cesión de los datos sin autorización. - Recoger y tratar los datos especialmente protegidos (nivel de seguridad alto) sin consentimiento del afectado. - No cesar en el uso ilegítimo de los tratamientos de los datos habiendo sido avisado anteriormente. - La transferencia de datos con destino a otros países sin un nivel de protección equiparable. - Tratar los datos especialmente protegidos de forma ilegítima e incumpliendo los principios de la LOPD. - No atender u obstaculizar de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación u oposición. - No atender de forma sistemática el deber legal de notificación de la inclusión de los datos de	3 años	300.506,05 € a 610.012,10 €

Tabla 3: Infracciones y sanciones.

3.2. LSSICE

La Ley 24/2002 de *Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSICE)* está en vigor desde el 11 de Octubre de 2002.

Dicha Ley se aplica a diferentes **actividades** y a **empresas/profesionales** que prestan servicios de la sociedad de la información. Las actividades contempladas en la Ley se pueden ver en la Tabla 4.

	ACTIVIDADES
Servicios de la sociedad de la Información	* Contratación de bienes y servicios por vía electrónica. * Organización y gestión de subastas por medios electrónicos o de mercados y centros comerciales virtuales. * Gestión de compras en la red por grupos de personas. * Envíos de comunicaciones comerciales. * El suministro de información por vía telemática. * Vídeo bajo demanda y distribución de contenidos previa demanda.
Servicios de Intermediación	* Servicio de acceso a Internet. * Transmisión de datos por redes de telecomunicaciones. * Realización de copia temporal de las páginas de Internet solicitadas. * Alojamiento o servicios suministrados por otros. * Provisión de instrumentos de búsqueda, acceso, y recopilación de datos o enlaces a otros sitios de Internet.

Tabla 4: Actividades a las que se aplica la LSSICE

Se considera que una empresa/profesional es un **prestador de servicios**, siempre que presenten una actividad económica, en los siguientes casos:

- La organización y gestión de subastas por medios electrónicos o de mercados y centros comerciales virtuales.
- La gestión de compras en la red por grupos de personas.
- El envío de comunicaciones comerciales.
- El suministro de información vía telemática.
- El suministro, recepción, y en general la distribución de vídeo y otro tipo de contenidos previa petición individual.

Y se **aplica a**:

- Prestadores de servicios de la sociedad de la información establecidos en España.
- Prestadores de servicios de la sociedad de la información establecidos en un *estado miembro* de la Unión Europea o del Espacio Económico Europeo.

- Prestadores de servicios de la sociedad de la información establecidos en un estado *no perteneciente* a la Unión Europea o del Espacio Económico Europeo.

Además, todo el que desee prestar un servicio de la sociedad de la información está sujeto a:

- Un **régimen** que regula estos servicios en el mercado.
- **Obligaciones** que todas las empresas o profesionales que presten estos servicios deben cumplir.
- Deberes de **colaboración y régimen de responsabilidad**.

También se controlan las comunicaciones comerciales y la contratación vía electrónica.

La LSSICE establece diferentes **infracciones** en función de su gravedad y cada una de ellas se sanciona con multas. Se muestran todos los datos en la Tabla 5.

Infracción	Supuesto	Prescripción	Sanción
Leves	* No inscripción en el registro de nombres de dominio * No permitir acceso fácil, directo y gratuito a información general. * Incumplimiento de normas sobre comunicaciones comerciales. * Envío de comunicaciones electrónicas no solicitadas. * En caso que el destinatario sea un consumidor, no facilitar información previa a la celebración de un contrato. * Incumplimiento de la obligación de confirmar la recepción de la petición de contratación	6 meses	hasta 30.000€
Graves	* No informar mediante medios electrónicos sobre denominación social, e-mail y precios. * Envío masivo de comunicaciones comerciales. * No poner a disposición del usuario las condiciones generales de la contratación como condición previa al proceso de contratación electrónica. * Incumplir de forma habitual la obligación de confirmar la recepción del pedido. * La resistencia a la actuación inspectora.	2 años	30.001€ hasta 150.000€
Muy graves	* Incumplimiento de medidas restrictivas de la libre prestación del servicio ordenadas por el órgano competente. * Incumplimiento de las órdenes relativas a las suspensión de la transmisión, el alojamiento de datos, acceso a red o prestación de cualquier otro servicio de intermediación.	3 años	150.001€ hasta 600.000€

Tabla 5: Infracciones y sanciones LSSICE

4. POLÍTICA DE SEGURIDAD

Toda empresa, incluidas las PYMEs y microPYMEs, debe definir y poner en práctica una política de seguridad que asegure que los accesos que se realizan a los servicios e información de la empresa se lleven a cabo sólo por personas autorizadas. En este sentido es importante recalcar que no solamente es necesario tener en cuenta los accesos de personal ajeno a la compañía, sino también del acceso otorgado a las distintas personas de nuestra organización. Actualmente, al cumplir con LOPD se está generando una política de seguridad.

La política de seguridad debe ser asumida por la empresa como una inversión, ya que en caso de un ataque o una pérdida de información, no sólo debe valorarse el coste directo de dicho hecho, sino la pérdida de imagen y credibilidad que puede sufrir la compañía.

Conocidos los riesgos de la falta de seguridad, sólo resta indicar que debe incluirse un plan de seguridad y un plan de contingencia que sería el complemento final de un sistema seguro.

Cada empresa aplicará el plan de seguridad según sus necesidades. La siguiente lista enumera todos los conceptos que deberían especificarse, pero cada empresa la adaptará a su caso concreto. Dependiendo de la complejidad de nuestra compañía, tanto en organización del personal, como en los sistemas y servicios existentes, nuestra política deberá ser más o menos restrictiva.

4.1. Plan de seguridad

Los elementos a definir en el documento de política de seguridad de una empresa son los siguientes:

- Arquitectura de los sistemas existentes: sistemas de red, servidores, comunicaciones, etc.
- Acceso físico a los diferentes equipos.
- Definición de los perfiles existentes (roles, categorías de acceso).

- División de los bloques de información según su contenido, alcance y visibilidad de la misma.
- División de los servicios y aplicaciones existentes.
- Política de acceso de los diferentes perfiles a los recursos identificados (información y servicios/aplicaciones). Altas y bajas de recursos humanos. Privacidad de los datos interna y externamente.
- Política de encriptación de datos, tanto en información actual como en información de copias de seguridad.
- Política de securización de servidores.
- Política de copias de seguridad.
- Política de contraseñas, firmas electrónicas, etc.
- Política de aplicaciones corporativas instaladas en los equipos del usuario final
- Política de actualización de antivirus.
- Política de utilización del correo electrónico.
- Política de navegación en Internet.
- Aplicación de la LOPD (Ley Orgánica de Protección de Datos de Carácter Personal) a los datos sensibles de la empresa, incluidas las PYMEs.

4.2. Plan de contingencia

Como complemento al plan de seguridad es necesario contar con un plan de contingencia, ante fallos tanto de los sistemas como de las personas encargadas de los mismos.

Para cada uno de los sistemas identificados como críticos en el plan de seguridad es necesario elaborar una lista de acciones a llevar a cabo en caso de cualquier fallo que les pueda afectar. Dicha lista debe ser clara y concisa, orientada a que pueda realizarla alguien con poca o ninguna experiencia en el sistema basándose en unas instrucciones detalladas y secuenciales que faciliten la recuperación del recurso o sistema afectado, aunque sea en un modo de funcionamiento a bajo rendimiento o con prestaciones mínimas.

En el caso de sistemas altamente críticos debería contemplarse la posibilidad de implantar equipos redundantes, equipos de reserva, etc. Además, debe existir también el plan de contingencia ante fallo total.

El plan con sus acciones debe ser conocido y aceptado tanto por los responsables de sistemas como por los gestores de la empresa. Los planes de contingencia suelen centrarse especialmente en el fallo de equipos y sistemas y tienden a olvidar los recursos humanos.

Es importante definir las acciones a llevar a cabo ante la marcha de alguno de los integrantes del departamento de sistemas informáticos ya que por su conocimiento sobre el estado de los sistemas en materia de seguridad pueden crear una situación delicada. Es también necesario insistir en la necesidad de documentar las actividades y formas de actuar de estos equipos de trabajo, de forma que su actividad pueda ser emprendida por un nuevo equipo en un corto espacio de tiempo.

5. CONCLUSIONES

A través de este capítulo, hemos visto los posibles peligros que existen actualmente en las comunicaciones a través de Internet. Para ello, hemos estudiado brevemente las diferentes medidas que se pueden tomar para prevenir los ataques en las redes informáticas.

El plan de seguridad de la información de una organización debe tratar las amenazas que pueden surgir tanto desde el exterior como desde el interior de la organización: virus, hackers, los propios empleados, etc.

En la actualidad, la tecnología existente permite incluir sistemas de seguridad en las aplicaciones con unos costes razonables. Es conveniente planificar los procedimientos de seguridad antes de implantarlos y se debe estar familiarizado con técnicas como los certificados digitales, cifrado, y cortafuegos/firewalls.

Finalmente, no hay que olvidar cumplir con la normativa vigente para evitar posibles infracciones.

6. REFERENCIAS

- **Normativa de seguridad: LOPD y LSSICE.**
 - ✓ <http://www.portaley.com/protecciondatos/>
 - ✓ <http://www.delitosinformaticos.com>
 - ✓ <http://www.boe.org>
 - ✓ Autoevaluación : www.onnet.es
 - ✓ www.derecho.com
 - ✓ www.leydatos.com
 - ✓ Plataforma de servicios para despachos profesionales y PYMES:
www.loupdate.com
- **Virus**
 - ✓ www.zonavirus.com
 - ✓ www.sinvirus.com/
 - ✓ www.monografias.com/trabajos/estudiovirus.shtml
 - ✓ Enciclopedia de virus: www.pandasoftware.es/enciclopedia
 - ✓ Recursos contra virus: www.ropecadenas.com.ar/virus.htm
 - ✓ Información y vacunas contra virus: www.entrebtsd.com/php/virus
- **Criptografía y firmas y certificados digitales**
 - ✓ Criptografía asimétrica, presentación Power Point
<http://www.eumed.net/cursecon/ecoinet/seguridad/asimetricas.ppt>
 - ✓ Seguridad en Internet. <http://www.iec.csic.es/cryptonomicon>
 - ✓ Revista sobre conceptos técnicos, herramientas criptográficas y seguridad en Internet. <http://www.kriptopolis.com>
 - ✓ Criptografía y seguridad informática gratis: www.hormiga.org/criptografia.htm
 - ✓ <http://www.digitalsignatures.org>