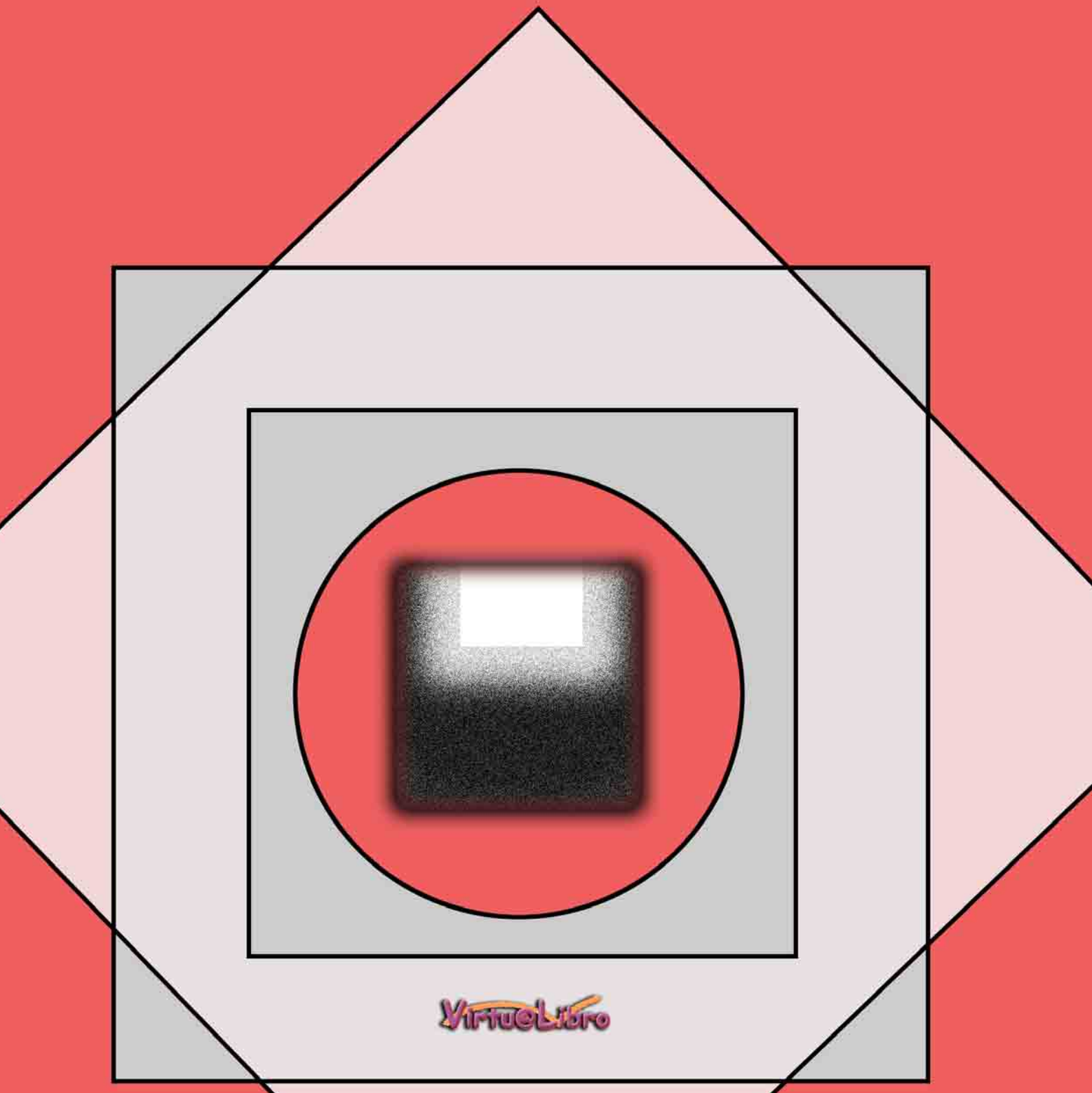
Protección de la información



Jose Luis Rivas López

DIRECCIÓN Y COORDINACIÓN: José Luis Rivas López
jlrivas@uvigo.es

DISEÑO DE LA CUBIERTA : Santiago Rivas López

PUBLICADA EN EL 2.003

Manuel Murguía 25-8ºA, 15011 La Coruña (España)
www.virtualibro.com

ISBN: 84-95660-89-X
Depósito Legal: C-1730-2003

Manufactured in Spain – Realizado en España

Para todas aquellas personas que han sido silenciadas. En especial a ese Sol que vuelve a brillar después de años de inactividad. No dejes que nadie te vuelva apagar.

Además me gustaría dedicárselo a mi familia y a Bernard por su paciencia ante éste pesado, GRACIAS.

AGRADECIMIENTOS

A virtualibro por publicar este libro sin animo de lucro

ÍNDICE

PRÓLOGO

José Luis Rivas López

Con este manual pretendemos dar un enfoque global de cómo proteger los datos que guardamos en los equipos y los que se suelen transmitir. Por tanto, el objetivo que nos marcamos es documentar que se puede hacer para asegurar en lo posible tanto los sistemas como las redes, teniendo en cuenta que ningún sistema se puede asegurar al cien por cien, debido a que siempre que haya una vulnerabilidad en el sistema es por donde va a ser atacado. La seguridad es como una cadena. De nada sirve que una cadena sea muy buena si uno de sus eslabones es defectuoso. La cadena se rompe.

Por este motivo dividimos este manual en 3 partes bien diferenciadas:

- La primera de ellas tratamos la parte técnica viendo la seguridad en los sistemas, en la red y en las aplicaciones WAP. Así como una introducción a los sistemas de auditoria normalizadas.

- En la segunda veremos las cuestiones legales, tratando: la base histórica jurídica de la protección de datos, la directiva europea 95/46/CE y la legislación española con su L.O.P.D.

- Finalmente explicamos como adaptarnos a la legislación española así como un ejemplo práctico de cómo implantar la L.O.P.D. en un sistema informático de un centro de estudios que imparte un curso.

CAPITULO 1

SEGURIDAD EN LOS SISTEMAS

José Ramón Sousa Vazquez

1.1 INTRODUCCIÓN

SEGURIDAD DE LA INFORMACIÓN es el estudio de los métodos y medios de protección de los sistemas de información y comunicaciones frente a revelaciones, modificaciones o destrucciones de la información, o ante fallos de proceso, almacenamiento o transmisión de dicha información, que tienen lugar de forma accidental o intencionada. La seguridad de la información se caracteriza como la protección frente a las amenazas de Confidencialidad, Integridad y Disponibilidad y pueden ser Amenazas de fuerza mayor, fallos de organización, humanos o técnicos o actos malintencionados. Algunas de las amenazas más frecuentes están relacionadas con el incumplimiento de las medidas de seguridad y con la administración incorrecta de los sistemas y la comisión de errores en su configuración y operación. El incumplimiento de las medidas de seguridad, como consecuencia de actos negligentes o falta de controles adecuados o la administración incorrecta del sistema y errores en la configuración de parámetros, originan daños que podrían haber sido evitados o por lo menos minimizados. Según las responsabilidades del usuario y la importancia de la norma incumplida, los daños podrían llegar a ser de gravedad.

1.2 SEGURIDAD FÍSICA

La seguridad física suministra protección ante accesos no autorizados, daños e interferencias a las instalaciones de la organización y a la información. Los requisitos sobre seguridad física varían considerablemente según las organizaciones y dependen de la escala y de la organización de los sistemas de información. Pero son aplicables a nivel general los conceptos de asegurar

áreas, controlar perímetros, controlar las entradas físicas e implantar equipamientos de seguridad. Las líneas de actuación recomendadas son:

En relación con la adecuación de locales:

- Definir de forma proporcionada las medidas que garanticen la seguridad de las áreas a proteger en relación con los requisitos de seguridad de la información que se almacene o procese.
- Construir barreras físicas del suelo al techo para prevenir entradas no autorizadas o contaminación del entorno. Las ventanas y puertas de las áreas seguras deben estar cerradas y controlarse periódicamente.
- Construir las instalaciones de forma discreta y minimizar las indicaciones sobre su propósito, evitando signos obvios (fuera o dentro del edificio) que identifiquen la presencia de las actividades cuya seguridad se desea.
- No identificar en directorios telefónicos y de los vestíbulos de la organización las localizaciones informáticas.
- Proteger los locales de amenazas potenciales como fuego, humos, agua, polvo, vibraciones, agentes químicos o radiaciones electromagnéticas. Instalar en el área un equipamiento apropiado de seguridad que debe revisarse regularmente de acuerdo con las instrucciones de los fabricantes.
- Separar las áreas de carga y descarga de material de las áreas a proteger.
- Documentar debidamente los procedimientos de emergencia y revisar esta documentación de forma regular.

En relación con la instalación de líneas de telecomunicaciones:

- Considerar medidas para proteger los cables de líneas de datos contra escuchas no autorizadas o contra daños.

En relación con la ubicación de equipamiento, materiales y copias de respaldo:

- Situar en áreas seguras los equipos a proteger donde se minimicen los accesos innecesarios a las áreas de trabajo, distanciadas de las zonas de acceso público y de las zonas con aproximación directa de vehículos públicos. Definir perímetros de seguridad con las correspondientes barreras y controles de entrada.
- Ubicar los terminales que manejen información y datos sensibles en lugares donde se reduzca el riesgo de que aquellos estén a la vista.
- Almacenar los materiales peligrosos y/o combustibles a una distancia de seguridad del emplazamiento de los ordenadores.
- Ubicar el equipamiento alternativo y copias de respaldo en sitios diferentes y a una distancia conveniente de seguridad.
- En relación con la entrada y salida física de personas y soportes de información:
- Controlar la entrada en exclusiva al personal autorizado a las áreas que se hayan definido como áreas a ser protegidas. Autorizar sólo con propósitos específicos y controlados los accesos a estas áreas, registrando los datos y tiempos de entrada y salida.
- Restringir el acceso a las áreas seguras del personal de los proveedores o de mantenimiento a los casos en que sea requerido y autorizado. Aun con acceso autorizado deben restringirse sus accesos y controlarse sus actividades.
- Definir normas y controles relativos a la posible salida/entrada física de soportes de información.

1.3 SEGURIDAD DE SISTEMAS

A la hora de hablar de seguridad en los sistemas, existen numerosos aspectos a ser considerados. Se hace muy difícil listar todos y cada uno de los posibles problemas de seguridad. Para ello existen en Internet herramientas que facilitan esa labor. Uno de los lugares de más reconocidos en esta área es

la **lista SANS/FBI de las veinte vulnerabilidades más importantes**. La mayoría de los ataques a sistemas computacionales vía Internet que acaban teniendo éxito pueden ser relacionados con el abuso de alguna de las 20 vulnerabilidades aquí descritas. Estas pocas vulnerabilidades son la base de la mayoría de los ataques exitosos, simplemente porque los atacantes son oportunistas - toman el camino más fácil y conveniente.

En el pasado, los administradores de sistemas afirmaban que no corregían muchas de estas brechas simplemente porque no sabían qué vulnerabilidades eran más peligrosas, y estaban demasiado ocupados para corregirlas todas. Algunos escáneres de vulnerabilidades son capaces de buscar 300, 500 o incluso hasta 800 vulnerabilidades, privando a los administradores de sistemas de la perspectiva necesaria para asegurar una adecuada protección contra los ataques más comunes.

Actualizaciones

La lista **'Top 20' SANS/FBI** es un documento vivo. Incluye instrucciones paso a paso y referencias adicionales para la resolución de los problemas.

Registros CVE

Encontrará referencias a registros **CVE** (Exposiciones y Vulnerabilidades Comunes) en cada vulnerabilidad, y es posible que se encuentre también con registros **CAN**. Los registros **CAN** son candidatos para ser **CVE** pero que no han sido completamente verificados.

Puertos a bloquear en el Firewall

Bloqueando estos puertos en el **firewall** u otro dispositivo de protección de perímetro, agregará una capa extra de defensa que le ayudará a protegerse de errores de configuración.

Análisis automatizado. Auditoria

Hay métodos que realizan búsqueda de vulnerabilidades de forma manual. Una aproximación más práctica para encontrar vulnerabilidades en sistemas **Unix** o **Windows** es usar una herramienta de análisis automatizado.

Vínculos al índice de vulnerabilidades ICAT

Cada referencia **CVE** se encuentra vinculada a su vulnerabilidad asociada en la lista del servicio del Instituto Nacional de Standards y Tecnología **ICAT** (http://icat.nist.gov/).

Las vulnerabilidades que afectan a todos los sistemas (G)

G1 - Instalaciones por defecto de sistemas y aplicaciones

La mayoría del software, incluyendo sistemas operativos y aplicaciones, viene con **scripts** de instalación o programas de instalación. Para poder dejar los sistemas operativos lo más rápido posible, con la mayor parte de funciones disponibles o habilitadas, y con la ayuda de muy poco trabajo por parte del administrador los **scripts** típicamente instalan más componentes de los que se necesitan en realidad. Muchos usuarios no son conscientes de lo que está realmente instalado en sus propios sistemas, dejando peligrosos programas de demostración en ellos por el simple hecho de que no saben que están ahí.

G2 - Cuentas sin contraseña o contraseñas débiles

La mayoría de los sistemas se encuentran configurados para usar contraseñas secretas como primera y única línea de defensa. Los nombres de usuario (**user IDs**) son relativamente fáciles de conseguir. Es por esto que si un atacante puede determinar el nombre de una cuenta y su contraseña correspondiente, él o ella pueden entrar en la red. Dos grandes problemas lo constituyen las contraseñas fáciles de adivinar y las contraseñas por defecto, pero aún así, uno mucho mayor son las cuentas sin contraseña.

G3 – Respaldos (backups) incompletos o inexistentes

Cuando ocurre un incidente, la recuperación requiere respaldos actualizados y métodos probados para restaurar la información. Se deben de verificar tanto el respaldo como la restauración.

G4 – Gran número de puertos abiertos

Tanto los usuarios legítimos como los atacantes se conectan a los sistemas por medio de puertos. Cuantos más puertos se encuentren abiertos más formas hay para que alguien se conecte. Es importante mantener abiertos sólo los puertos imprescindibles para que el sistema funcione correctamente.

G5 – Insuficiente filtrado de los paquetes con direcciones de inicio y destino inadecuadas

La falsificación de direcciones **IP** es un método comúnmente utilizado por los atacantes para cubrir sus huellas cuando atacan a una víctima. Utilizar un mecanismo de filtrado sobre el tráfico que entra en la red (**ingress filtering**) y el que sale (**egress filtering**) le ayudará a lograr un alto nivel de protección.

G6 – Registro de eventos (logging) incompleto o inexistente

Una de las máximas de la seguridad es, "la prevención es ideal, pero la detección es fundamental". Cada semana se descubren nuevas vulnerabilidades y existen muy pocas formas de defenderse de los ataques que hagan uso de las mismas. Una vez que usted ha sido atacado, sin registros (**logs**) hay muy pocas probabilidades de que descubra qué hicieron realmente los atacantes.

G7 – Programas CGI vulnerables

La mayoría de los servidores Web, incluyendo **IIS** de **Microsoft** y **Apache**, permiten el uso de programas **CGI** (**Common Gateway Interface**)

para proporcionar interactividad a las páginas Web. De hecho, la mayoría de los servidores Web vienen con programas **CGI** de ejemplo preinstalados. Desgraciadamente demasiados programadores de **CGIs** pasan por alto el hecho de que sus programas proporcionan un vínculo directo entre cualquier usuario en cualquier parte de Internet y el sistema operativo en la máquina que se encuentra ejecutando el servidor Web.

Vulnerabilidades más críticas en sistemas Windows (W)

W1 - Vulnerabilidad Unicode (Salto de directorio en servidores Web - Web Server Folder Traversal)

Unicode proporciona un número único para cada carácter, sin importar cuál sea la plataforma, cuál sea el programa o cuál sea el lenguaje. El estándar **Unicode** ha sido adoptado por la mayoría de los fabricantes, incluyendo **Microsoft**. Mediante el envío a un servidor **IIS** de una **URL** creada cuidadosamente con secuencias inválidas de **Unicode UTF-8**, un atacante puede forzar a que el servidor literalmente entre y salga de cualquier directorio y ejecute scripts de forma arbitraria.

W2 - Desbordamiento de Buffer en extensiones ISAPI

Microsoft Internet Information Server (**IIS**) es un servidor Web que se encuentra en la mayoría de los sitios basados en **Microsoft Windows 2000** y **Microsoft Windows XP**. Cuando se instala **IIS**, se instalan también automáticamente varias extensiones **ISAPI** mediante el uso de **DLLs**. Varias de las **DLLs**, como **idq.dll**, contienen errores de programación que causan que éstas realicen un chequeo incorrecto de límites.

W3 - Exploit para RDS del IIS (Servicios de información remota Microsoft)

Microsoft Internet Information Server (IIS) es un servidor Web que se encuentra en la mayoría de los sitios basados en **Microsoft Windows 2000** y

Windows XP. Es posible explotar fallos de programación en los servicios **RDS** de **IIS** con el fin de ejecutar comandos remotos con atributos administrativos.

W4 - NETBIOS - recursos compartidos en red no protegidos

El protocolo SMB (**Server Message Block**), también conocido como CIFS (**Common Internet File System**), permite habilitar la compartición de recursos a través de la red. Habilitar la propiedad de compartir archivos en máquinas Windows las hace vulnerables tanto al robo de información como a ciertos tipos de virus que se propagan con rapidez. Las máquinas **Macintosh** y **UNIX** son también vulnerables a ataques de este tipo si los usuarios habilitan la compartición de archivos.

W5 -Fuga de información a través de conexiones de tipo "sesión nula"

Una conexión de tipo "sesión nula", también conocida como "entrada anónima al sistema", es un mecanismo que permite a un usuario anónimo obtener información (como nombres de usuario y recursos compartidos) a través de la red, o conectarse sin autenticarse contra el sistema.

W6 - Hashing débil en SAM (LM hash)

A pesar de que la mayor parte de los usuarios de Windows no tienen necesidad de soporte para **LAN Manager**, Microsoft almacena las contraseñas **LAN Manager** por defecto, tanto en los sistemas **Windows 2000** como en **Windows XP**. Dado que **LAN Manager** utiliza un esquema de cifrado mucho más débil que el resto de los utilizados por **Microsoft**, las contraseñas **LAN Manager** pueden ser descifradas en un corto espacio de tiempo.

Vulnerabilidades más críticas en sistemas Unix (U)

U1 - Desbordamiento de Buffer en los servicios RPC

Las llamadas a procedimiento remoto (**RPCs**) hacen posible que programas que se encuentran ejecutándose en un sistema ejecuten a su vez otros programas en un segundo sistema. Este tipo se servicios son ampliamente utilizados para acceder a servicios de red tales como el compartir archivos a través de **NFS** o **NIS**. Existen evidencias de que la mayor parte de los ataques distribuidos de denegación de servicio efectuados durante 1999 y principios del 2000 fueron lanzados desde sistemas que habían sido comprometidos debido a vulnerabilidades en los **RPC**.

U2 - Vulnerabilidades en sendmail

Sendmail es un programa que envía, recibe y redirecciona la mayor parte del correo electrónico procesado en máquinas **UNIX** y **Linux**. Lo extendido de su uso en Internet lo convierte en uno de los objetivos prioritarios de los hackers. A lo largo de los años han sido descubiertos en sendmail diversos defectos como la posibilidad de ejecutar código arbitrario por desbordamientos a la hora de tratar los mensajes que recibe.

U3 - Debilidades en BIND

El paquete **Berkeley Internet Name Domain** (BIND) es una de las implementaciones más utilizadas del Servicio de Nombres de Dominio (**DNS**). De acuerdo con un estudio realizado a mediados de 1999, nada menos que el 50% de todos los servidores **DNS** conectados a Internet estaban utilizando versiones vulnerables de **BIND**. En un caso que podría servir como ejemplo de un ataque clásico a **BIND**, los intrusos borraron los logs del sistema e instalaron herramientas que les permitieron conseguir privilegios de administrador.

U4 - Los comandos "r"

Las relaciones de confianza son ampliamente utilizadas en el mundo **UNIX**, especialmente para la administración de sistemas. Las empresas habitualmente asignan a un único administrador la responsabilidad sobre docenas o incluso centenares de sistemas. Los administradores a menudo utilizan relaciones de confianza a través del uso de los comandos "r" para poder saltar de sistema en sistema convenientemente. Los comandos "r" permiten acceder a sistemas remotos sin tener que introducir ninguna contraseña. Los siguientes comandos "r" son a menudo utilizados: **rlogin, rsh y rcp**.

U5 – LPD (demonio del protocolo de impresión remota)

En **UNIX**, el demonio "**in.lpd**" proporciona los servicios necesarios para que los usuarios puedan hacer uso de la impresora local. **LPD** espera dichas peticiones escuchando en el puerto TCP 515. Los programadores que desarrollaron el código que transfiere trabajos de impresión de una máquina a otra, cometieron un error que se ha traducido en una vulnerabilidad de desbordamiento de buffer.

U6 – sadmind y mountd

Sadmind permite la administración remota de sistemas **Solaris**, proporcionando un interfaz gráfico para labores de administración de sistemas. **Mountd**, por otro lado, controla y arbitra el acceso a los volúmenes **NFS** en los sistemas **UNIX**. Debido a errores de programación cometidos por los desarrolladores de estas aplicaciones, existe la posibilidad de utilizar desbordamientos de buffer en las mismas para conseguir acceso como super-usuario en los sistemas afectados.

U7 – Nombres de comunidad SNMP por omisión

El Protocolo Simple de Administración de Red (**Simple Network Management Protocol - SNMP**) es ampliamente utilizado por los

administradores de red para supervisar y administrar todo tipo de dispositivos de red, desde enrutadores hasta impresoras u ordenadores. El único mecanismo de autenticación que **SNMP** usa es un "nombre de comunidad" no cifrado. Los posibles agresores pueden utilizar esta vulnerabilidad en **SNMP** para reconfigurar o incluso desactivar dispositivos remotamente. La captura del tráfico **SNMP**, por otra parte, puede revelar una gran cantidad de información sobre la estructura de la red, así como de los dispositivos y sistemas conectados a la misma. Toda esa información puede ser utilizada por parte de los intrusos para seleccionar blancos y planear ataques.

Puertos comúnmente vulnerables

Bloquear estos puertos constituye tan sólo un requisito mínimo necesario para la seguridad perimetral y no una lista exhaustiva para la configuración del **firewall**. Una aproximación mucho mejor es bloquear todos aquellos puertos que no son utilizados, e incluso cuando esté convencido de que dichos puertos están siendo bloqueados, aún debería supervisarlos de cerca para detectar intentos de intrusión.

1. **Servicios de Inicio de Sesión** -- telnet (23/tcp), SSH (22/tcp), FTP (21/tcp), NetBIOS (139/tcp), rlogin et al (512/tcp through 514/tcp)
2. **RPC y NFS**-- Portmap/rpcbind (111/tcp y 111/udp), NFS (2049/tcp y 2049/udp), lockd (4045/tcp y 4045/udp)
3. **NetBIOS en Windows NT** -- 135 (tcp y udp), 137 (udp), 138 (udp), 139 (tcp). Windows 2000 - los puertos anteriores y además el 445(tcp y udp)
4. **X Windows** - del 6000/tcp al 6255/tcp
5. **Servicios de Nombres** -- DNS (53/udp) a todas las máquinas que no sean servidores de nombres, transferencias de zona DNS (53/tcp) excepto desde servidores secundarios externos, LDAP (389/tcp y 389/udp)
6. **Mail** -- SMTP (25/tcp) a todas las máquinas que no sean encaminadores de correo externos, POP (109/tcp y 110/tcp), IMAP (143/tcp)

7. **Web -- HTTP** (80/tcp) y SSL (443/tcp) excepto a los servidores web externos, y también puede bloquear otros puertos altos que son comúnmente utilizados para la ubicación de servicios HTTP (8000/tcp, 8080/tcp, 8888/tcp, etc.)
8. **"Pequeños servicios"**-puertos inferiores al 20/tcp y 20/udp, y time (37/tcp y 37/udp)
9. **Otros** -- TFTP (69/udp), finger (79/tcp), NNTP (119/tcp), NTP (123/udp), LPD (515/tcp), syslog (514/udp), SNMP (161/tcp y 161/udp, 162/tcp y 162/udp), BGP (179/tcp), SOCKS (1080/tcp)
10. **ICMP**-bloquee los mensajes ICMP "echo request" entrantes (ping y Windows traceroute), "echo reply" salientes, "time exceeded", y "destination unreachable" excepto los mensajes "packet too big" (tipo 3, código 4). (Este punto asume que está dispuesto a renunciar a los usos legítimos de los mensajes "ICMP echo request" en aras de evitar el uso malicioso de los mismos).

1.4 SEGURIDAD EN SERVICIOS WEB

Cuando una organización dispone de un servicio Web invita a todo el mundo a realizar peticiones HTTP. Existen multitud de ataques contra los diversos sistemas que dan soportes a este tipo de servicios. **Esto significa que el código del servicio Web es parte del perímetro de seguridad**. Aquí se tratarán las vulnerabilidades de servicios Web más serias, posteriormente se podrá ahondar en ellas a través de la documentación que se señalará. Se tratarán 10 categorías de vulnerabilidades que requieren un tratamiento inmediato, además debe de ser incluida en el diseño y planes de los proyectos para realizar estos servicios. Los jefes de proyecto deberían incluir una parte esencial de su tiempo a incluir aspectos relacionados con la seguridad, como diseño de mecanismos, políticas de seguridad, robustez de sistemas y revisión de código.

S1 – Parámetros no validados.

Los servicios Web utilizan información de las peticiones **HTTP** para saber como responder. Los atacantes exploran cualquier parte de la petición **HTTP**, como url, cabeceras, cookies y campos ocultos. Si no existe un mecanismo que permita una fuerte y centrada validación de parámetros, existe un riesgo potencial. Estos parámetros deben convertirse a su forma más simple antes de ser validados para evitar código malicioso enmascarado. Este proceso se llama **canonicalización**. La validación en el lado del cliente es una buena idea de eficiencia y usabilidad pero nunca de seguridad. Se hace necesario por lo tanto chequeo de parámetros en el servidor.

S2 – Control de acceso violado.

Los controles de acceso y autorización, es la forma en que un servicio Web da acceso a los contenidos y funciones a unos usuarios frente a otros. Este control se realiza tras la autentificación y decide lo que los usuarios autentificados pueden realizar. Suena como un problema trivial pero es difícil de implementar correctamente. Un control bien hecho debe tener en consideración el contenido y funciones que se proveen. Además, los usuarios suelen estar agrupados con diferentes roles y privilegios. Los desarrolladores con frecuencia desestiman la creación de un adecuado control de acceso de hecho muchos de los controles que existen no son definidos sino que se disponen según se desarrolla la aplicación.

S3 – Ruptura en el manejo de control de cuentas y sesiones.

El manejo de las cuentas y de las sesiones incluye todos los aspectos de manejo de usuarios y sesiones activas. La autentificación es una de las partes de este proceso, pero incluso sólidos mecanismos de autentificación pueden ser anulados por funciones erróneas de manejo de credenciales, cambio de palabra de paso, olvido de palabra de paso, recordatorio de palabra de paso, actualización de cuenta. Existen muchas implementaciones de administración de claves con fallos que pueden comprometer a los usuarios del sistema. En

muchas ocasiones las sesiones no están protegidas, un atacante puede recoger una sesión activa y asumir la entidad de un usuario, la creación de sistemas con sesión protegida fuertemente, se implementa mediante un control de su ciclo de vida que en ocasiones es olvidado por muchos desarrolladores. Con frecuencia se utilizan contraseñas en claro embebidas en los ficheros de configuración o en el código.

S4 – Desbordamiento de buffer.

Los atacantes externos usan el desbordamiento de buffer para corromper la ejecución de los servicios Web. Enviando entradas cuidadosamente preparadas a la aplicación, se puede conseguir que esta ejecute un código arbitrario, incluso tomar el control de la máquina. No es fácil de descubrir, e incluso cuando se hace es extremadamente difícil de explotar. Sin embargo, se han conseguido identificar numerosos errores de este estilo en muchos productos y componentes. El desbordamiento de buffer se presenta tanto en los contenidos estáticos como dinámicos.

S5 – Errores por inyección de comandos.

La inyección de código permite a los atacantes introducir código dañino a través del servicio Web a otros sistemas. Estos ataques son llamadas de sistema, utilización de programas externos mediante intérprete de comandos y llamadas **SQL** a las bases de datos de **backend**. Cualquier lenguaje puede ser incluido en aplicaciones pobremente diseñadas y luego ejecutarse. Muchas aplicaciones Web utilizan facilidades del sistema operativo o de programas externos para realizar sus funciones. La inyección de comandos puede ser fácil de descubrir y explotar pero también es bastante oscuro su conocimiento. El rango de problemas que pueden ocurrir es muy amplio, incluso la destrucción del sistema.

S6 – Problemas con el manejo de errores.

El manejo no adecuado de los errores puede introducir una variedad de problemas de seguridad. El problema más común es un detallado mensaje de error interno donde se da información de las trazas, registros de bases de datos y códigos de error. Estos mensajes revelan detalles de la implementación que no deberían de ser mostrados. Las aplicaciones Web frecuentemente generan condiciones de error que deben manejarse mediante un adecuado esquema que provea una información escueta para el usuario, de diagnóstico para los administradores y no útil para los posibles atacantes. Un buen mecanismo para controlar los errores sería el incluir mensajes de error simples acompañados de su registro.

S7 – Uso inseguro de la criptografía.

Muchas aplicaciones Web tienen una necesidad de almacenar información sensible, como son contraseñas, número de tarjetas de crédito o información de la propiedad. Con frecuencia las técnicas de cifrado se usan para proteger esta información. Con la evolución de las técnicas de cifrado esto resulta cada vez más fácil y los desarrolladores cada vez cometen más errores al integrarlo en su aplicación. De hecho se sobreestima la protección que se obtiene con el cifrado y no se controla la seguridad de otros aspectos del sitio.

S8 – Errores de implementaciones de administración remota

Existen interfaces administrativas que proveen potentes facilidades para controlar una aplicación Web. Estas son el control eficiente de usuarios, datos y contenidos del sitio. En muchos casos los sitios soportan una variedad de roles administrativos que permiten una granularidad muy fina en la administración del sitio. Los problemas comunes que ocurren en esta área incluyen la no utilización de autentificación y cifrado para el acceso, la mala definición de las funciones de administración, errores en la separación entre los usuarios y administradores y dar capacidades administrativas que no son necesarias.

S9 – Fallos en sistemas con scripts XSS

Las vulnerabilidades en este caso ocurren cuando un atacante utiliza una aplicación Web para enviar código dañino, generalmente **JavaScript** a otro usuario. Cuando se recoge la entrada del usuario sin filtrar se puede llegar a introducir código que afecte a otros posibles usuarios del sistema. Hay dos tipos los almacenados y los de por reflexión. En el primer caso se almacena en el servidor el código y en el segundo el servidor se utiliza como transporte para acceder a otro usuario final. Las posibilidades de que se descubran estos errores es muy alta ya que solo se necesita paciencia y un navegador. Además existen numerosas herramientas que permiten "automatizar" estas tareas.

S10 – Falta de configuración correcta en los servidores

Los servidores son los encargados de servir los contenidos y de llamar a las aplicaciones que generan dichos contenidos. Además se proveen numerosos servicios añadidos como pueden ser almacenamiento, servicio de directorio, correo, mensajería, etc. Con frecuencia el grupo de desarrollo esta separado del grupo de operación y este es uno de los puntos fuertes a ser considerado cuando se habla de seguridad. Debe de existir interacción entre estos dos grupos. Hay numerosos apartados de configuración que deben de ser considerados: Aplicación de parches de correción, mala configuración que permite el listado de directorios, ficheros no necesarios, permisos incorrectos, servicios no necesarios, cuentas por defecto con contraseñas por defecto, mensajes demasiado informativos, falta de uso de cifrado donde es necesario. Estos problemas pueden ser fácilmente detectados con el uso de escáneres que detectan estas vulnerabilidades. El tener software seguro con configuraciones seguras es el primer paso para dotar de seguridad a un sistema.

1.5 VIRUS

¿Qué son los virus?

Son programas que se introducen en nuestros ordenadores de formas muy diversas. Este tipo de programas son especiales ya que pueden producir efectos no deseados y nocivos. Una vez el virus se haya introducido en el ordenador, se colocará en lugares donde el usuario pueda ejecutarlos de manera no intencionada. Hasta que no se ejecuta el programa infectado o se cumple una determinada condición, el virus no actúa. Incluso en algunas ocasiones, los efectos producidos por éste, se aprecian tiempo después de su ejecución.

¿Qué elementos infectan los virus?

El objetivo primordial de los virus son los ficheros que se encuentran en un medio de almacenamiento como los discos duros o disquetes. Más concretamente serán infectados todos aquellos archivos, ficheros o documentos (los tres términos indican el mismo concepto, en general) que tengan la característica de ser programas. Un programa no es más que un fichero cuya extensión es **EXE** o **COM**, que se puede ejecutar para que realice determinadas operaciones.

Medios de entrada más habituales para los virus

- **Unidades de disco extraibles:** Algunos de estos medios de almacenamiento pueden ser los disquetes, CD-ROMs, unidades Zip y Unidades Jazz. Si alguno de ellos se encontrase infectado y trabajásemos con él en un ordenador, éste será infectado.
- **Redes de ordenadores:** Existen conexiones entre cualquiera de los ordenadores que forman parte de la red, pudiendo transferirse información entre ellos. Si alguna de esta información transmitida de un ordenador a otro estuviese infectada, el ordenador en el que se recibe será infectado.

- **Internet:** Cada día más se utilizan las posibilidades que brinda Internet para obtener información, realizar envíos y recepciones de ficheros, recibir y publicar noticias, o descargar ficheros. Cualquier virus puede introducirse en nuestro ordenador al mismo tiempo que la información recibida. A través de Internet la infección podría realizarse empleando diferentes caminos como los siguientes:
    - **Correo electrónico:** En un mensaje enviado o recibido se pueden incluir documentos o ficheros (fichero adjunto o anexado). Estos ficheros podrían estar infectados, contagiando al ordenador destinatario.
    - **Páginas Web:**Las páginas que visitamos en Internet son ficheros de texto o imágenes escritos en un lenguaje denominado **HTML**. No obstante también pueden contener programas denominados Controles **ActiveX** y **Applets** de **Java** que son programas. Estos sí pueden estar infectados y podrían infectar al usuario que se encuentre visitando esa página.

Objetivos de los virus

El objetivo de los virus, la mayoría de las veces es destructivo, pero no siempre. En ocasiones son obras maestras de la programación, que persiguen el reto de aprender o de demostrar los fallos de seguridad, de sistemas operativos o Internet. Programados en ensamblador (código de máquina) u otros lenguajes de alto nivel, los virus son cada vez más potentes y afectan a más archivos, como es el caso de el **OUTLOOK.PDFWorm**, el primer gusano que se presenta en un archivo **PDF** (**Portable Document Format**), el conocido formato de **Adobe Acrobat**. Aunque claramente, este último en la actualidad puede considerarse como un virus de laboratorio encaminado más a ser una prueba de concepto.

Cuando un virus comienza su infección, entra en acción el código, que dependiendo de su programación, será más o menos destructivo, provocando problemas al sistema informático del usuario. Se comportan a veces de forma

similar a los biológicos, aunque hay una diferencia muy clara. Los virus informáticos siempre se introducen en el sistema cuando el usuario los ejecuta. Por lo tanto si tenemos un antivirus actualizado y nos abstenemos de abrir archivos de procedencia sospechosa, desconocida, podemos estar a salvo de estos, por lo menos en un porcentaje muy alto. Pero en los creadores de estos programas informáticos víricos, en ocasiones, podemos encontrar obras de "ingeniería social" que propician que el usuario ejecute un virus sin prácticamente darse cuenta, por ejemplo al recibir un correo de una persona conocida diciéndonos “Hola cómo estás... te mando esto para tus comentarios”, tenemos la situación del conocido gusano **Sircam**.

Ahora bien, un troyano es un programa que crea una puerta trasera (es decir proporciona la posibilidad de un acceso no autorizado) al equipo de cómputo de la víctima, de tal forma que le abre un puerto (o canal de comunicación) por donde se puede acceder a su sistema. Como tales, suelen encontrarse pegados a otros programas mediante diversas utilidades específicamente diseñadas para ello, y ocultando su función real mediante la apariencia de un programa que aparentemente funciona bien, como podría ser un simple salva pantallas.

Algunos de ellos permiten incluso realizar funciones que de otra forma no sería factible. Existe una analogía en su funcionamiento (la cual discrepa con su origen e intención) con los programas de control remoto legítimos o legales. De hecho se diferencian únicamente en el modo de instalación y en que invariablemente no aparecen en la bandeja de sistema ni en la barra de estado. Constan de dos partes: cliente y servidor. El servidor es quien permite que los intrusos ingresen de hecho a nuestra computadora, y que tengan incluso la posibilidad de enviar nuestra dirección **IP** a alguna dirección de correo electrónico, a una lista de correo, al **ICQ**, o a un canal de **IRC**. Para librarnos de ellos, lo mejor es el sentido común: No aceptarles regalos a desconocidos, ni ejecutables de ninguna clase.

Un caballo de Troya (o troyano) es un programa aparentemente útil, novedoso, o atractivo que contiene funciones ocultas que permiten, por

ejemplo, obtener privilegios de usuario (siempre que el programa se ejecute), suponiendo un enorme problema de seguridad. Generalmente un caballo de Troya no tiene efecto sin la colaboración involuntaria del usuario a quien va dirigido. Los caballos de Troya son normalmente instalados por los propios usuarios inadvertidamente o bien por intrusos que han obtenido acceso sin permiso al sistema a través de otros medios. Aunque conceptualmente algunos autores consideren que no son virus como tales, estos pueden **realizar acciones destructivas** como algunos virus. Al constar de dos programas, un servidor y un cliente. El servidor es por ejemplo nuestro equipo (para hacernos una idea) y el cliente es quien intenta "entrar" en nuestra computadora, una vez que lo ha logrado, de acuerdo a las características de dicho troyano, bien puede borrar archivos de nuestro disco duro, formatearlo, abrir la unidad de cd-rom, realizar capturas de nuestro escritorio, de lo que tecleamos, incluso existen troyanos que copian ficheros sensibles del sistema y los envían a una dirección de correo electrónico. Estos "Caballos de Troya" suelen estar contenidos en programas ejecutables y a través del chat, por ejemplo **mIRC** nos pueden enviar este tipo de "programas", o a través del **ICQ**. Normalmente suelen quedarse residentes en memoria e introducen código en el registro de Windows para que cada vez que encendamos nuestro equipo puedan quedar activados.

Mucho es lo que se ha escrito acerca de cómo erradicar los gusanos, troyanos o puertas traseras de un sistema. Lo único que podemos remarcar es que actualmente el trabajo preventivo es asunto de tres por lo menos. Se requiere de mantener un buen antivirus bien configurado y actualizado, tener al día todas las actualizaciones de seguridad y conocer aunque sea de manera básica las diversas utilerías para erradicación de los troyanos más comunes.

Virus de ingeniería social

Una de las armas más peligrosas que puede emplear un virus de nueva creación para conseguir una rápida propagación es el empleo de las denominadas “Técnicas de Ingeniería Social”. Estas técnicas consisten en

utilizar un reclamo para atraer la atención del usuario y conseguir que abra un archivo que acaba de recibir y que, en realidad, contiene un código malicioso.

Uno de los trucos más utilizados para este fin es el de incluir nombres o frases de temas que, en el momento de su creación, se encuentran de máxima actualidad, para así conseguir un mayor interés por el mensaje enviado. Sin ir más lejos, uno de los últimos virus aparecidos en escena ha sido el **Prestige**, un nuevo gusano de correo electrónico que hace alusión a la catástrofe del petrolero del mismo nombre. En este caso, el mensaje de correo electrónico que recibe el usuario y que lleva por asunto: "fotos INEDITAS del **PRESTIGE** en el fondo del Atlántico", lleva un archivo adjunto que, supuestamente, permite acceder a material fotográfico. Sin embargo, lo que realmente incluye dicho fichero es un virus.

Otra de las formas empleadas por los creadores de virus para llamar la atención de los internautas es utilizar el nombre de un personaje famoso, ya sea del mundo del deporte, de la vida política o del espectáculo, para atraer a un mayor número de víctimas. Al llegar la Navidad es habitual que proliferen correos electrónicos que adjuntan pequeñas aplicaciones gráficas, en forma de felicitaciones de Pascua o del nuevo año. Conscientes de ello, los creadores de virus aprovechan para generar códigos que, bajo un inocente aspecto, aluden a la Navidad para engañar al usuario y conseguir que ejecute el archivo que contiene al código malicioso, contribuyendo así a su difusión.

El verdadero peligro de los hoax.

Desde hace ya varios años, Internet, y en especial el correo electrónico, ha servido como escenario para la difusión de los denominados virus hoax, es decir, mensajes con falsas alarmas sobre virus informáticos que se distribuyen en cadena a través del correo electrónico. Normalmente, estas cadenas van involucrando cada vez a un mayor número de usuarios, al sugerirse al receptor reenviar la información a todas las direcciones de correo posibles para extender la supuesta advertencia de un nuevo virus. Esta rápida propagación

se debe, fundamentalmente, a la ingenuidad de los internautas, ya que al no saber distinguir un hoax de un virus, los usuarios envian dicha información como un acto de buena fe.

A pesar de que no son realmente virus, sin duda alguna, este tipo de amenazas son consideradas dañinas ya que muchas veces implican pérdida de productividad y tiempo de las personas que reciben estas alertas. Asimismo hay que contar con la saturación de información que producen en la Red, debido a la gran cantidad de información que tienen que procesar los servidores. Y es que, algunos de los hoax más populares llevan más de tres años distribuyéndose de usuario en usuario, a pesar de los esfuerzos y recursos empleados por importantes organizaciones para desmentirlos.

Habitualmente, la gran mayoría de estos mensajes tienen en común una serie de particularidades propias dentro de sus textos. Así por ejemplo, siempre incluye frases o expresiones catastrofistas del tipo: "Alerta", "No existe cura" o "Destruye todos los archivos irremediablemente". Por otro lado, un gran número de estos mensajes suelen citar a empresas de prestigio del sector, ya sean fabricantes de hardware o software o empresas de seguridad, para dar mayor credibilidad al supuesto virus.

En la gran mayoría de los casos estos rumores surgen de los propios ordenadores de internautas bromistas (de ahí la traducción al español de **hoax**: "trampa, broma, bulo...)", cuya finalidad es crear alarma entre los cibernautas, recopilar gran cantidad de direcciones de correo, incitar al propio receptor a causar daños en su ordenador o la simple notoriedad del receptor. Sin embargo, en algunas ocasiones, el rumor suele coincidir con hechos o situaciones que se dan en la vida cotidiana. Sin embargo, algunos de estos bulos si pueden llegar a causar daños más serios en los equipos informáticos de los usuarios. Un claro ejemplo fue el **hoax** "**Sulfnbk.exe**" donde aconsejaba que todo ordenador que tuviera dicho archivo debiera eliminarlo del disco duro provocando que se dañara un archivo de sistema.

Si en alguna ocasión recibimos un mensaje con estas características la persona que lo ha enviado seguramente ignora su falsedad. Si no se conoce la autenticidad de dicho mensaje, lo más aconsejable averiguarlo a través de las páginas de Internet de las diferentes compañías de seguridad y, si se decide reenviarlo, ocultar las direcciones de correo para que los receptores no reciban el resto de contactos.

CAPITULO 2

SEGURIDAD EN LA RED

Miguel Jiménez Polo

2.1 INTRODUCCIÓN

El objetivo de este capítulo es ayudar a entender los fundamentos de la protección de una infraestructura de red. La seguridad en redes es un tema complejo, debido en parte a la abundancia de tecnologías de seguridad, que exige estar permanentemente al día en los agujeros de seguridad de sistemas y en las soluciones.

Las estadísticas del CERT dan una idea de la importancia de la seguridad en las redes. Cada año se incrementa el número de incidentes de seguridad, lo que hace que sea necesario invertir en formación, tecnología y equipos adecuados para nuestra empresa.

2.2 AMENAZAS Y ATAQUES. COMO PROTEGERNOS

Las amenazas más comunes que pueden afectar a una empresa son de muchos tipos, pero la mayoría de ellas se pueden englobar en tres categorías básicas:

- Acceso no autorizado. Tiene lugar cuando alguien no autorizado consigue acceder a un recurso y además podría alterarlo.

- Suplantación de identidad. Está relacionado con lo anterior, pero además incluye la capacidad de presentar credenciales de alguien o algo que no se es: apropiación de la clave privada, obtención de usuario/contraseña, etc.

- Denegación de servicio (DoS). Es una interrupción del servicio, generalmente debido a que temporalmente no está disponible. Existen muchos ataques DoS, la mayor parte de ellos producidos desde el protocolo IP. Los más conocidos son:

  - Ataque SYN de TCP. Cuando se inicia una conexión TCP, el host destino recibe un paquete de sincronización con el bit SYN activado y contesta con un paquete de acuse de recibo de sincronización con los bits SYN y ACK activados. Para establecer la conexión, el host destino deberá recibir un ACK del SYN/ACK enviado. Un atacante podría beneficiarse de la siguiente forma: una vez que ha enviado un paquete SYN y el servidor ha respondido con SYN/ACK, el cliente no responde con el ACK esperado, creando una conexión medio abierta. Si este proceso se produce repetidas veces llega un momento en que el servidor no es capaz de aceptar nuevas conexiones. Aunque estas conexiones caducan pasado un time-out, el atacante podría seguir enviando paquetes SYN (con IP spoofing: dirección origen falsificada) más rapidamente que este time-out. Así se pueden denegar servicios TCP como correo, web, etc. Por medio de dispositivos firewall o proxy se pueden interceptar y limitar estas conexiones.

  - Ping de la muerte. Explota el punto débil de la fragmentación de grandes paquetes de petición de ECHO del protocolo ICMP. Si enviamos un paquete muy grande, el receptor puede tener problemas al reensamblarlo. Si esto lo realizamos de forma continuada produciremos sobrecarga tanto en la red como el sistema atacado. La variante SMURF hace esto mismo pero a las direcciones de broadcast de una subred, por lo que todas las máquinas de la subred responderán a esta dirección. Si además el atacante realiza IP spoofing, todas las máquinas de la subred enviarán un paquete de respuesta a esta dirección IP.

Los principales orígenes de los ataques son personas (empleados, ex-empleados, curiosos,piratas, terroristas, intrusos remunerados, etc), software (defectuoso, herramientas de seguridad, puertas traseras, bombas lógicas,

canales ocultos, virus, gusanos, caballos de Troya) y catástrofes (incendios, inundaciones, etc). La mayor parte de incidentes de seguridad son realizados por software del tipo gusanos y virus.

Para protegernos de estos ataques hay una serie de pasos que debemos realizar en cualquier infraestructura de red. Son los siguientes:

- Análisis de amenazas. Consiste en identificar las amenazas que podemos sufrir, los recursos que poseemos y asignar un valor a cada recurso. Una amenaza puede ser cualquier persona, objeto o evento que si se consuma puede causar daños en nuestra red, y posibles pérdidas económicas.

- Evaluación de posibles pérdidas y su probabilidad. Hay que evaluar cuales son las consecuencias inmediatas y futuras de una amenaza consumada, teniendo en cuenta su probabilidad. Cuanto mayor sea la posibilidad de producirse, más estrictas deberán ser las medidas de seguridad. Hay que decidir qué recurso requiere protección. Las pérdidas más comunes son: robo de datos, pérdida de la integridad de los datos e indisponibilidad de los recursos.

- Definición de una política de seguridad. Una vez identificados los recursos vitales y analizadas las amenazas, es el momento de diseñar la normativa de seguridad. Esta política contiene las directrices y procedimientos en materia de seguridad que los miembros de una organización deben seguir para asegurar la misma. Para que una política de seguridad sea efectiva deberá ser aceptada y apoyada por todos los niveles de empleados de una organización, especialmente el cuerpo directivo. En la redacción de la misma deberán estar implicados varios agentes. En primer lugar **la dirección** -que tiene el presupuesto y la autoridad-, en segundo lugar **el personal técnico** (administradores de sistemas, red y seguridad) -que conoce qué puede y qué no puede técnicamente hacerse-, en tercer lugar una representación de **los grupos de usuarios** afectados por la política de seguridad (dando la formación pertinente si es necesario) y por último **un asesoramiento legal**. Una buena política de seguridad se caracteriza por

su capacidad de **generar los procedimientos y publicaciones** técnico-administrativas pertinentes, de **ser aplicada eficazmente** (mediante herramientas de seguridad o sanciones ahí donde la prevención no fuera técnicamente posible) y de **definir con claridad las áreas de responsabilidad** de usuarios, administradores y directivos.

- Implantación de la política. Una vez definida hay que llevarla a cabo realizando el diseño de los elementos, asi como la adquisición y configuración de los mismos.

Por otra parte también es necesario saber qué hacer en caso de tener algún incidente de seguridad. Es muy importante tener un plan operativo en el caso de cualquier problema de seguridad para poder reaccionar. El resultado de no hacerlo así puede ser una toma de decisiones apresurada que dañe el seguimiento de la fuente del incidente, la recopilación de pruebas para la persecución del atacante, la recuperación del sistema y la protección de datos valiosos. Un plan o **política de gestión de incidentes de seguridad** deberá incluir:

- Preparación y planificación (cuales son los objetivos en la gestión de un incidente)
- Notificación (quién debe contactarse en el caso de un incidente)
- Identificación de un incidente (si es un incidente y cómo es de serio)
- Gestión (que debería hacerse cuando ocurre un incidente)
- Notificación (quién debería ser informado sobre el incidente)
- Protección de las pruebas y *logs* de actividad (qué registros deberían guardarse antes, durante y después del incidente)
- Contención (cómo puede limitarse el daño)
- Erradicación (cómo eliminar las causas del incidente)
- Recuperación (cómo restablecer el servicio y los sistemas)
- Seguimiento (qué acciones deberían tomarse después de un incidente)
- Repercusiones (cuáles son las implicaciones de incidentes pasados)
- Respuesta administrativa a incidentes

Existen diversos organismos que se encargan de la gestión de incidentes en las distintas zonas geográficas. Los más conocidos son los CERTs (Computer Emergency Response Team). A nivel mundial está el www.cert.org creado por DARPA en 1988, mientras que a nivel español y dentro de la red de investigación tenemos el cert de Rediris en www.rediris.es/cert. Los CERTs coordinan los incidentes de seguridad dentro de su área de administración: notifican incidentes, publican alertas, informan sobre vulnerabilidades, y en general responden de la foma más eficiente posible ante las amenazas de seguridad de las redes. Para ello es muy importante la figura del PER (Persona de Enlace con Rediris), pues es el responsable y la persona de contacto de cada una de las instituciones afiliadas a Rediris.

Hay que resaltar que el ciclo de la seguridad es continuo, esto quiere decir que no termina nunca, sino que continuamente hay que revisar cada una de las fases anteriores.

2.3 CIFRADO BÁSICO

Entendemos por Criptografía (*Kriptos*=ocultar, *Graphos*=escritura) la técnica de transformar un mensaje inteligible, denominado *texto plano*, en otro que sólo puedan entender las personas autorizadas a ello, que llamaremos *criptograma* o *texto cifrado*. El método o sistema empleado para encriptar el texto en claro se denomina algoritmo de encriptación. Los participantes en una transacción de información deben estar seguros de que se han cumplido ciertos objetivos asociados con la seguridad de los datos. Los objetivos más importantes son los siguientes:

- *Confidencialidad*: Consiste en mantener oculta la información para todos aquellos que no están autorizados a verla, es decir la información transmitida y almacenada sólo está accesible a las partes autorizadas.

- *Integridad de los Datos*: Evitar la alteración de los datos, por parte de un tercero; debe ser posible por tanto detectar cualquier modificación de la información almacenada y transmitida La comprobación de la integridad se suele realizar mediante firmas electrónicas, generalmente basadas en funciones hash.

- *Autentificación*: Consiste en asegurar que las personas que intervienen en el proceso de comunicación son las que dicen ser. El método más usado para proporcionar autenticidad es la firma digital.

- *No Repudiación*: Permite a cada lado de la comunicación probar fehacientemente que el otro lado ha participado en la comunicación.

El cifrado simétrico de claves, o cifrado de clave secreta, utliza una clave común y el mismo algoritmo de cifrado para codificar y decodificar. El éxito de este cifrado depende de que se cambie la clave con frecuencia, que estas claves sean seguras y que se distribuyan de forma segura.

El cifrado asimétrico de claves, o cifrado de clave pública, utiliza dos claves relacionadas: una pública y otra privada. Los mensajes que se encriptan con la clave pública solo pueden descifrarse con la privada (confidencialidad e integridad). Los mensajes que se encriptan con la clave privada solo pueden descifrarse con la pública (autenticación). Con doble cifrado conseguimos ambas características. En este caso el emisor cifraría su mensaje con la clave pública del receptor, consiguiendo confidencialidad e integridad, y después lo firmaría con su clave privada, ofreciendo autenticación. Cuando el mensaje llega al receptor, lo descifra primero con la clave pública del emisor y después con su clave privada.

Las funciones hash toman un mensaje de entrada de cualquier longitud y genera un código de longitud fija, cumpliendo lo siguiente: la misma entrada debe crear siempre la misma salida, que sea imposible que dos mensajes creen la misma salida y con la salida no debe obtenerse la entrada. De esta forma se obtiene una huella de un mensaje o archivo, que nos sirve para

garantizar la integridad del mismo. Para ello el emisor envía un archivo y su función hash. El receptor recibe ambos datos y pasa el archivo por la misma función hash que usó el emisor. Si ambas funciones coinciden, el receptor puede estar seguro que el archivo no fue modificado. Las funciones hash también se utilizan para firmar digitalmente un documento. Si un emisor pasa un mensaje por una función hash, y la salida de esta función se cifra con la clave privada de emisor, el resultado es la firma digital, obteniendo integridad y autenticación.

Certificados digitales

Es un mensaje firmado digitalmente que se suele utilizar para verificar la clave pública de alguien. Los certificados necesitan un formato común, y mayoritariamente siguen el estandar X.509. Las Autoridades de Certificación (CA) se responsabilizan de la validez de los certificados: recepción, distribución y cancelación. Cuando una CA envía un certificado con la clave pública de alguien, lo firma con su clave privada para darle autenticación. Una Infraestructura de Claves Públicas (PKI) proporciona una eficiente y fiable administración de claves y certificados.

Autenticación

Todos los métodos de autenticación obligan a especificar quien o qué se es y mostrar las credenciales adecuadas para demostrar que uno es quien dice ser. Estas credenciales suelen ser algo que se conoce (como una contraseña), que se tiene (como una tarjeta inteligente) o que se es (biometría). Como las contraseñas típicas suelen ser fáciles de descifrar o adivinar, hay métodos más robustos como la contraseña de un solo uso, o las contraseñas por tokens.

En las conexiones de acceso telefónico, que suelen utlizar el protocolo PPP, se incluyen métodos de autentifiación como el PAP, CHAP y EAP. En todos los casos es el dispositivo el que se autentifica. PAP es el más sencillo, las contraseñas se envían sin cifrar, por lo que no tiene protección frente a ataques de prueba y error. CHAP utiliza un intercambio de señales a tres vías,

mediante el desafío de un secreto que se pasa por una función hash. De esta forma el secreto nunca se envía por la red. EAP soporta múltiples mecanismos de autentificación, por lo que es más flexible.

Muchos protocolos requieren la comprobación de la autenticación antes de proporcionar derechos de acceso y autorización, tales como TACACS+ y RADIUS. Este último fue desarrollado como protocolo de autenticación y contabilidad de un servidor de acceso, que se ha propuesto como estandar en la RFC 2058. Utiliza UDP como transporte y es de tipo cliente servidor. El cliente suele ser un NAS (Servidor de Acceso a Red) de un determinado ISP y el servidor RADIUS suele ser un demonio en un unix o W2000. El servidor RADIUS puede soportar distintos métodos de autentificación. Cuando recibe un usuario o contraseña, puede utlizar PAP, CHAP o EAP, o tambíen otras formas de autenticación como ficheros password/shadow en Unix y LDAP. El proceso de autenticación es el siguiente: un usuario realiza una llamada al NAS, quien solicita usuario y clave. El NAS, que es cliente RADIUS, envía el nombre de usuario y la contraseña cifrada al servidor, el cual acepta o deniega el servicio en función de que sean correctas.

Comunicaciones seguras

Aparte de conocer la identidad es necesario garantizar la integridad y confidencialidad de los datos. Existe muchas tecnologías que proporcionan servicios de seguridad en varias capas TCP/IP. Los protocolos de seguridad de la capa de aplicación proporcionan mayor flexibilidad para controlar los parámetros de la aplicación, pero el uso de un protocolo para cada aplicación no resulta práctico. Los protocolos de seguridad de la capa de transporte, como SSL y SSH se están generalizando. SSL se utiliza mucho en transacciones web y se ha convertido en un estandar de facto, mientras que SSH suele usarse para acceso a servidores remotos en vez de Telnet y para FTP seguro. Ipsec es capaz de proteger cualquier tipo de aplicación en la capa de red, propocionando control de acceso, autenticación y confidencialidad.

Las redes privadas de acceso telefónico virtual (VPDN) permiten a las empresas ampliar sus redes privadas a través de las líneas telefónicas. Las nuevas tecnologías permiten que los usuarios remotos y los sitios se conecten de forma segura a la infraestructura de la empresa. Existen tres protocolos similares que cumplen este fin: L2F de Cisco, PPTP de Microsoft y L2TP de varios fabricantes. Este servicio es ofertado por varias operadoras actualmente. De esta forma los trabajadores de una empresa pueden conectarse a los servicios de ésta desde cualquier ubicación como si estuvieran en la empresa (con las limitaciones de velocidad propias del medio de comunicación), sin necesidad de pasar por el firewall institucional, ya que el router de la empresa está conectado punto a punto con el del proveedor de servicios, con las siguientes ventajas: direccionamiento IP asignado por la empresa y autenticación de usuarios realizado en la empresa.

2.4 ESTRATEGIS DE SEGURIDAD

Para lograr una red lo más segura posible, debemos asegurar todos los componentes de la misma. En este apartado iremos viendo ideas para asegurar nuestra desde desde el nivel físico hasta las aplicaciones. En el nivel físico debemos tener en cuenta que toda la infraestructura de comunicaciones debe estar controlada, y ser accesible únicamente por el personal informático. Asimismo es necesario un cuidadoso diseño de VLANs, de forma que las más críticas estén lo más aisladas posibles.

En el nivel de red, la opción más obvia de control es el establecimiento de listas de acceso en los routers. En los routers Cisco tenemos varios tipos de listas, siendo las más usadas las estándar y las extendidas. Las listas estandar permiten filtrar por direcciones IP, mientras que las extendidas permiten un control mas fino a través de protocolos como tcp, udp, icmp, eigrp, etc y sus puertos.

Un nivel más avanzado de protección son los firewalls o cortafuegos, que realizan una inspección avanzada de todos los paquetes, filtrado del contenido de aplicaciones, autencación, cifrado, NAT, VPNs, entre otras

funciones. Un firewall suele instalarse en la entrada de Internet a la red corporativa, o bien, en determinadas zonas donde se ubican los servidores críticos. En infraestructuras complejas podría ser necesario instalar varios firewall, uno en cada zona crítica, por ellos varios productos comerciales implementan firewalls virtuales, de forma que un único equipo da servicio a varias VLANs. Si lo que queremos es filtrar unos pocos equipos podemos usar firewalls de host, que suelen ser por software. Los firewalls de red permiten filtrar el tráfico de una red, y puede hacerse con equipos dedicados a ellos (denominados Appliance) o con PCs con el software adecuado (libre o comercial).

Los equipos appliance tienen el hardware y el software dedicado a la función que realizan, por lo que están optimizados para la inspección de tráfico y el sistema operativo no es muy conocido por los posibles intrusos. Ejemplos son los PIX de Cisco, los NetScreen y los Checkpoint sobre hardware Nokia. Además algunos routers permiten la inclusion de módulos firewall en sus chasis, como sucede con el módulo PIX sobre routers Cisco 6500. El principal problema de los dispositivos dedicados es el precio. Hay que tener en cuenta que en un entorno profesional los firewall deben estar redundados, bien funcionando uno y el otro en espera o bien haciendo balanceo de carga.

Otra opción es montar un software de firewall sobre un ordenador (W2000, linux, Solaris). Esta opción es más barata pero primero tenemos que asegurarnos que la máquina está perfectamente protegida, además de actualizarla convenientemente. Ejemplos son las típicas aplicaciones de firewall sobre linux, y los Checkpoint sobre Solaris.

Además de estos firewall de propósito general, existen otros específicos para la protección de servidores web públicos. De esta forma se puede filtrar aplicaciones web, contenidos, correos web-mail con virus, realizar autenticación de usuarios, gestión del ancho de banda para multimedia, filtrado de URLs, filtrados contra DOS, además de hacer de proxy. Ejemplo de estos firewalls son los Blue Coat.

Si bien los firewall pueden detener la mayor parte de los ataques, también existe la necesidad de saber que está sucediendo en mi red, es decir, si alguien está intentado atacarnos. Esto es importante para detener ataques incontrolados lo antes posible. Para ello existen los detectores de intrusión (IDS), que es un dispositivo que analiza el tráfico de una red y lo compara con una base de datos de patrones de ataques conocidos. Cuando detecta un intento de ataque avisa a una consola de monitorización y podría, según la tecnología, poner una regla en el firewall para detenerlo. A la hora de implantar un IDS es importante determinar donde colocar los sensores (antes y después del firewall, en la zona DMZ, en segmentos de red críticos), actualizar los patrones convenientemente y la forma de gestionar las alarmas. Existen distintas tecnologías de IDS: appliances, tarjetas de un router, por software, de host, etc, cada una de ellas adaptada según las necesidades. Existe un dispositivo más completo denominado detector de intrusión y prevención (IDP) que además de analizar el tráfico, bloquea los ataques producidos. Ejemplo de ello es el NetScreen-IDP.

En otras ocasiones es interesante conocer si los equipos de nuestra red son vulnerables a ciertos ataques. Por ejemplo, cuando se producen invasiones masivas de gusanos queremos saber qué equipos de nuestra red podrían ser víctimas de esos ataques. Para ello usamos los escaners, los cuales chequean equipos o redes buscando estas vulnerabilidades. El Nmap de linux o el Retina para windows permite encontrar qué equipos de nuestra podrían ser atacados. Para analizar el tráfico de una red y buscar posibles atacantes también pueden usarse los snifers de red. Si tenemos un equipo en una red que está atacando a otros ordenadores y no sabemos cual es, con un snifer de red podemos ver las tramas que circulan por la red y averiguar, conociendo los patrones del ataque, de que equipo se trata.

Otra estrategia importante de seguridad es el uso de antivirus corporativo, tanto en los servidores de correo como en los puestos de trabajo, siendo de vital importancia la actualización de patrones.

Existen además herramientas de gestión de tráfico que permiten optimizar el ancho de banda de nuestra red, priorizando tráfico de las aplicaciones importantes en detrimento de otras.

Por último, y para terminar, todos los dispositivos de los que hemos hablado generan un montón de información que es necesario clasificar, comparar, filtrar, que hace que el estudio de un ataque se convierta en una ardua tarea. Para ello existen dispositivos que realizan una gestión centralizada de logs. Estos equipos reciben información de sistemas heterogéneos, como IDS, firewalls, antivirus, syslog, etc, y realizan detección de ataques correlacionando los distintos logs, análisis forense e informes de actividad entre otras cosas. Un ejemplo de esto es el NetIQ.

Como conclusión hemos de decir que existen múltiples tecnologías y equipamiento de seguridad, pero tenemos que tener en cuenta los servicios que queremos ofrecer, el grado de seguridad que queremos dar, el presupuesto del que disponemos y el personal disponible. En general, a mayor grado de seguridad, mayor dificultad tendremos para ofrecer servicios a los usuarios. Hay que llegar a un compromiso entre servicios y seguridad. En casi todas las instalaciones en las que se pasa de un acceso libre a una acceso seguro se producen problemas debido a que algunos servicios dejan de funcionar para los usuarios. Es por ello importante estar respaldado por una política de seguridad que aclare estas cuestiones, además de estar al tanto de la legislación vigente. En cuanto al personal, si no se dispone del adecuado, existen empresas que realizan consultoría y monitorización remota de nuestra red en estos casos.

CAPITULO 3

SISTEMAS DE AUDITORÍA NORMALIZADA

José Enrique Ares Gómez

3.1 INTRODUCCIÓN

Auditoria vocablo de origen latino que significa control de libros contables o revisión de cálculos. Actualmente se utiliza el término Auditoria para evaluar la aptitud de los procesos empresariales e iniciar acciones de mejora y vigilar el efecto de las acciones iniciadas, su función es como la de un instrumento para descubrir puntos débiles, sugerir mejoras y controlar la eficacia de las accionasen los sistemas.

En las auditorias se debe tener en cuenta la implicación del "capital humano" en el desarrollo de las empresas, para evaluar la relación y los impactos de las actividades, los recursos y el ambiente tanto interno como externo. Una Auditoria que ponga en evidencia las carencias en los Sistemas de Gestión, aporta una magnifica oportunidad para *provocar un cambio importante de mentalidad entre los responsables y los usuarios del sistema auditado*

3.2 CARACTERISTICAS Y TIPOS DE AUDITORIA

Un requisito para ejecutar sistemáticamente auditorias de todo tipo es poseer un concepto claro sobre los puntos a observar, la secuencia y la asignación de responsabilidades y de autoridad, las Auditorias suelen presentar los siguientes a**spectos comunes:**

- Debe realizarlas personal muy cualificado y especializado, con agilidad mental, capacidad de comprensión e intuición, visión panorámica y distanciamiento crítico respecto a los procesos de la empresa.

- La función del auditor más descubrir defectos, debe hallar las causas y buscar posibilidades de mejora, lo que exige una buena intuición y capacidad de colaboración.

Las auditorias que se limitan tan sólo descubrir los errores, suelen producir fricciones internas y actúan contra la idea inicial de generar acciones de mejora. Otras características comunes de los diversos tipos de auditoria son:

- Los resultados de la auditoria han de estar bien documentados.
- Promover discusión sobre las causas y sugerencia de acciones.
- El establecimiento de plazos para introducir las mejoras.
- La vigilancia de las acciones de mejora introducidas.

Hay que mantener una preocupación permanente por mejorar el entorno de trabajo, minimizando las labores que no aportan valor. En cada auditoria se restablece el nivel de calidad, que en caso de no existir controles, se iría degradando, por ello el objetivo común es la ***supresión de defectos mediante auditorias.***

Tras identificar las causas del problema se debe:

- Elaborar y priorizar soluciones alternativas, con posterior formulación y aplicación de acciones concretas.
- Evaluar el estado alcanzado, comparándolo con el objetivo definido y, si es necesario, mejorarlo.

El nivel de mejora definido es el punto de partida para otras acciones optimizadoras, al analizar puntos débiles y elaborar mejoras, mediante, observación, evaluación y documentación de los parámetros relevantes, se logra visualizar los objetivos, los estados y la eficacia de las acciones, ***El Auditor debe comprobar que en la empresa el aumento de las exigencias de cualificación se satisface a través de programas de formación, en la***

planificación y la implantación de nuevas tecnologías y actividades, ***debe motivar para que las*** **no conformidades sean una buena ocasión para el replanteamiento de los criterios y adecuarlos a los requerimientos técnicos y legislativos.**

Después de conocer las características comunes, **podemos clasificar las Auditorias en diferentes tipos según su enfoque, la vinculación del auditor y su frecuencia de realización**.

3.2.1 TIPOS DE AUDITORIA SEGÚN ENFOQUE

Teniendo en cuenta el enfoque hacia aspectos características del sistema productivo podemos diferenciar entre **Auditorias de Producto, de Proceso y de Sistema.**

La Auditoria de Producto examina el producto fabricado e inspeccionado para:

- Comprobar, si se cumplen las especificaciones fijadas.
- Determinar dónde aparecen los principales defectos, los errores y sus causas.

Las Auditorias de Proceso tienen como objetivo es analizar los puntos débiles de ciertos procesos o procedimientos cuando:

- Tienen gran número de operaciones o presentan particularidades tecnológicas.
- Es afectado por muchas magnitudes de influencia.
- Consta de muchas estaciones de procesos.
- Se requiere una planificación y utilización a largo plazo.

La Auditoria de Sistema comprueba la eficacia y la inexistencia de defectos en todo el sistema de gestión o en subsistemas esenciales del mismo. Debe controlar su efectividad e introducir y vigilar las acciones de mejora. Se

analizan los procedimientos o instrucciones, su contenido, su seguimiento y, sobre todo, su capacidad de lograr los objetivos planteados.

3.2.2 TIPOS DE AUDITORIA SEGÚN VINCULACIÓN

Respecto a la vinculación del auditor con la institución auditada hay:

- La auditoria externa la realiza otra entidad totalmente independiente de la institución auditada
- La auditoria interna se realiza con los mismos criterios que la externa por el propio personal de la entidad auditada.

3.2.3 TIPOS DE AUDITORIA SEGÚN FRECUENCIA

Respecto a la frecuencia de realización existen:

- **Auditorias extraordinarias** También llamadas "adicionales" o "espontáneas", se usan cuando se hacen cambios esenciales en la organización de la empresa (funcional u operativa).
- **Auditorias de repetición** Tiene lugar cuando en una auditoria anterior se han apreciado defectos y trata de comprobar si se han introducido y son eficaces las acciones propuestas.
- **Auditorias continuadas** Se realizan periódicamente, con una frecuencia preestablecida y planificada. En general, con estas auditorias se observan mejoras destacadas del sistema, es decir, contribuyen a evitar desviaciones no permitidas. Con este método se aprecia una variación discontinua de la magnitud objetivo.

3.3 PLANIFICACIONES DE INSPECCIONES

La base para el control de un sistema es el plan de inspecciones que debe incluir recomendaciones, directrices, esquemas y posibles datos de experiencias previas teniendo en cuenta la función de los productos, máquinas o instrumentos a inspeccionar, la secuencia de utilización, los documentos, los instrumentos y equipos disponibles.

Se deben considerar los aspectos económicos, las estructuras y las tareas para análisis de datos de inspecciones a largo y corto plazo. la evaluación posterior de los datos resulta tanto más eficaz cuanto mejor planificada esté su recogida. Las etapas clásicas de la planificación de inspecciones son:

- Seleccionar las propiedades a controlar.
- Relacionar las inspecciones a realizar.
- Determinar las unidades, cantidades y frecuencias de control.
- Fijar las secuencias de control de cada propiedad.
- Especificar los instrumentos y equipos a emplear.
- Elegir el método de control.
- Especificar los documentos requeridos.
- Preparar instrucciones para realizar las inspecciones.

En *la directriz VDI/VDE/DGQ2619 para planificar inspecciones* se describe el modo, las actividades y decisiones esenciales, cada paso incluye planes complementarios.

3.4 CONCEPTOS PARA LA GESTIÓN DE NORMAS, REGLAMENTOS Y SU APLICACIÓN

Los documentos que establecen los requisitos técnicos que deben cumplir los productos y los servicios. Son las reglamentaciones técnicas y las normas técnicas.

Las Reglamentaciones Técnicas, son de obligado cumplimiento y están establecidos por las diferentes Administraciones públicas.

Las Normas Técnicas, tienen un carácter voluntario y se establecen por consenso implicando a los usuarios y a los productores de bienes y servicios

La Acreditación, es el procedimiento por el cual una entidad u organismo tiene autoridad para reconocer formalmente que otra entidad y/o

organismo es competente para efectuar unas tareas específicas. Estas entidades **fundamentan su actividad en los principios de independencia, imparcialidad, transparencia y objetividad, reconocida internacionalmente**, **la entidad encargada de estas actividades en España es ENAC (Entidad Nacional de Acreditación).** Las Entidades acreditables en España son:

- **Entidades de certificación**: "*entidades públicas o privadas, con personalidad jurídica propia, que se constituyen con la finalidad de establecer la conformidad solicitada con carácter voluntario, de una determinada empresa, producto, proceso, servicio o persona a los requisitos definidos en normas o especificaciones técnicas*" (Real Decreto 2200/1995).
- **Entidades auditoras y de inspección**: "*entidades públicas o privadas con personalidad jurídica propia, que se constituyen con la finalidad de determinar a, a solicitud de carácter voluntario, si las actividades y los resultados relativos a la calidad satisfacen a los requisitos previamente establecidos y si estos requisitos se llevan a cabo efectivamente y son aptos para alcanzar los objetivos*" (Real Decreto 2200/1995).
- **Organismos de control**: "*entidades públicas o privadas, con personalidad jurídica, que se constituyen con la finalidad de verificar el cumplimiento de carácter obligatorio de las condiciones de seguridad de productos e instalaciones de industrias, establecidas por los Reglamentos de Seguridad Industrial, mediante actividades de certificación, ensayo, inspección o auditoría*" (Real Decreto 2200/1995).

Las Entidades de Certificación deben tener implantado un sistema imparcial, transparente y objetivo, disponiendo de los mecanismos precisos para la certificación de productos, servicios y sistemas. **Con el fin de demostrar las características anteriores en España, debe estar acreditada por ENAC para certificar**:

- Sistemas de aseguramiento de la calidad, según las Normas UNE-EN ISO 9001.
- Sistemas de gestión medioambiental de actividades empresariales, según la Norma ISO 14000.
- **Otros sistemas.**
- Productos.

El Marcado CE, indica que un producto cumple con la directiva o directivas comunitarias que le son de aplicación (Baja Tensión, Compatibilidad Electromagnética, Máquinas, etc.). No puede haber Marcado CE de un tipo de producto si no hay una directiva que así lo especifique.

Las Redes de agrupación de organismos. Están configuradas por organismos **que tiene firmados convenios de reconocimiento dentro de su ámbito de aplicación**.

- La actual Red Internacional de Certificación **IQNet** (International Certification Network) tiene su origen en la red que agrupaba a organismos de certificación de sistemas dentro del ámbito europeo denominada Red Europea de Certificación pasando hace unos años a tener un carácter internacional.
- Esta red de organismos de certificación de los sistemas ISO 9001, ISO 9002, ISO 9003 e ISO 14001 esta configurada por los principales organismos de certificación y coordina los proyectos internacionales de certificación.
- Los miembros de la IQNet tienen convenios de reconocimiento de los certificados y de los informes de auditoría realizados por sus miembros. Por ello si un sistema de gestión ha sido auditada por uno de los miembros de la red IQNet y se le ha concedido un certificado, el resto de los miembros reconocen dicho certificado.

3.5 MÉTODOS Y SISTEMAS DE GESTIÓN

El auditor debe de conocer métodos de anales para utilizarlos par detectar fallos y proponer soluciones para su mejora en los sistemas de gestión. Los Sistemas de Gestión de Calidad se suelen fundamentar en:

- El modelo EFQM, para la auto-evaluación
- Las normas ISO 9000 e ISO 14000, para la certificación
- Las normas EN 45000, para la acreditación.

3.5.1 EL ANALISIS MODAL DE FALLOS, EFECTOS Y CRITICIDADES

El Análisis Modal de Fallos, Efectos y Criticidades AMFEC es un método para evaluar el diseño de un producto, servicio o proceso, detectando lo antes posible sus puntos débiles y se evalúa la probabilidad de que ocurra un fallo, así como el efecto del mismo.

De manera más concreta, un AMFEC es como un sumario de las ideas de los técnicos especializados, incluyendo un análisis de cada punto en el que podría tener lugar un problema basado en sus experiencias y en situaciones pasadas, por ello se puede obtener una información valiosa para definir y dar prioridad posteriormente a las características que podrían necesitar controles especiales, es de utilidad tanto en el diseño de nuevos productos/servicios/procesos como en modificaciones importantes de los mismos. Para desarrollar esta metodología, los etapas a seguir son:

1. Definir las funciones que realiza.
2. Identificar los Modos de Fallo de las cada una de las funciones de la materia objeto de estudio.
3. En cada uno de los Modos de Fallos se determina los Efectos que tales fallos supondrían para el cliente, al objeto de identificar estos Efectos a veces es necesario recurrir a análisis físicos o modelos matemáticos.
4. Se buscan las causas que han producido tales efectos:

5. Se indican los sistemas de control establecidos para evitar que se produzcan las causas de los fallos.
6. Se definen los índices para evaluar cada uno de los Modos de Fallo, que son los siguientes:
   - Índice de ocurrencia (O): Es la probabilidad de que suceda el fallo debido a las causas establecidas. Se define una escala del 1 al 10, en la que se asigna a cada valor la posibilidad de que el fallo se produzca, según unos criterios definidos.
   - Índice de gravedad (G): Es el índice que indica la importancia del Efecto en el caso de que ocurra el Fallo. Se establece una escala del 1 al 10 para evaluar la gravedad mediante un criterio previamente establecido.
   - Índice de detección (D): Indica la posibilidad se detectar el Causa del Fallo, una vez que éste ha ocurrido ya. Se define una escala del 1 al 10, asignando valores según criterios previamente establecidos.
7. Para cada uno de los Fallos potenciales, se calcula un coeficiente, resultante de multiplicar los tres índices (O * G * D), denominado Índice de Prioridad de Riesgos.

En función del resultado obtenido, y teniendo en cuenta que el valor del índice de prioridad de riesgos, se obtiene una lista de los posibles fallos de un producto / servicio / proceso y las causas que los motivarían, pudiendo establecerse acciones preventivas -en los casos de valores altos del producto O*G*D- en el diseño para evitar que esto se produzca.

3.5.2 ESTRUCTURA DEL MODELO EFQM

A medida que los principios de la calidad se han extendido, han ido surgiendo **modelos de auto-evaluación** que presentan diferencias en cuanto a su enfoque y conjunto de criterios para su gestión .***El modelo europeo a la calidad EFQM de Excelencia Empresarial*** es un iniciativa empresarial, y fue constituida en 1988, por catorce empresas y la organización EOQ (European Organization for Quality a la que pertenece laAsociación Española para la

Calidad la AEC)) y presentado por primera vez en 1992 y define la **excelencia empresarial** como:

"*prácticas sobresalientes en la gestión de la organización y logro de resultados basados en conceptos fundamentales que incluyen:*

- la orientación hacia los resultados.
- la orientación al cliente.
- liderazgo y perseverancia.
- procesos y hechos.
- implicación de las personas.
- mejora continua e innovación.
- alianzas mutuamente beneficiosas y responsabilidad social ".

Los aspectos a valorar dentro de este modelo están desglosados en dos categorías, **agentes facilitadores** y **resultados**:

- AGENTES FACILITADORES, que contemplan criterios relativos a "**cómo**" han de llevarse a cabo ciertas actividades,
  - Liderazgo.
  - Política y Estrategia.
  - Personas.
  - Alianzas y Recursos.
  - Procesos.

- RESULTADOS, que muestran criterios indicativos de "**qué**" se ha alcanzado
  - Resultados en los Clientes.
  - Resultados en las Personas.
  - Resultados en la Sociedad.
  - Resultados Clave.

En los criterios referentes a los resultados -a excepción de los Resultados Clave- se contemplan tanto las medidas internas de la organización como las medidas relativas a la percepción que sobre la empresa poseen los

clientes -Resultados en los Clientes-, los empleados -Resultados en las Personas- y la sociedad -Resultados en la Sociedad-.

3.5.3 ISO 9001

A partir el año 2000, las ediciones de las ISO 9001, ISO 9002 e ISO 9003 **han quedado integradas en una sola norma la ISO 9001**, para optar por la certificación de los sistemas de la calidad, estando presenten los siguiente principios:

- Organización enfocada al cliente.
- Liderazgo.
- Participación del personal.
- Enfoque a proceso.
- Enfoque del sistema hacia la gestión.
- Mejora continua.
- Enfoque objetivo hacia la toma de decisiones.
- Relación mutuamente beneficiosa con el suministrador.
- Compatibilidad con otros SG como ISO 14000.

Como aspectos más reseñables podemos identificar los relativos a:

- La Alta Dirección: se enfatiza el papel desempeñado por los altos directivos de la empresa y la determinación de objetivos mensurables en todas las funciones y niveles de la organización.
- La mejora continua: cualquier organización que opte por la certificación, ha de disponer de un sistema de mejora continua de la gestión de la calidad.
- La satisfacción del cliente: se requiere llevar a cabo un seguimiento de la satisfacción del cliente para valorar el sistema de calidad de la empresa.
- La comunicación interna: la organización ha de sistematizar sus actividades de comunicación interna y contrastar su efectividad.

- La interacción entre procesos: se han de definir los procesos y su interrelación. Estos procesos son tanto verticales como horizontales.
- Los recursos: se ha de evaluar la eficacia de las actividades que redunden en la calidad y la necesidad de los recursos empleados.

3.5.4 EN 45000 / UNE66500

El desarrollo de estas normas europeas establece los criterios generales para la acreditación de entidades de certificación, de inspección y de laboratorios. En España la acreditación se encuentra definida en la **Ley 21/1992 de Industria y en la norma UNE-EN 45020** de la siguiente manera:

- "*Reconocimiento formal de la competencia técnica de una entidad para certificar, inspeccionar o auditar la calidad, o un laboratorio de ensayo de calibración industrial*" (Ley 21/1992 de Industria).
- "*Procedimiento por el cual un organismo autorizado reconoce formalmente que un organismo o individuo es competente para llevar a cabo tareas específicas*" (UNE-EN 45020).

La Ley 21/1992 de Industria establece las actuaciones de las Administraciones Públicas en materia de seguridad y calidad industrial, y define los agentes a través de los cuales se instrumentan las acciones a seguir.

Además en su artículo 3 especifica:

1. Se consideran industrias, a efectos de la presente Ley, las actividades dirigidas a la obtención, reparación, mantenimiento, transformación o reutilización de productos industriales, el envasado y embalaje, así como el aprovechamiento, recuperación y eliminación de residuos o subproductos, cualesquiera que sea la naturaleza de los recursos y procesos técnicos utilizados.

2. Asimismo estarán incluidas en el ámbito de aplicación de esta Ley, los servicios de ingeniería, diseño, consultoría tecnológica y asistencia técnica directamente relacionados con las actividades industriales.

3. ***Se regirán por la presente Ley, en lo no previsto por su legislación específica:***

a) .....

f) ***Las actividades industriales relacionadas con el transporte y las telecomunicaciones****.*

g) .....

3.5.5 ISO 14000

ISO 14000 contiene los requisitos del sistema de gestión, basado en un proceso dinámico que sigue el ciclo de planificar, poner en práctica, comprobar y revisar. La integración de las materias medioambientales en el sistema global de gestión puede contribuir a la consecución de una mayor eficiencia y a la clarificación de las responsabilidades. El sistema debería capacitar a la organización para:

a) Establecer una política medioambiental adecuada para la organización;

b) Identificar los aspectos medioambientales que surjan de las actividades, productos y servicios, pasados existentes o planificados de la organización, para determinar los impactos ambiental es significativos;

c) Identificar los requisitos legales y reglamentarios aplicables;

d) Identificar las prioridades y fijar los objetivos y metas medioambientales adecuados;

e) Establecer una estructura y un programa(s), para llevar a cabo la política y alcanzar l os objetivos y metas;

f) Facilitar la planificación, control, seguimiento, acciones correctoras, actividades de auditoría y revisión para asegurar que se cumple con la política y que el sistema de gestión medioambiental sigue siendo apropiado;

g) Ser capaz de adaptarse a circunstancias cambiantes.

3.5.6 SISTEMA DE GESTIÓN DE LA PREVENCIÓN DE RIESGOS LABORALES (SGPRL)

Para lograr la eficacia del sistema se debe diseñar para satisfacer las necesidades de la organización en materia de seguridad y salud, mejorar la cuenta de resultados y proteger los intereses de la organización, cumpliendo con la legislación vigente **y adoptando un compromiso de mejora continua de la acción preventiva.**

- El SGPRL constituye un mecanismo o herramienta para lograr la mejora continua, cuyo ritmo será determinado por la organización en base a sus condicionantes específicos.

- Esta herramienta debe de ser la adecuada para que la organización que la emplee pueda conseguir los objetivos (a nivel estratégico, y a nivel técnico) que se proponga en materia de prevención.

- El SGPRL supone un enfoque estructurado y lógico en materia de Prevención

3.5.7 SISTEMAS INTEGRADOS DE GESTIÓN

Los sistemas generales para gestión de la calidad, de la prevención de riesgos laborales y la gestión medioambiental deben resolverse numerosos problemas, utilizando métodos y documentos similares y es conveniente implantar una

ESTRUCTURA DOCUMENTAL DE INTEGRACION

- Manual de Gestión.
- Procedimientos.
- Instrucciones operativas.

El Manual de Gestión integrado de los Sistemas de Calidad, Medio Ambiente y Prevención de Riesgos Laborales, consta de una estructura basada en un tronco común (Secciones Generales) a los tres sistemas de gestión y el desarrollo de los mismos en los capítulos siguientes de forma integrada o específica para los mismos, describiéndose en cada capítulo el alcance del mismo. El Manual de Gestión propuesto se estructura en:

Secciones Generales

1. Índice del Manual de Gestión
2. Control de modificaciones del Manual de Gestión
3. Contenido y gestión del Manual
4. Definiciones
5. Política de Empresa
6. Organización

El Manual de Gestión Integrado es un documento de carácter genérico que deberá desarrollarse mediante la emisión de una colección de **procedimientos** para:

1. La elaboración, revisión y el control de documentos y datos del sistema.
2. El control de los registros del sistema.
3. La realización de las comunicaciones
4. El control del proceso operacional
5. La gestión de medidas preventivas y de protección.
6. La investigación de accidente, incidentes
7. La identificación y el control de las no conformidades.
8. La gestión de acciones correctoras y preventivas.
9. La gestión de la formación y la cualificación del personal.
10. La gestión de auditorias.
11. ..... etc.

Las Instrucciones Operativas describen de manera pormenorizada las operaciones a realizar en las diferentes actividades. Estos documentos deben describir, las operaciones que se realizan, en el orden en el que se desarrollan incluyendo tanto las propias de ejecución como las de protección del ambiente en el que se llevan a cabo.

De esta forma es como se puede conseguir una integración completa de los tres sistemas de gestión. Debido a la particularidad de dichas instrucciones en función de la empresa y la actividad a desarrollar no se ha incluido ninguna propuesta al respecto.

3.6 AUDITORIAS LEGALES EN S.P.R.L.

Las actuaciones de los auditores tendrán en cuenta los objetivos establecidos en el artículo 30 del Capítulo V del Reglamento de los Servicios de Prevención 39/1997. **Se evaluarán los aspectos de gestión del sistema de prevención y requerimientos especificados en la Ley 31/1995 de Prevención de Riesgos Laborales.**

El proceso de auditoría permitirá, finalmente, disponer de un criterio adecuado y suficiente para emitir un dictamen sobre la **adecuación, capacidad y eficacia del Sistema de Prevención** implantado.

Las fases del proceso auditor son las siguientes:

PROPUESTA TÉCNICO-ECONÓMICA Se elabora teniendo en cuenta la carga de trabajo del equipo auditor asignado al proyecto.

EL PLAN DE AUDITORIA Se acuerda durante las reuniones de planificación con el Responsable de Prevención. Se establecen fechas, horarios, lugares, interlocutores, documentación y tema a tratar en cada una de las jornadas.

LA AUDITORÍA DOCUMENTAL Se realiza con los miembros del Servicio de Prevención, en la misma se analiza la organización de la Empresa y se analiza la documentación que soporta la actividad preventiva que se está llevando a cabo.

LA AUDITORÍA TÉCNICA Se realiza con los Delegados de Prevención, con la Dirección de la Empresa y con aquellas personas con funciones específicas en prevención de riesgos.

ELABORACIÓN Y ENTREGA DEL INFORME para dejar constancia de las conclusiones finales sobre la eficacia del sistema de gestión de acuerdo a los objetivos requeridos.

Durante el desarrollo del proceso auditor se van avanzando las conclusiones parciales que se vayan obteniendo, con el doble propósito de contrastar las opiniones y de que se puedan solucionar antes del cierre del informe, con el Servicio de Prevención, la Dirección de la Empresa y los Representantes de los trabajadores para contrastar del informe de auditoría. El informe definitivo deberá contener según los casos, los ***elementos*** siguientes:

- Datos de la empresa auditada y auditora.
- Objeto, carácter y alcance de la auditoría.
- Normativa de aplicación.
- Metodología seguida.

Desarrollo de la auditoría, se reflejan los pormenores del plan de auditoría, la identificación de los componentes del equipo auditor y de los representantes del auditado, fechas de la auditoría, actuación desarrollada, etc.

En los resultados de la auditoría; se gradúan las desviaciones o no conformidades en función de su gravedad:

- **Desviación mayor:** Ausencia parcial o total de un requisito normativo, incumplimiento no justificado, error repetitivo o actividad preventiva no realizada necesaria para garantizar la salud de los trabajadores frente a un riesgo grave.
- **Desviación menor:** Incumplimiento específico o puntual de un requisito normativo o de una actividad preventiva necesaria para garantizar la salud de los trabajadores frente a un riesgo leve.
- **Observación**: Aspecto de la actividad auditada que implica un potencial riesgo de no conformidad o que permita una potencial mejora que sea de interés para el Sistema de Prevención de Riesgos Laborales.
- **Conclusiones**, en base a la recogida de evidencias durante la auditoría, se reflejan las conclusiones finales sobre la eficacia del Sistema de Prevención de acuerdo a los objetivos indicados en el art. 30 del RD 39/1997, RSP.

3.7 AUDITORIA LEGAL Y DE SEGURIDAD O TÉCNICA

La Auditoria Legal y la Auditoria de Seguridad o Técnica son complementarias, con su realización se pretende garantizar a la empresa auditada , en el ámbito de la Ley Orgánica 15/1999 de Protección de Datos, la correcta adaptación al Real Decreto 994/1999*,* de 11 de junio por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, en cuanto al procedimiento, documentación y requisitos exigidos así como otorgar garantías a la dirección, relativas a la fiabilidad, eficiencia y seguridad del sistema, proporcionando información precisa para el proceso de toma de decisiones y su realización permite:

- Identificar las fuentes de riesgo de fallos en la seguridad de los sistemas informáticos y elaborar un plan de actuación para minimizarlos.

- La obtención de informes detallados, razonados y documentados, sobre el estado tecnológico actual de la empresa, sus problemática y las posibles soluciones

Para la elección de **un Auditor de actividades** relacionados con Protección de Datos Personales debemos tener en cuenta:

1. Los servicios que permitan cubrir las diferentes necesidades que podamos tener en materia de protección de datos.
2. La especialización en este tipo de servicios.
3. Características de los servicios que se desarrollan de forma presencial en las instalaciones de los clientes, para evaluar directamente la realidad de la diferente problemática que tiene cada empresa.
4. Solvencia de su metodología de trabajo y resultados suficientemente contrastados con éxito.
5. Capacidad para dar respuestas eficaces a organizaciones con múltiples centros de trabajo.
6. Experiencias en los trabajos realizados y resultados suficientemente contrastados.

CAPITULO 4

APLICACIONES WAP

Javier Rodeiro Iglesias

4.1 INTRODUCCIÓN

En estos últimos años el parque de teléfonos móviles está aumentando de manera considerable, dicho crecimiento es debido a la gran aceptación que ha tenido el teléfono celular o teléfono móvil en la actual Sociedad de la Información. Estamos por tanto llegando a un punto en el que la dependencia de la tecnología de comunicación se hace más patente.

Hasta el momento la combinación de la telefonía móvil e Internet no satisfacía las expectativas creadas, sobre todo por las limitaciones de las redes de comunicación inalámbricas y la inoperabilidad de los terminales. Dichos obstáculos son ahora superados por la tecnología WAP (Wireless Application Prototocol), la cual viene a superar estas limitaciones para convertirse en un nuevo estándar lleno de posibilidades. Esta tecnología posibilitará el acceso a Internet sin la necesidad de un ordenador y un modem, pudiéndose realizar ésta a través de nuestro terminal móvil.

La tecnología de comunicación inalámbrica GSM basada en técnicas de conmutación de circuitos (ancho de banda no superior a 9,6 Kbps) ha evolucionado a la tecnología de comunicación GPRS de conmutación por paquetes llegando a alcanzar un ancho de banda de hasta 164 Kbps. Gracias a este ancho de banda las posibilidades para implantar un acceso a Internet mejoran considerablemente. De esta forma, cualquier cosa que se haga desde su PC conectado a Internet podrá hacerse desde su dispositivo móvil.

No obstante la revolución en este campo no viene con el paso de la tecnología de comunicación GSM a la GPRS, si no con la tecnología UMTS (Universal Mobile Telecommunications System). Los expertos consideran que para principios del 2001 estará en servicio la tecnología GPRS y para el año 2002 esta previsto que veamos los primeros esfuerzos para llegar a la denominada banda ancha, gracias a la tecnología UMTS. Esta tecnología, podrá llegar a una tasa de transmisión de hasta 2 Mbps, posibilitando la recepción de imágenes y vídeo con gran facilidad. Por el momento habrá que conformarse con la banda estrecha de la tecnología GPRS y esperar que todas las redes de telecomunicaciones se integren para conseguir la tan ansiada banda ancha en la telefonía móvil.

WAP (Wireless Application Prototocol) es un conjunto de protocolos que toma las características tanto de Internet como de los estándares desarrollados para terminales móviles. En este sentido puede funcionar tanto en redes de transporte GSM como en GPRS o UMTS. Está por tanto, optimizado para superar las deficiencias de la telefonía móvil actual. Como consecuencia de ello, los entornos creados expresamente en tecnología HTML no son legibles e interpretables por este nuevo protocolo, para ello, se ha creado un nuevo lenguaje de marcas, un lenguaje de script y un interfaz de aplicaciones, WML, WMLScript y WTAI.

4.1.1 GSM

El estándar GSM es el sistema de telefonía móvil más usado alrededor del mundo [Castro2001] (51 % del mercado compartido de todos los teléfonos celulares, tanto analógicos como digitales), con más de 215 millones de usuarios en América, Europa, Asia, África y Australia; dicho estándar hace uso de un conjunto de algoritmos criptográficos para proporcionar los mecanismos de seguridad del sistema (Autenticación y Confidencialidad), los algoritmos son:

- A3 Algoritmo de autenticación
- A5/1 - A5/2 Algoritmos de cifrado
- A8 Algoritmo de generación de clave

Dichos algoritmos fueron desarrollados de forma secreta. En el proceso de autenticación y generación de claves el sistema hace uso de una clave secreta (Ki) que servirá como entrada al algoritmo correspondiente (A3 o A8). Dicha clave es conocida únicamente por el SIM (Subscriber Information Module) y el operador, estas claves son diferentes para el algoritmo autenticación y generación de claves empleando un número secreto aleatorio (RAND) generado por el operador.

La mayoría de los proveedores GSM utilizan un algoritmo denominado COMP128 tanto para A3 como para A8, este algoritmo es criptográficamente débil y no es difícil de romperlo y clonar teléfonos móviles. En Abril de 1998, un grupo de investigación de Berkeley publicó un análisis de COMP128. Este ataque puede ser llevado simultáneamente a cabo sobre tantos teléfonos en un rango de radio tan amplio como canales tenga la estación base con la que se lleva a cabo el delito. Demostrando en esta investigación, que todas las implementaciones A8 que se habían examinado, incluyendo las pocas que no usaban COMP128, eran deliberadamente débiles.

El procedimiento de cifrado esta basado en la suma OR exclusiva de los bits a transmitir, el algoritmo ocupado para la generación de las secuencias de cifrado y descifrado es secreto y se denomina A5, del cual existen dos versiones: A5/1 y A5/2. Este tiene dos entradas: el Nº de trama (22 bits) y la clave de cifrado KC (64 bits), con estas entradas el algoritmo desarrolla procedimientos matemáticos obteniendo a su salida dos secuencias binarias de 114 bits, una de las cuales se utiliza para cifrar y la otra para descifrar.

Entre los meses de Mayo y Agosto de 1999 se analizaron los algoritmos A5/1 y A5/2 encontrándose que los dos algoritmos encargados del cifrado en

GSM son imperfectos, el ataque al cual fue sometido el algoritmo A5/1 lo realizaron Alex Biryokov y Adi Shamir mientras que el ataque al A5/2 fue realizado por Marc Briceno, Ian Goldberg y David Wagner, los cuales encontraron que el A5/2 es el más débil de los dos algoritmos de cifrado ya que este puede ser roto en tiempo real sin ningún problema; teniendo un factor de trabajo de aproximadamente 216.

4.1.2 GRPS Y UMTS

GPRS (General Packet Radio Services) es un nuevo conjunto de servicios desarrollado por el ETSI (European Telecommunication Standard Institute) los cuales se añadirán a los actuales que posee GSM, se van a introducir durante el año 2000, básicamente añade conmutación de paquetes de datos a todos los niveles de la red GSM. GPRS ofrece funciones de autenticación, control de accesos, confidencialidad de la identidad del usuario y confidencialidad de la información. Los algoritmos empleados en el proceso de Autenticación son los mismos que los de GSM (A3 y A8), mientras que el algoritmo utilizado para el cifrado de los datos de usuario ha sido modificado debido a la naturaleza del tráfico de GPRS, dicho algoritmo denominado GPRS A5 fue definido por 5 personas en SAGE (Security Advisor Group of Experts) del ETSI y no se encuentra disponible de forma pública. A GPRS se le denomina como la generación 2.5, ya que es el paso intermedio a los nuevos sistemas de 3ª generación.

UMTS (Universal Mobile Telephone System) es el sistema de telefonía móvil de 3ª generación el cual se encontrará disponible a partir del año 2002, UMTS será capaz de alcanzar velocidades entre 384 kbps para entornos de redes de banda ancha y 2.0 Mbps para entornos locales. Respecto a los mecanismos de seguridad del sistema UMTS estos se encuentran en la fase de desarrollo, han sido propuestos diferentes mecanismos para proporcionar autenticación, confidencialidad y generación de claves.

4.2 WAP

WAP (Wireless Access Protocol) un sistema completamente nuevo que combina dos tecnologías: Internet y las comunicaciones móviles, el cual fue realizado por 4 compañías (Nokia, Motorola, Ericsson y Unwired Planet).

Dicho protocolo proporcionará todos los servicios (Navegación, Correo Electrónico, Comercio Electrónico, etc.) que tiene disponible el usuario con Internet. El modelo WAP es basado en la arquitectura definida en el World Wide Web (WWW) adaptándolo a los nuevos requisitos del sistema haciendo uso de una pila de protocolos similares a los empleados en Internet, basándose en un modelo de capas al igual que el sistema OSI, cada una de estas capas del modelo de referencia emplea uno o varios protocolos los cuales tienen la función de interpretar la información que recibe de la capa inmediata inferior y adaptarla para que la capa inmediata superior pueda repetir la misma operación y llegar a la capa de aplicación. El terminal móvil hará uso de un "pequeño navegador" similar a Netscape Navigator o Internet Explorer encargado de la coordinación con la pasarela, a la que realiza peticiones de información; peticiones que son tratadas y encaminadas al servidor de información adecuado. Una vez procesada en el servidor, la información se envía a la pasarela, que la procesa y la envía al teléfono móvil.

La capa de transporte viene definida por el protocolo WDP (Wireless Datagram Protocol), este permite hacer uso de las mismas aplicaciones en diferentes tipos de portadoras (distintas frecuencias o distintos protocolos de acceso al medio) o señales de información. En la capa de seguridad se emplea el protocolo WTLS (Gíreles Transport Layer Security) el cual es derivado del SSL 3.1, es basado en el sistema abierto TLS 1.0 proporcionando los elementos de seguridad de confidencialidad, integridad y autenticación; la verificación de la autenticación, no-repudio son dadas por una PKI (Public Key Insfraestructure). La capa de transacción esta basada en WTP (Wireless Transaction Protocol) derivado del TCP, la función principal de esta capa es eliminar los datagramas no utilizados y preparar la información para la capa superior. WSP (Wireless Session Protocol), es el protocolo que se empleará en la capa de sesión y está preparado para agrupar varias operaciones WTP

siendo encargado también del restablecimiento de las conexiones que excedan el tiempo de vida asignado al iniciar la conexión. La última capa, la de aplicación define la interfaz de usuario en el teléfono, hace uso de: Wireless Markup Language (WML), WMLScript y Gíreles Telephony Application (WTA).

Al igual que UMTS los mecanismos de seguridad de WAP se encuentran en una etapa de desarrollo aunque ya existen algunas herramientas que se apoyan en dicho estándar para ofrecer los elementos de confidencialidad, integridad, autenticidad y no-repudio.

Así tenemos W/Secure y Baltimore Telepathy los cuales contienen una implementación de WTLS, existen diferentes forma de implementar dichos mecanismos de seguridad, entre los cuales tenemos:

- Autenticación mutua sobre la interfaz aire, la cual serviría para establecer parámetros importantes de seguridad.
- Cifrado interfaz aire, para emplear este tipo de cifrado es necesario hacer uso de diferentes claves de control junto con la información de señalización.
- Cifrado punto a punto: por medio de este tipo de cifrado la aplicación puede verificar las claves de administración sin ningún problema y de esta manera los datos que hace uso la aplicación nunca serán expuesta fuera de ella.

4.2.1 LENGUAJES DE MARCAS

En los años 60, IBM intentó resolver sus problemas asociados al tratamiento de documentos en diferentes plataformas a través de GML (*Generalized markup Language*).

El principal problema era que cada aplicación utilizaba sus propias marcas para describir los diferentes elementos [Wap]. Las *marcas* son códigos que indican a un programa cómo debe tratar su contenido y así, si se desea que un texto aparezca con un formato determinado, dicho texto debe ir delimitado por la correspondiente marca que indique como debe ser mostrado en pantalla o impreso. Y lo mismo ocurre con todas las demás características de cualquier texto. Ejemplos pueden tenerlos en mente los usuarios de WordPerfect.

Conociendo este sistema y conociendo a la perfección el sistema de marcas de cada aplicación sería posible pasar información de un sistema a otro sin necesidad de perder el formato indicado. La forma que IBM creó para solventar esto se basaba en tratar las marcas como texto accesible desde cualquier sistema, texto plano, código ASCII. Y la norma se denominó GML (General Modeling Language).

Más tarde GML pasó a manos de ISO y se convirtio en SGML (ISO 8879), Standart Generalized Markup Language. Esta norma es la que se aplica desde entonces a todos los lenguajes de marcas, cuyos ejemplos más conocidos son el HTML y el RTF.

Los lenguajes de marcas no son equivalentes a los lenguajes de programación aunque se definan igualmente como "lenguajes". Son sistemas complejos de descripción de información, normalmente documentos, que si se ajustan a SGML, se pueden controlar desde cualquier editor ASCII. Las marcas más utilizadas suelen describirse por textos descriptivos encerrados entre signos de "menor" (<) y "mayor" (>), siendo lo más usual que existan una marca de principio y otra de final.

Se puede decir que existen tres utilizaciones básicas de los lenguajes de marcas: los que sirven principalmente para describir su contenido, los que sirven más que nada para definir su formato y los que realizan las dos funciones indistintamente. Las aplicaciones de bases de datos son buenas

referencias del primer sistema, los programas de tratamiento de textos son ejemplos típicos del segundo tipo, y aunque no lo parezca, el HTML es la muestra más conocida del tercer modelo.

4.2.2 WML

WML son las siglas de Wireless Markup Languaje Las características principales de WML son:

- Soporte para imágenes y texto, con posibilidad de texto con formato.
- Tarjetas agrupadas en barajas. Una pagina WML es como una página HTML en la que hay una serie de cartas, al conjunto de estas cartas se les suele llamar baraja.
- Posibilidad de navegar entre cartas y barajas de la misma forma que se navega entre páginas Web.
- Manejo de variables y formularios para el intercambio de información entre el teléfono celular y el servidor.

WML es un lenguaje de marcas similar al HTML. WML es compatible con XML 1.0. Las páginas WML son llamadas barajas ya que están compuestas por cartas, un navegador WAP, solo puede mostrar una carta al mismo tiempo.

4.2.3 WMLSCript

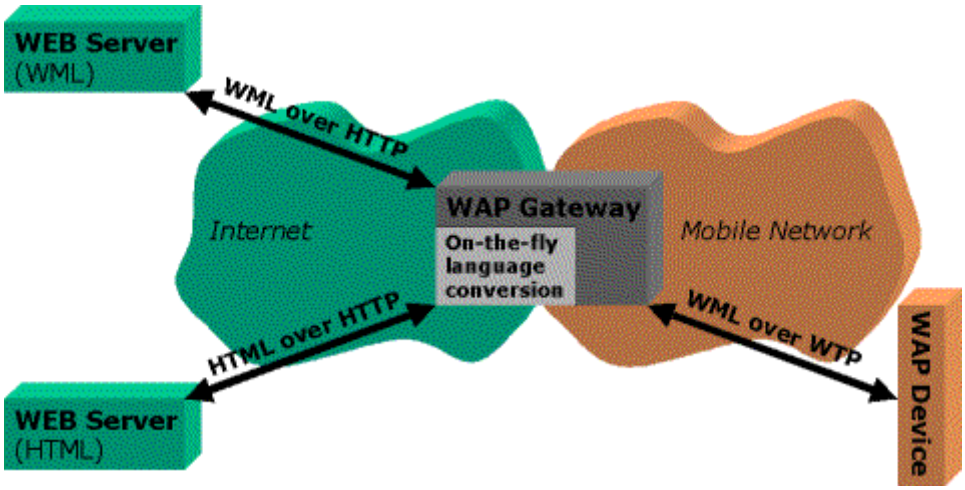
WMLS son las siglas de Wireless markup Language Script y es un lenguaje de programación que se utiliza para realizar páginas para cualquier elemento que utilice la tecnología WAP, como son algunos teléfonos móviles. Puede considerarse un dialecto de JavaScript. La intención de los creadores de WMLScript era dotar con un poco de inteligencia a las páginas WML, aunque está inteligencia es por ahora limitada.

4.2.4 SERVIDORES WAP

Internet se compone de miles de servidores que almacenan las páginas que vemos (o las aplicaciones que generan dichas paginas) a los que acceden los clientes (los navegadores, generalmente). El sistema seguido por WAP no es muy diferente. Ahora los clientes son los dispositivos móviles y los servidores deben seguir almacenando las páginas y aplicaciones.

La única consideración que hay que hacer es que hay que conectar la red inalámbrica (telefonía móvil) a Internet, de forma que el dispositivo portátil pueda hacer una petición de pagina WML al servidor.

Para conectar ambas redes las especificaciones WAP asumen que habrá un gateway WAP que convierte las peticiones WAP a peticiones WEB, y las respuestas WEB a respuestas WAP, como vemos en la siguiente figura [Wap]:



En teoría, el gateway debe poder convertir paginas HTML, sobre la marcha, en paginas WML. Sin embargo, puesto que WML esta pensado y diseñado para presentar información en pantallas muy pequeñas, y no es tan

potente, visualmente, como HTML, esa translación de información HTML a WML puede ser complicada de hacer (mas aun si hay scripts, animaciones, imágenes grandes, etc).

4.3 SEGURIDAD APLICACIONES INALÁMBRICAS

Según John Fallon, Director de Desarrollo Técnico del Mercado en Baltimore Technologies ha llegado la hora de que los operadores de móviles adopten una infraestructura de seguridad que haga posible operaciones seguras a través de móviles si no quieren quedarse a las puertas del nuevo "ecosistema" del comercio móvil. Europa está resultando un terreno muy fértil para lo que, en ocasiones, parece más una "jungla móvil" que un entorno de comercio móvil[VirusProt2002].

No es de extrañar si se tiene en cuenta que está previsto que el mercado europeo de comercio a través de telefonía móvil crezca desde los 323 millones de euros del año pasado hasta 23.000 millones para 2003 (Durlacher Research Ltd., Enero de 2000), momento en el que se espera que haya más de mil millones de abonados con teléfono móvil.

Todos se están apresurando a acotar sus terrenos; empresas de cualquier tipo están abriendo portales en este nuevo comercio móvil, desde bancos a empresas de ocio. Sin embargo, los operadores de móviles en Europa son, sin duda, los mejor equipados para sobrevivir en este nuevo e-cosistema, pues cuentan ya con una relación mediante su factura con los nuevos clientes y controlan el portal por defecto que está preinstalado en el momento de la distribución de los teléfonos móviles y otros dispositivos de acceso a Internet.

Siendo conscientes de estas fuerzas orgánicas, la mayoría de los operadores de redes móviles en toda Europa están ya construyendo portales móviles, sobre todo servicios de información que utilizan datos desde portales o

suministradores de contenidos existentes pertenecientes a terceros. Dichos portales ya exigen grandes inversiones, pero con escasos resultados en lo que respecta a generar ingresos (excepto mediante cuotas telefónicas). Los operadores de móviles que no tengan previsto pasar del suministro de dichos portales de información al suministro de portales de operaciones, seguro que se quedarán a las puertas de esta nueva jungla móvil. En este artículo se analiza cómo evitar que esto suceda.

Los operadores de móviles no pueden permitirse el lujo de quedarse de brazos cruzados ante el comercio móvil. Es cierto que se prevé un aumento de sus ingresos a corto plazo por las cuotas telefónicas pero, a largo plazo, la competencia provocará una significativa reducción de estas cuotas. Es necesaria una estrategia que genere una mayor propiedad y control de este nuevo mercado electrónico a través de telefonía móvil, a la vez que aumentan al máximo los posibles ingresos. Los operadores de móviles deben colocarse en el centro del desarrollo del comercio electrónico, específicamente el comercio móvil (que se refiere a operaciones dinerarias a través de dispositivos móviles más que comercio en su sentido más amplio). De no hacerlo así, se exponen a perder importantes flujos de ingresos debido al continuo descenso de los precios en sus servicios de voz.

A corto plazo es necesaria una estrategia para que los operadores de móviles asciendan en la cadena de valor. La mayoría de ellos ha comenzado con buen pie gracias a la construcción de portales de información y la incorporación de nuevas aplicaciones para el comercio a través de móviles tales como correo electrónico y envío instantáneo de mensajes. No obstante, en el futuro los operadores de móviles deberán participar en los ingresos derivados de operaciones y en la gestión segura del pago derivado de la operación. La buena noticia es que cuentan con un plazo ilimitado para acceder a las ventajas del mercado con respecto a otros importantes competidores. El motivo de ello es que todos poseen datos sobre sus abonados, tienen acceso a la ubicación del cliente, ejercen control sobre las tarjetas SIM que se distribuyen con los teléfonos móviles y cuentan con la capacidad adicional de cargar los bienes y servicios directamente en las facturas del teléfono.

Sin embargo, los operadores de móviles carecen de experiencia en el suministro de 'entornos fiables' para operaciones electrónicas en el contexto de acceso a Internet desde teléfonos móviles. Asimismo necesitan actuar con rapidez antes de que las ventajas de que disponen ahora desaparezcan por la apertura de servicios de acceso a Internet desde móviles directamente a sus abonados. Para su evolución en el campo del suministro de servicios de operaciones seguras es esencial la adopción y la integración a gran escala de Portales con Infraestructura Inalámbrica de Clave Pública (WPKI).

El Portal WPKI proporciona la infraestructura necesaria para crear un 'entorno fiable' para el comercio y las operaciones a través de móviles. Antes de examinar con más detalle los componentes de una WPKI, es importante comprender lo que dicha infraestructura debe ofrecer para generar este 'entorno fiable'.

Los cuatro elementos claves de dicho entorno son:

- **Confidencialidad** - Garantía de que nadie pueda estar escuchando.
- **Autentificación** - Garantía de que las personas con las que se está tratando son quienes dicen ser.
- **Integridad** - Garantía de que la información que envía o recibe no se ve alterada durante el trayecto.
- **No repudio** - Garantía de que los acuerdos son legalmente vinculantes.

El Portal WPKI cumple estas cuatro condiciones mediante criptografía asimétrica, firmas y certificados digitales y las autoridades pertinentes necesarias para su ejecución: Autoridades de Certificación (CAs) y Autoridades de Registro (RAs).

La integración de una WPKI en un portal de información puede generar fácilmente un portal de operaciones seguras. Únicamente dicha infraestructura permitirá a los proveedores de portales inalámbricos ofrecer con seguridad servicios externos adicionales a los clientes, tales como servicios financieros, de compra de entradas y de información no gratuitos. En el caso de operadores de móviles, dichos servicios podrán facturarse en el actual recibo de teléfono, efectuando la transformación de proveedor de portal de 'información' a portal de 'operación' con mayor facilidad que, incluso, para los demás competidores importantes.

Como alternativa, un Portal PKI puede asimismo facilitar la asociación efectiva con otras organizaciones del comercio a través de móviles, tales como bancos u otros proveedores de telefonía móvil, garantizando siempre que los proveedores de portales para móviles conservan el control y ofrecen una amplia gama de servicios a sus clientes o abonados.

Vamos a analizar cómo los componentes de una WPKI, incluyendo dos elementos esenciales como son un Portal PKI y un Sistema de Gestión de Certificados [formado por una Autoridad de Certificación (CA) y una Autoridad de Registro (RA)], garantizan un entorno fiable:

- Todos los individuos de una WPKI disponen de una "pareja de claves", formados por una clave pública y una clave privada. Las parejas de claves están ligadas matemáticamente utilizando criptografía asimétrica y cada una de ellas es única.
- El emisor de un mensaje emplea la clave privada para firmarlo digitalmente. La firma digital es la prueba de la identidad del usuario, el equivalente a una firma manuscrita legal.
- El receptor del mensaje utiliza la clave pública correspondiente para verificar la firma. Dado que es la única clave que coincide, sólo con ella se puede verificar la firma y probar que el emisor es la persona que dice

ser, además de comprobar que los datos no han sido modificados en forma alguna (comprobación de integridad).

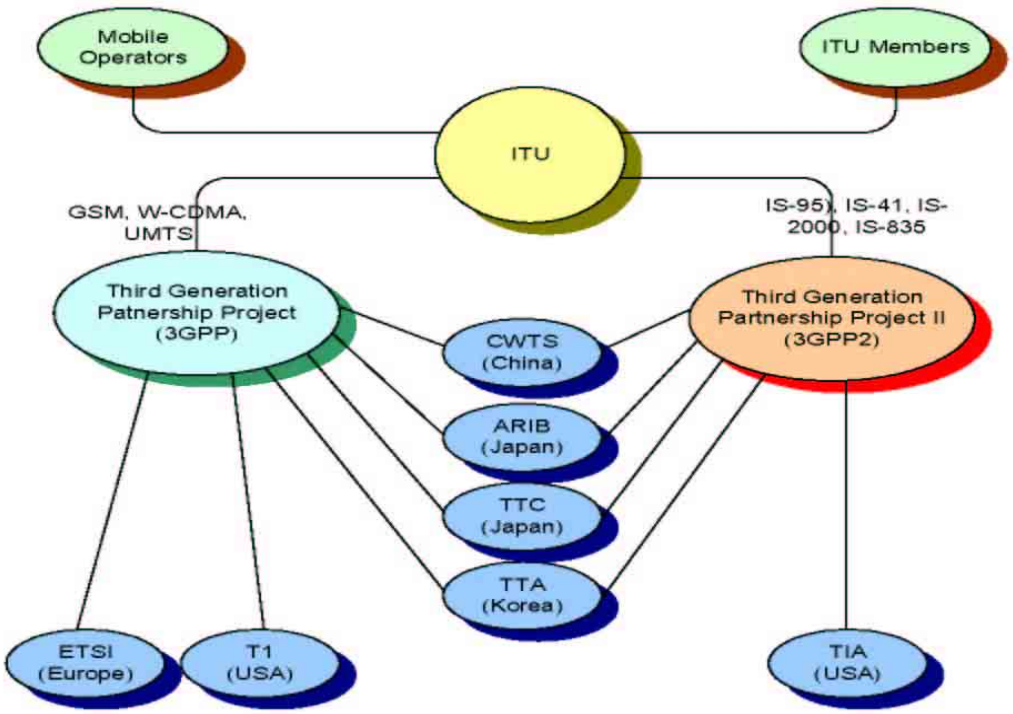
4.4 MECANISMOS DE SEGURIDAD

WAP nos ofrece una arquitectura flexible de seguridad, centrándose en proporcionar seguridad entre la conexión que posee un usuario y un servidor WAP, es decir, en general no ofrece mecanismos de seguridad extremo a extremo entre el usuario del terminal móvil y el servidor Web de Internet. Sin embargo, muchas aplicaciones requieren servicios de seguridad extremo a extremo (en particular es especialmente crítica la autenticación entre clientes y servidores Web). A continuación se evalúan diferentes opciones para ofrecer estos servicios extremo a extremo, estudiando el compromiso entre el nivel de seguridad requerido y la complejidad y coste de la solución adoptada. Se consideran las siguientes opciones:

- *Confiar en el servidor WAP y utilizar el mecanismo de autenticación de la red móvil:* En este caso se cede toda la autenticación del cliente a la propia red móvil, y el servidor WAP establece una conexión SSL con el servidor Web. Esta solución requiere confianza total en el servidor WAP, pero es fácilmente implantable y en la red móvil no es necesario utilizar el protocolo WTLS.
- *Confiar en el servidor WAP y utilizar WTLS entre cliente y servidor WAP:* Se aumenta la seguridad en la red móvil, pero nuevamente es necesaria una confianza total en el servidor. Requiere que los terminales móviles y el servidor WAP implementen WTLS.
- *Utilizar una conexión WTLS con el servidor Web remoto:* Esta solución no requiere confianza en el servidor WAP (las medidas de seguridad se implementan extremo a extremo). A cambio, requiere que el servidor de Internet ofrezca un servidor WTLS.

- *Proteger la comunicación a nivel de aplicación:* Ciertas aplicaciones críticas requerirán servicios especiales de seguridad (como no repudio) que forzosamente se deben ofrecer a nivel de aplicación.

4.5 ENTIDADES DE REFERENCIA



4.6 REFERENCIAS

[VirusProt2002] http://www.virusprot.com/Art5.html 07/05/2002

[Castro2001] Castro, J.C., Forné J. Acceso seguro a internet móvil. Departamento de Matemática Aplicada y Telemática. Universidad Politécnica de Cataluña. 2001.

[wap]Maria Isabel García Arenas.

CAPITULO 5

BASE HISTORICA JURÍDICA DE LA PROTECCIÓN DE DATOS

Iñigo C. Pintos Fraile

5.1 INTRODUCCIÓN

El objetivo del derecho ha sido siempre regular las relaciones entre los seres humanos que viven dentro de una sociedad conforme a unos principios y normas a los que se deben someter las personas para poder vivir en paz y bajo la idea de justicia.

De esta definición de los objetivos del derecho quisiera destacar ahora la palabra <<sociedad>>. En la actualidad las nuevas tecnologías, la información, las telecomunicaciones han cobrado tal importancia se puede hablar de un nuevo tipo de sociedad, LA SOCIEDAD DE LA INFORMACIÓN; nunca la información había tenido tanta importancia, no sólo por la cantidad de conocimientos que ahora se pueden almacenar y procesar, sino por la difusión que se le puede dar, lo cual tiene aspectos positivos (una mayor difusión de la cultura) como negativos (fácil difusión de conductas delictivas) lo cual supone numerosos nuevos retos al legislador, nuevos problemas que se añaden a los ya existentes que, a su vez, resultan afectados y matizados; el derecho tendrá que responder, bien regulando ex-novo, bien adaptando las figuras jurídicas existentes; esta sociedad va a exigir (exige) nuevas profesiones, nuevos tipos de contratos (a su vez nuevas regulaciones como lugar de celebración, lugar y momento de la aceptación…), etc.

Dentro de estos nuevos retos, la protección de los datos ha sido objeto de especial preocupación por parte de los legisladores como veremos a continuación y posteriormente al hablar de la legislación comunitaria.

Quisiera aclarar, antes de nada, lo erróneo de la expresión "protección de datos", ya señalada por la doctrina[1]; En modo alguno el objeto de protección son los datos en si, sino que a la persona a la que se quiere proteger impidiendo la recogida y manipulación de sus datos pueda causarle alguna perturbación no deseada; Se intenta evitar cualquier posible intromisión ilícita en la vida privada del individuo por la utilización de los mismos. Si tomáramos cualquier base de datos, a la que le retiráramos todos las indicaciones que pudieran asociarlos o identificar a persona alguna (nombre, apodo, etc) por muy íntimos, personales sensibles, o como quiera calificar los datos que la LOPD califica mas asépticamente como de nivel alto, esos datos no merecerían protección alguna de la ley de esta ley orgánica.

5.2 EL ORIGEN DE PROBLEMA

Como ya apunté antes vivimos una sociedad en el que las comunicaciones y la información adquiere una importancia inusitada: Un rumor hace caer la bolsa, una falsa noticia puede provocar una guerra, la ausencia de noticias eleva los rumores. El control de la información no sólo trae poder "saber es poder"; sin entrar en grandes ámbitos de política nacional o internacional, la información tiene gran relevancia en el ámbito privado: información en manos propias hace crecer empresas, y en manos ajenas las hace caer.

Evidentemente para tener información hace falta recabar datos, el problema surge cuando, bien desde los poderes públicos bien desde la empresa los derechos fundamentales del individuo se van a ver o pudieran verse, afectados. La respuesta desde el derecho clásico ha sido la defensa del derecho a la intimidad, haremos un somero estudio de dicho derecho, su insuficiencia, y la creación la aparición de un nuevo derecho por nuestro TC

[1] Guía Práctica protección de Datos; Miguel Ángel Davara Rodríguez

5.3 INTIMIDAD VERSUS PRIVACIDAD

5.3.1 SEMÁNTICAMENTE

Por intimidad: se debe entender, según la RAE una zona espiritual íntima reservada de una persona o de un grupo, especialmente de una familia.

Por privacidad: ámbito de la vida privada a la tiene derecho a proteger de cualquier intromisión

5.3.2 EL DERECHO DE LA INTIMIDAD

La función del derecho fundamental a la intimidad del art. 18.1 CE es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad. Dentro de la intimidad podríamos hablar de sentimientos, pensamientos e inclinaciones guardados en nuestro interior: las inclinaciones políticas, religiosas, sexuales, que pueden o no ser compartidas pero dentro de un ámbito restrictivo (así se protege el secreto de las comunicaciones en especial, de las postales, telegráficas y telefónicas)

La privacidad

Es un término que algunos califican de barbarismo, (es decir, sería, para este sector, un término incorrecto y que debía ser sustituido por <<intimidad>>, vocablo que sí sería adecuado) y otros, entre los que me incluyo, lo calificamos como un necesario neologismo que, empleado en el ámbito de protección de datos se conservaba inexistente en el diccionario de la Real Academia española hasta que, finalmente se produce su incorporación en la edición del 2001; Como vemos la privacidad es un concepto más amplio de la vida de la persona más allá de lo que es propiamente íntimo.

La constitución española sólo habla de intimidad, (al igual que el Código penal) mientras que la LOPD, (y en su día la LORTAD) habla de privacidad

La confusión entre ambos puede ser debida a la frágil frontera de zonas comunes que los separa y al tiempo los aúna: la intimidad forma parte de la privacidad, pero no al contrario; dicho de otra forma: los asuntos íntimos son privados, pero no todos los asuntos privados son íntimos.

En relación con los datos, en principio pudiera parecer, la Constitución sólo garantiza la no intromisión en nuestra intimidad, y parecería que nadie pudiera entonces, recabar datos sobre nuestras creencias, vida sexual, etc., quedando fuera de protección la parte de nuestra vida que no es tan íntima; pero sucede que, cuando se van recabando datos de una persona que en principio podríamos calificar como poco transcendentes, es decir si a mi me recaban los datos de las películas que he visto, a que reuniones ha ido, que libros ha leído… datos que por sí, individualmente, pueden, aparentemente, ser datos inocuos en cuanto sus consecuencias, puede que no me importe; pero puede que me de cuenta que en su conjunto si la adquieran, si sumamos diferentes datos se podría, perfectamente un perfil psicológico del mi persona, lo que facilitaría intromisiones; (Téngase en cuenta la gran capacidad de almacenar datos, de transmitirlos, de entrecruzarlos incluso mediante programas que responden a ese fin como la técnica del “data mining”); evidentemente los datos aislados tienen su importancia: el que alguien diga mi profesión, puede no importarme, (más me disgustaría que se supiese lo que tengo en mi cuenta bancaria y en ninguno de dos casos estamos en ámbito de la intimidad), sin embargo puede que ya no me gustará tanto figurar en ciertas bases de datos en poder de ciertas personas aún con el mero dato de profesión (un policía no le gustaría que este dato fuese sabido). Incluso mi número de teléfono es posible que no quisiera que fuera divulgado. Sin embargo, repito al parecer, se tiene la sensación que dichos datos no tienen porque ser regulados y que cierta parte de nuestra vida privada pudiera ser expuesta sin más consideraciones.

Cuando en España aún no se estaba concienciado de los problemas que pudieran surgir, en 15-XII-1983 una sentencia del TC alemán promulgó una muy interesante sentencia en la que se partía de la idea de la libertad personal como autodeterminación individual, la cual incluiría la autodeterminación informativa. Las personas tienen derecho a saber y a decidir por sí mismas cuando y dentro de qué límites procede revelar datos referentes a su vida. La vida moderna facilita las intromisiones en nuestra vida privada: aparatos de escucha, teleobjetivos. La autodeterminación del individuo exigía que se tuviese el derecho de, al menos, saber quien y con que fines alguien sabe algo de él… lo interesante de la sentencia es que vaticinaba que el derecho a la intimidad no puede ser concebido como un mero derecho de prohibir intromisiones, sino que además se hacía necesario una participación activa de la persona, había que dotarla de ciertos derechos para conocer dónde figuraba información sobre él, con que fines y que tipo de información (todo ello sin hablar de la insuficiencia del término intimidad).

La ausencia de regularización hizo proliferar empresas que recababan datos de maneras más o menos ortodoxas, se sacaran de los hábitos de compra de sujetos sus perfiles psicológicos y que, finalmente comercializaban los propios datos vendiéndolos a otras empresas y que, a su vez sorprendían al despistado ciudadano de cómo podían acertar tanto a la hora de hacer sus ofertas.

Con la firma en 1982, del Convenio del Consejo de Europa sobre protección de datos personales respecto al tratamiento automatizado de datos personales, España parecía empezar a darse cuenta del problema que se avecinaba.

Pero es el Tribunal Constitucional el que va a ir reconociendo la insuficiencia del concepto intimidad;

- ya en 1984 la sentencia 110/1984 afirmó que “los distintos apartados del artículo 18 de la Constitución tienen como finalidad principal el respeto a un ámbito de vida privada, personal y

familiar, que debe quedar excluido del conocimiento ajeno y de las intromisiones de la tecnología, salvo autorización del interesado; lo que ha ocurrido es que el avance de la tecnología actual y el desarrollo de los medios de comunicación de masas han obligado a extender esta protección más allá del aseguramiento del domicilio como espacio físico en que normalmente se desenvuelve la intimidad, y del respeto a la correspondencia, que es o puede ser medio de conocimiento de aspectos de la vida privada".

La entrada en la Comunidad Europea en 1986 (que implica la aceptación de la normativa europea, dónde ya existía una preocupación) y el nacimiento en 29 octubre de 1992 de la LORTAD (Hoy derogado por la LOPD) cambiarán el panorama. Como estos temas serán objeto de la ponencia de mañana si quisiera ahora hablar de las Sentencias que han ido naciendo en nuestro TC y que desembocan en el nacimiento de un nuevo derecho

La jurisprudencia del Tribunal Constitucional (Sentencias 254/1993, de 20 de julio; 143/1994, de 9 de mayo; 11/1998, de 13 de enero; 94/1998, de 4 de mayo y 202/1999, de 8 de noviembre) ha venido señalando que el artículo 18.4 de la Constitución ampara y protege el derecho de cada individuo frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, que constituye lo que se ha denominado "libertad informática"

Dos sentencias son clave en esta evolución:

- La STC 254/1993: Se trataba, de un recurso de amparo consiste en determinar si la negativa a suministrar la información solicitada, acerca de los datos personales del actor que la Administración del Estado posee en ficheros automatizados, vulnera o no los derechos fundamentales a la intimidad y a la propia imagen que le reconoce el artículo 18 CE, tanto en su

apdo. 1 como en el 4. La solicitud presentada por el recurrente a las autoridades de la Administración del Estado se basaban a los dos primeros apartados del artículo 8 del Convenio, a cuyo tenor «cualquier persona deberá poder: a) Conocer la existencia de un fichero automatizado de datos de carácter personal, sus finalidades principales, así como la identidad y la residencia habitual o el establecimiento principal de la autoridad controladora del fichero. b) Obtener a intervalos razonables y sin demora o gastos excesivos la confirmación de la existencia o no en el fichero automatizado de datos de carácter personal que conciernan a dicha persona, así como la comunicación de dichos datos en forma inteligible».

- (los tribunales inferiores habían rechazado las pretensiones ya que, decían que el convenio no era de aplicación directa en España faltando actividad interna del legislador español.) Un dato curioso es que durante aquel periplo jurisdiccional del ahora recurrente, había sido aprobada la LORTAD.
- Falla la sentencia: << sin embargo, es lo cierto que los textos internacionales ratificados por España pueden desplegar ciertos efectos en relación con los derechos fundamentales, en cuanto pueden servir para configurar el sentido y alcance de los derechos recogidos en la CE (…). Es desde esta segunda perspectiva desde la que hay que examinar la presente demanda de amparo. Dispone el artículo 18.4 CE que «la Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos». De este modo, nuestra CE ha incorporado una nueva garantía constitucional, como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona, de forma en último término no muy diferente a como fueron originándose e incorporándose históricamente los distintos derechos

fundamentales. **En el presente caso estamos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la CE llama «la informática».** (Fundamento jurídico 6, reiterado luego en las sentencias del Tribunal Constitucional 143/1994, fundamento jurídico 7, 11/1998, fundamento jurídico 4, 94/1998, fundamento jurídico 6, 202/1999, etc)

- En el punto SÉPTIMO se plantea el problema de cuál deba ser ese contenido mínimo, provisional, en relación con este derecho o libertad que el ciudadano debe encontrar garantizado, aun en ausencia de desarrollo legislativo del mismo.

  Un primer elemento, el más «elemental», de ese contenido es, sin duda, negativo, respondiendo al enunciado literal del derecho: el uso de la informática encuentra un límite en el respeto al honor y la intimidad de las personas y en el pleno ejercicio de sus derechos. Ahora bien, la efectividad de ese derecho puede requerir inexcusablemente de alguna garantía complementaria (…). La llamada «libertad informática», es así, también, derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data).

- Las facultades precisas para conocer la existencia, los fines y los responsables de los ficheros automatizados dependientes de una Administración Pública donde obran datos personales de un ciudadano son absolutamente necesarias para que los intereses protegidos por el artículo 18 CE, y que dan vida al derecho fundamental a la intimidad, resulten real y efectivamente protegidos. Por

ende, dichas facultades de información forman parte del contenido del derecho a la intimidad, que vincula directamente a todos los poderes públicos, y ha de ser salvaguardado por este Tribunal, haya sido o no desarrollado legislativamente STC 11/1981, FJ 8, y 101/1991, FJ 2).

- Por consiguiente, se otorga amparo y se ordena al Gobernador Civil le comunique sin demora la existencia de los ficheros automatizados de datos de carácter personal que dependen de la Administración Civil del Estado, sus finalidades, y la identidad y domicilio de la autoridad responsable del fichero. Igualmente, deberá comunicarle en forma inteligible aquellos datos personales que le conciernen, pero tan sólo los que obren en aquellos ficheros sobre los que el Gobernador Civil ostente las necesarias facultades.

La argumentación de esta Sentencia 254/1993 es temida en cuenta por otra nueva sentencia que va a dar un nuevo paso.

- La **STS 292/2000, DE 30 DE NOVIEMBRE** Esta sentencia es consecuencia de un recurso de inconstitucionalidad presentado por el defensor del pueblo contra el artículo 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal)

  - el artículo 21.1 de la Ley Orgánica de Protección de Datos, referido a la posibilidad de que, mediante norma de rango inferior a ley, pudiera darse cesión de datos entre Administraciones Públicas. El Constitucional va a apreciar la nulidad de este art y va a reconocer la necesidad de existencia de una ley, mucho más si la cesión de datos produce sin el consentimiento del interesado y, añade, que

es necesario que la Ley también que ésta determine el destino de los datos después de la cesión.

- 24.1 y 2 ("Otras excepciones a los derechos de los afectados") por vulneración de los arts. 18.1 y 4 y 53.1 CE. El tribunal declarará contrarios a la Constitución y nulos los incisos "impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones públicas" y "o administrativas" del apartado 1º del art. 24, y todo su apartado 2, de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal

Un estudio detallado de la Sentencia debería ser objeto de una ponencia monográfica, lo que me interesa ahora es que la 292/2000 marca un hito histórico en el protección de datos da lugar al reconocimiento del derecho, diferente del derecho a la intimidad (o a la libertad informática amparada en este derecho según vimos en Sentencia anterior) en la que se reconoce un nuevo derecho al que calificamos de derecho Fundamenta a la protección de Datos.

Este derecho se distingue conceptualmente este derecho del que protege la intimidad personal, previsto en el primer apartado del artículo 18. Mientras que la función de éste último es proteger de las intromisiones de terceros, en contra de la voluntad del afectado, la vida personal y familiar, el derecho a la protección de datos garantiza a la persona el control sobre sus datos personales, sobre su uso y destino, que se traduce en un poder de disposición sobre los mismos, que impone a los poderes públicos la prohibición de que se conviertan en fuentes de esa información sin las debidas garantías.

El objeto de este derecho no se reduce a los datos íntimos de la persona, sino que alcanza a todo tipo de dato personal sea o no íntimo, (es decir, entramos en lo que denominamos privacidad, e incluyo datos que por públicos no dejan de estar en la esfera de la privacidad de la persona), y cuya

utilización, o mero conocimiento por parte de otras personas pueda causar consecuencias al sujeto. Ya no sólo es una defensa <<**frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos>>** que decía la sentencia anterior… sino un derecho sobre todo dato de una persona.

La función principal de este derecho es garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros determinados deberes que básicamente, y como van a ser objeto de la ponencia de mañana, me limito a citar: el previo consentimiento para la recogida, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar los mismos.

Se planteó si era verdaderamente un Derecho Fundamental al no estar recogido de forma expresa en la constitución pero esto es debido a una razón muy clara, siguiendo el voto particular del Magistrado don Manuel Jiménez de Parga y Cabrera:

<<No ha de sorprendernos que en la Constitución Española de 1978 no se tutelase expresamente la libertad informática. Veintidós años atrás la revolución de la técnica en este campo apenas comenzaba y apenas se percibía. No hemos de extrañarnos tampoco por la omisión de esta materia en los Estatutos de Autonomía de las Comunidades españolas. El entorno es ahora distinto del que fue nuestro mundo en 1978. La informática no ofrecía las actuales posibilidades para el quehacer vital, tanto positivas como negativas, con la adecuada protección de la dignidad de la persona. Muy significativo al respecto es que en la recentísima Carta de Derechos Fundamentales de la Unión Europea se haya incluido como una de las primeras libertades (art. 8) la resultante de la protección de datos de carácter personal>>.

- Como todo derecho, también tiene sus limites

- la Constitución art. 105 b) que la ley regulará el acceso a los archivos y registros administrativos "salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas" (en relación con el art. 8.1 y 18.1 y 4 CE),
- El TC ha declarado que la persecución y castigo del delito constituye, asimismo, un bien digno de protección constitucional, a través del cual se defienden otros como la paz social y la seguridad ciudadana. Bienes igualmente reconocidos en los arts. 10.1 y 104.1 CE (Tribunal Constitucional 166/1999, fundamento jurídico 2).
- También el Tribunal Constitucional ha considerado que la distribución equitativa del sostenimiento del gasto público y las actividades de control en materia tributaria (art. 31 CE) como bienes y finalidades constitucionales legítimas capaces de restringir los derechos del art. 18.1 y 4 CE. (STC 143/1994)

En resumen

- Protección de datos e intimidad son derechos distintos Este derecho fundamental a la protección de datos, es diferente del derecho a la intimidad del art. 18.1 CE, con quien comparte el objetivo de ofrecer una eficaz protección de la vida privada, dota a la persona de un más amplio campo de protección a la par que impone deberes a terceros (de acción y omisión) y cuya regulación debe ser por ley

  - La función del derecho fundamental **a la intimidad** del art. 18.1 CE es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad (por todas sentencia del Tribunal Constitucional

144/1999, de 22 de julio, fundamento jurídico 8). O lo que es lo mismo: excluir ciertos datos de una persona del conocimiento ajeno

- En cambio, **el derecho fundamental a la protección de datos** persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para los derechos del afectado. El derecho a la protección de datos garantiza a los individuos un poder de disposición sobre esos datos. Asimismo se impone tanto a los poderes públicos como al ámbito privado el cumplimiento de una serie de medidas y conductas con fin de prevenir los riesgos que puedan derivarse del acceso o divulgación indebidas de dicha información.

Hecha esta diferenciación el contenido del derecho de Protección de datos incluye: El poder de disposición sobre los propios datos personales que dota a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales; Básicamente: el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos. Es decir: puede exigir al titular del fichero que le informe de qué datos posee sobre su persona, accediendo a los ficheros, saber qué destino han tenido, si dichos datos son o no cedidos; y, en su caso, exigir que modifique o cancele

Por otra parte el concepto de dato relevante a estos efectos es ampliado más allá de los datos sean o no derechos constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar o cualquier otro bien constitucionalmente o legalmente amparado. No se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo,

cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos (todo dato) de carácter personal. Incluso alcanza a aquellos datos personales públicos, que por el hecho de ser accesibles al conocimiento de cualquiera, no deben escapar escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. Todos los datos amparados que identifiquen o permitan la identificación de la persona, todos, están dentro de este derecho por que todos, en un determinado momento, ambiente, solos o en conjunto pueden llegar a tener consecuencias para la persona.

En fin, son elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos. Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin, y, el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos...

Lo afirmado sobre el significado y el contenido del derecho a la protección de datos personales no sólo cumple los mandatos constitucionales citados sino que también cumplen con la normativa europea que será objeto de la siguiente ponencia.

CAPITULO 6

DIRECTIVA EUROPEA 95/46/CE

Iñigo C. Pintos Fraile

6.1 INTRODUCCIÓN

A continuación se verá la especial relevancia que la normativa Europea en la materia de protección de datos con un especial estudio de la 95/46/CE.

6.2 EVOLUCIÓN Y LA PREOCUPACIÓN DE EUROPA POR LA PROTECCIÓN DE DATOS

Se ha hablado de la nueva sociedad que ha nacido: <<la sociedad de la información>> y se ha concretado en lo referente a la protección de datos. Además de lo dicho anteriormente hay que añadir otras características para el ámbito internacional:

- en primer lugar esta nueva sociedad minimiza la relevancia de las fronteras, con lo que exige una mayor coordinación entre las diferentes legislaciones
- las medidas que se tomen sobre protección de datos pueden quedar mermadas por la no existencia de semejantes medias normativas fuera del país
- la experiencia nos muestra que la existencia de mercados comerciales interestatales hace que unos estados mas protectores se vean perjudicados frente a estados sin tales garantías

Estas afirmaciones son válidas a nivel internacional pero nos limitaremos al ámbito europeo.

Por una parte la existencia de un mercado común hace necesario una armonización entre las legislaciones con fin de que ningún país se vea perjudicado tanto en el correcto funcionamiento de sus mercados como en una merma de los derechos de sus ciudadanos

En Europa, se ha combinado siempre el interés por el desarrollo económico, se recuerda que la Unión Europea nación como un mercado común, con la preocupación por la protección de los derechos de sus ciudadanos.

Si su primer objetivo era el económico, y en este sentido pronto comenzó con un papel fundamental en la armonización de las legislaciones de los estados miembros con fin de no perjudicar el comercio, los derechos fundamentales siempre fue una cuestión que estuvo presente.

En relación a la sociedad de la información, y en concreto de la protección de datos, enumeraré una serie de hitos importantes, que no son todos, pero, quizá, si sean los más relevantes:

- 1993 el Consejo Europeo reunido en Bruselas solicita a un grupo de expertos que elaborase un informe sobre las medidas específicas que deben estudiar la comunidad y los estados miembros para el establecimiento de infraestructuras en el ámbito de la información; Este grupo da como resultado el informe <<Europa y la sociedad global de la información. Recomendaciones al Consejo Europeo>> conocido como <<Informe Bangemann>> (llamado así por el comisario que lo encabezaba Martín Bangemann); Este informe analiza el fenómeno de las nuevas tecnologías y el impacto que tendrán en el futuro europeo. En su capítulo 3 destacan la necesidad de armonizar las diferentes legislaciones y la en especial las referidas a las materias que protejan la intimidad de los individuos (conscientes del trasiego de datos que esta sociedad demanda)

- 1994 el Consejo Europeo de Corfú acoge con gran interés este informe y aboga por la creación de una <<estructura reglamentaria clara y estable (especialmente en lo que atañe al proceso a los mercados, a la compatibilidad entre las redes, a los derechos de propiedad intelectual, a la protección de datos y a los derechos de autor)>>
- un mes después (julio 1994) la Comisión pone en marcha un plan de actuación denominado: << Europa en marcha hacia la Sociedad de la Información>> en el que, dentro de las medidas de orden normativo, propone una mayor defensa de la intimidad
- en 1996 se publica un primer borrador del informe titulado <<La construcción de la sociedad europea de la información para todos nosotros>> En ella se recogen, al tiempo que las ventajas, los peligros de que con la proliferación de la información detallada que registra nuestros movimientos, compras y perfiles… la SI se convierta en "intrusiva"

Con estas premisas, y dado que las diferentes legislaciones estatales suponían un obstáculo para la libre circulación de la información y crear trabas adicionales para los operadores económicos y los ciudadanos. Entre estas trabas figuraban

- tener que registrarse o ser autorizado a tratar datos por las autoridades de control de varios Estados miembros,
- la necesidad de ajustarse a distintas normas
- y la posibilidad de tener limitaciones para transferir datos a otros estados miembros
- sin contar que algunos Estados carecían de legislación sobre protección de datos.

Con objeto de allanar los obstáculos a la libre circulación de datos, sin merma la protección de los mismos, se formularon una serie de directivas que armonizarían las diferentes legislaciones.

6.3 ¿QUÉ ES UNA DIRECTIVA?

Dice el artículo 249 del tratado constitutivo de la unión Europea:

<< Para el cumplimiento de su misión, el Parlamento Europeo y el Consejo conjuntamente, el Consejo y la Comisión adoptarán reglamentos y directivas, tomarán decisiones y formularán recomendaciones o emitirán dictámenes, en las condiciones previstas en el presente Tratado.

(…)

La directiva obligará al Estado miembro destinatario en cuanto al resultado que deba conseguirse, dejando, sin embargo, a las autoridades nacionales la elección de la forma y de los medios.

(…).>>

Las principales directivas son:

95/46/CE, de 24 de octubre, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos, con la finalidad de que los estados miembros armonizaran y adaptaran sus legislaciones internas a los esenciales principios que contenía.

97/66/CE, de 15 diciembre, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones, que es de aplicación a la prestación de servicios públicos de telecomunicación en las redes públicas de telecomunicación de la Comunidad, y especialmente a través de la red digital de servicios integrados (RDSI) y las redes móviles digitales públicas.

La Directiva 2000/31/CE, de 8 de junio, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, y en particular el comercio electrónico en el mercado interior, aún no siendo una

norma específica sobre la materia recogió importantes disposiciones relativas a las obligaciones de los prestadores de servicios de la sociedad de la información en materia de privacidad, y a las medidas adoptables con relación al comercio electrónico.

Directiva 2002 /58/CE de 12 de julio de 2002 relativa al tratamiento de los datos personales, y a la protección de la intimidad en el sector de las comunicaciones electrónicas. (Directiva sobre la privacidad y la protección de la intimidad en el sector de las comunicaciones electrónicas)

Para el tema que tratamos la más importante es la directiva **95/46/CE, de 24 de octubre**

6.4 LA DIRECTIVA 95/46/CE, DE 24 DE OCTUBRE

6.4.1 INTRODUCCIÓN: EL OBJETIVO DE LA DIRECTIVA

Es la primera norma de derecho derivado que regula un derecho fundamental.

Es fácil apreciar su objetivo lograr que el progreso económico, social, político y cultural que puede derivarse del uso de las nuevas tecnologías, (y que se propugna desde las instancias europeas), no supongan merma del este derecho de las personas a la no intromisión de su vida privada.

Al tiempo que se reconoce las posibilidades del uso de la informática a efectos del desarrollo económico, se reconoce también la necesidad de un mayor flujo de datos y la posibilidad de que los derechos de los individuos queden mermados por el mismo; Esto en una lectura más bondadosa, porque otra lectura sería el intentar evitar que las diferencias de legislación y un excesivo número de trabas normativas pudiera afectar el intercambio de flujos de información; sobre ello volveré seguidamente

En los “considerandos” de la propia directiva, mientras que en el número dos se habla del respeto a los derechos:

<<Considerando que los sistemas de tratamiento de datos están al servicio del hombre; que deben, cualquiera que sea la nacionalidad o la residencia de las personas físicas, respetar las libertades y derechos fundamentales de las personas físicas y, en particular, la intimidad, y contribuir al progreso económico y social, al desarrollo de los intercambios, así como al bienestar de los individuos>>

El tres destaca la necesidad de que el buen funcionamiento del mercado interior, se de también una libre circulación de datos personales de un Estado miembro a otro, aunque, menciona la necesaria protección de los derechos fundamentales de las personas; esta idea de necesidad de fluidez de circulación de datos (que será repetida en posteriores considerandos) parece ser la idea primordial y a ello responde la necesidad de eliminar las diferencias entre los estados (nº7 a 9) con fin de de que ello favorezca el comercio.

Esta sería la interpretación más maliciosa que la anterior. En cualquier caso la directiva se preocupa de desarrollar el derecho intentando que no haya merma en su vida privada

Dice el Artículo 1

<<- 1. Los Estados miembros garantizarán, con arreglo a las disposiciones de la presente Directiva, la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales.

2. Los Estados miembros no podrán restringir ni prohibir la libre circulación de datos personales entre los Estados miembros por motivos relacionados con la protección garantizada en virtud del apartado 1.>>

Observamos, (aunque ya veremos mas adelante que no se limita a datos de carácter íntimo y, de hecho, como dato personal objeto de protección se define en artículo 2 a) por dato personal debe entenderse << toda

información sobre una persona física identificada o identificable >>), la alusión a la intimidad sigue presente

Aunque la legislación aplicable, como vimos antes, es la que desarrolle cada estado, la directiva impone, a los estados miembros una serie de mínimos que el desarrollo legislativo estatal debe cumplir entre otros

Las características principales de la directiva:

1 EN CUANTO A LOS DATOS EN SÍ MISMOS Y SU RECOGIDA

Los datos deben ser:

- tratados de manera lícita; recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines;
- adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente;
- exactos y, cuando sea necesario, actualizados; deberán tomarse todas las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados;
- conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente.

Sin embargo, no debemos olvidar que hablamos de un derecho reconocido de la persona a disponer de sus propios datos, por ello se exigen el consentimiento (de forma inequívoca dice el art 7) del interesado salvo en determinadas circunstancias:

- para la ejecución de un contrato en el que el interesado sea parte o para la aplicación de medidas pre-contractuales adoptadas a petición del interesado, o

- el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento, o
- proteger el interés vital del interesado, o
- cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos, o
- satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva.

2 ESTABLECE CATEGORIA ESPECIAL DE DATOS

La directiva si establece unas ciertas categorías de datos cuyo tratamiento está prohibido, en principio y salvo determinadas excepciones, referidos al origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad. Aunque se establecen algunas salvedades;

3 ESTABLECE UN DERECHO DE INFORMACIÓN DEL INTERESADO

En cualquier caso el interesado siempre deberá conocer, tanto si se le recaban personalmente sus datos como si se recaban a por medio de otra persona diferente:

a) la identidad del responsable del tratamiento y, en su caso, de su representante;

b) los fines del tratamiento de que van a ser objeto los datos;

c) cualquier otra información tal como:

- los destinatarios o las categorías de destinatarios de los datos,

- el carácter obligatorio o no de la respuesta y las consecuencias que tendría para la persona interesada una negativa a responder,
- la existencia de derechos de acceso y rectificación de los datos que la conciernen, en la medida en que, habida cuenta de las circunstancias específicas en que se obtengan los datos, dicha información suplementaria resulte necesaria para garantizar un tratamiento de datos leal respecto del interesado.

4 ESTABLECE DERECHOS DE ACCESO, OPOSICIÓN

El interesado no debe limitarse a saber que en un momento se han recabado sus datos, sino que tiene derecho a conocer cuales son los datos que se están tratando; tal derecho tiene su correlativo en el deber del responsable de tratamiento a proporcionar la información (sin costes para el interesado) la confirmación de la existencia o inexistencia del tratamiento de datos que le conciernen, así como información por lo menos de los fines de dichos tratamientos, las categorías de datos a que se refieran y los destinatarios o las categorías de destinatarios a quienes se comuniquen dichos datos; toda la información disponible sobre el origen de los datos y, en su caso, la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la presente Directiva, en particular a causa del carácter incompleto o inexacto de los datos;

El interesado también podrá oponerse, en cualquier momento y por razones legítimas propias de su situación particular, a que los datos que le conciernan sean objeto de tratamiento, En caso de oposición justificada, el tratamiento que efectúe el responsable no podrá referirse ya a esos datos;

5 OBLIGACIONES DEL REPONSABLE DE TRATAMIENTO

Naturalmente el interesado no puede estar vigilando que los datos, una vez que ha consentido en cederlos, no sean utilizados para otros fines o lleguen a personas a las que no se los ha cedido; por ello se establece la obligación al responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la

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

También se prevé la figura de tratamientos por encargo que deberá estar regulada por un contrato u otro acto jurídico que vincule al encargado del tratamiento con el responsable del tratamiento, y que disponga, en particular:

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

6 SE ESTABLECE UNA AUTORIDAD DE CONTROL

Los Estados miembros deberán contar con una Autoridad de Control, que supervisará las actividades de los responsables del tratamiento de datos en la forma que reglamentariamente se desarrolle. Hemos de señalar a este respecto, que el reglamento 45/2001, de 18 de septiembre, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios, contemplaba también la creación de un Supervisor Europeo de Protección de datos, cuyo estatuto se encuentra en este momento en fase de elaboración.

Tale autoridades tendrán:

- poderes de investigación, como el derecho de acceder a los datos que sean objeto de un tratamiento y el de recabar toda la información necesaria para el cumplimiento de su misión de control;
- poderes efectivos de intervención, como, por ejemplo, el de formular dictámenes antes de realizar los tratamientos, y garantizar una publicación adecuada de dichos dictámenes, o el de ordenar el bloqueo, la supresión o la destrucción de datos, o

incluso prohibir provisional o definitivamente un tratamiento, o el de dirigir una advertencia o amonestación al responsable del tratamiento o el de someter la cuestión a los parlamentos u otras instituciones políticas nacionales;

- capacidad procesal en caso de infracciones a las disposiciones nacionales adoptadas en aplicación de la presente Directiva o de poner dichas infracciones en conocimiento de la autoridad judicial.
- Las decisiones de la autoridad de control lesivas de derechos podrán ser objeto de recurso jurisdiccional.
- y atenderán las solicitudes que cualquier persona, o cualquier asociación que la represente, le presente en relación con la protección de sus derechos y libertades respecto del tratamiento de datos personales. Esa persona será informada del curso dado a su solicitud.

7 REGULA LA TRANSFERENCIA DE DATOS PERSONALES A PAÍSES TERCEROS

El capítulo IV – regula la transferencia de datos personales a países terceros (fuera del ámbito de la unión Europea) que podrá efectuarse <<cuando, sin perjuicio del cumplimiento de las disposiciones de Derecho nacional adoptadas con arreglo a las demás disposiciones de la presente Directiva, el país tercero de que se trate garantice un nivel de protección adecuado>> o cuando concurran otras circunstancias como:

a) el interesado haya dado su consentimiento inequívocamente a la transferencia prevista, o

b) la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales tomadas a petición del interesado, o

c) la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar en interés del interesado, entre el responsable del tratamiento y un tercero, o

d) La transferencia sea necesaria o legalmente exigida para la salvaguardia de un interés público importante, o para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial, o

e) la transferencia sea necesaria para la salvaguardia del interés vital del interesado, o

f) la transferencia tenga lugar desde un registro público que, en virtud de disposiciones legales o reglamentarias, esté concebido para facilitar información al público y esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones que establece la ley para la consulta.

8 SE POTENCIA LA CREACIÓN DE CÓDIGOS DE CONDUCTA

Un punto interesante es la recomienda la promoción de la elaboración de códigos de conducta sectoriales destinados a contribuir a la correcta aplicación de las disposiciones nacionales en materia de protección de datos personales..

Y se establece la creación de una o más autoridades públicas se encarguen de vigilar la aplicación en su territorio de las disposiciones adoptadas por ellos en aplicación de la presente Directiva. Estas autoridades ejercerán las funciones que les son atribuidas con total independencia.

Se debe recordar que todas estas son medidas que los Estados miembros deben adoptar pues son los Estados los destinatarios de las directivas.

En resumen

En octubre de 1995 el parlamento europeo adoptó las líneas maestras de lo que sería la política europea sobre protección de datos, tanto en cuanto su procesamiento, recopilación, etc, como la circulación de los mismos bajo dos ideas principales

- el concepto de datos como derecho inalienable del ciudadano
- la idea que la transmisión de datos debe contar con la suficiente fluidez para ser motor del comercio.
- La idea de que diferentes protecciones de datos en diferentes estados producirían una situación de desigualdad
- Y dota de un contenido la protección del derecho.

CAPITULO 7

L.O.P.D.

Victor A. Salgado Seguín

7.1 ORIGEN DE LA NORMATIVA NACIONAL

No hay duda de la importancia que las tecnologías de la información y de la comunicación han alcanzado en los últimos años. Las llamadas TIC (*Tecnologías de la Información y de la Comunicación*) han entrado nuestra sociedad de un modo extremadamente acelerado, produciendo una auténtica *revolución de la información*, del mismo modo que en su día fue la *revolución industrial*; amenazando con transformar por completo nuestra idea de sociedad y de las estructuras que la conforman.

Tal es la importancia de este nuevo entorno que ya estamos viviendo que el Derecho no puede desconocerlo. La tradicional lentitud de las leyes a la hora de regular nuevas figuras y realidades sociales se hace aquí aún más dramática donde el fenómeno crece a ojos vista en cuestión de meses, incluso de días.

La enorme capacidad de tratamiento y transmisión de la información que ofrecen las nuevas tecnologías hacen más acuciante la necesidad de proteger los derechos fundamentales del individuo, en concreto los contemplados en el artículo 18 de nuestra Constitución, el *derecho al honor, a la intimidad personal y familiar y a la propia imagen*.

El apartado 4º de dicho precepto dice: *"La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos"*. Tal era la concienciación del

constituyente del 78 sobre la posible incidencia perjudicial de las nuevas tecnologías sobre estos derechos.

Para cumplir con dicha disposición, se adoptó la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD).
A nivel comunitario, con posterioridad a la promulgación de la LORTAD, se aprobó la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, 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.

Debido a esta Directiva, fue necesario modificar la legislación española mediante la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD). Esta nueva Ley que derogó y sustituyó a la LORTAD, pero no así a sus reglamentos de desarrollo, los cuales siguen vigentes en todo lo que no se opongan a esta nueva regulación.

7.2 DIFERENCIAS ENTRE LA LORTAD Y LA NUEVA LOPD

A pesar de lo que pueda parecer en primera instancia, por el hecho de que sea una nueva ley, la LOPD es muy similar a la LORTAD. Es más, prácticamente el 85% de su redacción y de sus artículos coinciden “punto por punto” con la de su predecesora.

Entonces... ¿Cuáles son sus diferencias?. La primera y más destacada tiene que ver con su nombre: si nos fijamos, la LORTAD se llamaba “Ley Orgánica Reguladora del Tratamiento Automatizado de Datos de carácter personal” mientras que la LOPD se denomina, simplemente, “Ley Orgánica de Protección de Datos de carácter personal”. Por tanto, la diferencia está en el término “automatizado”: así, mientras que la LORTAD se centraba solamente

en las bases de datos informatizadas, la nueva LOPD se extiende también a las bases de datos en otro tipo de soportes: papel, filminas, etc.
Las otras diferencias más significativas, son las siguientes:

- Incorporación de la figura del "Encargado del Tratamiento", diferenciándose del "Responsable del Fichero", que se define como "la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento".
- Cambio del concepto de "cesión de datos" por el de "comunicación de datos" e introducción de un artículo nuevo (art. 12) que regula específicamente el "acceso a los datos por cuenta de terceros".
- Modificación del Tratamiento de los ficheros privados con fines de publicidad y prospección comercial y creación del llamado "Censo Promocional" (artículos 30 y 31 LOPD).
- Ampliación y modificación del régimen aplicable al "Movimiento Internacional de Datos" (artículo 33 y 34 LOPD).
- Autorización de la creación de Órganos correspondientes de la Comunidades Autónomas en materia de Protección de Datos, parcialmente homólogos de la Agencia de Protección de Datos (artículo 41 LOPD).
- Obligación de registrar y adaptar a la LOPD los ficheros de datos personales en soportes no automatizados (papel, filminas, etc.) antes del 24 de octubre del 2007 (Disposición Transitoria Primera LOPD).

Evidentemente, existen muchas otras diferencias, menos relevantes, que obviamos en el presente artículo por su limitada extensión y su carácter divulgativo.

A continuación, nos centraremos en la LOPD y abordaremos los aspectos más importantes de la misma en los siguientes epígrafes.

7.3 OBJETO Y ÁMBITO DE APLICACIÓN DE LA LOPD

El artículo 1 de la LOPD define su objeto, en desarrollo del artículo 18.4 de la Constitución Española, que no es otro que *"limitar el uso de la informática"* y medios análogos con el fin de proteger el *"pleno ejercicio"* del derecho al honor y a la intimidad personal y familiar.

El ámbito de aplicación de la LOPD viene determinado en su artículo 2º. En su párrafo 1º, se establece la regla general para, a continuación, determinar una serie de excepciones en los párrafos siguientes. Este sistema de excepciones va a ser la tónica general de la Ley, contribuyendo al oscurecimiento de su articulado y a la limitación de su alcance.

Regla general:

> "La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.".

Excepciones:

El párrafo 2º del artículo 2 excluye la aplicación de la LOPD para los siguientes ficheros:

- A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.
- A los ficheros sometidos a la normativa sobre protección de materias clasificadas.
- A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante, en estos supuestos el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia de Protección de Datos.

7.4 DEFINICIONES

Siguiendo el modelo de las directivas comunitarias, la LOPD introduce una serie de definiciones *"ope legis"* de los términos fundamentales que maneja, y siempre con efectos únicamente de lo dispuesto en ella.

Se recogen en el artículo 3 de la Ley y destacamos las siguientes:

1- *Datos de carácter personal:*

La Ley define los mismos como *"cualquier información concerniente a personas físicas identificadas o identificables".*

En primer lugar, cabe destacar que sólo se refiere a la "información" y no a la "opinión". Este dato es fundamental ya que la información tiene la obligación de ser veraz y viene protegida por el derecho fundamental a la Libertad de Información (artículo 20.1.d) de la Constitución), mientras que la opinión no se le impone dicha limitación y se protege por un derecho independiente: la Libertad de Expresión (artículo 20.1.a) de la Constitución).

De este modo y *strictu sensu* podemos afirmar que en el concepto de dato de carácter personal no están incluidas las opiniones vertidas por otras personas sobre ellas sino solamente las informaciones que son las que realmente tienen una obligación de veracidad (principio de calidad que veremos posteriormente). Con las dificultades que dicha distinción puede conllevar en la práctica, como en el caso de los "diagnósticos", sean médicos, sociales o psicológicos, que siendo los mismos opiniones profesionales no por ello dejan de tener una cierta obligación de veracidad. Ante la duda, cabe incluir dichos elementos en el concepto de dato personal.

En segundo lugar, cabe destacar de la definición que sólo se refiere a las personas *físicas*, dejando de lado a las *jurídicas* cuyos datos no se ven protegidos por esta Ley. Asimismo dichas personas no necesitan estar

identificadas plenamente, sino que basta con que se pueda deducir su identidad con relativa facilidad.

Ejemplos de estos datos son: nombre, apellidos, dirección, edad, estado civil, profesión, sexo, edad, etc.

2- *Fichero automatizado:*

Para la ley, este fichero es *"todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso"*.

Hemos de recordar aquí que, así como la anterior LORTAD sólo se refería a ficheros informáticos, esta Ley también engloba otro tipo de soportes como el papel. Si bien, la Disposición Adicional Primera de la LOPD prorroga su aplicación a dichos soportes no automatizados hasta el 24 de octubre de 2007 (a excepción del ejercicio de derechos de acceso, rectificación y cancelación por los interesados, que veremos posteriormente).

3- Tratamiento de datos:

Se definen como las "*operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias"*.

Todos estos elementos forman parte del procesamiento y uso de la información, se utilice o no la informática para ello.

4- *Responsable del fichero:*

Para la LOPD, el responsable del fichero es aquella *"persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento"*.

Éste concepto es sumamente importante ya que nos indica el sujeto contra el que hay que dirigirse directamente en caso de violación de los preceptos contenidos en la Ley con relación a los datos bajo su control.

5- *Encargado del tratamiento:*

Para la LOPD, el encargado del tratamiento es aquella *"la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento"*.

Como vimos anteriormente, es una novedad en relación a la LORTAD que no contemplaba esta figura.

6- *Afectado:*

Se define al afectado como aquella *"persona física titular de los datos que sean objeto del tratamiento"*. Ya hemos destacado que las personas jurídicas quedan fuera del ámbito de protección de la Ley.

7- *Procedimiento de disociación:*

Este procedimiento responde a *"todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable"*.

Este sistema asegura el anonimato de los afectados y, por tanto, su derecho al honor y a la intimidad. Un ejemplo paradigmático de este sistema son los datos estadísticos.

7.5 PRINCIPIOS DE LA PROTECCIÓN DE DATOS

El Título II de la LOPD, artículos 4 a 12, se dedican a enumerar los principios informadores fundamentales en la protección de datos de carácter personal. A continuación veremos uno por uno dichos principios:

7.5.1 CALIDAD DE LOS DATOS

El artículo 4 define los siguientes principios vinculados con la necesaria calidad de los datos:

1- Principio de finalidad:

Los datos personales deben ser *"adecuados, pertinentes y no excesivos"* con relación al ámbito y fines para los que fueron recogidos.
Asimismo, dichos datos *"no podrán usarse para finalidades incompatibles"* de las fijadas en el momento de su recogida. Y, consecuentemente, deberán ser *"cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados y registrados"*[2]. Este ultimo punto lo denomino coloquialmente como el "Principio del derecho al olvido" que todo interesado tiene en relación a sus datos.

2- Principio de calidad de los datos "strictu sensu":

Los datos personales deben ser *"exactos y puestos al día".* En caso contrario, la LOPD impone la obligación de que los datos erróneos sean cancelados y sustituidos por los correctos de oficio, sin perjuicio de los derechos de rectificación y cancelación por parte del afectado. (artículo 16)

[2] El artículo 4 determina una excepción a dicha cancelación: su posible *valor histórico*, que deberá responder siempre a su legislación específica y aun procedimiento que reglamentariamente debe determinarse a tal fin (artículo 4.5, párrafo tercero).

3- Principio de almacenamiento de los datos:

La Ley no impone ningún sistema determinado de almacenamiento, pudiendo éste ser automatizado o no. El único requisito que exige, en el párrafo sexto de su artículo 4, es que dicho sistema permita *"el ejercicio del derecho de acceso por parte del afectado"*.

4- Principio de licitud:

En la recogida de datos:

Artículo 4.7; *"Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos"*.

En la clasificación de los datos:

Artículo 4.1, párrafo 2º; *"En su clasificación sólo podrán utilizarse criterios que no se presten a prácticas ilícitas"*.

En la finalidad de su utilización:

Artículo 4.1, párrafo 1º; *"...y las finalidades legítimas para las que se hayan obtenido".*

7.5.2 DERECHO DE INFORMACIÓN EN LA RECOGIDA DE DATOS

En el momento de la recogida de datos personales, el artículo 5 de la Ley impone la obligación de informar a los afectados sobre determinados extremos.

La información facilitada debe cumplir los siguientes requisitos:

1- Se ha de realizar con carácter previo a la solicitud de los datos.

2- Debe ser *expresa, precisa e inequívoca*.

El contenido obligatorio de dicha información es el siguiente:

a- Existencia de un fichero automatizado de datos de carácter personal, finalidad de la recogida de éstos y destinatarios de la información.

b- Carácter obligatorio o facultativo de la respuesta del afectado a las preguntas que le sean planteadas.

c- Consecuencias de la obtención de los datos o de la negativa a suministrarlos.

d- Posibilidad de ejercitar los derechos de acceso, rectificación y cancelación.

e- Identidad y dirección del responsable del fichero.

Éste requisito de información no será exigible, reza el apartado 3 del artículo 5, si *"el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban"*. Sin duda, el problema está en determinar, en la práctica, cuándo se puede deducir o no dicha información.

7.5.3 CONSENTIMIENTO DEL AFECTADO

El artículo 6 de la LOPD determina la necesidad del consentimiento del afectado para el tratamiento automatizado de sus datos personales.
Éste consentimiento incluso podrá ser *revocado*, según el apartado 3 del mismo artículo, *"cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos"*.

Como no podía ser de otro modo, existen una serie de excepciones en las que no se exige el consentimiento del afectado. Son las siguientes:

1- Cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias;

2- Cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento;

3- Cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de LOPD, o

4- Cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

7.5.4 DATOS ESPECIALMENTE PROTEGIDOS

El artículo 7 de la Ley regula la esfera de datos especialmente sensibles, que afectan de una manera muy directa al derecho al honor y a la intimidad.

Por tanto, estos datos requieren de un régimen jurídico más estricto que el resto para garantizar convenientemente su protección.

Estos datos personales se concretan en dos grupos fundamentales:

1- Ideología, afiliación sindical, religión o creencias.

2- Origen racial, salud o vida sexual.

3- Relativos a la comisión de infracciones penales o administrativas.

7.5.4.1 IDEOLOGÍA, RELIGIÓN O CREENCIAS

El artículo 16 de la Constitución, garantizador de la libertad ideológica, religiosa y de culto, recoge en su párrafo 2º que *"nadie podrá ser obligado a declarar sobre su ideología religión o creencias"*.

Atendiendo a este precepto, el artículo 7 de la LOPD, en sus apartados 1º y 2º, recoge una especial protección para los datos relativos a estas materias, en los siguientes extremos:

- Con relación al derecho a la información en la recogida de estos datos: se advertirá al interesado de su derecho a no declarar sobre los mismos.
- Con relación al consentimiento: debe ser "expreso y por escrito" del afectado para el tratamiento automatizado de dichos datos. De otro modo, no se podrán utilizar en dicho proceso.

7.5.4.2 ORIGEN RACIAL, SALUD O VIDA SEXUAL

El apartado 3º del artículo 7 de la LOPD se encarga de su regulación especial, indicando que éstos datos sólo podrán ser recabados, tratados automatizadamente y cedidos mediando dos requisitos:

1º) Con una finalidad de *"interés general"*.
2º) Mediante autorización:
   - Concedida por una Ley,
   - o mediante consentimiento expreso del afectado.

Con relación a los datos relativos a la salud, el artículo 8 permite su tratamiento automatizado por las instituciones y centros sanitarios, tanto públicos como privados, así como los profesionales, de los que el afectado sea paciente o en que haya de ser tratado[3]. Todo ello con las limitaciones que impone el artículo 11 de la LOPD en cuanto a la cesión de dichos datos y el artículo 10 en cuanto al deber de secreto sobre los mismos.

Interesa además destacar, atendiendo a los dos grupos de datos vistos, que la LOPD prohíbe expresamente todos *"los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, religión, creencias, origen racial o étnico, o vida sexual"*. (artículo 7.4)

[3] De acuerdo con lo dispuesto en los artículos 8, 10, 23 y 61 de la Ley 14/1986, de 25 de abril, General de Sanidad; 85.5, 96 y 98 de la Ley 25/1990, de 20 de diciembre, del Medicamento; 2, 3 y 4 de la Ley Orgánica 3/1986, de 14 de abril, de medidas especiales en materia de Salud Pública, y demás Leyes sanitarias.

7.5.4.3 ELATIVOS A LA COMISIÓN DE INFRACCIONES PENALES O ADMINISTRATIVAS

El apartado 5º del artículo 7 de la LOPD limita la inclusión de estos datos únicamente al ámbito de los ficheros automatizados de las Administraciones Públicas competentes en función de sus normas reguladoras respectivas.

Por tanto, cualquier inserción de dichos datos en el ámbito privado es ilegal y, por tanto, sancionable por la LOPD, en su Título VII.

7.5.5 DEBER DE SECRETO

En cuánto al *deber de secreto*, el artículo 10 de la Ley lo extiende, no solamente al responsable del fichero, sino también a todos *"quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal"*.

Dicho deber de secreto sobre los datos personales que se manejen, adquiere la misma entidad *"ope legis"* que el secreto profesional, subsistiendo sus efectos con posterioridad a la finalización de sus relaciones con el titular o con el responsable del fichero, según el caso.

7.5.6 SEGURIDAD DE LOS DATOS Y DEBER DE SECRETO

El artículo 9 de la Ley determina la obligación del responsable del fichero de *"adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado"*.

Dichas medidas deberán adoptarse con relación:

- al estado de la tecnología,
- a la naturaleza de los datos almacenados y
- a los riesgos a los que están expuestos (tanto humanos como naturales).

Sin embargo, la LOPD no define cuáles deben ser, en concreto, dichas medidas, sino que remite su determinación a la vía reglamentaria (apartados 2º y 3º del artículo 9). Dicha regulación se contiene en el *Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de las Medidas de Seguridad que deben cumplir los ficheros con datos de carácter personal*. Al final del presente artículo, realizaremos una breve exposición del contenido fundamental de este Reglamento.

7.6 LOS DERECHOS DE LAS PERSONAS

El Título III de la LOPD se dedica a definir los derechos del afectado con relación a sus datos tratados automatizadamente. Éstos derechos, por regla general, pueden ser ejercidos en cualquier momento, mientras sus datos sean utilizados. No poseen una prescripción ni una caducidad, salvo cuando se trate de impugnación de un acto ilegal o de la reclamación de una indemnización por el mismo.

Los derechos reconocidos en la LOPD son los siguientes:

1- Derecho de información.

2- Derecho de acceso.

3- Derechos de rectificación y cancelación.

4- Derecho de tutela de la administración.

5- Derecho de indemnización.

A continuación los veremos uno por uno en la redacción de la Ley.

7.6.1 DERECHO DE INFORMACIÓN

Éste derecho de información del afectado está contemplado en la LOPD en dos vertientes:

La primera, que podemos llamar *especial*, se contempla en el artículo 5 con relación al *derecho a la información en la recogida de datos*. Nos remitimos al apartado B del epígrafe anterior donde analizábamos su contenido.

La segunda, que podemos llamar *general*, se recoge en el artículo 14 de la Ley y garantiza que "*Cualquier persona podrá conocer, recabando a tal fin la información oportuna del Registro General de Protección de Datos, la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento"*. Dicho Registro General será de consulta pública y gratuita y está integrado en la Agencia de Protección de Datos[4], ente público designado por la LOPD para el cumplimiento de su normativa.

Por tanto, mediante el ejercicio de este derecho, en cualquiera de sus vertientes, el afectado podrá averiguar:

1- La existencia de un fichero de tratamiento automatizado de datos de carácter personal.
2- La finalidad concreta que cumple ese fichero.
3- La identidad del responsable de dicho fichero.

Estos datos pueden ser muy útiles de cara a identificar el fichero y su vinculación general, pero es necesario también poder acceder en concreto a los datos personales del afectado almacenados en dicho fichero. Esto último lo garantiza el siguiente derecho.

[4] Regulada en el Título VI de la LOPD, artículos 35 a 42. El Registro General de Protección de Datos se contempla en el artículo 39, determinando la inscripción en el mismo de:
a) Los ficheros automatizados de que sean titulares las Administraciones Públicas.
b) Los ficheros automatizados de titularidad privada.
c) Las autorizaciones a que se refiere la presente Ley.
d) Los códigos tipo a que se refiere el artículo 32 de la presente Ley.
e) Los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición.

7.6.2 DERECHO DE ACCESO

Se puede considerar integrado en el *derecho de información* pero, por su importancia, la LOPD le atribuye entidad propia en el artículo 15. Consiste en la capacidad del afectado para dirigirse al responsable del fichero y *"solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos"*.

Este derecho tiene un carácter personalísimo, debiendo ejercitarlo siempre el afectado directamente, salvo incapacidad o minoría de edad en la que debe acudir su representante legal.

La información se podrá obtener mediante mera visualización de los datos o a través de una comunicación por escrito, copia, telecopia o fotocopia *"en forma legible e inteligible"*, dice la Ley.

Para este derecho, la LOPD impone una limitación temporal a su ejercicio: sólo podrá ser ejercitado por el afectado *"a intervalos no inferiores a doce meses"*, salvo que se acredite un interés legítimo para ejercitarlo antes.

El artículo 17 de la LOPD remite a la vía reglamentaria para la regulación del procedimiento para ejercer el derecho de acceso. En la actualidad, el Real Decreto 1332/1994[5], de 20 de junio, se encarga de dicha regulación, entre otras cuestiones.

7.6.3 DERECHOS DE RECTIFICACIÓN Y CANCELACIÓN

Están recogidos conjuntamente en el artículo 16 de la LOPD. Éstos determinan que el afectado, si observa que sus datos recogidos en el fichero son inexactos o incompletos, tendrá derecho a rectificarlos o a cancelarlos, en su caso.

[5] 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 Datos de carácter Personal (B.O.E. núm. 147, de 21 de junio de 1994).

En este caso, si el responsable del fichero hubiese cedido dichos datos, deberá comunicar al cesionario dicha modificación o cancelación de los mismos, con el fin de que proceda del mismo modo.

> La cancelación no supondrá el borrado de los datos sino solamente su bloqueo de cara a ser reclamados por Administraciones Públicas, Jueces o Tribunales dada la obligación de conservar los datos durante los plazos previstos[6].

El Real Decreto 1332/94 se encarga de regular el procedimiento del ejercicio de estos derechos determinando el plazo de cinco días para hacerlos efectivos, a partir de la recepción de la solicitud del derecho de acceso.

7.6.4 DERECHO DE TUTELA DE LA ADMINISTRACIÓN

El artículo 18.1 de la LOPD confiere al afectado el derecho a impugnar todas las actuaciones contrarias a su normativa, ante la Agencia de Protección de Datos. El procedimiento a seguir en dicha reclamación se recoge en el Real decreto 1332/94, de 20 de junio.

Contra las resoluciones de la Agencia cabrá recurso contencioso-administrativo, tal y como determina el párrafo 2º del mismo artículo.

7.6.5 DERECHO DE INDEMNIZACIÓN

Dice el párrafo 3º del artículo 17 que *"los afectados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el responsable del fichero, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados"*.

El procedimiento para exigir la indemnización varía según la titularidad de los ficheros:

---

[6] A estos efectos, el apartado 5 del artículo 16 de la LOPD dice: *"Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado"*.

7.6.5.1 FICHEROS DE TITULARIDAD PÚBLICA

En este caso, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones Públicas. (artículo 19.2 de la LOPD)

Esta regulación se recoge en los artículos 139 a 144 de la Ley 30/1992, de 26 de noviembre, reguladora del Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Como consecuencia de la misma, todo particular que sufra una lesión en cualquiera de sus bienes o derechos como consecuencia del funcionamiento *normal o anormal* de los servicios públicos de una Administración Pública, tiene derecho a ser indemnizado por dicha Administración.

7.6.5.2 FICHEROS DE TITULARIDAD PRIVADA:

En el supuesto de que la lesión se produzca como consecuencia de datos recogidos en ficheros de titularidad privada, la acción de indemnización se ejercitará ante los órganos de la jurisdicción ordinaria, de acuerdo con lo dispuesto en el artículo 19.3 de la LOPD.

En este sentido, lo dispuesto por el artículo 1902 del Código Civil: *"El que por acción u omisión causa daño a otro, interviniendo culpa o negligencia, está obligado a reparar el daño causado"*.

En este caso, por tanto, no se trataría de una responsabilidad objetiva, a mi entender, sino de una responsabilidad subjetiva, solo exigible interviniendo culpa o negligencia en el tratamiento de los datos personales por parte del responsable del fichero o de un delegado del mismo.

7.7 REGLAMENTO DE MEDIDAS DE SEGURIDAD

Tal y como adelantamos en el presente artículo, entre las normas reglamentarias que se aprobaron en desarrollo de la antigua LORTAD, destaca especialmente el Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de las Medidas de Seguridad que deben cumplir los ficheros con datos de carácter personal.

Como vimos también anteriormente, la aprobación de la nueva LOPD no derogó dicho reglamento, a pesar de referirse a la antigua LORTAD, sino que lo mantuvo en vigor en todo lo que no se oponga a la nueva Ley.

El objeto de este reglamento es desarrollar el (antiguo y nuevo) artículo 9 de la LORTAD/LOPD. El párrafo primero del mismo dice lo siguiente:

> *"El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural."*

El incumplimiento de esta obligación, es decir "Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad", supone una falta grave sancionable con una multa de entre 10 y 50 millones de pesetas, o 60.000 a 300. euros aproximadamente, en base a los artículos 44.3 y 45.2 de la LOPD.

7.7.1 NIVELES DE PROTECCIÓN

Dentro del Reglamento de Medidas de Seguridad, existen tres niveles de seguridad distintos: el básico, el medio y el alto. Para saber qué nivel debemos de aplicar, debemos de referirnos al tipo de datos personales almacenados en

el fichero. Para ello, estaremos a lo dispuesto en el artículo 4 del Reglamento, de él se deduce lo siguiente:

1- Nivel básico:

- Aplicable a todos los sistemas con datos personales en general.

2- Nivel Medio:

- Datos de comisión de infracciones administrativas o penales,
- Datos de Hacienda Pública,
- Datos de servicios financieros,
- Datos sobre solvencia patrimonial y crédito y
- Conjunto de datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo.

3- Nivel Alto: para datos referidos a la

- Ideología,
- Religión,
- Creencias,
- Origen racial,
- Salud o vida sexual y
- Datos recabados para fines policiales.

Estas medidas de seguridad se aplican de forma cumulativa, así el nivel alto deberá cumplir también las reguladas para el nivel medio y el nivel bajo de seguridad.

7.7.2 DOCUMENTO DE SEGURIDAD

Sin animo de entrar pormenorizadamente en las medidas de seguridad concretas a aplicar, lo cual nos supondría otro artículo de similar extensión para abordarlas, solamente cabe destacar que todas las mencionadas medidas y

procedimientos de seguridad adoptados sobre el Sistema deberán estar recogidos en un único Documento de Seguridad que los detalle específicamente, según se recoge en el artículo 8 del Reglamento y sus concordantes. En concreto, dicho documento deberá contener, como mínimo, lo siguiente:

- Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.
- Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este Reglamento.
- Funciones y obligaciones del personal.
- Estructura de los ficheros con datos de carácter personal y información que los tratan.
- Procedimiento de notificación, gestión y respuesta ante las incidencias.
- Los procedimientos de realización de copias de respaldo y de recuperación de los datos.

Por ultimo, dicho Documento deberá mantenerse permanentemente actualizado y adaptado a la legislación vigente en cada momento. Deberá ser conocido y aplicado por todo el personal con acceso al Sistema, en base al artículo 9.2 del Reglamento.

CAPITULO 8

ADAPTACIÓN A LA LOPD

José Luis Rivas López

8.1 INTRODUCCIÓN

En este capitulo se explican las diferentes fases para poder adaptar los sistemas existentes al Reglamento según el nivel del fichero. Recuerde que existen tres niveles:

- **Nivel Básico**: Aquellos ficheros con datos de carácter personal.

- **Nivel Medio**: Aquellos con datos relativos a Hacienda Publica, Servicios Financieros, Servicios de Información sobre la solvencia patrimonial y crédito o comisión de infracciones administrativas o penales, o ficheros cuyo conjunto de datos puedan ofrecer un perfil psicológico de la persona (por ejemplo, el currículum vitae).

- **Nivel Alto**: Aquellos ficheros con datos de ideología, religión, creencias, origen racial, salud o vida sexual, así como los que contengan datos recabados para fines policiales sin consentimiento de las personas afectadas.

8.2 ANÁLISIS DE LA SEGURIDAD

En esta fase se procederá a analizar los ficheros que contengan datos de carácter personal y se establecerá el nivel que ocuparán según el Reglamento. También habrá que comprobar si alguno se encuentra registrado en la Agencia de Protección de Datos. Al finalizar el análisis se deberá realizar

un informe detallado de todos lo puntos que hayan sido analizados con sus conclusiones.

8.2.1 NIVEL BAJO

En el nivel bajo habrá que comprobar los siguientes puntos en cada fichero:

- La seguridad en los accesos a través de las redes de comunicación.
- La seguridad de los ficheros en el lugar de la ubicación física.
- La seguridad de los datos fuera del lugar de ubicación física del fichero.
- La existencia de un Responsable de los ficheros automatizados con datos de carácter personal.
- La existencia de un registro de incidencias.
- La existencia de mecanismos de identificación y autenticación.
- La existencia de listados de usuarios, claves y renovación.
- La existencia de un listado actualizado de usuarios con acceso.
- La existencia de métodos de inventariado y clasificación de los soportes informáticos, en dónde se almacenan los datos con acceso restringido.
- La existencia de métodos de realización de copias de seguridad que garanticen la reconstrucción de los datos en el

momento en que se produzca la pérdida o destrucción de los mismos, así como un calendario de realización de copias de seguridad. Las copias de seguridad deberán estar documentadas en todo momento.

- La existencia de un calendario de controles periódicos para comprobar el cumplimiento de la propia normativa y medidas a adoptar en caso de desechar o reutilizar un soporte.

8.2.2 NIVEL MEDIO

Referente al nivel medio, además de comprobar los puntos referentes al nivel bajo, tendrá que comprobar los siguientes puntos en cada uno de los ficheros:

- La existencia de un control de acceso físico a los locales donde se encuentren los ficheros.

- La existencia de mecanismos que identifiquen a cualquier usuario que acceda y que comprueben su autorización para ello.

- La existencia de mecanismos que limiten los accesos reiterados y no autorizados.

- Que los mecanismos de gestión de entrada y salida de soportes informáticos cumplen los requisitos del presente Reglamento.

- Los procedimientos de recuperación de datos son autorizados por la persona responsable del fichero.

- La existencia de auditorias de seguridad cada dos años, como mínimo.

8.2.3 NIVEL ALTO

Se tendrá que comprobar todo los puntos anteriores, además de:

- Los datos están cifrados antes de la distribución y transporte de los soportes que los contengan.

- La existencia de un registro de accesos a la información, dónde conste al menos la identificación del usuario, hora y fecha, fichero accedido y si ha sido denegado o aceptado, con un “logging“ de al menos 2 años. Se deberá realizar un informe de este registro al menos una vez al mes.

- La ubicación de las copias de seguridad se realiza en lugares diferentes al de los equipos informáticos.

- La transmisión de datos se realiza mediante cifrado de dichos datos o por cualquier otro mecanismo que garantice la integridad de los mismos.

8.3 ELABORACIÓN DEL DOCUMENTO DE SEGURIDAD

En esta fase se tendrá que elaborar un documento por cada fichero como los de los capítulos 7, 10 ó 13, dependiendo del nivel que le corresponda al fichero.

8.4 IMPLEMENTACIÓN DEL DOCUMENTO DE SEGURIDAD

En esta fase se procederá a implementar lo que marquen los diferentes documentos de seguridad, que no es más que un reflejo de lo que la ley nos rige.

8.5 FORMACIÓN DE LOS RESPONSABLES

La formación es un punto que a lo largo de cualquier plan de seguridad es importante a tener en cuenta. Una buena formación sobre todo a los

responsables de seguridad y de los ficheros, que no tienen porque coincidir, es algo indispensable para obtener un buen grado de seguridad.

Dicha formación deberá hacer hincapié en:

- Control de acceso.
- Identificación y autenticación.
- Gestión de soportes.
- Registro de incidencias.
- Copias de respaldo y recuperación.

8.6 AUDITAR

Aunque sólo es obligado en el nivel medio, es recomendable hacerlo en todos ellos una vez finalizado el plan de adaptación, así como regularmente al menos cada dos años (art 17.1 del Reglamento de Medidas de Seguridad). Se deberá hacer hincapié en:

- Identificación de puntos débiles.
- Recomendaciones para el cierre de las brechas de seguridad.
- Análisis de los sistemas operativos.
- Creación de un manual de operaciones de seguridad.
- Análisis de los ficheros automatizados.
- Análisis de la red de comunicaciones.

- Análisis de los mecanismos de acceso remoto.

8.7 ALTA DE FICHEROS

Paralelamente, se deberá realizar el alta en el Registro General de la Agencia de Protección de Datos. Para ello, la declaración se puede realizar a través de Internet o mediante soporte magnético, para lo cual deberá proceder a descargar e instalarse el programa de ayuda para la generación de notificaciones a través de Internet o en soporte magnético, que se encuentra disponible en el apartado Registro General de Protección de Datos de la página Web de la Agencia y seguir las instrucciones que dicho programa le irá facilitando.

Asimismo, y si no quiere o no puede utilizar ninguna de las dos formas anteriores, se informa que el formulario en papel lo puede obtener de la página Web de la Agencia en Internet, accediendo al apartado Registro General de Protección de Datos o fotocopiándolo directamente del Boletín Oficial del Estado.

Hay que señalar que tanto el formulario como la inscripción es gratuita, y en cuanto a la remisión, esta ha de realizarse por correo o entregándola en mano en el Registro de la Agencia de Protección de Datos, salvo que se realice a través de Internet.

En el supuesto de haber optado por la declaración a través de internet, se le indica que la hoja de solicitud generada por el programa se deberá enviar al número de fax 914483680, o bien a través de correo ordinario.

Cada notificación de fichero podrá englobar varias operaciones y procedimientos técnicos que permitan la recogida, grabación, conservación, elaboración, etc., de datos personales.

CAPITULO 9

APLICACIÓN PRÁCTICA DE LA L.O.P.D.

José Luis Rivas López

9.1 INTRODUCCIÓN

Se describirá cómo aplicar la legislación vigente sobre protección de datos de carácter personal en centros públicos que imparten cursos propios como por ejemplo: Masters, de postgrado, de extensión universitaria, etc. Para ello utilizaremos la impartición de un curso de auditorias como ejemplo, viendo el sistema informático empleado para su gestión.

9.2 DESCRIPCIÓN DEL CASO

Un departamento de una universidad imparte un curso de auditorias. El curso está dirigido por un profesor titular, así como la subdirectora que es profesora asociada perteneciendo a otro departamento. Además dicho curso tiene contratado los servicios de una secretaría. Para la gestión del curso se ha elaborado: una base de datos para la gestión tanto de los alumnos como de los profesores, ficheros de contabilidad, así como documentos de Word (cartas para los alumnos, memorias, etc.). Todo el sistema informático usado trabaja en un entorno Windows XP Professional y será utilizado por las tres personas antes mencionadas. Tendremos una base de datos para profesores y alumnos en la que guardaremos los siguientes datos: NIF, nombre completo, domicilio del trabajo y particular, teléfono y correo-e. Además a los profesores también se guardará el tiempo de docencia, así como el tema que impartieron. En los ficheros de contabilidad se guardarán los nombres de los docentes con las cantidades que se les abonara además de los diferentes gastos en fungible (bolígrafos, fotocopias, tóneres, etc.), ordenadores con la correspondiente empresa proveedora.

9.3 FICHEROS

Según lo descrito anteriormente debemos inscribir tres ficheros de nivel básico en la Agencia de Protección de Datos (APD): el fichero de contabilidad, el fichero con datos alumnos/profesores y el fichero de acceso al sistema. En los tres el responsable del fichero es la propia universidad como persona jurídica que decide sobre la finalidad, contenido y uso de los ficheros y como responsable de seguridad el administrador del sistema que en este caso es el subdirector por sus conocimientos técnicos.

Además de inscribirlos en la APD habrá que hacerlo por medio de disposición general publicada en el Boletín Oficial del Estado ó Diario Oficial correspondiente indicando:

- La finalidad del fichero y los usos previstos para el mismo.
- Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.
- El procedimiento de recogida de los datos de carácter personal.
- La estructura básica del fichero y la descripción de los tipos de datos de carácter personal incluidos en el mismo.
- Las cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a países terceros.
- Los órganos de las Administraciones responsables del fichero.
- Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.

- Las medidas de seguridad con indicación del nivel básico, medio o alto exigible.

9.4 MEDIDAS A IMPLEMENTAR

Dado el nivel básico de los ficheros, en función del tipo de datos almacenados en los mismos, se deben implementar las siguientes medidas:

- Deberá redactarse un documento de seguridad, que estará permanentemente actualizado, en el que se indique el ámbito de aplicación del documento y recursos protegidos, en el que constará:
    - las funciones y obligaciones del personal
    - estructura de los ficheros con datos de carácter personal
    - normas y procedimientos de seguridad (sistema informático, sistema operativo, aplicaciones acceso a los ficheros, salvaguarda del sistema y protección de las contraseñas personales).
    - Un registro de incidencias y delimitado el procedimiento de respuesta ante las mismas (tipo de incidencia, fecha hora, personas que la detectan, medidas tomadas...)
    - Relación actualizada de usuarios
    - El nombramiento de un responsable de seguridad que verificará el cumplimiento de lo acordado en el documento con una periodicidad
    - Los procedimientos de realización de copias de respaldos y de recuperación de los datos

- El establecimiento de una correcta política de seguridad en la que se realizarán copias de respaldo y recuperación de datos

de manera que permita la reconstrucción en el mismo estado en que se encontraban al momento de producirse la pérdida;

- Se debe habilitar un sistema de login y un password individual y distinto para cada usuario, el cual limite el acceso a la información sólo a las partes de la aplicación que sea necesaria para el desarrollo de sus funciones. Se recomienda que este control de acceso debe estar estructurado en grupos, en base a unas políticas basadas en los perfiles de la actividad de los usuarios, de forma que cada usuario estará asignado al grupo que corresponde a su actividad y sólo tendrá acceso a los datos que necesite para la misma.

- Habilitar soportes externos de respaldo y recuperación "backup" (u otro sistema) de los ficheros; dichos soportes deberán estar debidamente etiquetados e identificados con fecha y nombre del sistema si se tuviese varios sistemas. Estos soportes se podrán almacenar en la ubicación de la información original. La periodicidad de la copia de seguridad debe ser tal que permita la recuperación total de la información en caso de pérdida de los datos originales, pero dependerá de la cantidad de información, su variabilidad y del método y los sistemas que se están utilizando. Es obligatorio realizar al menos una copia semanal, salvo que en dicho período no haya habido alteración de los datos almacenados, pero se recomienda como mínimo una diaria, bien completa o incremental, y al menos una copia completa semanal.

- Considerando que el ordenador del Master dispone de impresora para emitir los correspondientes informes y que éstos pueden contener datos personales de los alumnos y/o profesores, tales informes en soporte papel, que son archivados en carpetas, aunque en sentido estricto les resultará aplicable la LOPD 15/99 hasta octubre del año 2007,

por ser un soporte distinto del electrónico, en cuanto al Reglamento de Medidas de Seguridad, pueden resultar incluidos en el concepto general de “soporte informático” a que se refiere el artículo 13, puesto que se tratan de impresiones de ficheros informatizados, por lo que debemos aplicarles preventivamente las medidas de seguridad previstas para el nivel correspondiente a los datos personales que contienen, que como se ha dicho antes será de nivel básico.

BIBLIOGRAFÍA

- **INFORMACIÓN SOBRE SEGURIDAD DEL MINISTERIO DE CIENCIA Y TECNOLOGÍA**
  http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S

- **LISTA DE LAS 20 VULNERABILIDADES MÁS CONOCIDAS**
  http://www.sans.org/top20/spanish_v2.php

- **PROYECTO OPEN WEB APPLICATION SECURITY**
  http://www.owasp.org

- **PORTAL DEDICADO A LA SEGURIDAD EN CASTELLANO**
  http://www.hispasec.com

- **PORTAL DE REFERENCIA A NIVEL MUNDIAL**
  http://www.securityfocus.com

- **METODOLOGÍAS DE SEGURIDAD**
  http://www.isecom.org/

- **ZONA DE DEDICADA A LA SEGURIDAD EN MICROSOFT**
  http://www.microsoft.com/technet/treeview/?url=/technet/security/current.asp?frame=true

- **ZONA DE DEDICADA A LA SEGURIDAD EN SUN**
  http://sunsolve.sun.com/pub-cgi/show.pl?target=patchpage

- **SEGURIDAD EN EL MUNDO LINUX**
  http://www.linuxsecurity.com/

- **INFORMACIÓN SOBRE VIRUS DEL MINISTERIO DE CIENCIA Y TECNOLOGÍA**
  http://www.alerta-antivirus.es/virus/ver_pag.html?tema=V

- **INFORMACIÓN DE VIRUS DE MCAFEE**
  http://vil.nai.com/vil/content/alert.htm

- **INFORMACIÓN DE VIRUS DE PANDA SOFTWARE**
  http://www.pandasoftware.es/virus_info/enciclopedia/

- **LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL**
  Ruiz Carrillo, Antonio.
  Editorial BOSCH Barcelona 2001

- **NUEVA GUÍA PRÁCTICA DE PROTECCIÓN DE DATOS**
  Davara Rodríguez, Miguel Ángel;
  Universidad Pontificia de Comillas Madrid 2001

- **DELITOS INFORMÁTICOS Y DELITOS COMUNES COMETIDOS A TRAVÉS DE LA INFORMÁTICA**
  Berenguer, Enrique y Roig Torres, Margarita;
  Editorial TIRANT LO BLANCH; 2001

- **LA PROTECCIÓN DE DATOS EN LAS TELECOMUNICACIONES**
  Davara Rodríguez, Miguel Ángel
  UNIVERSIDAD DE COMILLAS 2000

- **MEMORIAS de la AGENCIA PROTECCIÓN DE DATOS OCTUBRE 1998 - 1999- 2000 -2001**

- **MANUAL DE DERECHO INFORMÁTICO**
  Davara Rodríguez, Miguel Ángel
  Editorial Aranzadi 2001

- **LEGISLACIÓN SOBRE DATOS DE CARÁCTER PERSONAL**
  Editorial TECNOS 2002

- **LA DIRECTIVA COMUNITARIA DE PROTECCIÓN DE LOS DATOS DE CARÁCTER PERSONAL**
  Heredero Higueras, Manuel.
  Editorial Aranzadi Madrid 1997

- http://geneura.ugr.es/~maribel/wap/introduccion/index.shtml

- **PARTNERSHIP PROJECT AND FORUMS**

  Mobile Partnership Projects

  3GPP : http://www.3gpp.org

  3GPP2 : http://www.3gpp2.org

  Mobile Technical Forums

  3G All IP Forum: http://www.3gip.org

  IPv6 Forum: http://www.ipv6forum.com

- **MOBILE MARKETING FORUMS**

  Mobile Wireless Internet Forum:http://www.mwif.org

  UMTS Forum : http://www.umts-forum.org

  GSM Forum : http://www.gsmworld.org

  Universal Wireless Communication: http://www.uwcc.org

  Global Mobile Supplier: http://www.gsacom.com

- **LINUX SEGURIDAD TÉCNICA Y LEGAL**
  Rivas López, José Luis ; Ares Gómez, José Enrique, Salgado Seguín, Victor A.
  Editorial: Virtualibro S.C.

- **IMPLANTACIÓN DE LA LOPD EN LOS SISTEMAS**
  Rivas López, José Luis ; Ares Gómez, José Enrique, Salgado Seguín, Victor A.

- **LEY DE SERVICIOS DE LA SOCIEDAD DE LA INFORMACION**: *LEY 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. ("B.O.E." núm. 166, de 12 de julio de 2002)*

- **LEY ORGANICA DE PROTECCION DE DATOS**: *LEY ORGÁNICA 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal. ("B.O.E." núm. 298, de 14 de diciembre de 1999)*

- **REGLAMENTO DE MEDIDAS DE SEGURIDAD**: *REAL DECRETO 994/1999, de 11 de junio. Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de caractes personal. ("B.O.E." núm. 151, de 25 de junio de 1999)*

- **RESOLUCION de 22 de junio de 2001**: *Acuerdo por el que se concreta el plazo para la implantación de medidas de seguridad de nivel alto en determinados sistemas de información. ("B.O.E." núm. 151, de 25 de junio de 2001)*

- **RECOMENDACIONES A USUARIOS DE INTERNET**: *el objetivo de este documento, es concienciar al usuario de Internet, de que sus datos*

personales pueden ser utilizados de forma irregular... ("Agencia de Protección de Datos")

- **REGLAMENTO (CE)N 45/2001 DEL PARLAMENTO EUROPEO Y DEL CONSEJO**: *relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos ("Diario Oficial de las Comunidades Europeas")*

- **RECOMENDACIÓN WP 43**: *sobre determinados requisitos mínimos para la recogida en línea de datos personales en la Unión Europea. (Aprobada el 17 de mayo de 2001)*

- **LA APLICACIÓN DE LA LOPD EN EL ÁMBITO SANITARIO**: *La aplicación de la LOPD en el ámbito sanitario, pone de manifiesto la necesidad de una especial protección de los datos personales relativos a la salud.*