Implantacion de la LOPD en los sistemas

Jose L. Rivas López·J. Enrique Ares Gómez·Victor A. Salgado Seguín

AUTORES : *José Luis Rivas López*
José Enrique Ares Gómez
Víctor A. Salgado Seguín

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

DISEÑO: Santiago Rivas López

REVISIÓN: *Raquel Cores Cobas*
Sergio Pazos Gonzalez
Antonio Gómez Lorente

PRIMERA EDICIÓN

A Inma Valeije

A mi familia y amigos por tenerlos ahí siempre que se les necesita. Especialmente a mis padres, hermano, mis primas Ana y Luanda, mi prima María y su marido Javier..

Me gustaría destacar entre mis amigos a: Heman y Sonia por se como son, por su valentía a la hora de enfrentarse a la vida y sobre todo por permitirme ser su amigo. Chicos sabéis que aunque muchas veces no dé señales de vida os tengo en mi corazón.

José Luis Rivas López

A mí hija Elena.

Victor Alberto Salgado Seguín

En primer lugar a Ana, Iria, Noa e Iago va por vosotros y por todos aquellos familiares, amigos y compañeros contribuyen a que el día a día sea más fácil por ello se siembra futuro

José Enrique Ares Gómez

AGRADECIMIENTOS

Gracias a: ***Antonio Gómez Lorente, Raquel Cores Cobas*** *y* ***Sergio Pazos Gonzales****, quiénes revisaron este trabajo. También nos gustaría dar las gracias a* ***Santiago Rivas López*** *quién diseño la portada y los separadores.*

AUTORES

José Luis Rivas López
José Enrique Ares Gómez
Víctor A. Salgado Seguín

DIRECCIÓN Y COORDINACIÓN

José Luis Rivas López

Índice

PARTE III. NIVEL MEDIO

PARTE IV. NIVEL ALTO

PARTE V. APÉNDICES

Prólogo

0

El libro de José Luis Rivas, José Enrique Ares y Víctor Salgado, que tengo la satisfacción de prologar, trata de analizar la implantación de la Ley Orgánica de Protección de Datos Personales en los sistemas. La sociedad de la información o del conocimiento, apoyada sobre el desarrollo de las tecnologías de la información no es el resultado de una decisión política, sino que es un hecho, un hecho propio de finales del siglo XX que tiene, a la vez, aspectos positivos y negativos. Corresponde a los poderes públicos facilitar y favorecer los aspectos positivos y tratar de paliar en la medida de lo posible los negativos.

En el ámbito de la Administración pública, las nuevas tecnologías, especialmente internet, contribuyen a mejorar la actividad administrativa en beneficio del interés general[1]. La Constitución establece que la Administración Pública debe servir con objetividad los intereses generales y actuar de conformidad con el principio de eficacia –art. 103.1 CE-[2]. La utilización de las tecnologías de la información por los poderes públicos materializan este objetivo de eficacia, al facilitar un nuevo cauce de relación entre la Administración y los ciudadanos, de manera que ésta no sea sólo presencial, sino también telefónica o a través de internet. De esta forma, la relación ciudadano-administración se vuelve, por

[1] AA.VV, *Las Tecnologías de la Información en las Administraciones Públicas,* MAP, 2000

[2] L. PAREJO, *Eficacia y Administración. Tres estudios*, Madrid, INAP, 1995.

tanto, más cómoda y más sencilla, contribuyéndose así a mejorar la satisfacción de los ciudadanos hacia una Administración a la que ven cada vez más cercana[3].

Además, las nuevas tecnologías no deben servir sólo para mejorar la información que las Administraciones Públicas dan a los ciudadanos sino también para permitir la tramitación telemática. Es decir, es importante no sólo que se pueda acceder de manera telemática a la información de los principales servicios, sino que el ciudadano pueda iniciar la tramitación de un procedimiento administrativo, presentando su solicitud cómodamente desde el ordenador, para pedir, por ejemplo, una subvención, matricularse en una Universidad o solicitar cita en un Centro de Salud[4]. Esto, lógicamente, hay que hacerlo con las garantías necesarias de identidad, integridad y confidencialidad, a través de firma electrónica avanzada. Al mismo tiempo, facilitar el canal de internet para relacionarse con la Administración obliga a la automatización del *back office* administrativo, es decir, a la mecanización de los procedimientos y a trabajar en red.

La Administración no es libre. Está obligada por su función constitucional de servicio eficaz a los ciudadanos y al interés general a adoptar políticas de calidad y de modernización administrativa y a impulsar la utilización de las nuevas tecnologías en la actuación interna de la Administración y en su relación con los ciudadanos. Además, el desarrollo económico exige cambios en la Administración. La iniciativa pública en la actividad económica –art. 128.1 CE-, la función modernizadora de los poderes públicos sobre los distintos sectores económicos –art. 130 CE- y la actividad de estímulo del crecimiento de la renta y de la riqueza –art. 131 CE- no debe limitarse a impulsar la

---

[3] AA.VV, *Libro blanco para la mejora de los servicios públicos. Una nueva Administración al servicio de los ciudadanos.* MAP,2000; J. Chias, *Marketing Público. Por un Gobierno y una Administración al servicio del público*, McGraw-Hill, Madrid, 1995. págs. 31-48 *Gestión y Evaluación de la Calidad en los Servicios Públicos, Segundas Jornadas sobre la medición y mejora de los servicios públicos,* INAP-Asociación Española para la Calidad, 1995, esp. págs. 15-49 Una concepción del administrado o del ciudadano como cliente se puede ver en *La Administración al Servicio del Público*, INAP, Madrid, 1991, *passim*, esp. págs. 129-141 o "Per una política de millora de les relacions entre l'Administració i els ciutadans. *Administration as a service. The Public as a client*", Comitè Assessor per a l'estudi de l'organització de l'Administració, *La funció organizativa*, cit, págs. 28-39.Sobre los servicios de auditoría interna de la Administración, cfr. J. Mas & C. Ramió, *Tècniques D'Auditoria Operativa Aplicades a L'Administració Pública*, Generalitat de Catalunya, Departament de Governació. Comitè Assessor per a l'estudi de l'organització de l'Administració, Barcelona, 1992.

[4] Cfr. AA.VV, *Telemedicina, atención sanitaria y sus aspectos legales*, MSC-CGPJ, 2002, págs. 91-150.

innovación tecnológica de las empresas y de la sociedad. Es la propia Administración la que debe cambiar. La nueva economía exige una nueva Administración; el *e comerce* exige un *e government.*

El avance en la sociedad de la información, que tiene indudables elementos positivos para el desarrollo económico y para la eficacia administrativa, también presenta elementos de incertidumbre y riesgo. Uno de los principales es que las nuevas tecnologías supongan el establecimiento de una nueva frontera de desigualdad, al estar ajenos a este desarrollo algunos grupos sociales, no tanto por razones de renta sino por razones de edad. Es decir, que las nuevas tecnologías sean un arma para la aparición de una nueva discriminación, una nueva barrera, esta vez ya no por razones de sexo, raza, o religión, sino por las posibilidades de acceso a la sociedad de la información, al conocimiento de estas nuevas tecnologías.

Es obligación de los poderes públicos, como señala el art. 9.3 CE, promover las condiciones para que la libertad y la igualdad de las personas y de los grupos sociales sean reales y efectivas, evitando los obstáculos que impidan o dificulten su plenitud y garantizar la participación de todos los ciudadanos en la vida económica, política, social y cultural. Es imprescindible, por tanto, una labor pública de fomento de estas nuevas tecnologías dentro de la sociedad, no sólo a través de la educación sino también mediante la formación continua y los servicios sociales.

Igualmente, a la vez que se facilita a través de las nuevas tecnologías la participación social y la relación entre representantes y representados, sobre todo para conocer necesidades y problemas locales de los ciudadanos, es necesario también no sacar conclusiones precipitadas sobre el uso de las nuevas tecnologías, para que éstas, en la medida en que facilitan la sobre-representación de determinados grupos, los más dinámicos, no supongan un atentado al principio democrático y a la soberanía popular. Además, otros derechos fundamentales pueden verse vulnerados a través de las tecnologías de la información. Así, la propiedad intelectual o la necesaria protección de la juventud y de la infancia pueden verse burladas a través de la pornografía en internet. El secreto de las comunicaciones, que hasta ahora incluía las telegráficas, postales y telefónicas, puede verse menoscabado por el acceso indebido al correo electrónico.

Especialmente, existe el peligro de que las tecnologías de la información entren en conflicto con el derecho a la intimidad**.** La informática facilita ilimitadas posibilidades para recoger datos personales, tratarlos, conservarlos y transmitirlos. La tecnología es capaz de mover un gran volumen de información y de ponerla en relación, de manera que se construyan perfiles de nuestra personalidad, que pueden llegar a justificar decisiones públicas o privadas y que puedan limitar nuestra libertad o a condicionar nuestro modo de actuar. A través de tratamientos de datos se puede llegar a saber si tengo una enfermedad grave, si estoy afiliado a un sindicato, si tengo algún hijo con alguna minusvalía, cuál es mi nivel de renta, mi situación familiar o mis hábitos de conducta.

Con anterioridad al establecimiento de un derecho específico a la protección de datos de carácter personal la tutela tenía que ser desarrollada a través de la invocación de un derecho más amplio a la intimidad y a la privacidad personal, recogido en todos los textos internacionales y constitucionales. Así, la Declaración Universal de los Derechos Humanos de 10 de diciembre de 1948 proclama en el artículo 12 que "nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".

En nuestro país, la Constitución Española de 1978 reconoce en el art. 18 el derecho al honor, a la intimidad personal y familiar, a la propia imagen, el derecho a la inviolabilidad del domicilio y al secreto de las comunicaciones. El principal desarrollo legislativo que se ha producido hasta ahora del derecho a la intimidad, reconocido en el art. 18.1 de la Constitución, ha sido la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. Esta Ley, básicamente, desarrolla el contenido de este derecho como límite a la libertad de expresión y al derecho a la información, en los términos previstos en el art. 20.4 CE. La principal doctrina y jurisprudencia constitucional sobre el derecho a la intimidad ha tratado sobre todo de deslindar estos dos derechos enfrentados[5]

[5] Cfr. SSTTC 117/1994; 231/1998; 76/1990; C. RUIZ MIGUEL, *La configuración constitucional del derecho a la intimidad*, Tecnos, Madrid, 1995; F. HERRERO-TEJEDOR, *Honor, intimidad y propia imagen*, Colex, Madrid, 1984; P. A. MUNAR, "Derecho a la intimidad", *Enciclopedia Jurídica* Básica, Cívitas, Madrid, 1995, III, págs. 3725-3728; J. VIDAL MARTINEZ, *El derecho a la intimidad en la Ley Orgánica de 5 de mayo de 1982*, Madrid, 1984; L. M.

La Constitución Portuguesa de 1976 y la Constitución Española de 1978 fueron las primeras en ser conscientes de la necesidad de configurar un derecho específico a la protección de datos personales. La Constitución Portuguesa de 1976 afirma, por un lado, de manera más genérica en el art. 26.2, que "[l]a ley establecerá garantías efectivas contra la utilización abusiva, o contraria a la dignidad humana, de informaciones referentes a las personas y a las familias". Pero, por otro lado, dedica un precepto expreso a esta cuestión, el art 35, que señala:

1. Todo ciudadano tendrá derecho a tener conocimiento de lo que conste en forma de registros informáticos acerca de él y de la finalidad a que se destinan esos datos, y podrá exigir su rectificación, así como su actualización, sin perjuicio de lo dispuesto en la ley sobre secretos de Estado y secreto de actuaciones judiciales.
2. Se prohíbe el acceso a ficheros y registros informáticos para el conocimiento de datos personales referentes a terceros y la respectiva interconexión, salvo en casos excepcionales previstos por ley.
3. No podrá utilizarse la informática para el tratamiento de datos referentes a convicciones filosóficas o políticas, afiliación a partidos o a sindicatos, fe religiosa o vida privada, salvo cuando se trata del tratamiento de datos estadísticos no identificables individualmente.
4. La ley definirá el concepto de datos personales para fines de registro informático, así como de bases y bancos de datos y las respectivas condiciones de acceso, constitución y utilización por entes públicos y privados.
5. Se prohíbe la asignación de un número nacional único a los ciudadanos.
6. La Ley determinará el régimen aplicable a los flujos de datos allende las fronteras, estableciendo formas adecuadas de protección de los datos personales y de otros cuya salvaguardia se justifique por razones de interés nacional.

FARIÑAS MANTONI, *El derecho a la intimidad,* Madrid, 1983; D. ORTEGA, *Derecho a la información versus derecho al honor*, CEPC, Madrid, 1999..

Más recientemente, los reformas de los textos constitucionales están incluyendo preceptos que garantizan un derecho a la protección de datos personales. Así, la Ley Fundamental del Reino de los Países Bajos, revisada en 1983, ha señalado que "[l]a ley establecerá las normas de protección de la intimidad personal en relación con la indagación y difusión de datos personales –art. 10.2- y que "[l]a ley dictará normas sobre el derecho de toda persona a que se le dé conocimiento de los datos recogidos sobre ella y del uso que se hiciere de los mismos, así como al perfeccionamiento de dichos datos" –art. 10.3-. La Constitución de Finlandia de 1919 –a partir de la reforma de 1980- señala –art. 8- que "[l]a ley establecerá normas de detalle sobre la salvaguardia de los datos de carácter personal". La Constitución de Suecia de 1994 afirma en el art. 3 que "[t]odo ciudadano quedará protegido, en la medida que se disponga en detalle por la ley, contra la violación de la integridad de su persona resultante del registro de información sobre él mediante tratamiento electrónico de datos". En cambio Bélgica, con un texto refundido de 1994 de la Constitución originaria de 1831, sigue limitándose en el art. 22 a afirmar que "[t]odos tendrán derecho al respeto de su vida privada y familiar, excepto en los casos y en las condiciones que establezca la ley"-

Al reconocimiento de este derecho ha contribuido, sin duda, los Tratados internacionales y el Derecho de la Unión Europea. Especial mención merece el Convenio 108 de 28 de enero de 1981 del Consejo de Europa, para la protección de las personas en lo que respecta al tratamiento automatizado de los datos personales, los principios de los derechos y libertades. En el ámbito de la Unión Europea, hay que destacar la Directiva 95/46 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[6]. Recientemente, en el Tratado de Niza, de 2000, donde se consagra la Carta de Derechos Fundamentales de la Unión Europea, se establece:

---

[6] Un análisis de los primeros pasos sobre la cuestión en el ámbito europeo, sobre la distinta protección de datos en los diferentes Estados de la Unión Europea, y, más en concreto, sobre la Directiva 95/46 se puede ver en M. A. DAVARA, *La protección de datos en Europa*, Universidad de Comillas ICAI-ICADE, Madrid, 1998, págs. 41-59. Un estudio sistemático de las legislaciones de protección de datos de los países de la Unión Europea, centrándose en las divergencias normativas, se puede ver en A. TÉLLEZ AGUILERA, *La protección de datos en la Unión Europea. Divergencias normativas y anhelos unificadores*, Edisofer, Madrid, 2002, págs. 329-349.

1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernen.
2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.
3. El respeto a estas normas quedará sujeto al control de una autoridad independiente.

En lo que respecta a nuestro país, la Constitución Española de 1978 ha regulado de manera específica esta cuestión. Así, en el mismo precepto donde se reconoce el derecho al honor, a la intimidad personal y familiar, a la propia imagen y se salvaguarda la inviolabilidad del domicilio y el secreto de las comunicaciones, se establece que "[l]a 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" –art. 18.4 CE-. Llama la atención que la única vez que la Constitución habla de la informática, lo hace para limitar su uso. Se trata de que un elemento provechoso no sea utilizado para recortar la privacidad de las personas. Es, por tanto, una respuesta constitucional ante una amenaza concreta. Así, frente al riesgo que suponen los tratamientos de datos personales por medios informáticos, se ha reconocido un derecho específico de protección de datos personales, como ha afirmado recientemente la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre.

La antigua proclamación del derecho a la intimidad no era una protección bastante frente a la nueva realidad del progreso tecnológico. El Tribunal Constitucional, en su Sentencia 292/2000, de 30 de noviembre, ha hablado de la existencia de un derecho a la autodeterminación informativa o de libertad informática, que se puede definir como el derecho al control que tiene toda persona sobre sus datos personales insertos en un programa informático y que le faculta para decidir quién posee sus datos y para qué los va a usar, pudiendo oponerse a esa posesión o uso. Este derecho no tiene un carácter abstracto o genérico. Atribuye a su titular un haz de facultades que consiste en el poder jurídico de imponer a terceros la realización o la omisión de determinados comportamientos. Dentro del contenido de este derecho fundamental, se encuentran los principios de calidad de los datos, información en la recogida de los mismos y

consentimiento del afectado para su tratamiento. También el derecho de acceso sobre sus datos de carácter personal sometidos a tratamiento, oposición, rectificación y cancelación. El Legislador ha establecido reglas objetivas sobre el tratamiento de datos personales para que el ciudadano recupere el poder de disposición y control sobre sus datos y ha establecido instituciones específicas, como las Agencias de Protección de Datos, que refuerzan este derecho a la autodeterminación informativa

La primera Ley que desarrolló este derecho en nuestro país fue la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal[7], que ha sido derogada por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal[8]. La Ley Orgánica 15/1999, que es analizada en el Primer Capítulo de este libro, ha tenido la virtualidad de extender el derecho a la protección de datos a los tratamientos no automatizados y sustentados sobre un soporte-papel, en consonancia con la Directiva 95/46, del Parlamento y el Consejo relativa a la protección de las personas físicas con respecto al tratamiento de los datos personales y a la libre circulación de esos datos. El art. 1 de la LOPD señala como objeto "garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas y, especialmente, de su honor, intimidad personal y familiar". Es decir, que el derecho fundamental de protección de datos es una concretización del derecho a la intimidad para los tratamientos de datos, un derecho más específico dentro del más general derecho de privacidad personal

---

[7] Cfr. E. DEL PESO NAVARRO y MIGUEL ANGEL RAMOS, *Lortad. Análisis de la Ley*, Díaz de Santos, 1994, págs. 169-180.

[8] Uno de los mejores estudios sobre la LOPD es el de J. APARICIO, *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*, Aranzadi, Navarra, 2002. Cfr. también J. J. MARTÍN CASALLO y J. A. MARTÍN PALLÍN, "Intimidad, privacidad y protección en la nueva Ley Orgánica 15/1999, en M. A. DAVARA, *XIV Encuentros sobre Informática y Derecho 2000-2001* Aranzadi, Navarra, 2001 págs. 51-53 y 55-59. Cfr. como referencias más generales P. LUCAS MURILLO, *El derecho a la autodeterminación informativa,* Tecnos, Madrid, 1990; P. LUCAS MURILLO, *Informática y Protección de Datos Personales*, CEC, Madrid, 1993; A. E PÉREZ LUÑO, *Manual de Informática y Derecho*, Ariel, Barcelona, 1996; J. M. ALVAREZ CIENFUEGOS, *La defensa de la intimidad de los ciudadanos y la tecnología informática*, Aranzadi, Pamplona, 1999; H. CAMPUZANO, *Vida privada y datos personales*, Tecnos, Madrid, 2000.

La legislación de protección de datos personales presenta una cierta complejidad. Así, por una parte, es una materia muy técnica, con un vocabulario propio. Esto ha hecho que tanto la Directiva 95/46 como LOPD contengan un grupo de definiciones de qué se entiende por datos de carácter personal, fichero, tratamiento de datos, responsable del fichero o del tratamiento, afectado o interesado, procedimiento de disociación, encargado del tratamiento, consentimiento del interesado, cesión o comunicación y fuentes accesibles al público –art. 3 LOPD-. Por otro lado, la LOPD ha sido redactada con una técnica legislativa defectuosa. Así, no tiene exposición de motivos por lo que no conocemos la *voluntas legislatoris*, uno de los criterios de interpretación para determinar el sentido de las normas jurídicas. La LOPD, además, se encuentra llena de excepciones en lo relativo a su ámbito de aplicación –art. 2.2- y matizada por lo previsto en otras legislaciones más específicas, como la estadística, la del régimen electoral general, la de régimen del personal de las Fuerzas Armadas, del Registro Civil, del Registro Central de Penados y Rebeldes o la de la legislación que regula imágenes y sonidos obtenidas por las Fuerzas y Cuerpos de Seguridad –art. 2.3 LOPD-. Todas estas dificultades traen causa de su azarosa tramitación parlamentaria. Lo que inicialmente era un Proyecto del Gobierno de reforma de la LORTAD para adecuarla a la Directiva 95/46, sobre la base de un Anteproyecto elaborado por la Agencia de Protección de Datos del Estado, se transformó por completo en la Comisión Constitucional del Congreso de los Diputados, que se lanzó a elaborar ex novo una nueva Ley Orgánica de Protección de Datos Personales, que quizás fuera en esos momentos innecesaria. En todo caso, la preparación y redacción de un texto nuevo en sede parlamentaria que no había recibido un estudio adecuado a través del Poder Ejecutivo –de las distintas Secretarías Generales Técnicas y Subdirecciones Generales de Normativa de los distintos Ministerios, de la Abogacía del Estado y del Consejo de Estado- y que sólo pudo ser enmendado parcialmente ha favorecido la aprobación de un texto menos cuidado y con defectos graves de carácter sistemático.

Además, la LOPD no ha sido objeto hasta ahora de desarrollo reglamentario. La normativa de rango infralegal es toda ella desarrollo de la LORTAD. Esto es lo que ocurre con el Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal; el 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; el Real Decreto 1428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos; la Instrucción 1/1995, de 1 de marzo, de la Agencia de Protección de Datos, relativa a la prestación de servicios de solvencia patrimonial y crédito, la Instrucción 2/1995, de 4 de mayo, de la Agencia de Protección de Datos, sobre medidas que garantizan la intimidad de los datos personales recabados como consecuencia de la contratación de un seguro de vida de forma conjunta con la concesión de un préstamo hipotecario o personal; la Instrucción 1/1996, de 1 de marzo, de la Agencia de Protección de Datos, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los edificios; la Instrucción 2/1996, de 1 de marzo, de la Agencia de Protección de Datos, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los casinos y salas de bingo; y la Instrucción 1/1998, de 19 de enero, de la Agencia de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación. Por tanto, todavía no se dispone de una normativa que haya tratado de dar coherencia y sistemática a la LOPD.

El derecho fundamental a la protección de datos personales tiene un contenido que se encuentra descrito en la LOPD y un contenido esencial al que ha hecho mención la STC 292/2000, de 30 de noviembre. Dentro de ese contenido esencial se encontrarían el principio de calidad de los datos, el principio de información y el principio de consentimiento del afectado. Quisiera destacar especialmente el principio de secreto profesional –configurado como un auténtico deber de secreto y de confidencialidad- al que están obligados todas las personas que intervienen en tratamientos de datos de carácter personal, y el principio de seguridad de los datos, que es una garantía de la confidencialidad, y que es el objeto de este libro.

Merece especial interés la obligación que señala LOPD de garantizar el principio de seguridad y la normativa reglamentaria que lo desarrolla. Esta normativa no es un elemento formalista o rigorista. La seguridad es una garantía de la integridad de la información, de la disponibilidad de la información, y, sobre todo, de la confidencialidad, ya que al limitar el acceso a la información se salvaguarda nuestra intimidad y privacidad. Consciente de esta preocupación fue ya la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal. La LOPD continúa estableciendo en el art. 9 que el “responsable del fichero, o en su caso, el

encargado del tratamiento, debe adoptar medidas tanto técnicas como organizativas necesarias que garanticen la seguridad de los datos y eviten su alteración, perdida, 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". Así se establece que no se registrarán datos de carácter personal en ficheros automatizados que no reúnan las condiciones que se determinen con respecto a su seguridad e integridad por la vía reglamentaria. Esta vía reglamentaria ha sido el Real Decreto 994/1999, de 11 de junio, que aprueba el Reglamento de Medidas de Seguridad y que ha establecido los requisitos y condiciones que deben reunir los ficheros automatizados y las personas que intervengan en su tratamiento. Este es el objeto central del libro que prologamos. Los ficheros que contengan datos de ideología, religión creencias, origen racial, salud, vida sexual, están sometidos a medidas de seguridad de nivel alto, plazo de implantación que, después de sucesivas prórrogas, expiró el 26 de junio de 2002. La Ley también recuerda en el art. 10 que el responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsisten aún después de finalizar sus relaciones con el titular del fichero, o, en su caso, con el responsable del mismo.

Lógicamente, estas obligaciones no son meramente teóricas sino que su omisión es una infracción muy grave. Así, el 44.3 LOPD señala que es una infracción muy grave "la vulneración del deber de guardar secreto sobre los datos de carácter personal a que hacen referencia los apartados 2 y 3 del art. 7", siendo una infracción grave "mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen".

Quisiera para terminar hacer unas reflexiones sobre la oportunidad y el contexto en el que se presenta este libro de José Luis Rivas, Víctor Salgado y Enrique Ares. Realmente, la búsqueda de la seguridad no supone un problema informático. Las conclusiones sobre las primeras pre-auditorías de los ficheros de nivel alto suelen detectar una implantación generalizada de las medidas de seguridad de nivel alto, especialmente, de las medidas de carácter técnico. Presentan más lagunas de cumplimiento las medidas de carácter organizativo y funcional. Así, la mayoría de los productos informáticos que ofrece el mercado –como se describe en este libro- permite el cumplimiento de las medidas de

seguridad de nivel alto. De hecho, una información almacenada en un soporte informático que disponga de las medidas de seguridad de nivel alto estará siempre mejor guardada –con una más segura confidencialidad- que si esa información se mantiene en un soporte papel –los denominados ficheros manuales-estructurados-. De esta forma, se puede concluir que las tecnologías de la información no son tanto un amenaza para el derecho a la intimidad sino que, al contrario, son una garantía de este derecho, por lo que se hace aconsejable la migración de esta información desde los ficheros manuales a los ficheros informatizados.

Este Prólogo es, también, una oportunidad para reconocer el trabajo desarrollado hasta ahora por los auditores de sistemas de información. Las empresas de auditoría informática han prestado hasta ahora una enorme colaboración en la concienciación de los ciudadanos sobre este derecho fundamental de protección de datos personales. De hecho, los auditores de sistemas de información se encuentran en el origen de esta materia, en concreto, de la normativa de seguridad. No obstante, la auditoría informática se extendía y se extiende a un ámbito mucho más amplio que el de la protección de datos. Estas empresas seguirán prestando un apoyo importante al poder ser las encargadas de desarrollar la auditoría bianual –en este caso externa- de los ficheros de nivel medio y de nivel alto que exige el art. 17 del Real Decreto 994/1999.

Al mismo tiempo, cualquier actividad que desde este campo se desarrolle, como la elaboración de Códigos Tipo o las Certificaciones, puede contribuir a mejorar la seguridad de la información y la credibilidad de las empresas en el mercado, facilitando el comercio electrónico y las telecomunicaciones. En esta dirección se ha aprobado recientemente la Norma ISO/UNE 17799 de Gestión de Seguridad de la Información, y cuyo objetivo es contar con un sistema de gestión que permita ofrecer a empresas y organizaciones instrumentos, a través de un código de buenas prácticas, para garantizar al máximo posible la seguridad de su información[9]. La Norma ofrece una visión global de la seguridad de la información y contempla la seguridad como un proceso y no como un producto ya que “la seguridad de la información no es sinónimo de seguridad informática”. La Norma no sólo incluye aspectos técnicos sino también aspectos jurídicos, al

[9] Los objetivos fundamentales de la Norma son: garantizar la confidencialidad, integridad, disponibilidad y autenticación de la información; aportar herramientas y procedimientos de gestión efectivos; y obtener un nivel de seguridad proporcionado a los riesgos existentes en la organización.

extenderse al ámbito de la organización, pues en lo que respecta a la información es tan importante la seguridad informática como la seguridad jurídica[10]. No obstante, no se deben confundir los reguladores con los regulados. La autoridad de control sigue siendo la Agencia de Protección de Datos; las empresas de auditoría son, en cambio, sectores regulados. El hecho de que una empresa tenga un sello o una certificación no garantiza plenamente que no cometa una infracción administrativa. Lógicamente, cuando se contrata una consultoría de seguridad, se pone de manifiesto que se tiene una preocupación sobre esta materia y que hay una buena predisposición para cumplir la legislación. En todo caso, las empresas que ofrecen estos servicios deben saber separar la actividad de consultoría de la de auditoría, para no confundir al mercado, como se está haciendo en otros sectores como el financiero.

De todas estas cuestiones trata este libro de José Luis Rivas, Enrique Ares Gómez y Víctor Salgado Seguín, *Implantación de la LOPD en los sistemas*. Es un libro importante para un momento importante: la finalización del plazo de implantación de las medidas de seguridad de nivel alto. Es un libro claro y preciso. Da respuestas y aporta soluciones. Por todo ello, podemos recomendar vivamente su lectura.

Madrid, abril de 2003

Antonio Troncoso Reigada
Director de la Agencia de Protección de Datos
De la Comunidad de Madrid

[10] Dentro de los aspectos jurídicos de la Norma ISO/UNE 17799 destacaríamos, además de la protección de datos de carácter personal, el cumplimiento de la normativa de Propiedad Intelectual y de comercio electrónico, la normativa laboral, en especial, en todo aquello que tenga que ver con la regulación y limitación del uso por parte de los empleados de una organización de sus sistemas de tratamiento de la información, y la normativa procesal, fundamentalmente en cuanto a la aptitud de la información, cualesquiera que sean los formatos en los que ésta se presente, incluidos los digitales, para ser objeto de prueba en un procedimiento judicial y condiciones y requisitos para tal fin. Dentro de los aspectos técnicos y organizativos de la Norma ISO/UNE 17799 señalaríamos la salvaguarda de los registros de la empresa, el análisis de riesgos, la documentación de la política de seguridad de la información, la asignación de responsabilidades de seguridad, la formación y entrenamiento para la seguridad de la información, el registro de las incidencias de seguridad y la gestión de la continuidad del negocio

A finales del siglo XX, se incrementó la capacidad de tratamiento y transmisión de la información que ofrecen las nuevas tecnologías, haciendo mucho más necesario proteger los derechos fundamentales del individuo, en concreto: el *derecho al honor, a la intimidad personal y familiar y a la propia imagen*. Para proteger a los ciudadanos de este peligro se crearon una serie de leyes y medidas que deben adoptar las empresas e instituciones que cuentan con sistemas de información

Por tanto, el objetivo del manual, en esta etapa, es documentar qué se puede hacer para aplicar la Ley Orgánica de Protección de Datos (L.O.P.D.) así como el Reglamento de Medidas de Seguridad también conocida como Real Decreto 994/1.999.

Nos hemos dirigido a profesionales que tengan o no base sobre dicho tema. Para ello, explicaremos paso a paso cómo aplicar cada artículo en cada uno de los sistemas operativos que conviven en el mercado y que se utilizan normalmente: Linux, Windows NT, Windows 2000, Windows XP y sistemas de gestión en general. Aunque explicamos algunas de las maneras de implantarlas en estos sistemas es recomendable tener un manual sobre ellos si no se tienen unos amplios conocimientos. El objetivo de este manual no es aprender a utilizar estos sistemas, sino saber aplicar la vigente legislación sobre dichos sistemas.

El libro está divido en 5 partes o secciones bien diferenciadas. Cada una de ellas está divida a su vez en una serie de capítulos.

- La primera parte tiene el nombre de "*Aspectos generales*". En el primer capítulo introduciremos la L.O.P.D. y el segundo describiremos los diferentes sistemas, así como los derechos de autor.

- En esta parte llamada "*Nivel básico*" comentamos todo lo referente a la implantación en este nivel desde las cuestiones de identificación y autentificación hasta el desarrollo de las copias de seguridad.

- A la siguiente parte se le ha puesto el nombre de "*Nivel medio*". En ella recogemos qué pide el Reglamento en cuanto a seguridad física de los locales, así cómo efectuar una auditoria legal. En el último capítulo de este tema comentaremos cómo desarrollar el documento de seguridad

- En esta parte, llamada "*Nivel Alto*" describiremos de una manera detallada la implantación de dicho nivel en los sistemas. Trataremos asuntos relacionados con la telecomunicación y las copias de seguridad entre otros temas.

- La última parte se corresponde a una serie de apéndices donde se podrá encontrar un plan de adaptación para aplicar a los sistemas ya existentes la LOPD, las posibles sanciones por incumplimiento, las preguntas más frecuentes y la legislación.

1

Introducción a la LOPD

En este capítulo se hará una pequeña introducción a la legislación española más concretamente nos centraremos en el motivo de las leyes referentes a la protección de la información y su evolución hasta la actual Ley Orgánica de Protección de Datos de Carácter Personal y el Reglamento de Medidas de Seguridad.

Por este motivo veremos:

¿Qué es la LOPD?
¿Por qué surgió?
¿Por qué se paso de la LORTAD a la LOPD?
Diferencias entre la LOPD y la LORTAD
Cuando hay que aplicar que la LOPD
Reglamento de Medidas de Seguridad
Niveles de protección

1.1 ¿QUÉ ES LA LOPD?

LOPD son las siglas abreviadas de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Esta Ley fundamentalmente tiene el objetivo de proteger a las personas físicas con respecto al tratamiento que se pueda realizar de sus datos propios por distintos sujetos, ya sean públicos o privados.

Dicha regulación pretende, fundamentalmente, establecer un control sobre quién tiene dichos datos, para qué los usa y a quién se los cede. Para ello, impone una serie de obligaciones a los responsables de dichos ficheros de datos: como son las de recabar el consentimiento de los titulares de los datos para poder tratarlos, comunicar a un Registro especial la existencia de dicha base de datos y su finalidad, así como mantener unas medidas de seguridad mínimas de la misma, en función del tipo de datos recogidos. Por otro lado, la LOPD reconoce una serie de derechos al individuo sobre sus datos como son los de información, acceso, rectificación e, incluso, de cancelación de los mismos en determinados supuestos.

Finalmente, se designa a una entidad: la Agencia de Protección de Datos, como órgano administrativo encargado de hacer cumplir la LOPD y sus reglamentos, pudiendo inspeccionar e imponer fuertes sanciones a aquellos sujetos que no cumplan con la misma.

A continuación veremos los orígenes y el fundamento de dicha regulación.

1.2 ¿POR QUÉ SURGIÓ?

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: el *derecho al honor, a la intimidad personal y familiar y a la propia imagen*. Estos derechos están recogidos en las constituciones de los

Estados Miembros[1], así como en el artículo 8 del Convenio Europeo para la protección de los Derechos Humanos y de las Libertades Fundamentales[2].

En lo que se refiere a la legislación nacional, el apartado 4º del artículo 18 de la Constitución Española dice 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"*. Tal era la concienciación de nuestro 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)[3].

---

[1] Artículo 18 de la Constitución Española de 1978:

> *"1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.*
>
> *(...)*
>
> *4. 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."*

[2] Artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, adoptado en Roma el 4 de noviembre de 1950:

> *"1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.*
>
> *2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuando esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás."*

[3] Ley Orgánica 5/1992, de 29 de octubre, de *Regulación del Tratamiento Automatizado de los Datos de Carácter Personal*. Boletín Oficial de Estado de 31 de octubre de 1992.

En desarrollo de la LORTAD, se han dictado diversos reglamentos: el Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la misma; el Real Decreto 428/1993, de 26 de marzo, modificado por el Real Decreto 156/1996, de 2 de febrero, que regula el Estatuto de la Agencia de Protección de Datos; y, especialmente destacado, el Real Decreto 994/1999, de 11 de junio, de Medidas de Seguridad aplicables a los ficheros con Datos de carácter personal, cuyo análisis nos ocupará la mayor parte de esta obra.

1.3 ¿POR QUÉ SE PASO DE LA LORTAD A LA LOPD?

La LORTAD se adoptó teniendo en cuenta los trabajos preparatorios del Proyecto de Directiva del Parlamento Europeo y del Consejo relativa a la Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales y a la Libre Circulación de estos Datos[4].

Por tanto, 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[5].

Dicha Directiva debía ser transpuesta al Derecho español, en un plazo fijado, para que surtiera plenamente sus efectos. Debido a ello, y a las diferencias fundamentales detectadas entre la directiva y la LORTAD, posteriormente se aprobó la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal (LOPD) que

---

[4] Dicho proyecto desembocó en 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*. Diario Oficial nº L 281, de 23 de noviembre de 1995. Pág. 31.

[5] V. Nota nº4.

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 la nueva Ley.

1.4 DIFERENCIAS ENTRE LA LORTAD Y LA 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 manual y no las consideramos pertinentes dado su carácter práctico y su ámbito específico centrado fundamentalmente en las Medidas de Seguridad aplicables.

1.5 CUÁNDO HAY QUE APLICAR LA LOPD

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".*

En este punto es necesario saber lo que la Ley entiende por "datos de carácter personal":

El artículo 3 de la LOPD define a los mismos como *"cualquier información concerniente a personas físicas identificadas o identificables".*

Es de destacar que solo 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.

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.

1.6 REGLAMENTO DE MEDIDAS DE SEGURIDAD

Tal y como adelantamos en el epígrafe 1.2, 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, en base a los artículos 44.3 y 45.2 de la LOPD.

Dicho Reglamento, será nuestro objeto fundamental de estudio a lo largo de la presente obra.

1.7 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 acumulativa, así el nivel alto deberá cumplir también las reguladas para el nivel medio y el nivel bajo de seguridad. Véase el esquema siguiente.

En los siguientes capítulos de este manual, iremos describiendo cada uno de los niveles de seguridad, así como las medidas concretas aplicables en cada uno de los mismos.

2

Introducción a los sistemas

En este capítulo vamos a ver los conceptos básicos sobre los sistemas con los que vamos a trabajar antes de empezar a explicar como aplicar la LOPD sobre dichos sistemas.

En este capitulo se verán:

1) Linux
2) Windows NT
3) Windows 2000
4) Windows XP
5) Sistemas de gestión
6) Derechos de autor

2.1 LINUX

Linux es un sistema operativo[1] multitarea[2] y multiusuario[3] iniciado para crear una versión de trabajo de UNIX en ordenadores IBM PC o compatibles, es decir, en máquinas basadas en tecnologías x86. Por tanto, el objetivo fue crear un clon de UNIX, en el que no hubiera ningún software comercial con derechos y que pudiese ser utilizado por gente de todo el mundo.

Linux fue desarrollado como afición por Linus Torvald mientras estaba estudiando en la universidad de Helsinki en Finlandia con tan sólo 23 años. Linus intentaba crear una versión más sólida de Minix. Minix es un programa desarrollado por el Dr. Andrew Tannebaum para la demostración de varios conceptos que se encuentran en los sistemas operativos.

Aunque Linux es gratuito, no es un software de dominio público debido a que Linus tiene los derechos de autor del núcleo (kernel) y muchas de las utilidades de dicho sistema operativo están bajo la licencia GNU General Public Licence. Esta licencia permite a los creadores de un programa conservar sus derechos de autor, pero permite a otros programadores venderlos después de haberlos modificados sin poder limitar los derechos anteriores. Todo esto lleva consigo la facilitación del código fuente.

2.1.1 LAS DISTRIBUCIONES

Desde que Linus creo el primer núcleo y los primeros programas, Linux ha sufrido un enorme impulso. Dicho impulso ha permitido que un número elevado de empresas, muchas de ellas nuevas, y usuarios se dediquen a crear nuevas distribuciones y nuevos programas. En la actualidad nos podemos encontrar desde aplicaciones ofimáticas hasta programas de ingeniería.

Una cosa hay que tener clara: a pesar de las numerosas distribuciones que existen, ninguna distribución es mejor que otra. Lo importante es aprender y

[1] Un sistema operativo administra todos los recursos disponibles (impresoras, discos duros, memoria, ratón, etc.)
[2] Permite ejecutar muchos programas al mismo tiempo sin parar la ejecución de los otros programas.

acostumbrarse a una de ellas. Una vez elegida una que se adapte a nuestras necesidades y a nuestros gustos, es recomendable mantenernos con ella.

Pero lo más importante es que ésta esté bien configurada. Un sistema bien configurado nos evitará muchos problemas.

A continuación se muestra alguna de las distribuciones más populares:

DISTRIBUCCIÓN	INSTALACIÓN GRÁFICA	DETECCIÓN HARDWARE	FORMATO PAQUETES	IDIOMA	DIRECCIÓN WEB
Corel Linux	ν	ν	deb	inglés	http://www.corel.com
Debian	χ	χ	deb	español	http://www.debian.org
Esware Linux	ν	ν	rpm	español	http://www.esware.com
HispaFuentes	ν	χ	rpm	español	http://www.hispafuentes.com
Mandrake	ν	χ	rpm	inglés	http://www.linux-mandrake.com
Red Hat	ν	χ	rpm	inglés	http://www.redhat.com
Slackware	χ	χ	tgz	inglés	http://www.cdrom.com
SuSE Linux	ν	χ	rpm	español	http://www.suse.de
Turbolinux	ν	χ	rpm	inglés	http://www.turbolinux.com

2.1.2 LOS SHELLS

Los shells son herramientas que, nos permiten interaccionar activamente mediante una línea de comandos con el sistema operativo. En la actualidad existen numerosos shells cada una de ellas con diferentes características. Eligiendo los usuarios las que mejor se adapten a sus necesidades y sus gustos. Los mas usados son: sh, bash, csh y ksh.

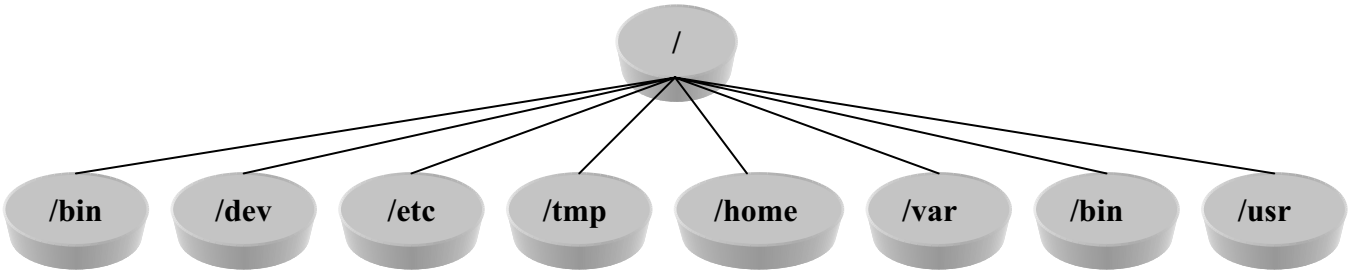
Para guardar la información que usa mientras se ejecutan utilizan lo que es conocido como entorno. Para ver los diferentes variables de entorno y para modificarlas se utilizan el comando *env* o *set* dependiendo de shell utilizado.

[3] Permite ofrecer servicios a varios usuarios a la vez, ejecutando uno o varios programas a la vez.

2.1.3 ESTRUCTURA DE DIRECTORIOS

Una estructura de directorios es un mecanismo para organizar los diferentes ficheros en un sistema operativo. Los sistemas Linux como en Unix implementan los grafos acíclicos. Este tipo de grafos permite que el mismo fichero o subdirectorio esté en varios directorios diferentes. Esta es la manera que tiene tanto Linux como Unix para compartir ficheros y directorios entre varios usuarios.

A continuación se muestra la estructura que tiene Linux:



- */* , directorio raíz del sistema de archivos. A partir de él se coloca toda la estructura de directorios.

- */sbin*, directorio que contiene los programas en la inicialización del sistema y en su recuperación.

- */dev*, directorio que contiene los archivos de los dispositivos: discos duros, disquetes, impresoras, ratón, puerto serie, etc.

- */etc*, directorio que contiene los archivos de configuración del sistema.

- */home*, directorio que contiene los directorios de trabajo de los usuarios.

- */var*, contiene los directorios y archivos de supervisión del sistema (monitorización, archivos de correo, archivos de seguridad, etc.).

- */var/spool*, contiene los directorios de los archivos temporales del spooling[4].
    - */var/spool/lp*, para los archivos de impresoras.
    - */var/spool/mail*, para los correos de los usuarios.
- */var/adm*, */var/*log contiene archivos de registro y contabilidad del sistema.
- */var/tmp*, contiene archivos temporales.

♦ */usr*, directorio que contiene los directorios accesibles al usuarios.

- */usr/bin*, contiene algunos programas ejecutables y utilidades del sistema operativo.
- */usr/sbin*, contiene bastantes programas ejecutables para la administración del sistema.
- */usr/lib*, contiene librerías para programas y lenguajes de programación (C, C++, Perl, etc.).
- */usr/share/man*, */usr/*man contiene los archivos de las paginas man.
- */usr/doc*, */usr/info* contiene la documentación de los programas.
- */usr/X11R6* contiene el entorno gráfico de usuario (versión 11 Release 6), más conocido como X-Windows.

[4] El *spooling* consiste en salvar copias de los archivos para un posterior procesamiento.

2.2 WINDOWS NT

Windows es un sistema operativo multitarea de 32 bits y multiusuario, desarrollado por Microsoft, cuyas características más importantes son:

- *Fiabilidad*. Gracias a la utilización de un modelo cliente/servidor interno, un modelo plana de 32 bits, un modelo multitarea preferente y el sistema de ficheros NTFS.

- *Rendimiento*. Debido a que fue diseñado en 32 bits, tiene características de multitarea y multiproceso y su soporte de CPU RISK.

- *Portabilidad*. Ya que utiliza una arquitectura de micro-kernel modular y un sistema de archivos configurables.

- *Compatibilidad*. Soporta aplicaciones MS-DOS, Windows 3.x, Windows 95, POSIX y OS/2 1.X.

- *Escalabilidad*. Gracias a que soporta multiplataforma y multiprocesador.

- *Seguridad*. Utiliza un modelo de seguridad de dominio, un sistema de archivos de NTFS. Windows NT tiene la certificación C2, obtenido del gobierno de EEUU. Además posee características de tolerancia a fallos y la entrada al sistema con CTRL + ALT + DEL.

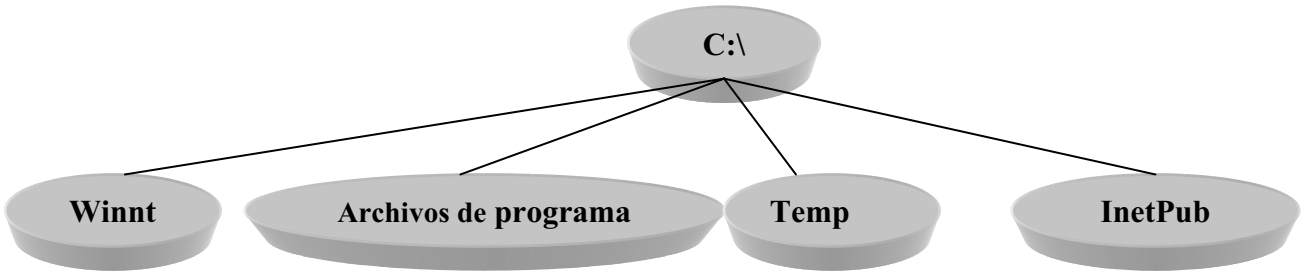
2.2.1 VERSIONES

Tanto para Windows NT 3.51 como para Windows NT 4.0 existen dos versiones: Server y Workstation. Tanto la versión Server como Workstation en la 4.0 poseen las mismas características de seguridad y de entorno. Aunque ambas poseen servicios de red, la Workstation sólo permite compartir directorios e impresoras (P2P), mientras que la versión Server permite la administración de la red basadas en servidores. En la siguiente tabla se muestran algunas de sus características:

CARACTERÍSTICAS	SERVER	WORKSTATION
Máx. nº de procesadores	32	2
Nº máx de conexiones en red	Ilimitado	10
Servidor de aplicaciones en la red	Si	No
Nº máx. RAS simultáneos	256	1

2.2.2 ESTRUCTURA DE DIRECTORIOS

En este sistema operativo como en el anterior implementan la organización de los ficheros con grafos acíclicos. A continuación se muestra la estructura que tiene Windows NT:



- *C:*, directorio raíz del sistema de archivos.
- *C:\Winnt*, directorio donde se ubica el sistema operativo
  - *C:\Winnt\system32*, contiene algunos programas ejecutables y utilidades del sistema operativo de 32 bits.
  - *C:\Winnt\system*, contiene algunos programas ejecutables y utilidades del sistema operativo.
  - *C:\Winnt\Config*, contiene algunos de los ficheros de configuración.
  - *C:\Winnt\Fonts*, directorio que contiene las fuentes.
  - *C:\Winnt\Repair*, directorio que contiene los ficheros que copia cuando crea el disco de reparación

- *C:\Winnt\Profiles*, directorio que contiene la información de las cuentas (escritorio, datos de programas, etc.)

♦ *C:\Archivos de programa*, directorio en el cual se instalan las aplicaciones

♦ *C:\Temp*, directorio donde se crean los ficheros temporales.

♦ *C:\InetPub*, directorio que contiene la información de los servicios de red (gopher, web, ftp, etc.)

2.3 WINDOWS 2000

Windows 2000 es producto de la evolución natural del Windows NT 4.0, de ahí que permanezca parte del núcleo. Incluye mejoras para los servicios de red, web y aplicaciones. Además, suministra una mayor compatibilidad, escalabilidad y reduce los costos de computación mediante unos servicios de administración eficaces y flexibles.

2.3.1 VERSIONES

En Windows 2000 existen dos versiones: Server y Workstation. Tanto la versión Server como Workstation poseen las mismas características de seguridad y de entorno. Aunque ambas poseen servicios de red, la Workstation sólo permite compartir directorios e impresoras (P2P), mientras que la versión Server permite la administración de la red basadas en servidores. Dentro del Windows 2000 Server nos encontramos 3 versiones:

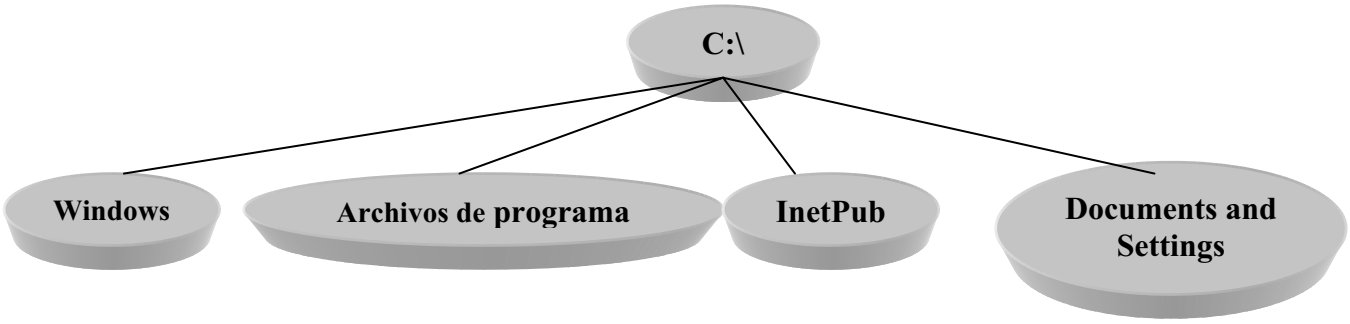
- Windows 2000 Server, que es el sucesor del Windows NT 4.0 Server. Está pensado para su uso como mainstream de trabajo en grupo y como servidor de departamento.

- Windows 2000 Advanced Server es el sucesor de Windows NT 4.0 Server Enterprise. Está pensado como servidor de servidor de rango medio.

- Windows 2000 Datacenter Server ofrece los niveles más altos en rendimiento.

2.3.2 ESTRUCTURA DE DIRECTORIOS

Tanto este sistema operativo como en el anterior implementan la organización de los ficheros con grafos acíclicos. A continuación se muestra la estructura que tiene Windows 2000:



- *C:*\, directorio raíz del sistema de archivos.

- *C:**Windowst*, directorio donde se ubica el sistema operativo:

  - *C:**Winnt**system32*, contiene algunos programas ejecutables y utilidades del sistema operativo de 32 bits.

  - *C:**Winnt**system*, contiene algunos programas ejecutables y utilidades del sistema operativo.

  - *C:**Winnt**Config*, contiene algunos de los ficheros de configuración.

- *C:\Winnt\Fonts*, directorio que contiene las fuentes.

- *C:\Winnt\Repair*, directorio que contiene los ficheros que copia cuando crea el disco de reparación.

♦ *C:\Archivos de programa*, directorio en el cual se instalan las aplicaciones.

♦ *C:\Documents and Settings*, directorio que contiene la información de las cuentas (escritorio, datos de programas, etc.).

♦ *C:\InetPub*, directorio que contiene la información de los servicios de red (gopher, web, ftp, etc.).

2.4 WINDOWS XP

Windows XP es un sistema operativo de la empresa Microsoft. Integra la base de códigos de Windows NT y Windows 2000, que presenta una arquitectura informática de 32 bits y un modelo de memoria protegida. También integra los puntos fuertes de Windows 2000 (seguridad, confiabilidad, etc.) con las mejores características de Windows 98 y Windows Me (Plug & Play, interfaz de usuario más sencilla, etc.). Algunas de las características más relevantes son:

- Los escenarios de reinicio se han reducido notablemente.

- Protección de los archivos principales del sistema sobre la sobreescritura por la instalación de aplicaciones.

- Incorpora IPSec permitiendo transmitir datos de forma segura a través de las redes.

- Tiene soporte para las tarjetas inteligentes también conocidas como Smart Cards.

2.4.1 VERSIONES

En la actualidad nos encontramos con dos versiones: Professional basado en tecnología NT y la Home. La primera es la evolución de Windows 2000 Professional mientras que la segunda sustituye a Windows Me. Nosotros nos centraremos en los sistemas basados en tecnología NT.

2.4.2 ESTRUCTURA DE DIRECTORIOS

La estructura de directorios de este sistema operativo es similar a Windows 2000. Véase sección 2.3.2

2.5 SISTEMAS DE GESTIÓN

Un sistema de gestión es una aplicación[5] de base de datos que presenta datos de forma útil, introduce o actualiza información en la base de datos, además de realizar operaciones con dichos datos.

Hay muchas maneras de desarrollar sistemas de gestión mediante la programación con C, C++, Pascal, COBOL, Delphi, etc. y la utilización de base de datos Infomix, Oracle, SQL Server, Access, etc. También se pueden desarrollar con los generadores de aplicaciones que han sacado las casas de bases de datos.

Por tanto, debido a la gran variedad de posibilidades a la hora de desarrollar sistemas de gestión, no vamos a explicar de una manera concisa esta cuestión. Aunque, si explicaremos de una manera genérica sacando los puntos comunes en todos ellos así como, los problemas que nos solemos encontrar por no cumplir las medidas de seguridad.

[5] Una aplicación es un programa que realiza una tarea

2.6 DERECHOS DE AUTOR

2.6.1 LA PROPIEDAD INTELECTUAL DEL SOFTWARE

Los derechos que el autor tiene sobre su obra o creación están protegidos en nuestra legislación bajo el régimen jurídico de la Propiedad Intelectual. En concreto, el artículo 10 de la Ley de Propiedad Intelectual Española dispone que *"son objeto de propiedad intelectual todas las creaciones originales literarias, artísticas o científicas expresadas por cualquier medio o soporte, tangible o intangible, actualmente conocido o que se invente en el futuro"*. Seguidamente, dicho artículo enumera las obras o creaciones específicas protegidas bajo este ámbito (libros, obras artísticas, etc.). Entre ellas, el apartado i) incluye a los programas de ordenador como susceptibles de ser protegidos bajo esta regulación.

Por tanto, el software en nuestro país se protege igual que una obra literaria o artística, en contra de otros países en los que se protege como una invención o patente, dentro del otro régimen referido a la Propiedad Industrial. En nuestra opinión, estimamos que el Régimen de la Propiedad Intelectual es mucho más beneficioso para el programador que el de Patentes. En el primer caso, el autor del programa adquiere los derechos sobre el mismo desde el momento en que introduce las líneas de código en el ordenador. Sin embargo, en el segundo caso no tiene los derechos sobre su creación hasta que lo registra como patente en el organismo competente.

Profundizando más, el Régimen Jurídico de la Propiedad Intelectual garantiza unos "derechos morales" del autor que son inalienables, aunque se cedan los derechos para usar o comercializar el programa. Estos derechos son: el de paternidad de la obra y el de modificación de la misma. De este modo, el autor o programador tendrá siempre el derecho a ser reconocido como tal en los "créditos" del programa o en su "Copyright". De igual modo, toda modificación o alteración de la obra que pueda menoscabar su prestigio o dignidad como autor deberá contar siempre con su aprobación.

Estos derechos pervivirán, como decíamos, aunque se transmitan o cedan a un tercero los llamados "derechos patrimoniales" sobre el programa, como son el derecho de

reproducción, el de distribución, el de comunicación pública o el de transformación del programa de ordenador, algunos de los cuales veremos más adelante.

Tradicionalmente, los programas informáticos se vienen elaborando por uno o varios programadores que trabajan para una compañía de software. Esta empresa se reserva todos los derechos patrimoniales o de explotación de la obra, a cambio de una remuneración a los programadores por su trabajo. Los programas creados se comercializan por la compañía en el mercado y podrá, a su vez, modificarlos o actualizarlos posteriormente, rentabilizando a su vez dichas actualizaciones.

En este tipo de programación y comercialización del software generalmente denominado como "Software Propietario", el código fuente del programa nunca se hace público, permaneciendo dentro de la compañía bajo acceso exclusivo de los empleados programadores.

Cumpliendo este sistema, nos encontramos con la mayor parte del software producido en el mundo, principalmente bajo el entorno Windows o Macintosh. Las empresas más conocidas en este sector son Microsoft, Apple, Compaq, Corel o Adobe entre otras.

2.6.2 UN SISTEMA ALTERNATIVO: LOS DERECHOS DE AUTOR EN LINUX

Actualmente ha surgido una fórmula alternativa de programación, con ocasión de la aparición y posterior desarrollo de los sistemas operativos compatibles con UNIX y, más concretamente, con la explosión de Linux. Este nuevo sistema está revolucionando el modo de entender y explotar los derechos de autor sobre el software en todo el planeta.

Para poder entender este sistema *"sui generis"* es necesario hacer referencia a los orígenes de Linux. Tal y como hemos visto al comienzo del capítulo, este sistema operativo surgió a partir de un proyecto lúdico de Linus Torvald. Este programador decidió hacer público su software en Internet y solicitar la participación de cualquiera para su

desarrollo. Así, Linux creció como un trabajo colectivo y desinteresado de cientos y luego de miles de programadores que contribuyeron a su definición y desarrollo posterior.

De este modo, no se puede hablar de un único autor o de un colectivo agrupado bajo una única empresa propietaria de los derechos de explotación, sino de un programa "casi" (y luego veremos porqué lo de "casi") de dominio público al que cualquiera que lo desee puede acceder, copiar, modificar y usar de una forma libre y casi gratuita.

¿Quiere esto decir que Linux carece de derechos de autor? Pues hemos de decir que no. A pesar de estas especiales características, Linux no es un programa "de dominio público" (es decir, totalmente "libre") desde un punto de vista jurídico. A continuación veremos por qué:

2.6.2.1 LA LICENCIA PÚBLICA GNU

Este nuevo sistema de creación, uso y modificación del software, no sólo se limita al sistema operativo de Linux, sino que se aplica también a muchos de los programas informáticos desarrollados para este entorno. Esta nueva política de programación se recoge principalmente bajo la llamada GNU General Public License (GNU GPL), que es una licencia pública creada por la Free Software Foundation bajo el proyecto "Gnu No es Unix", y cuya última versión data de junio de 1991.

En realidad, cabe decir que el proyecto Gnu No es Unix (GNU), sobre el que se basa esta licencia, es anterior al propio Linux ya que nació en 1983 con la misma filosofía de "software libre" que este último, pero no es hasta el desarrollo de este sistema operativo cuando esta licencia alcanza su pleno apogeo y llega a convertirse en el régimen de explotación de derechos de los programas, alternativo al *tradicional* del "software propietario" a nivel mundial.

Pasando a analizar el contenido de esta licencia pública GNU, sus dos objetivos fundamentales son:

1) Proteger el software bajo "Copyright".

2) Dar el permiso legal para copiar, distribuir y/o modificar el software libremente.

En definitiva, cuando la licencia habla de “software libre” está haciendo referencia a libertad, no a precio. Estas Licencias Públicas Generales están diseñadas para asegurar que se tenga la libertad de distribuir copias de software libre (y cobrar por ese servicio si quiere), que se reciba el código fuente o que pueda conseguirse, si se quiere, que se pueda modificar el software o usar fragmentos de él en nuevos programas libres y que se sepa que se pueden hacer todas estas cosas.

A efectos de la legislación española, lo que se pretende es conservar intactos los derechos morales sobre la obra y permitir la libre explotación por terceros de los derechos patrimoniales siempre y cuando se cumplan una serie de condiciones recogidas expresamente en la licencia. Por ejemplo, si se distribuyen copias de uno de estos programas, sea gratuitamente o a cambio de una contraprestación, se debe dar a los receptores todos los derechos que se tienen sobre la misma. Se debe asegurar que ellos también reciben, o pueden conseguir, el código fuente del programa. Y se deben mostrar estas condiciones de forma que conozcan sus derechos.

Para una exposición más clara, pasaremos a exponer los derechos de explotación conferidos por la licencia y, a continuación, las obligaciones o limitaciones a los mismos.

2.6.2.2 DERECHOS CONFERIDOS POR LA LICENCIA PÚBLICA GNU:

Esta licencia *pública* afecta exclusivamente a los derechos de reproducción, distribución y transformación de la obra. Cualquier otra actividad distinta de éstas no está cubierta por esta *licencia*, está fuera de su ámbito. El acto de ejecutar el programa no está restringido y los resultados del programa están cubiertos únicamente si sus contenidos constituyen un trabajo basado en el programa, independientemente de haberlo producido mediante la ejecución del programa. El que esto se cumpla, depende de lo que haga el programa.

2.6.2.2.1 DERECHO DE REPRODUCCIÓN:

El derecho de reproducción viene definido en el artículo 18 de nuestra Ley de Propiedad Intelectual, el cual afirma que *"se entiende por reproducción la fijación de la obra en un medio que permita su comunicación y la obtención de copias de toda o parte de ella"*.

En la licencia pública GNU, este derecho confiere la capacidad de realizar copias del programa de ordenador en cualquier soporte y sin una limitación cuantitativa de las mismas.

2.6.2.2.2 DERECHO DE DISTRIBUCIÓN:

El artículo 19 de la LPI dispone que "se entiende por distribución la puesta a disposición del público del original o copias de la obra mediante su venta, alquiler, préstamo o de cualquier otra forma".

De este modo, la licencia nos permite distribuir libremente las copias del programa de ordenador bien gratuitamente o bien, incluso, cobrando un precio. Se entiende que solo cobraremos por el servicio de copia y por los soportes que aportemos, así como por manuales o documentación propia que incluyamos con el programa.

En caso de que se aporte algún otro servicio con el software, como es la asistencia técnica sobre el mismo o una garantía supletoria, también podremos incluirlo en el precio del producto.

2.6.2.2.3 DERECHO DE MODIFICACIÓN O TRANSFORMACIÓN:

Este derecho se regula en el artículo 21 de la LPI, el cual dispone que *"la transformación de la obra comprende su traducción, adaptación y cualquier otra modificación en su forma de la que se derive una obra diferente."*

El párrafo 2 de este precepto afirma que *"los derechos de propiedad intelectual de la obra resultante de la transformación corresponderán al autor de esta última, sin perjuicio de los derechos del autor de la obra preexistente".*

Así, la Licencia Pública GNU permite la modificación o transformación del programa completo o bien de una porción del mismo, formando una nueva creación o trabajo basado en él. De igual modo, autoriza a la libre reproducción y distribución de la nueva obra siempre y cuando se realice de acuerdo a la forma ya vista.

Dicha modificación, además, deberá cumplir con las condiciones y limitaciones impuestas en la licencia, que veremos a continuación.

2.6.2.3 CONDICIONES Y LIMITACIONES DE LA LICENCIA PÚBLICA GNU:

2.6.2.3.1 CONDICIONES PARA LA REPRODUCCIÓN Y DISTRIBUCIÓN DEL SOFTWARE:

La libertad para copiar y distribuir el software, bien sea el original o el modificado, incorpora la obligación de, además de lo señalado anteriormente, cumplir las siguientes condiciones:

a) Cualquier distribución del programa o de una modificación del mismo debe garantizar la libertad de reproducirla, distribuirla y modificarla libremente a su vez, en los mismos términos establecidos en la Licencia Pública GNU. De este modo, no podrá imponer al receptor ninguna restricción más sobre el ejercicio de los derechos aquí garantizados. Asimismo, se señala que el distribuidor no será responsable de hacer cumplir esta licencia por terceras partes.

b) Aportar o hacer accesible el código fuente del programa, mediante el cumplimiento de al menos una de las siguientes condiciones:

    a) Acompañarlo con el código fuente completo correspondiente, en formato electrónico, que debe ser distribuido en un medio habitualmente utilizado para el intercambio de programas.

b) Acompañarlo con una oferta por escrito, válida durante al menos tres años, de proporcionar a cualquier persona que lo reclame una copia completa en formato electrónico del código fuente correspondiente, a un coste no mayor que el de realizar físicamente su copia y su envío en un medio habitualmente utilizado para el intercambio de programas.

c) Acompañarlo con la información que se recibió ofreciendo distribuir el código fuente correspondiente. Esta opción se permite sólo para distribución no comercial y sólo si se recibió el programa como código objeto o en formato ejecutable, de acuerdo con el apartado anterior.

El código fuente de un programa es el conjunto de las líneas de programación en modo texto, escritas en el lenguaje correspondiente, antes de ser compiladas para crear el fichero ejecutable.

A los efectos de la Licencia Pública GNU, por “código fuente de un trabajo” se entiende la forma preferida del trabajo cuando se le hacen modificaciones. Para un trabajo ejecutable, se entiende por “código fuente completo” todo el código fuente para todos los módulos que contiene, más cualquier fichero asociado de definición de interfaces, más los guiones utilizados para controlar la compilación e instalación del ejecutable.

Como excepción especial a esta obligación, el código fuente distribuido no necesita incluir nada que sea distribuido normalmente (bien como fuente, bien en forma binaria) con los componentes principales (compilador, kernel y similares) del sistema operativo en el cual funciona el ejecutable, a no ser que el propio componente acompañe al ejecutable.

2.6.2.3.2. CONDICIONES PARA LA MODIFICACIÓN DEL SOFTWARE:

El derecho a la libre modificación o transformación del software bajo esta licencia pública está limitado por el cumplimiento de las siguientes condiciones:

1) Los ficheros modificados deberán incorporar anuncios prominentes indicando que esta circunstancia, su autor y la fecha en que se introdujeron los cambios.

2) Los derechos y condiciones de uso de las modificaciones producidas deberán cumplir con la Licencia Pública GNU, no pudiendo limitarse bajo ningún concepto, más allá de lo señalado en dicha licencia.

3) Si el programa modificado lee normalmente órdenes interactivamente cuando es ejecutado, debe hacer que, cuando comience su ejecución para ese uso interactivo de la forma más habitual, muestre o escriba un mensaje que incluya un anuncio de Copyright y de que no se ofrece ninguna garantía (o, por el contrario, que sí se ofrece garantía) y que los usuarios pueden redistribuir el programa bajo estas condiciones e indicando al usuario cómo ver una copia de esta licencia. (Excepción: si el propio programa es interactivo, pero normalmente no muestra ese anuncio, no se requiere que su trabajo basado en el programa muestre ningún anuncio).

Estos requisitos se aplican al trabajo modificado como un todo. Si partes identificables de ese trabajo no son derivadas del programa, y pueden, razonablemente, ser consideradas trabajos independientes y separados por ellos mismos, entonces esta licencia y sus términos no se aplican a esas partes cuando sean distribuidas como trabajos separados. Pero cuando distribuya esas mismas secciones como partes de un todo que es un trabajo basado en el programa, la distribución del todo debe ser según los términos de esta licencia, cuyos permisos para otros licenciatarios se extienden al todo completo y, por lo tanto, a todas y cada una de sus partes, con independencia de quién la escribió.

2.6.2.2.3 AUSENCIA DE GARANTÍA

Por último, cabe señalar que los programas protegidos bajo esta Licencia Pública GNU, debido a que pueden ser alterados y distribuidos un número indefinido de veces, deberán incorporar una cláusula especial de exoneración de responsabilidad de los programadores y de ausencia de garantía del mismo frente a posibles defectos o mal

funcionamiento del mismo y frente a posibles daños o perjuicios derivados de su utilización por parte del usuario.

A pesar de esta limitación, el programador o distribuidor, si lo estima oportuno, puede incluir algún tipo de *garantía* o *asistencia* respecto a sus modificaciones o distribuciones del producto (o respecto a todo el paquete). Tal y como hemos comentado anteriormente, por estos servicios y prestaciones extras que se aportan al software se puede percibir, y normalmente se hace, una contraprestación económica para su prestación.

3

Seguridad Física

En este capitulo trataremos todo lo concerniente a seguridad física en sistemas. Aunque el Reglamento de medidas de seguridad no dice nada en cuanto a este tema en el nivel básico, nosotros creemos que es fundamental por varios motivos. Pero la razón fundamental es que los sistemas centralizados (que son los que se usan la mayoría de las veces), el servidor que tiene la información no se le da la importancia que se le debiera en cuanto a este tema. También, trataremos cómo realizar el registro de incidencias y que debe de contener.

Por tanto veremos:

¿Cómo realizar un plan de seguridad física?
Acceso Físico.
Posibles amenazas a los sistemas en las salas donde están.
Registro de incidencias.

3.1 ¿CÓMO REALIZAR UN PLAN DE SEGURIDAD FÍSICA?

Para la realización de un plan de seguridad tendremos que plantearnos, a priori, las siguientes cuestiones:

- ¿Proporciono la suficiente protección para el grado de importancia de la información que tengo en los sistemas informáticos?

- Cuantificar las perdidas que se producirían si por accidente, error o mal intención el sistema o la información se destruye.

- ¿Proporciono la suficiente seguridad que la legislación vigente me marca para la importancia que tiene la información que se maneja.

- ¿Qué imagen daría si alguien entra en el sistema?

Una vez hechas estas preguntas, ya estaríamos preparados para realizar una descripción:

- Del lugar que se debe proteger, así como su entorno enumerando y describiendo sus puntos débiles y fuertes.

- De las defensas posibles y la manera de implementarla, así como su coste.

Para la realización sería interesante utilizar una herramienta potente y muy utilizada en ingeniería: la matriz D.A.F.O. (Debilidades Amenazas Fortalezas Oportunidades). Se trata de determinar todas las debilidades y las fortalezas de la cuestión objeto de análisis. Una vez enumeradas y descritas, hay que intentar pasar las debilidades a fortalezas y las amenazas a oportunidades.

3.2 ACCESO FÍSICO

Los sistemas deben estar en salas protegidas en donde el acceso sea restringido. Las paredes deberán ser sólidas, sin ventanas y los conductos del aire acondicionado o del climatizador deberán ser de un tamaño pequeño para que ninguna persona pueda acceder por ellos.

3.3 POSIBLES AMENAZAS A LOS SISTEMAS EN LA SALA DONDE ESTÁN

Los sistemas informáticos y/o telemáticos son sensibles a las condiciones que les rodea pudiendo causar la destrucción de los mismos. Las causas pueden ser muy diversas:

- *Temperaturas extremas*. Normalmente los sistemas toleran rangos entre 10ºC a 32ºC.

- *Incendios*. Son nefastos por dos motivos principalmente: destruyen todo donde estén y la manera de apagarlos puede también destruir los sistemas.

- *Humo*. Potente abrasivo que suele dañar los discos magneticos.

- *Agua*. Produce cortocircuitos en los sistemas electrónicos.

- *Humedad*. Tiene un punto a favor y otro en contra. La humedad es favorable por prevenir las cargas eléctricas, pero puede llegar a ser muy perjudicial por producir cortocircuitos si existe una gran cantidad de humedad.

- *Polvo*. Son nefastos por dos motivos: es menos abrasivo que el humo, pero lo suficiente para provocar cortocircuitos.

- *Explosiones*.

- *Vibraciones*. Pueden desconectar circuitos o estropear discos.

- *Tormentas*. Si no cuenta con un SAI puede producir desde un corte hasta quemar los sistemas.

- *Ruido eléctrico*. Consistente en picos de sobretensión, puede quemar el sistema.

- *Animales*. Pueden causar numerosos daños por su predilección por las corrientes.

3.4 REGISTRO DE INCIDENCIAS

En el art. 10 del Reglamento de medidas de seguridad nos obliga a tener un procedimiento de notificación y gestión de incidencias. Dicho procedimiento contendrá un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, la persona que realiza la notificación, a quién se le comunica y los efectos que se hubieran derivado de la misma.

4

Identificacion y Autentificación

Artículo 11. Identificación y autenticación.

1. El responsable del fichero se encargará de que exista una relación actualizada de usuarios que tengan acceso autorizado al sistema de información y de establecer procedimientos de identificación y autenticación para dicho acceso.

2. Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.

3. Las contraseñas se cambiarán con la periodicidad que se determine en el documento de seguridad y mientras estén vigentes se almacenarán de forma ininteligible.

4.1 ACCESO LÓGICO

4.1.1 LINUX

La manera que tiene Linux de guardar la información de acceso lógico es decir, nombre de entrada[1] y una contraseña[2], es mediante dos formas ambas de ellas utilizando el método criptográfico DES y MD5.

Aunque existen dos maneras sólo se va a explicar y recomendar el uso de uno porque es la que pasa los apartados 2 y 3 del artículo 11 del Reglamento de Medidas de Seguridad.

Con el paquete *Shadow* habrá dos ficheros que contengan la información. Uno de ellos es el */etc/passwd* con acceso de lectura para todo el mundo. Un ejemplo del fichero seria:

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:100:sync:/bin:/bin/sync
games:x:5:100:games:/usr/games:/bin/sh
man:x:6:100:man:/var/catman:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/spool/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
majordom:x:30:31:Majordomo:/usr/lib/majordomo:/bin/sh
postgres:x:31:32:postgres:/var/postgres:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
operator:x:37:37:Operator:/var:/bin/sh
list:x:38:38:SmartList:/var/list:/bin/sh
irc:x:39:39:ircd:/var:/bin/sh
ftp:x:100:50::/home/ftp:/bin/false
nobody:x:65534:65534:nobody:/home:/bin/sh
esper:x:1000:100:José Luis Rivas López:/home/esper:/bin/bash
objetivo4:x:1001:100:Santiago Rivas Alvarez:/home/objetivo4:/bin/bash
obj4:x:1002:100:Enrique Perez Rodriguez:/home/obj4:/bin/bash
jperez:x:1003:103:Josefina Perez Alvarez:/home/jperez:/bin/bash
baco:x:1004:104:Baco:/home/baco:/bin/bash
```

[1] Login

[2] Password

Como se puede observar los campos del fichero se separan por ":" y a continuación se describen su significado:

CAMPO	CONTENIDO
esper	El nombre de entrada (login) del usuario
x	Si este campo tiene una "x" significa que la contraseña se encuentra en el fichero */etc/*shadow. Por el contrario estaría la contraseña encriptada para ese nombre de entrada. El valor adecuado por la seguridad del sistema deberá ser un "x"
1000	El número de identificación del usuario (UID)
100	El número de identificación del grupo (GID) del usuario
José Luis Rivas López	El nombre completo del usuario
/home/esper	El directorio de trabajo del usuario
/bin/bash	El interprete de ordenes (shell) del usuario

El otro fichero que es donde guarda Linux la información de las contraseñas es */etc/shadow*. Un ejemplo de dicho fichero se muestra a continuación:

```
root:04YrFfi9SuUOY:11034:0:99999:7:::
daemon:*:10737:0:99999:7:::
bin:*:10737:0:99999:7:::
sys:*:10737:0:99999:7:::
sync:*:10737:0:99999:7:::
games:*:10737:0:99999:7:::
man:*:10737:0:99999:7:::
lp:*:10737:0:99999:7:::
mail:*:10737:0:99999:7:::
news:*:10737:0:99999:7:::
uucp:*:10737:0:99999:7:::
proxy:*:10737:0:99999:7:::
majordom:*:10737:0:99999:7:::
postgres:*:10737:0:99999:7:::
www-data:*:10737:0:99999:7:::
backup:*:10737:0:99999:7:::
operator:*:10737:0:99999:7:::
list:*:10737:0:99999:7:::
irc:*:10737:0:99999:7:::
ftp:!:10737:0:99999:7:::
nobody:*:10737:0:99999:7:::
esper:/36NMQjtSbMNg:10737:0:99999:7:::
objetivo4:8s11rz/eF7bI.:10737:0:99999:7:::
obj4:Tjvn9S6LP1IE6:10737:0:99999:7:::
jperez:01aK1FxKE9YVU:10737:0:99999:7:::
baco:/EJT5jjsow9Yg:10737:0:99999:7:::
```

Igual que el fichero */etc/*passwd los campos estan separados por ":". Los campos que componen dicho fichero se enumeran a continuación:

- Login.

- Contraseña encriptada.
- El número de días desde el 1 de Enero de 1.970 en el cual la contraseña ha sido cambiada.
- El número de días que faltan para que se le permita al usuario cambiar su contraseña.
- El número de días que faltan para que el usuario sea forzado a cambiar su contraseña.
- El número de días que se avisa al usuario de que su contraseña ha de ser cambiada.
- El número de días en los que el usuario debe cambiar su contraseña antes de que la cuenta sea desactivada.
- El número de días, desde el 1 de enero de 1970, que la cuenta lleva desactivada.
- Queda reservado.

Este paquete trae nuevos comandos que se van a describir a continuación[3]:

PROGRAMA	*FUNCIÓN*
chage	Se utiliza para cambiar el tiempo de caducidad
chfn	Permite a los usuarios cambiar su información del comando finger
chsh	Permite cambiar a los usuarios su shell predefinido
gpasswd	Permite añadir nuevos usuarios a un grupo
groupadd	Permite crear nuevos grupos
groupdel	Permite borrar un grupo
groupmod	Permite cambiar la información de un grupo
id	Muestra tu actual UID y la información relacionada
newgrp	Permite a los usuarios cambiarse de un grupo a otro durante la misma sesión o después

[3] Algunos de ellos no vienen con ciertas distribuciones para saber cuales se tiene basta con teclear *man –k shadow*

	de entrar en el sistema otra vez
passwd	Para cambiar la contraseña ya existente o para escribirla por primera vez
pwconv	Se usa para pasar los datos de */etc/passwd* a */etc/shadow*
pwunconv	Se usa para pasar los datos de */etc/shadow* a */etc/passwd*
su	Te permite correr una shell de un usuario distinto sin tener que salir de tu entrada al sistema
useradd	Añade un nuevo usuario
userdel	Permite borrar usuarios
usermod	Permite cambiar la información de un usuario

En las nuevas versiones además se incorpora PAM (Pluggable Autentification Method), un marco genérico para la gestión de autenticación, control de cuentas, sesiones y gestión de cuentas definido mediante el RFC 86.0 de la Open Software Foundation. En la siguiente tabla se muestra algunos módulos:

MODULO	**DESCRIPCIÓN**
pam_access	Definirá un estilo para el log de acceso.
pam_deny	Devuelve siempre un valor de fallo. Es interesante para la realización de un fichero muy restrictivo.
pam_nologin	Limitaremos el acceso al sistema
pam_permit	Devuelve siempre un valor de acierto. En caso de estar en la autentificación recibe el nombre de usuario.
pam_securetty	Limitaremos los terminales seguros
pam_time	Este módulo permite que restrinja la franja horario para el acceso a un servicio.
pam_unix	Es el módulo estándar de los sistemas Unix (*/etc/passwd* y */etc/shadow*)

4.1.2 WINDOWS NT

Windows NT guarda la información del acceso lógico en el archivo SAM (Security Accounts Manager). Por tanto, dicho fichero equivale al */etc/passwd* en los sistemas Unix. La SAM utiliza un algoritmo de hashing (encriptación en un solo sentido) y conforma uno de los cinco grupos del Registro y está localizada en el archivo *%systemroot%system32\config\sam*. El algoritmo de cifrados es el MD4 (Message Digest 4).

A partir del Service Pack 3 de NT, Microsoft permitió añadir otra capa de cifrado llamada *SYSKEY* (System Key) obteniendo así una clave de 128 bits. El *SYSKEY* se almacena de la tres maneras mostradas en la siguiente tabla:

MODO	DESCRIPCIÓN
1 (por defecto)	Se almacena en el Registro y se hace disponible al arrancar de un modo automático
2	Se almacena en el Registro y se hace disponibles al arrancar después de facilitar una contraseña
3	Se almacena en un disquete que debe ser introducido al arrancar

4.1.3 WINDOWS 2000

En los Windows 2000 autónomos la información de las cuentas y las contraseñas también se guardan en la SAM. Por el contrario, en los controladores de dominio, los datos de las cuentas de usuario se guardan en el Active Directory ubicado en %systemroot%\ntds\ntds.dit. Los hashes se guardaran en el mismo formato, pero con la diferencia que son accesibles por medios diferentes.

4.1.4 WINDOWS XP

Windows XP guarda la información del acceso lógico en el archivo SAM (Security Accounts Manager) como en las versiones anteriores.

4.1.5 SISTEMAS DE GESTIÓN

Los sistemas de gestión realizados con bases de datos del tipo Informix, Oracle, etc. si se configuran y se saben usar utiliza como usuarios y grupos los propios del sistema, así como sus contraseñas por tanto cifradas.

Por el contrario, los creados con bases de datos que no permiten lo antes mencionado emplean para crear usuarios y grupos la creación de tablas con dos campos: login y contraseña. Por desgracia, la gran mayoría de los sistemas de gestión que usan este método no tienen el campo de contraseña cifrado, por lo que no están cumpliendo las Medidas de seguridad 994/99.

Para solventar dicho problema hay diversas soluciones, aunque la más sencilla sería programar un método que cifre el campo contraseñas y luego para autentificar al usuario basta con cifrar la contraseña con el mismo método y comparar las contraseñas.

4.2 LAS CONTRASEÑAS

El apartado 3 del artículo 11 del Reglamento de Medidas de Seguridad dispone que las contraseñas deberán ser cambiadas con la periodicidad que determine el documento de seguridad, es recomendable como mínimo cada par de meses. Aunque no hay nada escrito en la legislación de cómo deben de ser las contraseñas, nosotros daremos una serie de normas. Debido a que una buena contraseña es la base de una buena defensa contra el acceso no autorizado a un sistema.

Una manera sencilla para pensar una contraseña y luego recordarla es a partir de una frase como por ejemplo: ¿Qué película emiten en televisión? La contraseña podría ser ¿Qp.2et#?. Fíjese que en la intercalación de números y caracteres especiales entre las letras, así como intercala letras mayúsculas y minúsculas. Esta intercalación es buena para evitar que las descubran mediante programas informáticos[4].

Muy malas contraseñas son:

- Tengan el mismo login.
- Tengan algún apellido o nombre del usuario de la cuenta, aunque estén seguidos o de números.
- Tengan el nombre de su jefe.
- Tengan el nombre de su ordenador.

Malas contraseñas son aquellas que:

- Tenga información que se obtenga fácilmente sobre usted:
  - Tengan el nombre de los hijos, la mujer, la novia.

[4] Véase apartado 4.2.1

- Tengan el nombre de algún animal que tenga en casa, sus padres, etc.
- Tengan la matricula del coche, moto, etc.
- Tengan el documento nacional de identidad (D.N.I.).
- Tengan el número de la Seguridad Social.
- Tenga el nombre de la calle donde vive, dirección, etc.
- Tenga el número de teléfono de su casa.
- Tengan el nombre alguno de sus mejores amigos.

Medianas contraseñas son aquellas que:

- Pertenezcan a algún diccionario.
- Tengan menos de 6 caracteres.
- Tengan la misma letra o el mismo número.

.

Algunas puntos que habrá que tener en cuenta son:

- No envíe por e-mail nunca su contraseña ni lo deje escrito en algún papel que este cerca del sistema.
- No dé su contraseña a nadie. La seguridad de su contraseña es su responsabilidad. Además, la utilidad de la contraseña es que nadie pueda entrar en su cuenta y dándosela a alguien no lo cumple.

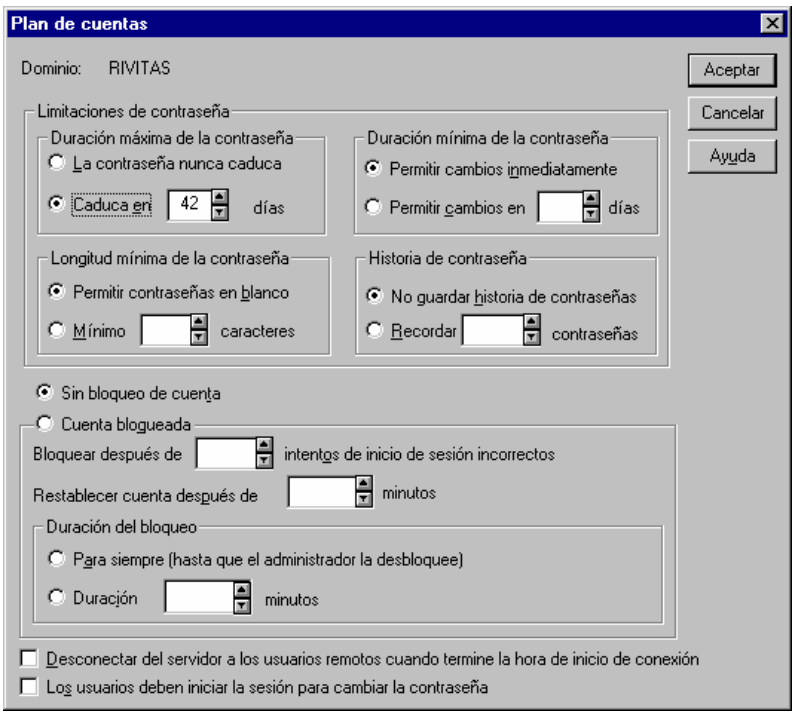
- Si tiene varias cuentas en distintos ordenadores no utilice la misma contraseña, ni parecida. De este modo, si entran en un ordenador no se comprometa la seguridad de los otros.

4.2.1 LINUX

Para configurar las diferentes opciones de las directivas de la contraseña basta con utilizar los programas que están en la tabla de la sección 4.1.1 del paquete *Shadow* y la configuración de los módulos del *PAM*.

4.2.2 WINDOWS NT

Para establecer la seguridad en las cuentas basta con hacer clic en el menú *Directivas* y luego elija *Cuenta* de la ventana "*Administrador de usuarios"* [5].



En la siguiente tabla se muestran las diferentes opciones del cuadro de dialogo:

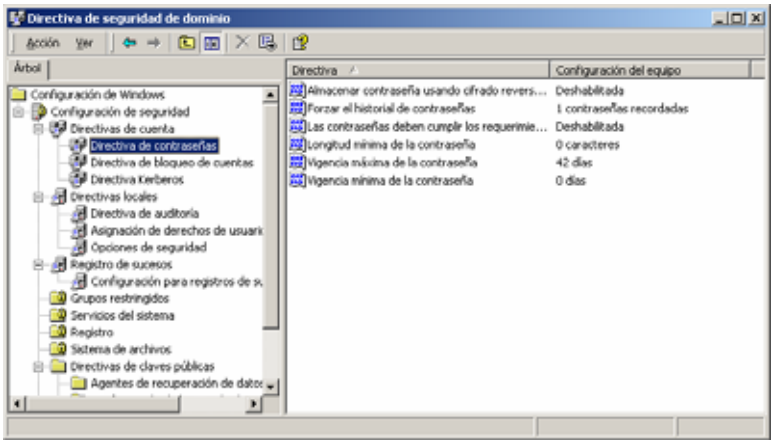
---

[5] Haga clic en *Inicio -> Programas -> Herramientas administrativas (Común) -> Administrador de usuario* para abrir la ventana *Administrador de usuario*

OPCIONES	DESCRIPCIÓN
Dominio	Muestra el nombre del dominio
Duración máxima de la contraseña	Periodo por el cual la contraseña no hace falta que sea cambiada. Su valor oscila entre 1 y 999 días.
Duración mínima de la contraseña	Periodo por el cual la contraseña debe ser usada antes de que el usuario la cambie. Su valor oscila entre 1 y 999 días.
Longitud mínima de la contraseña	Número mínimo de caracteres que puede tener la contraseña. Su valor oscila entre 1 y 14 caracteres.
Historia de la contraseña	Número de contraseñas nuevas que debe usar un usuario antes de poder utilizar una contraseña repetida. Su valor oscila entre 1 y 24 contraseñas.
Sin bloqueo de cuenta	La cuenta no se bloqueará nunca
Cuenta bloqueada	Si se utiliza esta opción nos permitirá definir el número de intentos antes de bloquear una cuenta por introducir mal la contraseña, así como la duración del bloqueo[6].
Desconectar del servidor a los usuarios remotos cuando termine la hora de inicio de conexión	Si está seleccionada, cuando una cuenta de usuario supere sus horas de conexión será desconectado.
Los usuarios deben iniciar la sesión para cambiar la contraseña	Si se activa los usuarios deberán iniciar una sesión antes de cambiar la contraseña.

4.2.3 WINDOWS 2000

Para configurar las diferentes opciones de cómo de deben ser las contraseñas en Windows 2000 basta hacer clic en *Inicio -> Programas -> Herramientas administrativas -> Directiva de seguridad del dominio*. Una vez hecho esto saldrá la siguiente ventana.

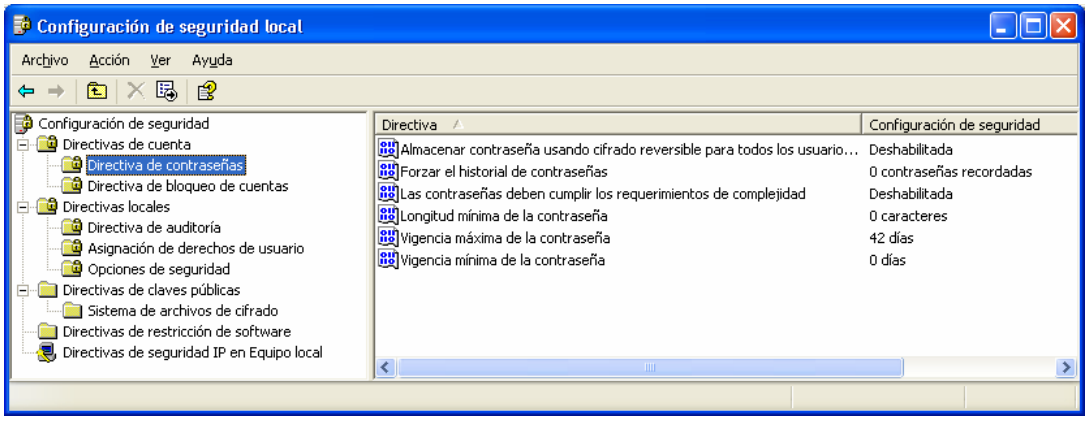


Después haga clic en la opción que desee modificar.

[6] Aunque en el nivel básico no se exige limitar la posibilidad de intentar reiteradamente el acceso no autorizado al sistema como en el nivel medio (art 18.2 del Reglamento de Medidas de Seguridad), es recomendable activarlo.

4.2.4 WINDOWS XP

Para configurar las diferentes opciones de como de deben ser las contraseñas en Windows XP basta hacer clic en *Inicio -> Panel de control -> Herramientas administrativas -> Directiva de seguridad local* . Una vez hecho esto saldrá la siguiente ventana.



Después haga clic en la opción que desee modificar.

4.2.5 DESCUBRIR CONTRASEÑAS MEDIANTE DICCIONARIOS

Desde el punto de vista legal la utilización de este tipo de software puede considerarse ilícita por vulnerar la intimidad de los usuarios. Para evitar en lo posible estos problemas es necesario advertir a los usuarios cuando soliciten el alta en el sistema o cuando firme el contrato. Obviamente que quede todo ello por escrito.

Si se detectase con este tipo de software alguna cuenta se puede bloquear la cuenta hasta avisar al usuario comunicándole que su contraseña no es valida. A continuación se muestra algunos de estos software:

SOFTWARE	UBICACIÓN
Crack	http://www.users.dircon.co.uk/~crypto/index.html
John the Ripper	http://www.bullzeye.net/tools/crackers/john.zip
L0phtcrack	http://www.l0pht.com
Killer Cracker	http://www.giga.or.at/pub/hacker/unix/kc9_11.tar.Z
Lard	http://www.rat.pp.se/hotel/panik/archive/lard.zip
PerlCrack	http://www.netrom.com/~cassidy/utils/pcrack.zip
Xcrack	http://www.netrom.com/~cassidy/utils/xcrack.pl

4.2.6 CHEQUEO DE LAS CONTRASEÑAS ACTIVAMENTE

Este método si que es recomendable desde el punto de vista legal porque cada vez que un usuario tiene que cambiar su contraseña o introducirla por primera vez la comprueba. Prueba si es fácil de descubrir y, si la pasa, se graba en la base de datos. Sino, se la hace repetir hasta que la pase.

SOFTWARE	UBICACIÓN
Passwd+	ftp://ftp.dartmouth.edu/pub/security/
Anlpasswd	ftp://coast.cs.purdue.edu/pub/tools/unix/anlpasswd/
Npasswd	http.//www.utexas.edu/cc/unix/software/npasswd/

4.3 USUARIOS

4.3.1 LINUX

Los usuarios estarán identificados por el sistema operativo por un nombre de entrada (login) y este a su vez por un número que recibe el nombre de UID[7]. Por ejemplo el 0 pertenece al root (superusuario).

4.3.1.1 CREAR UNA CUENTA

Para crear de una cuenta a un usuario se utilizará el comando *useradd*. A continuación se muestra cuales son las opciones:

OPCIÓN	DESCRIPCIÓN
-u [uid]	Especificar el UID del nuevo usuario. No hay un valor predeterminado, si no se añade dicha opción se utiliza el siguiente número disponible.
-g [grupo]	Asigna al usuario al grupo primario al que pertenece.
-G [grupo_adicional]	Asigna al usuario a grupos adicionales
-c [informacion]	Coloca información en el campo de información del usuario. Si info contuviese espacios encierrelos entre comillas “”“.
-d [directorio]	Especifica el directorio de trabajo del usuario
-s [shell]	Especifica el shell de trabajo por defecto del usuario
-k [directorio]	Copia el contenido de directorio en el directorio de trabajo del usuario. Si no se pone esta opción por definición estará */etc/skel*.
-e [fecha_de_caducidad]	Especifica la fecha en la cual la contraseña del usuario caduca. El formato es de la forma MM/DD/AAAA ó March

[7] User Identification Number

	26,2000 (formato largo).
-f [dias_de_inactividad]	Especifica los días en que la cuenta no ha sido usada, después de esos días el sistema la bloquea.

4.3.1.2 CAMBIAR ATRIBUTOS A UNA CUENTA

A lo largo de la vida laboral de un empleado en una misma empresa podrá cambiar sus obligaciones, deberes, cargo, etc.

Para la realización de estos cambios, el usuario no deberá estar conectado mientras se realicen los cambios. Para cambiar los atributos habrá dos comandos. El primero de ellos, *usermod*:

OPCIÓN	DESCRIPCIÓN
-u [uid]	Especificar el UID del nuevo usuario. No hay un valor predeterminado, si no se añade dicha opción se utiliza el siguiente número disponible.
-g [grupo]	Asigna al usuario al grupo primario al que pertenece.
-G [grupo_adicional]	Asigna al usuario a grupos adicionales
-c [informacion]	Coloca información en el campo de información del usuario. Si informacion contuviese espacios enciérrelos entre comillas “”“.
-d [directorio]	Especifica el directorio de trabajo del usuario
-s [shell]	Especifica el shell de trabajo por defecto del usuario
-l [nombre_de_entrada]	Modificamos el nombre de entrada del usuario
-e [fecha_de_caducidad]	Especifica la fecha en la cual la contraseña del usuario caduca. El formato es de la forma MM/DD/AAAA ó March 26,2000 (formato largo).
-f [dias_de_inactividad]	Especifica los dias en que la cuenta no ha sido usada, después de esos días el sistema la bloquea.

El segundo, *chage*:

OPCIÓN	DESCRIPCIÓN
-d [días]	Modifica el número de días contando desde el 1 de Enero de 1970 desde que la contraseña fue cambiada por última vez
-E [fecha de caducidad]	Sirve para modificar la fecha en que la cuenta va a caducar. Se puede expresar en días contando desde el 1 de enero de 1.970
-I [días antes del bloqueo]	Establece cuantos días permanece deshabilitada una cuenta con la contraseña caducada antes de bloquearse
-m [mínimo de días]	Sirve para definir el número de días mínimo entre cambios de contraseña
-M [máximo dedías]	Permite definir el número de días máximo entre cambios de contraseña
-W [días de aviso]	Permiten modificar el número de días que el sistema avisa al usuario de que la contraseña ha de ser cambiada

4.3.1.3 ELIMINAR UNA CUENTA

Para borrar una cuenta del sistema se utiliza el comando *userdel*. Para borrar tanto el usuario como su directorio de trabajo se teclearía:

u*serdel -r nombre_de_entrada*

4.3.1.4 BLOQUEAR UNA CUENTA

Las cuentas se pueden bloquear por diversos motivos: desde qué se ha detectado que un usuario tiene algún problema de seguridad en su cuenta hasta que el usuario va estar de viaje durante un periodo elevado en dónde no va utilizar esa cuenta. Al bloquear la cuenta en estos casos no evitamos que pueda ser usada por personal no autorizado.

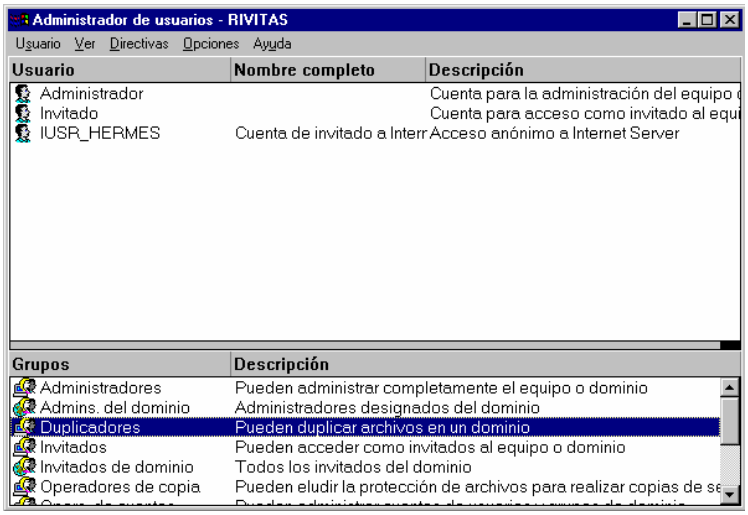
Para bloquear una cuenta habrá que editar el fichero */etc/passwd* y poner en el segundo campo un * como se muestra a continuación:

jlrivas::1100:101: José Luis Rivas López:/home/profesor/jlrivas:/bin/bash*

4.3.2 WINDOWS NT

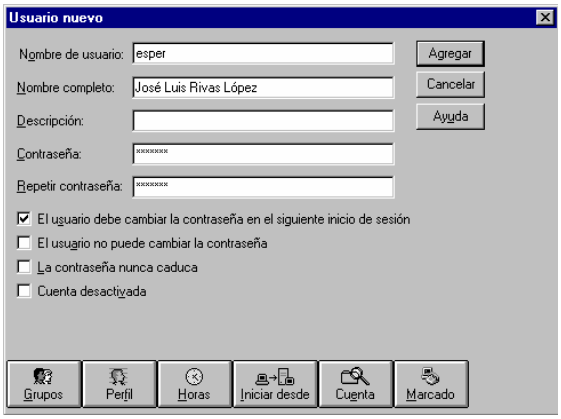
Los usuarios de este sistema están identifican por un SID (Security Identification) que, a diferencia de los sistemas Unix, es ajeno a los administradores. Un ejemplo de un SID sería S-1-1-12-123456789-123456789-12345678-1234.

La herramienta de administración de las cuentas de usuarios y grupos y planes de seguridad es el "*Administrador de usuarios*". Para abrirlo basta con hacer clic en *Inicio -> Programas -> Herramientas administrativas (Común) -> Administrador de usuarios*.



4.3.2.1 CREAR UNA CUENTA

Para la creación de nuevas cuentas basta ir al menú de *Usuario*. Aparecerá un menú desplegable dónde tendrá que elegir *Usuario Nuevo*. Inmediatamente después aparecerá un cuadro de dialogo con el nombre de Usuario Nuevo.



En la tabla se describen los diferentes apartados:

APARTADO	DESCRIPCIÓN
Nombre de usuario	También conocido como login, por tanto es el nombre de entrada en el sistema no pudiendo haber duplicados. No podrá incluir ninguno de los siguientes caracteres "/\:;|=,+*¿?<>
Nombre completo	Introduzca el nombre entero del usuario
Descripción	En este campo se describirá la cuenta
Contraseña	Introducirá la palabra de paso en el sistema. Puede introducir hasta 14 caracteres y diferencia entre mayúsculas y minúsculas
Repetir Contraseña	Sirve como medida de seguridad para comprobar que se ha introducido la contraseña que uno quería y no se ha equivocado al escribrirla
El usuario debe cambiar la contraseña al inicio	Esta opción obligará a cambiar la contraseña al usuario la

de sesión	próxima vez que entre en el sistema
El usuario no puede cambiar la contraseña	Esta opción no permitirá al usuario cambiar la contraseña
La contraseña nunca caduca	Al marcarla la contraseña nunca caducará.
Cuenta desactivada	Deshabilita la cuenta
Grupos	Indicará los grupos a los que pertenece el usuario
Perfil	Asignará un perfil del usuario, un archivo de comandos para inicio de la sesión o un subdirectorio particular para la cuenta del usuario
Horas	Asignará las horas a la que el usuario puede entrar en el sistema
Iniciar desde	Delimitará las estaciones de trabajo desde las cuales el usuario puede iniciar la sesión
Cuenta	Indicará el tipo de cuenta así como la fecha de caducidad
Marcado	Permitirá el uso de *Acceso telefónico a redes* en la cuenta

4.3.2.2 CAMBIAR ATRIBUTOS A UNA CUENTA

Para cambiar los atributos de una cuenta basta con hacer doble clic en la cuenta de usuario en la ventana *Administrador de usuarios*[8] y saldrá el cuadro de dialogo como el en el apartado anterior.

4.3.2.3 ELIMINAR UNA CUENTA

Para eliminar una cuenta señale la cuenta la que desee eliminar y luego pulse *Supr*.

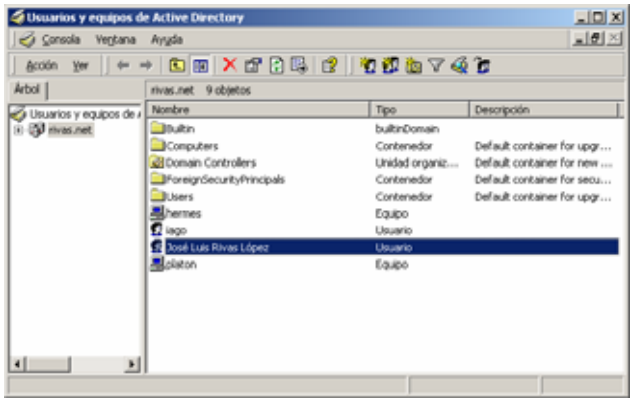
4.3.2.4 BLOQUEAR UNA CUENTA

Para bloquear una cuenta haga doble clic sobre el usuario y luego haga clic sobre *cuenta desactivada*.

4.3.3 WINDOWS 2000

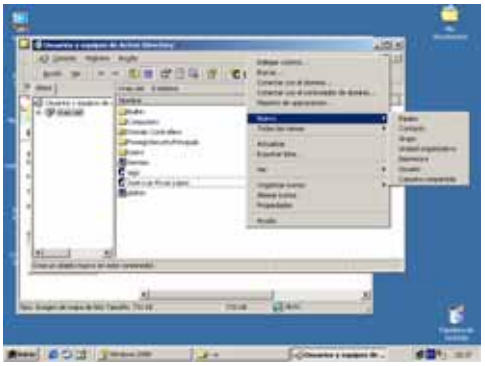
Los usuarios de Windows 2000 igual que los de Windows NT se identifican por un SID. La herramienta de administración de las cuentas de usuarios y grupos y planes de seguridad es el "*Usuarios y equipos Active Directory*". Para abrirlo basta con hacer clic en *Inicio -> Programas -> Herramientas administrativas -> Usuarios y equipos Active Directory*.

[8] Véase sección 4.3.2



4.3.3.1 CREAR UNA CUENTA

Para la creación de usuarios hay varias maneras. Una de ella es hacer clic con el botón derecho del ratón sobre el dominio. Desde el menú seleccionaremos *Nuevo* y luego elegiremos *Usuario.*



4.3.3.2 CAMBIAR ATRIBUTOS A UNA CUENTA

Para cambiar los atributos de una cuenta basta con hacer doble clic en la cuenta de usuario en la ventana *Administrador de usuarios*[9] y saldrá el cuadro de dialogo como en el apartado anterior.

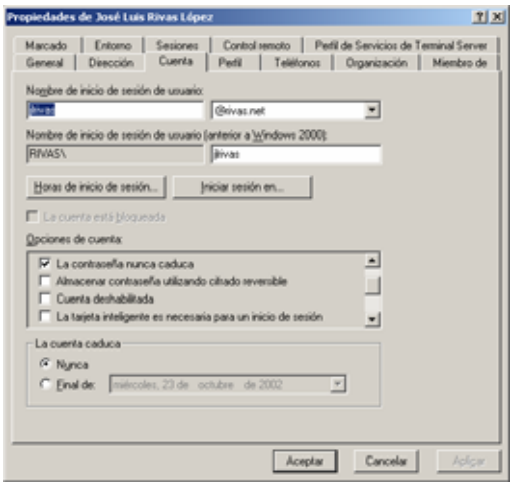
4.3.3.3 ELIMINAR UNA CUENTA

Para eliminar una cuenta señale la cuenta que desee eliminar y luego pulse *Supr*.

[9] Véase sección 4.3.2

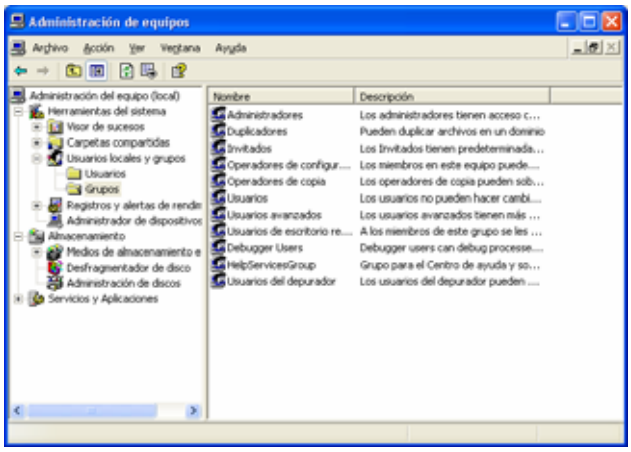
4.3.3.4 BLOQUEAR UNA CUENTA

Para bloquear una cuenta basta con hacer clic en la pestaña *Cuenta* del cuadro de dialogo de *Propiedades de "usuario"* y luego haga clic en cuenta deshabilitada en "*Opciones de cuenta*"



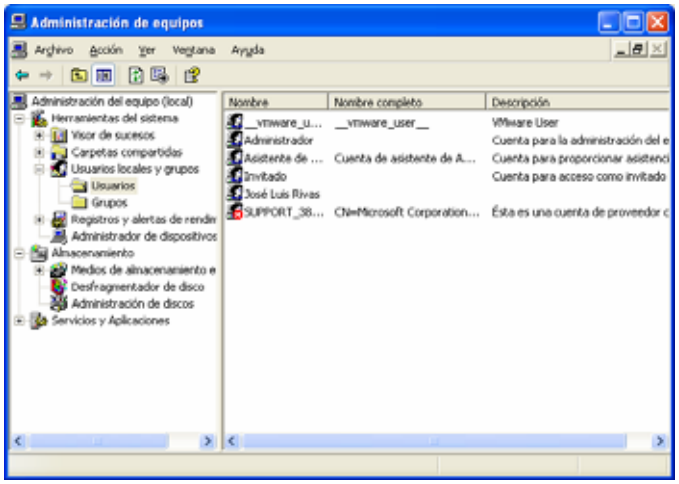
4.3.4 WINDOWS XP

Los usuarios de Windows XP se identifican de la misma manera que los de Windows 2000. Para la gestión de usuarios nos vamos encontrar con dos herramientas: una de ellas muy sencilla con pocas opciones y la otra más compleja, que permite más acciones, no sólo a nivel de usuario. Para abrir la segunda basta con hacer clic en *Inicio -> Panel de control -> Herramientas administrativas -> Administración de equipos*. Una vez hecho esto saldrá la siguiente ventana.



4.3.4.1 CREAR UNA CUENTA

Hay varias maneras para la creación de usuarios. Una de ella es hacer clic en "*Usuarios y grupos locales*", luego haga clic en *usuarios*. Desde el menú seleccionaremos *Usuario Nuevo* del menú *Acción*.



4.3.4.2 CAMBIAR ATRIBUTOS A UNA CUENTA

Para cambiar los atributos de una cuenta basta con hacer doble clic en la cuenta de usuario en la ventana *Administrador de equipos*, con lo que saldrá un cuadro de dialogo donde podremos cambiar los atributos.

4.3.4.3 ELIMINAR UNA CUENTA

Para eliminar una cuenta señale la cuenta que desee eliminar y luego pulse *Supr*.

4.3.4.4 BLOQUEAR UNA CUENTA

Para bloquear una cuenta basta con doble clic en el nombre de la cuenta, con lo que saldrá el cuadro de dialogo de *Propiedades de "usuario"*. Luego haga clic en cuenta deshabilitada.

4.3.5 SISTEMAS DE GESTIÓN

Las operaciones con los sistemas de gestión dependen de la manera en la que se ha programado, como ya comentamos en apartados anteriores.

4.4 GRUPOS

La existencia de grupos surge como alternativa a las cuentas de usuarios colectivos, los cuales no están permitidas por el Reglamento de Medidas de Seguridad. Por tanto, un grupo es un conjunto de cuentas de usuario que tienen permisos y derechos comunes.

4.4.1 LINUX

Igual que con las cuentas de usuarios, los grupos estarán identificados con un nombre de grupo y esta a su vez con un número que recibe el nombre de GID[10]. Por ejemplo, el 0 pertenece al grupo de root.

4.4.1.1 CREAR UN GRUPO

Para la creación de un grupo existen dos maneras:

1) Editando el fichero */etc/group* añadiéndoselo manualmente.

[10] Group Identification Number

2) Ejecutando el comando *groupadd* cuyos opciones son:

OPCIÓN	DESCRIPCIÓN
-g [gid]	Permite especificar el GID
-o	Permite la creación de un GID que no sea único

4.4.1.2 CAMBIO DE ATRIBUTOS

Igual que con los usuarios nos encontraremos con dos comandos para realizar cambios en los atributos de los grupos. El primero de ellos es *groupdel* con las siguientes opciones:

OPCIÓN	DESCRIPCIÓN
-g [gid]	Permite cambiar el GID
-n [nombre del grupo]	Permite cambiar el nombre del grupo
-o	Permite la creación de un GID que no sea único

El segundo, *gpasswd*, tiene las siguientes opciones:

OPCIÓN	DESCRIPCIÓN
-a [usuario]	Permite añadir a un usuario en un grupo
-A [usuario]	Permite añadir a un usuario en un grupo, pero con diferencia de la opción *–a [usuario]* tiene que ser un grupo de administración por ejemplo el grupo *root*.
-d [usuario]	Permite borrar a un usuario de un grupo
-M [miembros]	Permite especificar miembros
-r [grupo]	Permite borrar la contraseña de un grupo
-R [grupo]	Permite bloquear el acceso a un grupo por medio del comando *newgrp*

4.4.1.3 BORRAR UN GRUPO

Existen también dos maneras para dar de baja:

1) Editando el fichero */etc/group* y borrando la linea del grupo en cuestión.

2) Con el comando *groupdel*.

4.4.2 WINDOWS NT

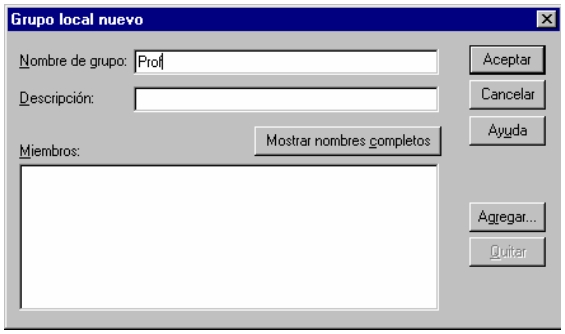
De igual manera que para los usuarios, los grupos se identifican con un SID, diferente entre ellos. Para realizar las diferentes operaciones descritas en las

subsecciones posteriores se tendrá que abrir el *Administrador de usuarios para dominios* como en el apartado 4.3.2.

4.4.2.1 CREAR UN GRUPO

Este sistema operativo permite la creación de grupos: globales y/o locales. Las diferencias entre ambos es que el primero se crean para organizar los usuarios de acuerdo al trabajo que realizan mientras que el segundo es para conceder permisos para acceder a diferentes recursos.

Para crearlo vaya al menú y haga clic en usuario. Luego elija la opción "*Grupo global nuevo*" o "*Grupo local nuevo*" dependiendo de la necesidad. Una vez realizado saldrá la siguiente ventana.



4.4.2.2 CAMBIO DE ATRIBUTOS

Haga doble clic sobre el grupo que quiera modificar y saldrá una ventana igual que la anterior.

4.4.2.3 BORRAR UN GRUPO

Para borrar habrá que seleccionar el grupo que se quiera borrar y luego teclee la tecla *supr*.

4.4.3 WINDOWS 2000

Los grupos de Windows 2000 igual que los de Windows NT se identifican por un SID. La herramienta de administración de las cuentas de usuarios y grupos y planes de

seguridad es el "*Usuarios y equipos Active Directory*". Para abrirlo basta con hacer clic en *Inicio -> Programas -> Herramientas administrativas -> Usuarios y equipos Active Directory* igual que en la sección 4.2.4.

4.4.3.1 CREAR UN GRUPO

Hay varias maneras para la creación de grupos. Una de ella es hacer clic con el botón derecho del ratón sobre el dominio. Desde el menú seleccionaremos *Nuevo* y luego elegiremos *Grupo*.

4.4.3.2 CAMBIO DE ATRIBUTOS

Para cambiar los atributos de un grupo basta con hacer doble clic en el grupo en la ventana *Administrador de usuarios*[11] y saldrá el cuadro de dialogo como en el apartado anterior.

4.4.3.3 BORRAR UN GRUPO

Para eliminar un grupo señale la cuenta que desee eliminar y luego pulse *Supr*.

4.4.4 WINDOWS XP

Los grupos de Windows XP están identificados de igual manera que los de la versión anterior, es decir Windows 2000. La herramienta de administración de equipos va a ser la que utilizaremos para realizar las acciones con los grupos. Para abrirlo basta con hacer clic en *Inicio -> Panel de control -> Herramientas administrativas -> Administración de equipos* igual que se explicaba en la sección 4.3.4.

4.4.4.1 CREAR UN GRUPO

Existen hay varias maneras para la creación de grupos. Una de ella es hacer clic con el botón derecho del ratón sobre la carpeta de G*rupos*. Desde el menú emergente seleccionaremos *Grupo nuevo*.

---

[11] Véase sección 4.3.2

4.4.4.2 CAMBIO DE ATRIBUTOS

Para cambiar los atributos de un grupo basta con hacer doble clic en el grupo en la ventana *Administrador de equipos* y saldrá el cuadro de dialogo como el en el apartado anterior.

4.4.4.3 BORRAR UN GRUPO

Para eliminar un grupo señale la cuenta que desee eliminar y luego pulse *Supr*.

4.4.5 SISTEMAS DE GESTIÓN

Idem del apartado 4.3.4

5

Control de Acceso

Artículo 12. Control de acceso.

1. Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.

2. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a datos o recursos con derechos distintos de los autorizados.

3. La relación de usuarios a la que se refiere el artículo 11.1 de este Reglamento contendrá el acceso autorizado para cada uno de ellos.

4. Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los datos y recursos, conforme a los criterios establecidos por el responsable del fichero.

5.1 PERMISOS

Los permisos dan la opción de permitir o denegar el acceso tanto de un fichero como de un directorio. Por tanto nos facilitaran dar acceso únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones a los usuarios autorizados. Esto es necesario en base al artículo 12 del Reglamento de Medidas de Seguridad.

5.1.1 LINUX

Los permisos se dividirán en cuatro subcampos:

-	rwx	rwx	rwx
tipo	permisos del	permisos del	permisos del
de	propietario	grupo	resto de
archivo	del fichero	del propietario	usuarios

Los tipos de archivos que podremos encontrar habitualmente son:

TIPO	DESCRIPCIÓN
-	Archivo normal
b	Dispositivos de bloques
c	Dispositivos de caracteres
d	Directorio
l	Enlace simbólico

Los siguientes subcampos nos muestran los permisos para: el propietario, el grupo y para el resto. Por tanto, se podrá definir si el archivo se puede escribir o modificar, leer y ejecutar.

TIPO	DESCRIPCIÓN
r	Lectura
w	Escritura, modificación o borrado
x	Ejecución

El comando *chmod*, permite modificar los permisos. A continuación se muestran las opciones más empleadas

OPCIÓN	DESCRIPCIÓN
-c	Sólo informa cuando ha realizado cambios

-f	No imprime mensajes de error sobre archivos en los que no se realizan el cambio
-R	Realiza las modificaciones de manera recursiva: directorios y archivos dentro de subdirectorios.

Este comando contempla dos sintaxis:

- *Permisos absolutos*: permite cambiar los permisos en octal[1]. Un ejemplo de esta sintaxis sería:

  chmod 500 archivo

  se le está dando a *archivo* permiso de lectura al propietario. A continuación se muestra los diferentes permisos en octal:

VALOR EN OCTAL	PERMISOS OTORGADOS
0100	Ejecución para el propietario
0200	Escritura y modificación para el propietario
0400	Lectura para el propietario
0010	Ejecución para el grupo
0020	Escritura y modificación para el grupo
0040	Lectura para el grupo
0001	Ejecución para los demás
0002	Escritura y modificación para los demás
0004	Lectura para los demás
2000	Bit de identificador de grupo (SGID)[2]
4000	Bit de identificador de usuario (SUID)[3]

- *Permisos relativos*: permite cambiar los permisos con letras. Un ejemplo de esta sintaxis sería:

  chmod u=rx archivo

  se le está dando a *archivo* permiso de lectura y ejecución al propietario. Este tipo de sintaxis se tendrá que establecer:

[1] Octal es un código en base 8 (0, 1, 2, 3, 4, 5, 6, 7)

[2] Este bit indica al sistema que el programa en ejecución tiene todos los permisos del grupo del archivo.

[3] Este bit indica al sistema que el programa en ejecución tiene todos los permisos del propietario del archivo.

- ¿A quién se le están dando los permisos?

OPCIÓN	DESCRIPCIÓN
a	Todos los usuarios
g	El grupo
o	Los demás
u	El propietario

- Tipo de operación

OPCIÓN	DESCRIPCIÓN
+	Agregar permisos
-	Eliminar permisos
=	Establece los permisos de forma absoluta

- Permisos

OPCIÓN	DESCRIPCIÓN
r	Lectura
w	Escritura y modificación
x	Ejecución
s	Bit de identificador de usuario (SUID)

5.1.2 WINDOWS NT

Para este apartado y el 5.1.3 se está usando el entorno de seguridad NTFS. Para configurar los permisos en este sistema operativo basta con utilizar uno de los siguientes dos programas: *Mi PC* o *Explorer* para poder movernos por los diferentes dispositivos, directorios, ficheros. Una vez decidido que objeto queremos modificar los permisos, sitúese con el puntero sobre dicho objeto y haga clic con el botón derecho. Una vez hecho esto se desplegará un menú donde elidirá la opción *propiedades* donde saldrá la siguiente cuadro de dialogo.

Luego pulse el botón de seguridad. Para añadir un usuario o grupo en la lista, haga clic en el botón *agregar* con lo que saldrá el cuadro de dialogo "*agregar usuarios y grupos*". Finalmente, para determinar el tipo de acceso elija las diferentes opciones en la lengüeta *tipo de acceso*.

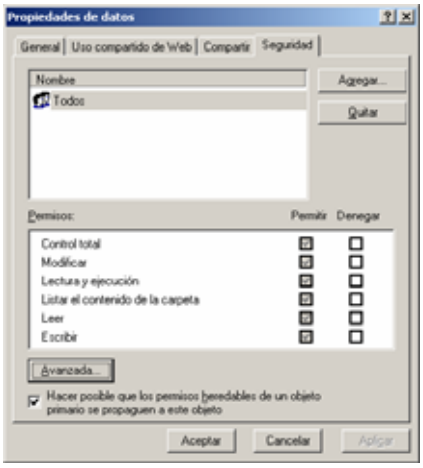
Por el contrario, para quitar un grupo o usuario señale el grupo o usuario y haga clic en el botón *quitar*.

Otra operación que podemos realizar será cambiar los permisos de un grupo o usuario. Para ello, sitúese sobre él y verá en *tipo de acceso* los permisos concedidos. Para modificarlos marque el triangulo que hay a la derecha del apartado y saldrán las posibles opciones. En la siguiente tabla mostraremos las diferentes tipos de acceso:

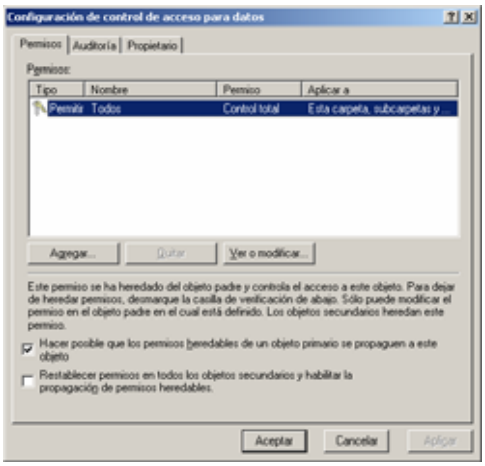
TIPO DE ACCESO	DESCRIPCIÓN
Sin acceso	El objeto no podrá ser accedido
Listar	Permite listar los archivos y subdirectorios de un directorio, pero no permitirá acceder a los nuevos creados en él
Lectura	Permite mostrar los subdirectorios y los ficheros, mostrar la información y atributos de los ficheros y cambiar a cualquier subdirectorio del directorio
Agregar	Permite escribir y ejecutar, pero no permiten modificar los archivos que hayan sido colocados allí
Agregar y Leer	Permite todo lo de agregar y el tipo de acceso de lectura
Cambio	Permite leer, escribir, ejecutar y borrar tanto
Control total	Permite hacer cualquier cosa en el objeto

5.1.3 WINDOWS 2000

En cuanto a Windows 2000 se realiza de la misma manera que con Windows NT, es decir usando: *Mi PC* y/o *Explorador*. Haga clic sobre el objeto que quiera modificar los permisos con el botón derecho, con lo que saldrá el siguiente cuadro de dialogo



Como se puede observar es muy parecido con el anterior sistema operativo. Si se hace clic en el botón *avanzada* saldría el siguiente cuadro de diálogo:



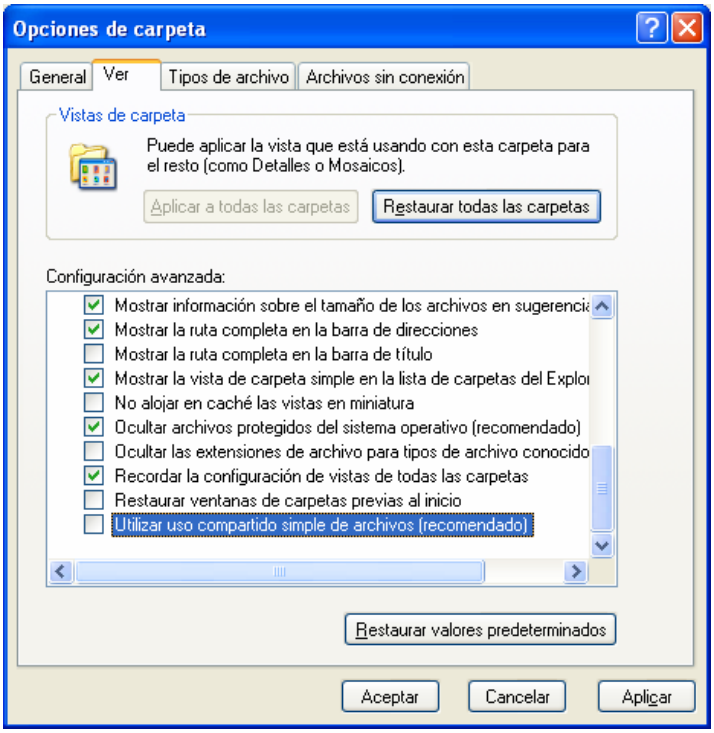
En cada entrada de la lista muestra un tipo de entrada[4], el nombre del principal de seguridad, una lista de permisos y dónde son aplicados.

5.1.4 WINDOWS XP

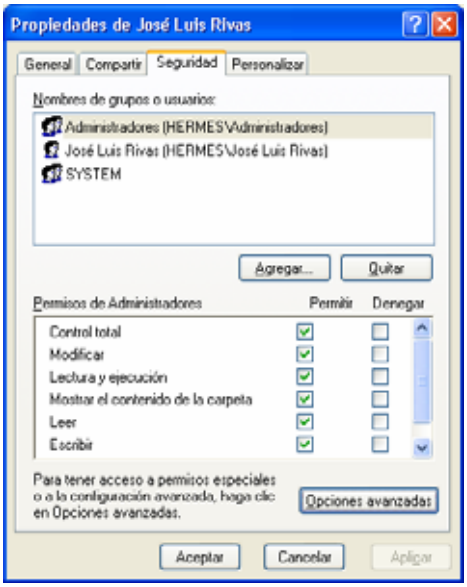
En Windows XP para realizarlo de la misma manera que con Windows 2000 habrá que hacer un pequeño cambio en la configuración, porque para que sea muy fácil de usar cuando se instala lo tiene instalado de manera asequible para un usuario sin conocimientos avanzados de sistemas. Para la realización de este cambio habrá que

[4] O permitir o denegar

hacer clic en *Inicio -> Panel de control -> Opciones de carpeta*. Luego en la pestaña *Ver*, bajo la *Configuración avanzada*, desactive *Utilizar uso compartido simple de archivos (recomendado)*.



Una vez hecho este paso se realiza de la misma manera que con Windows 2000, es decir usando: *Mi PC* y/o *Explorador*. Haga clic sobre el objeto del que quiera modificar los permisos con el botón derecho. Saldrá el siguiente cuadro de dialogo:



Como se puede observar es muy parecido al anterior sistema operativo.

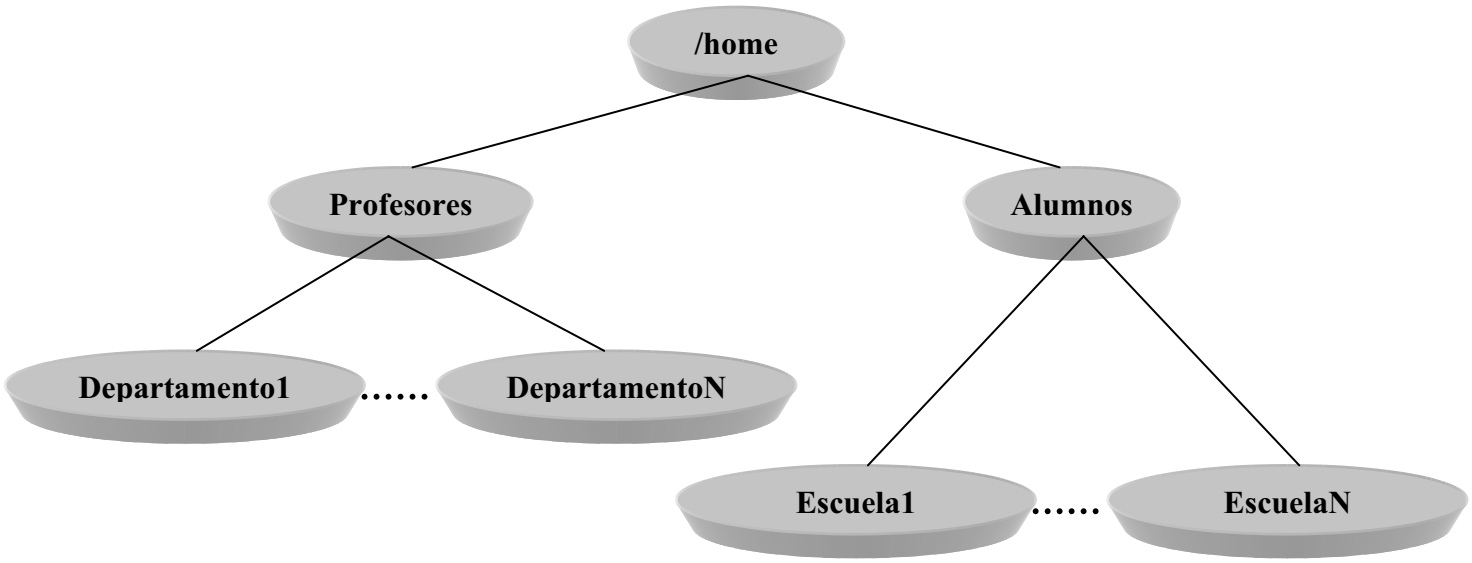
5.1.5 SISTEMAS DE GESTIÓN

En los apartados anteriores se han explicado las diferentes maneras que permiten los sistemas operativos para gestionar los permisos en los archivos y carpetas. Hay que tener en cuenta que los sistemas de gestión complicados son sistemas embebidos uno de otros, donde hay mucha información, es decir, en el caso de una clínica privada en donde hay: un médico, un A.T.S. y una secretaria. Se deberá habilitar un sistema de login y una contraseña individual y distinto para cada usuario como se ha comentado en el capítulo anterior, 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 estará estructurado en grupos, siguiendo 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. Por tanto, todo ello dependerá de cómo se ha hecho la implementación del sistema de gestión.

5.2 ADMINISTRAR LOS DIRECTORIOS DE TRABAJO

En la organización de los directorios de trabajo es recomendable que se agrupen de una forma lógica, porque de esta manera nos facilitará a la hora de administrar los permisos. Un ejemplo de cómo deberá ser esta manera es con el ejemplo de una universidad, dónde hay alumnos y profesores. Los profesores pertenecen a diferentes departamentos mientras que los alumnos estarán matriculados en diferentes facultades o escuelas.

A continuación se muestra un ejemplo gráficamente:



6

Copias de Seguridad

Artículo 14. Copias de respaldo y recuperación.

1. El responsable de fichero se encargará de verificar la definición y correcta aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

2. Los procedimientos establecidos para la realización de copias de respaldo y para la recuperación de los datos deberá garantizar su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

3. Deberán realizarse copias de respaldo, al menos semanalmente, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.

6.1 MÉTODO DE ROTACIÓN

El Reglamento de Medidas de Seguridad de la LOPD exige en el artículo 14.3 que deberá realizar al menos semanalmente, salvo que en dicho período no se hubiera producido ninguna actualización de los datos. Nosotros recomendaremos el "*método de rotación*" porque el artículo 14.2 obliga a la reconstrucción en el estado en que se encontraba al tiempo de producirse la perdida o destrucción y este método es el más adecuado para cumplirlo.

La explicación del método está pensado para una organización en la que se trabajan cinco días a la semana, de lunes a viernes, y dónde se está continuamente creando y modificando archivos. Aunque se va explicar para estas características será fácilmente extrapolable a otras condiciones.

- Tendrá que utilizar una cinta para cada mes del año, en los cuales se realizarán una copia de seguridad de todo el sistema al final del mes.

- Tendrá también que utilizar cuatro cintas para cada semana del mes. En ellas se realizarán los viernes una copia de todo el sistema.

- Realizará una copia de seguridad incremental[1] de lunes a jueves.

- Documente cada cinta especificando:

    - Nombre de la cinta. Por ejemplo: lunes, martes, semana1 semana2, enero, febrero, etc.

    - Fecha de creación de la copia.

    - Nombre del sistema/servidor a la cual pertenece.

[1] Este tipo realiza una copia solo de los archivos que han sido creados o modificados desde la última copia de seguridad.

- Si es un conjunto de volúmenes, enumérelas por su secuencia.

Habrá que tener en cuenta cuatro puntos:

1) Realice las copias cuando menos cargado este el sistema y cuando no este ningún usuario accediendo al sistema excepto el superusuario (root, administrador) . Se recomienda poner el sistema en monousuario.

2) Aunque el Reglamento no dice nada para nivel básico en donde ubicar las copias, hágalo en algún lugar apartado de la sala de los sistemas.

3) Realice cada cierto tiempo una simulación de restauración para comprobar que esta funcionando perfectamente el procedimiento de copias de seguridad.

4) Si reutiliza o desecha alguna de las cintas, según el artículo 20.3 del Reglamento, adopte medidas para evitar la recuperación posterior de la información personal. Por ejemplo se podrá realizar un formateo a bajo nivel o su destrucción física o incineración.

6.2 DISPOSITIVOS DE CINTA

Para la realización de las copias de seguridad existe una gran variedad de dispositivos:

- Dispositivo SCSI.
- Dispositivo ATAPI.
- Regrabadores o grabadores de CD.
- IOMEGA DITTO.
- IOMEGA ZIP.

- IOMEGA JAZ.
- Discos ópticos.
- Cintas DIC.
- Cintas DAT.

A continuación se muestra una tabla con algunos de los nombre que le otorga Linux

NOMBRE	DISPOSITIVO
/dev/fd0	Disquete
/dev/cdrom	CD-ROM, grabadores o regrabadores
/dev/tape	Cinta SCSI
/dev/nst0	Cinta SCSI
/dev/sd2x	Disco óptico

Por el contrario los sistemas de Microsoft les otorga letras. A continuación se muestran las asignaciones más comunes, aunque para poder verlas haga clic en el icono “Mi PC”.

NOMBRE	DISPOSITIVO
A	Disquete
D	CD-ROM, grabadores o regrabadores
E	Cinta SCSI

6.3 PROGRAMAS

En esta sección se explicaran las aplicaciones que vienen con los sistemas operativos para la realización de las copias de seguridad. Además de los que vamos explicar existen otros como los que muestran en la siguiente tabla:

SOFTWARE	UBICACIÓN
AMANDA	ftp://ftp.amanda.org/pub/amanda
BRU	http://www.estinc.com/
Kbackup	http://kbackup.sourceforge.net/
Backup Exec	http://www.veritas.com/
ARCserveIT	http://www.cai.com/

6.3.1 LINUX

En LINUX existen numerosos programas, pero uno de los más usados por su sencillez y porque viene en todas las distribuciones son: *dump* y *restore*.

Estos dos programas permiten realizar las copias de seguridad como se ha comentado en apartados anteriores.

A continuación se muestran algunas opciones de *dump*

OPCIÓN	DESCRIPCIÓN
0-9	Con este número indicamos el tipo de copia de seguridad. El 0 significa que es una copia de seguridad total de todo el sistema. El 1 significa que se realizaría una copia de seguridad incremental o progresiva con respecto a la última copia de seguridad total. El 2 significa que se realizaría una copia de seguridad incremental o progresiva con respecto a la última copia de seguridad incremental de nivel 1 que se haya realizado Así sucesivamente hasta el 9
b [*tamaño_ bloque*]	Especifica el número de kilobytes por copia .
B [*tamaño*]	Especifica el número de bytes que se copiarán en el destino.
d [*densidad_de_la_cinta*]	Especifica una densidad alternativa de la cinta.
f [*archivo/dispositivo*]	Especifica dónde se realiza la copia de seguridad.
T [*fecha*]	Especifica cuándo empieza la copia de seguridad, sobrescribiendo los datos de la fecha que se encuentre en */etc/dumpupdates*.
w	Se obtiene una lista de los archivos del sistema de los que se tendría que hacer una copia de seguridad.
W	Se obtienen unas estadísticas sobre qué archivos de sistema recientemente han sido objeto de una copia de seguridad .

Ejemplo de utilización en el cual se realizara una copia total de la partición */dev/hda3* en el dispositivo */dev/sdb1*:

d*ump 0uf /dev/sdb1 /dev/hda3*

Para su restauración se utiliza el programa *restore*, siendo sus opciones:

OPCIÓN	DESCRIPCIÓN
C	Con esta opción se verifica si la copia de seguridad se ha realizado de una manera satisfactoria, debido a que compara

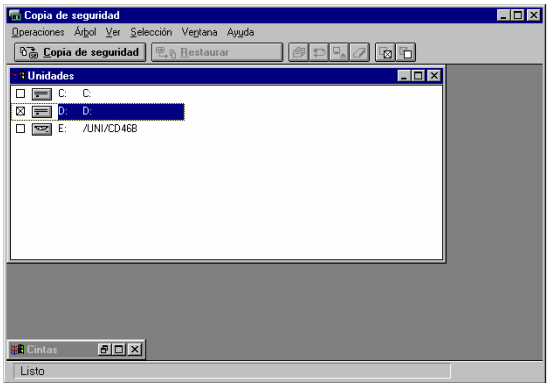
	el contenido de la copia de seguridad con los archivos que se encuentran en el disco.
D [*archivo_ del_ sistema*]	Se utiliza junto con la opción C. Especifica qué archivo de sistema recuperado deberá ser comparado .
f [*archivo/dispositivo*]	Especifica otro archivo o dispositivo con el que trabajar.
H	Restaura sólo el árbol de directorios, por tanto, no restaurará los archivos que contengan.
I	Modo interactivo.
R	Especifica que la restauración deberá incluir el fichero del sistema especificado.
R	Especifica que la restauración deberá usar la cinta definida durante el proceso de restauración.
s [*número*]	Especifica un fichero, en concreto, para restaurar en una cinta que almacena múltiples ficheros.
T [*directorio_ temporal*]	Especifica cuál va a ser el directorio temporal durante el proceso de recuperación de la copia de seguridad.
V	Modalidad detallada.
Y	Permite requerir la verificación cuando se encuentra un error.

6.3.2 WINDOWS NT

El soporte utilizado por el programa de copia de seguridad de este sistema operativo *NTBACKUP.EXE* es la cinta magnética.

Para la realización de las copias de seguridad de todos los archivos en Windows NT sólo podrá ser realizado por los grupos de "*administradores*" y los "*operadores de copia de seguridad*" por tener privilegios, mientras que los demás usuarios podrán realizarlos de aquellos archivos que tengan acceso de lectura, como es lógico.

Para ejecutar esta utilidad que viene con este sistema haga clic en el botón de *Inicio -> Programas -> Herramientas administrativas (Común) -> Copia de seguridad*. Una vez realizado saldrá la ventana siguiente:



Para la realización de la copia de seguridad realice los siguientes pasos:

1) Entre con un usuario que sea miembro del grupo de administradores u operadores de copia

2) Prepare la cinta. Normalmente las cintas nuevas no requieren preparación, aunque si ha sido utilizada se deberá formatear previamente. En la siguiente tabla se muestra algunas de las operaciones que se permiten en el menú *Operación*

OPERACIÓN	DESCRIPCIÓN
Borrar	Borra la información contenida en la cinta. Permite escoger entre realizar un *borrado rapido* (hace inutilizable para es sistema la cinta, pero manteniendo la información) y un *borrado seguro* (borra los datos no pudiendo acceder a los datos con ningún otro programa)
Tensar	Pensiona las cintas. Esta operación es necesario antes del primer uso, así como después de quince usos en las cintas DC-2000 y DC-6000
Expulsar	Saca la cinta de la unidad
Formatear	Formatea la cinta.

3) Elegir los archivos que se quieren realizar una copia de respaldo

4) Especificar las opciones de copia para ello haga clic en el botón "*copia de seguridad*" y saldrá el cuadro de dialogo "*Información sobre la copia de Seguridad*". En la siguiente tabla se describe dicho cuadro de dialogo.

TÍTULO	DESCRIPCIÓN
Cinta actual	Mostrará el nombre de la cinta, a no ser que no este cargada o no tenga un formato reconocido con lo que estará en blanco
Fecha de creación	Aparecerá la fecha de la creación o cuando fue reemplazada por última vez
Propietario	Mostrará quien inició la primera copia de seguridad en la cinta
Nombre de la cinta	Podrá cambiar el nombre de la cinta, para ello tendrá 32 caracteres.
Anexar	Con esta pestaña podrá elegir si quiere agregar la copia al final de la última realizada
Reemplazar	Por el contrario esta pestaña permite sobrescribir los datos de la cinta
Comprensión de hardware	Permitirá comprimir los datos
Comprobar después de la copia de seguridad	Esta pestaña permite decidir si se realizará una verificación después de la copia
Hacer copia de seguridad del Registro local	Permitirá realizar una copia de los ficheros del Registro (sólo estará disponible si se ha seleccionado una unidad local)
Limitar el acceso al propietario o al administrador	Si se elige esta opción sólo el propietario o los administradores podrán leer, escribir o borrar la cinta.
Tipo de copia	Permitirá indicar el tipo de copia deseado: normal, copia,

	diferencial, progresiva o incremental y diaria
Información de registro	Indicara las operaciones de cintas completadas

5) Realice la copia de seguridad. Para ello haga clic en el botón de aceptar. Una vez finalizado la copia se lo indicara.

Para la realización de la copia de seguridad realice los siguientes pasos:

1) Entre con un usuario que sea miembro del grupo de administradores u operadores de copia.

2) Elega los archivos que se quieren restaurar.

3) Especifique las opciones de restaurar. Para ello haga clic en el botón "*restaurar*" y saldrá el cuadro de dialogo "*Información de restauración*". En la siguiente tabla se describe dicho cuadro de dialogo.

TÍTULO	**DESCRIPCIÓN**
Nombre de unidad	Mostrará el nombre de la cinta a la que corresponde conjunto de copia seleccionado
Conjunto de copia	Indicará el nombre que se dio al conjunto de copia
Fecha de creación	Aparecerá la fecha y la hora de la copia
Propietario	Mostrará quien inició la primera copia de seguridad en la cinta
Restaurar	Se encontrarán las siguientes opciones: restaurar unidad (indique la unidad en la que se desea restaurar la información, ruta alternativa (especifique una ruta diferente de donde se ha realizado la copia), restaura el Registro local (reinicie el equipo una vez finalizado para que tenga efecto la restauración) y restaurar permisos de archivo (si no se marca esta opción, los archivos se restaurarán con los permisos que tuvieran asignados el directorio en el que se van a colocar)
Comprobar después de restaurar	Efectuará una comparación entre los archivos grabados en el disco y los originales de la cinta
Información de registro	Indicara las operaciones de cintas completadas

4) Restaure los archivos.

6.3.3 WINDOWS 2000

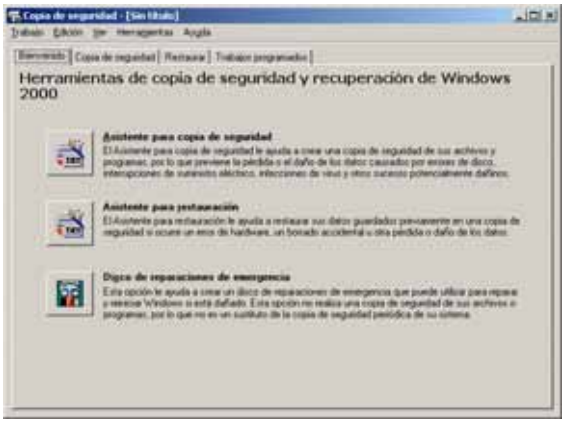
Para poder ejecutar la herramienta que permita hacer copias de seguridad haga clic en *Inicio -> Programas -> Herramientas administrativas -> Copia de seguridad*.

La aplicación que viene con este sistema operativo es una versión mejorada con respecto a Windows NT. Las mejoras más representativas son:

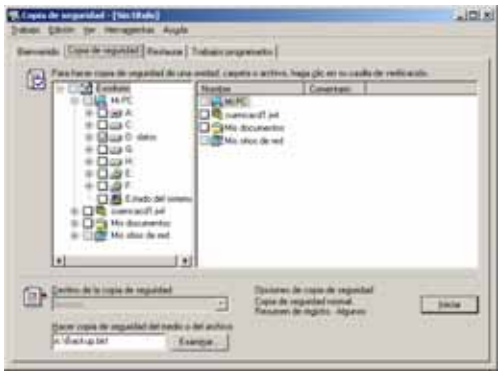
- Poder utilizar una gran diversidad de dispositivos para la realización de las copias.

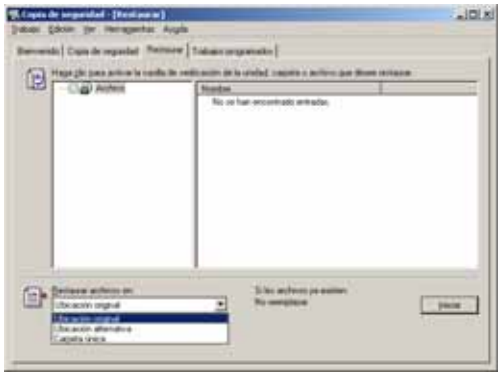
- No administra los medios ni los dispositivos de almacenamiento, las tareas de montar y desmontar una cinta o un disco las ejecuta ahora un servicio denominado "*Almacenamiento extraíble*"

- Asistentes de copia de seguridad y restauración, hojas de propiedades para grupos de medios libres, y acceso directo a Mis sitios de red.

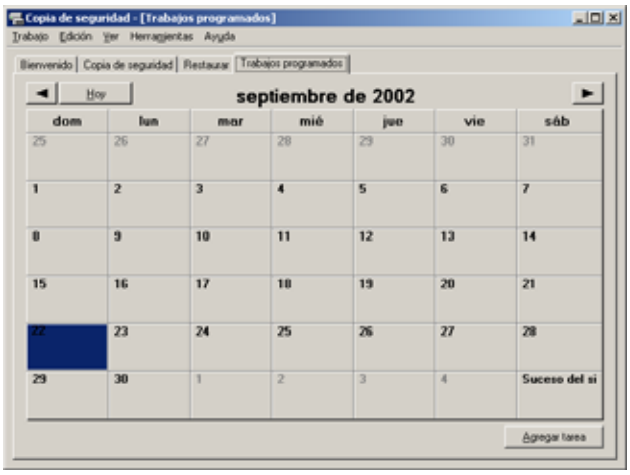


- Posibilidad completa de hacer copias de seguridad y restauración del Estado del sistema de Windows 2000, que incluye los archivos de sistema, el registro, los Servicios de componentes, la base de datos Active Directory, el servicio de duplicación de archivos y la base de datos de los servicios de certificación.





- Existencia de un "*Programador de tareas*" para automatizar los trabajos de copia de seguridad, no como con Windows NT, que tenía que utilizar el comando *at* o servicio *Schedule*.



Por tanto, no vamos a hacer una descripción exhaustiva debido a la gran similitud entre ambos.

6.3.4 WINDOWS XP

Para poder ejecutar la herramienta que nos permite la realización de copias de seguridad basta con hacer clic en *Inicio -> Todos los programas -> Accesorios -> Herramientas del sistema -> Copia de seguridad*. La aplicación que viene con este sistema operativo es muy parecida a la anterior. Por tanto, no vamos a hacer un descripción exhaustiva por la gran similitud entre ambos.

6.3.5 SISTEMAS DE GESTIÓN

Para la realización de copias de seguridad de los sistemas de gestión se utilizan cualquier de los programas anteriormente descritos debido a que como ya se ha comentado en capítulos anteriores los sistemas de gestión no dejan de ser aplicaciones dentro de estos sistemas operativos.

7

Documento de Seguridad

Artículo 8. Documento de seguridad.

1. El responsable del fichero elaborará e implantará la normativa de seguridad mediante un documento de obligado cumplimiento para el personal con acceso a los datos automatizados de carácter personal y a los sistemas de información.

2. El documento deberá contener, como mínimo, los siguientes aspectos:

a) Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.

b) Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este Reglamento.

c) Funciones y obligaciones del personal.

d) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.

e) Procedimiento de notificación, gestión y respuesta ante las incidencias.

f) Los procedimientos de realización de copias de respaldo y de recuperación de los datos.

3. El documento deberá mantenerse en todo momento actualizado y deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo.

4. El contenido del documento deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

7.1 INTRODUCCIÓN

Antes de tratar como debe ser un documento de seguridad, es necesario señalar que dichos documentos se pueden hacer de diferentes maneras, teniendo todas en común lo que exige el Reglamento de medidas de Seguridad en el art. 8.2

Además, también habría que comentar que el documento cambiará dependiendo del entorno en el que este el sistema de información. De hecho después de nuestra experiencia en la impartición de cursos, seminarios, talleres, cursos de postgrado, etc. sobre este tema en los últimos años, no nos gusta dar ejemplos de documentos de seguridad debido a que después se pueden tomar demasiado literalmente al aplicarlo en la práctica eludiendo, su necesario análisis y elaboración para cada caso concreto

7.2 PUNTOS A TENER EN CUENTA

El primer punto a tratar es el objeto del documento en el cual se describe el motivo de dicho documento. A continuación se deberá exponer el ámbito de aplicación con una especificación de los recursos protegidos. Otro de los puntos que habrá que tener en cuenta son las medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este Reglamento, así como de las funciones y obligaciones del personal. Además de la estructura de los ficheros con datos de carácter personal y una descripción de los sistemas de información que los tratan. Por último, habrá que describir los procedimientos de notificación, gestión y respuesta ante las incidencias y los de la realización de copias de respaldo así como, los de recuperación.

A continuación, mostramos un ejemplo de un documento de seguridad sacado de la página web de la Agencia de Protección de Datos de la Comunidad de Madrid:

7.3 EJEMPLO

Documento de Seguridad para ficheros automatizados de datos de carácter personal Nivel de seguridad básico

Fichero

Nº inscripción	NOMBRE DE FICHERO	

NOMBRE EMPRESA

Dirección General / Órgano / Organismo / Entidad

Fecha versión del Borrador del Documento de Seguridad	
Versión	
Sistema de Información	

ÍNDICE

ANEXOS

Nº de inscripción	NOMBRE DE FICHERO

1. Objeto del documento

El presente documento responde a la obligación establecida en el artículo 8 del Real Decreto 994/1999 de 11 de Junio en el que se regulan las medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

El fichero de datos: **NOMBRE DE FICHERO**, en adelante el Fichero, descrito en el documento de Notificación a la Agencia de Protección de Datos de la NOMBRE EMPRESA, que se adjunta en el Anexo A, se encuentra oficialmente clasificado como de **nivel de seguridad básico**, atendiendo a las condiciones descritas en el artículo 4 del Real Decreto citado, siendo por tanto aplicable a él todas las medidas de seguridad de **nivel básico** que se establecen en el Capítulo II del citado decreto.

2. Ámbito de aplicación

Este documento ha sido elaborado bajo la responsabilidad de la persona descrita en el apartado (1) del documento adjunto en el Anexo A, quien, como responsable del Fichero, se compromete a implantar y actualizar ésta Normativa de Seguridad de obligado cumplimiento para todo el personal con acceso a los datos protegidos o a los sistemas de información que permiten al acceso a los mismos.

Todas las personas que tengan acceso a los datos del Fichero, bien a través del sistema informático **NOMBRE DEL SISTEMA INFORMÁTICO** habilitado para acceder al mismo, o bien a través de cualquier otro medio automatizado de acceso al Fichero, se encuentran obligadas por ley a cumplir lo establecido en este documento, y sujetas a las consecuencias que pudieran incurrir en caso de incumplimiento.

Una copia de este documento con la parte que le afecte será entregada, para su conocimiento, a cada persona autorizada a acceder a los datos del Fichero, siendo requisito obligatorio para poder acceder a esos datos el haber firmado la recepción del mismo.

3. Recursos protegidos

La protección de los datos del Fichero frente a accesos no autorizados se deberá realizar mediante el control, a su vez, de todas las vías por las que se pueda tener acceso a dicha información.

Los recursos que, por servir de medio directo o indirecto para acceder al Fichero, deberán ser controlados por esta normativa son:

1) Los centros de tratamiento y locales donde se encuentren ubicados los ficheros o se almacenen los soportes que los contengan, su descripción figura en el Anexo E.

2) Los puestos de trabajo, bien locales o remotos, desde los que se pueda tener acceso al Fichero. La relación de esos puestos de trabajo está descrita en el Anexo E.

3) Los servidores, si los hubiese, y el entorno de sistema operativo y de comunicaciones en el que se encuentra ubicado el Fichero, que está descrito en el Anexo D.

4) Los sistemas informáticos, o aplicaciones establecidos para acceder a los datos, descritos en el Anexo C.

4. Funciones y obligaciones del personal

El personal afectado por esta normativa se clasifica en dos categorías:

1) **Administradores del sistema**, encargados de administrar o mantener el entorno operativo del Fichero. Este personal deberá estar explícitamente relacionado en el Anexo F, ya que por sus funciones pueden utilizar

herramientas de administración que permitan el acceso a los datos protegidos sáltandose las barreras de acceso de la Aplicación.

2) **Usuarios del Fichero**, o personal que usualmente utiliza el sistema informático de acceso al Fichero, y que también deben estar explícitamente relacionados en el Anexo F.

Además del personal anteriormente citado existirá un **Responsable de Seguridad del Fichero** cuyas funciones serán las de coordinar y controlar las medidas definidas en el documento, sirviendo al mismo tiempo de enlace con el **Responsable del Fichero**, sin que esto suponga en ningún caso una delegación de la responsabilidad que corresponde a éste último, de acuerdo con el R.D. 994/1999 de 11 de Junio.

Este documento es de obligado cumplimiento para todos ellos. Las funciones y obligaciones del personal están descritas en el Anexo H. Sin embargo, los administradores del sistema deberán además atenerse a aquellas normas, más extensas y estrictas, que se referencian en el Anexo G, y que atañen, entre otras, al tratamiento de los respaldos de seguridad, normas para el alta de usuarios y contraseñas, así como otras normas de obligado cumplimiento en la unidad administrativa a la que pertenece el Fichero.

5. Normas y procedimientos de seguridad

5.1 Centros de tratamiento y locales

Los locales donde se ubiquen los ordenadores que contienen el Fichero deben ser objeto de especial protección que garantice la disponibilidad y confidencialidad de los datos protegidos, especialmente en el caso de que el Fichero esté ubicado en un servidor accedido a través de una red.

5.1.1. Los locales deberán contar con los medios mínimos de seguridad que eviten los riesgos de indisponibilidad del Fichero que pudieran producirse como

consecuencia de incidencias fortuitas o intencionadas. La descripción de esos medios se encuentra en el Anexo E.

5.1.2. El acceso a los locales donde se encuentre el fichero deberá estar restringido exclusivamente a los administradores del sistema que deban realizar labores de mantenimiento para las que sean imprescindibles el acceso físico.

5.2 Puestos de trabajo

Son todos aquellos dispositivos desde los cuales se puede acceder a los datos del Fichero, como, por ejemplo, terminales u ordenadores personales.

Se consideran también puestos de trabajo aquellos terminales de administración del sistema, como, por ejemplo, las consolas de operación, donde en algunos casos también pueden aparecer los datos protegidos del Fichero.

5.2.1. Cada puesto de trabajo estará bajo la responsabilidad de una persona de las autorizadas en el Anexo F, que garantizará que la información que muestra no pueda ser vista por personas no autorizadas.

5.2.2. Esto implica que tanto las pantallas como las impresoras u otro tipo de dispositivos conectados al puesto de trabajo deberán estar físicamente ubicados en lugares que garanticen esa confidencialidad.

5.2.3. Cuando el responsable de un puesto de trabajo lo abandone, bien temporalmente o bien al finalizar su turno de trabajo, deberá dejarlo en un estado que impida la visualización de los datos protegidos. Esto podrá realizarse a través de un protector de pantalla que impida la visualización de los datos. La reanudación del trabajo implicará la desactivación de la pantalla protectora con la introducción de la contraseña correspondiente.

5.2.4. En el caso de las impresoras deberá asegurarse de que no quedan documentos impresos en la bandeja de salida que contengan datos

protegidos. Si las impresoras son compartidas con otros usuarios no autorizados para acceder a los datos de Fichero, los responsables de cada puesto deberán retirar los documentos conforme vayan siendo impresos.

5.2.5. Queda expresamente prohibida la conexión a redes o sistemas exteriores de los puestos de trabajo desde los que se realiza el acceso al fichero. La revocación de esta prohibición sera autorizada por el responsable del fichero, quedando constancia de esta modificación en el Libro de incidencias.

5.2.6. Los puestos de trabajo desde los que se tiene acceso al fichero tendrán una configuración fija en sus aplicaciones, sistemas operativos que solo podrá ser cambiada bajo al autorización del responsable de seguridad o por administradores autorizados del anexo F.

5.3 Entorno de Sistema Operativo y de Comunicaciones

Aunque el método establecido para acceder a los datos protegidos del Fichero es el sistema informático referenciado en el Anexo C, al estar el fichero ubicado en un ordenador con un sistema operativo determinado y poder contar con unas conexiones que le comunican con otro ordenadores, es posible, para las personas que conozcan estos entornos, acceder a los datos protegidos sin pasar por los procedimientos de control de acceso con los que pueda contar la aplicación.

Esta normativa debe, por tanto, regular el uso y acceso de las partes del sistema operativo, herramientas o programas de utilidad, o del entorno de comunicaciones, de forma que se impida el acceso no autorizado a los datos de Fichero.

5.3.1. El sistema operativo y de comunicaciones del Fichero deberá tener al menos un responsable, que, como administrador deberá estar relacionado en el Anexo F.

5.3.2. En el caso más simple, como es que el Fichero se encuentre ubicado en un ordenador personal y accedido mediante una aplicación local monopuesto, el

administrador del sistema operativo podrá ser el mismo usuario que accede usualmente al Fichero.

5.3.3. Ninguna herramienta o programa de utilidad que permita el acceso al Fichero deberá ser accesible a ningún usuario o administrador no autorizado en el Anexo F.

5.3.4. En la norma anterior se incluye cualquier medio de acceso en bruto, es decir no elaborado o editado, a los datos del Fichero, como los llamados "queries", editores universales, analizadores de ficheros, etc., que deberán estar bajo el control de los administradores autorizados relacionados en el Anexo F.

5.3.5. El administrador deberá responsabilizarse de guardar en lugar protegido las copias de seguridad y respaldo del Fichero, de forma que ninguna persona no autorizada tenga acceso a las mismas.

5.3.6. Si la aplicación o sistema de acceso al Fichero utilizase usualmente ficheros temporales, ficheros de "logging", o cualquier otro medio en el que pudiesen ser grabados copias de los datos protegidos, el administrador deberá asegurarse de que esos datos no son accesibles posteriormente por personal no autorizado.

5.3.7. Si el ordenador en el que está ubicado el fichero está integrado en una red de comunicaciones de forma que desde otros ordenadores conectados a la misma sea posible acceso al Fichero, el administrador responsable del sistema deberá asegurarse de que este acceso no se permite a personas no autorizadas.

5.4 Sistema Informático o aplicaciones de acceso al Fichero

Son todos aquellos sistemas informáticos, programas o aplicaciones con las que se puede acceder a los datos del Fichero, y que son usualmente utilizados por los usuarios para acceder a ellos.

Estos sistemas pueden ser aplicaciones informáticas expresamente diseñadas para acceder al Fichero, o sistemas preprogramados de uso general como aplicaciones o paquetes disponibles en el mercado informático.

5.4.1. Los sistemas informáticos de acceso al Fichero deberán tener su acceso restringido mediante un código de usuario y una contraseña.

5.4.2. Todos los usuarios autorizados para acceder al Fichero, relacionados en el Anexo F, deberán tener un código de usuario que será único, y que estará asociado a la contraseña correspondiente, que sólo será conocida por el propio usuario.

5.4.3. Si la aplicación informática que permite el acceso al Fichero no cuenta con un control de acceso, deberá ser el sistema operativo, donde se ejecuta esa aplicación, el que impida el acceso no autorizado, mediante el control de los citados códigos de usuario y contraseñas.

5.5 Salvaguarda y protección de las contraseñas personales

Las contraseñas personales constituyen uno de los componentes básicos de la seguridad de los datos, y deben por tanto estar especialmente protegidas. Como llaves de acceso al sistema, las contraseñas deberán ser estrictamente confidenciales y personales, y cualquier incidencia que comprometa su confidencialidad deberá ser inmediatamente comunicada al administrador y subsanada en el menor plazo de tiempo posible.

5.5.1. Sólo las personas relacionadas en el Anexo F podrán tener acceso a los datos del Fichero.

5.5.2. Cada usuario será responsable de la confidencialidad de su contraseña y, en caso de que la misma sea conocida fortuita o fraudulentamente por personas no autorizadas, deberá registrarlo como incidencia y proceder inmediatamente a su cambio.

5.5.3. Las contraseñas se asignarán y se cambiarán mediante el mecanismo y periodicidad que se determina en el Anexo G.

5.5.4. El archivo donde se almacenen las contraseñas deberá estar protegido y bajo la responsabilidad del administrador del sistema.

6. Gestión de incidencias

Una incidencia es cualquier evento que pueda producirse esporádicamente y que pueda suponer un peligro para la seguridad del Fichero, entendida bajo sus tres vertientes de confidencialidad, integridad y disponibilidad de los datos.

El mantener un registro de las incidencias que comprometan la seguridad de un Fichero es una herramienta imprescindible para la prevención de posibles ataques a esa seguridad, así como para persecución de los responsables de los mismos.

6.1.1. El responsable de seguridad de Fichero habilitará un Libro de Incidencias a disposición de todos los usuarios y administradores del Fichero con el fin de que se registren en él cualquier incidencia que pueda suponer un peligro para la seguridad del mismo.

6.1.2. Cualquier usuario que tenga conocimiento de una incidencia es responsable del registro de la misma en el Libro de Incidencias del Fichero o en su caso de la comunicación por escrito al responsable de seguridad o al responsable del Fichero.

6.1.3. El conocimiento y la no notificación o registro de una incidencia por parte de un usuario será considerado como una falta contra la seguridad del Fichero por parte de ese usuario.

6.1.4. La notificación o registro de una incidencia deberá constar al menos de los siguientes datos: tipo de incidencia, fecha y hora en que se produjo, persona que realiza la notificación, persona a quien se comunica, efectos que puede producir, descripción detallada de la misma. El procedimiento está descrito en el Anexo I.

7. Gestión de soportes

Soportes informáticos son todos aquellos medios de grabación y recuperación de datos que se utilizan para realizar copias o pasos intermedios en los procesos de la aplicación que gestiona el Fichero.

Dado que la mayor parte de los soportes que hoy en día se utilizan, como disquetes o CD-ROMs, son fácilmente transportables, reproducibles y/o copiables, es evidente la importancia que para la seguridad de los datos del Fichero tiene el control de estos medios.

7.1.1. Los soportes que contengan datos del Fichero, bien como consecuencia de operaciones intermedias propias de la aplicación que los trata, o bien como consecuencia de procesos periódicos de respaldo o cualquier otra operación esporádica, deberán estar claramente identificados con una etiqueta externa que indique de qué fichero se trata, que tipo de datos contiene, proceso que los ha originado y fecha de creación.

7.1.2. Aquellos medios que sean reutilizables, y que hayan contenido copias de datos del Fichero, deberán ser borrados físicamente antes de su reutilización, de forma que los datos que contenían no sean recuperables.

7.1.3. Los soportes que contengan datos del Fichero deberán ser almacenados en lugares a lo que no tengan acceso personas no autorizadas para el uso del Fichero que no estén por tanto relacionadas en el Anexo F.

7.1.4. La salida de soportes informáticos que contengan datos del Fichero fuera de los locales donde está ubicado el Fichero deberá ser expresamente autorizada por el responsable del Fichero. Utilizando para ello el documento adjunto en el anexo G.

8. Procedimientos de respaldo y recuperación

La seguridad de los datos personales del Fichero no sólo supone la confidencialidad de los mismos sino que también conlleva la integridad y la disponibilidad de esos datos.

Para garantizar estos dos aspectos fundamentales de la seguridad es necesario que existan unos procesos de respaldo y de recuperación que, en caso de fallo del sistema informático, permitan recuperar y en su caso reconstruir los datos del Fichero.

8.1.1. Existirá una persona, bien sea el administrador o bien otro usuario expresamente designado, que será responsable de obtener periódicamente una copia de seguridad del fichero, a efectos de respaldo y posible recuperación en caso de fallo.

8.1.2. Estas copias deberán realizarse con una periodicidad, al menos, semanal, salvo en el caso de que no se haya producido ninguna actualización de los datos.

8.1.3. En caso de fallo del sistema con pérdida total o parcial de los datos del Fichero existirá un procedimiento, informático o manual, que partiendo de la última copia de respaldo y del registro de las operaciones realizadas desde el momento de la copia, reconstruya los datos del Fichero al estado en que se encontraban en el momento del fallo. Ese procedimiento está descrito en el Anexo G.

Anexo A. Documentos de Notificación y Decretos

Documento de Notificación a la Agencia de Protección de Datos de Registro del Fichero.

Se adjuntará aquí una copia del documento de notificación de la creación, y en su caso de las posibles modificaciones del Fichero.

En este mismo apartado se recojera una copia de la publicación de la disposición de creación, y si procede de las modificaciónes.

Anexo B. Descripción detallada de la estructura del Fichero o la Base de Datos.

La descripción contendrá al menos los siguientes aspectos:

Ubicación física del Fichero, tipo de soporte, servidor, nombre del área o directorio etc…

Descripción lógica, archivos o tablas, registros o tuplas, campos o columnas, así como el formato, descripción y relaciones entre los mismos.

Gestor de base de datos, mecanismos de recuperación.

Anexo C. Descripción del sistema informático de acceso al fichero.

Descripción del Sistema Informático de acceso al Fichero

El sistema informático o aplicación de acceso al fichero es el conjunto de programas, específicamente diseñados para el caso o de propósito general, con los que normalmente se accede para consultar o actualizar los dato del Fichero.

La descripción deberá al menos contener los siguientes datos:

- *Nombre de la aplicación*
- *Si se trata de un paquete o producto estándar del mercado o de unos programas expresamente diseñados para ese propósito.*
- *Quién y en que fecha se programó.*
- *Responsables del mantenimiento.*
- *Tipo de control de acceso si lo tiene.*
- *Tipo de procedimientos de histórico de operaciones (logging) y de recuperación, si los tiene.*

Anexo D. Entorno de Sistema Operativo y de Comunicaciones del Fichero

Entorno de Sistema Operativo y de Comunicaciones del Fichero
(a ser cumplimentado por el administrador del sistema)

Deberá contener al menos los siguientes datos y aspectos:

Sistema operativo

Nombre y versión
Fabricante
Características generales (monopuesto, multiusuario, compartición de ficheros u otros recursos, etc..)
Control de acceso, características
Archivos de logging y procedimientos de recuperación propios del sistema.
Responsables del mantenimiento

Entorno de comunicaciones (si lo tuviese)

Tipo de red local (Ethernet, otras), ámbito y extensión.
Si existe conexión con otras redes locales o WAN, indicar el tipo de conexión (permanente, esporádica, etcc..), a través de redes públicas como Internet o con conexiones
privadas etc..
Hay compartición de recursos y archivos ?. Si es así indicar que tipo de sistema de red es
utilizado, sus límites y alcance.
Controles de acceso desde la red al sistema del Fichero.

Anexo E. Locales y equipamiento

Locales y equipamiento de los centros de tratamiento

Locales

Descripción de la ubicación física
Tipo de acceso:
Sistemas de continuidad
Equipamiento; armarios ignífugos, etc

Puestos de Trabajo

Descripción Equipos: Servidores, equipos, Impresoras
Relación de puestos de trabajo

Anexo F. Personal autorizado para acceder al Fichero

Nº de inscripción - Nombre de fichero

Responsable del Fichero

Nombre y Apellidos ..... Cargo .....

Fecha .....

Declaración de recepción y aceptación del documento

Declaramos haber leido el documento de seguridad adjunto y aceptamos el cumplimiento de las normas de seguridad expresadas en él, asumiendo las consecuencias que en caso contrario pudieran derivarse por ley.

Administradores del sistema

Nombre y Apellidos ..... Organismo .....

Fecha alta .....

Nombre y Apellidos ..... Organismo .....

Fecha .....

Nombre y Apellidos ..... Organismo .....

Fecha .....

Nombre y Apellidos ..... Organismo .....

Fecha .....

Nombre y Apellidos ..... Organismo .....

Fecha .....

Nombre y Apellidos ..... Organismo .....

Fecha .....

Nombre y Apellidos ..... Organismo .....

Fecha .....

Usuarios del Fichero

Nombre y Apellidos ..... Puesto Nº .....

Fecha .....

Nombre y Apellidos ..... Puesto Nº .....

Fecha .....

Nombre y Apellidos ..... Puesto Nº .....

Fecha .....

Nombre y Apellidos ..... Puesto Nº .....

Fecha .....

Personal autorizado para acceder al Fichero Hoja ...

Nombre y Apellidos ..... Puesto Nº .....

Fecha .....

Nombre y Apellidos ..... Puesto Nº .....

Fecha .....

Nombre y Apellidos ..... Puesto Nº .....

Fecha .....

Nombre y Apellidos ..... Puesto Nº .....

Fecha .....

Nombre y Apellidos ..... Puesto Nº .....

Nº de inscripción NOMBRE DE FICHERO

RESPONSABLE DEL FICHERO

Nombre y apellidos	Cargo	Alta	Baja

RESPONSABLE DE SEGURIDAD

Nombre y apellidos	Cargo	Alta	Baja

ADMINISTRADORES DEL SISTEMA

Nombre y apellidos	Organismo / Unidad Administrativa	Alta	Baja

Nº de inscripción NOMBRE DE FICHERO

USUARIOS DEL FICHERO

Nombre y apellidos	Unidad Administrativa	Nº inventario Puesto Trabajo	Alta	Baja

Anexo G. Procedimientos de control de accesos, respaldo y recuperación y gestión

Procedimientos de control y seguridad

Contendrá al menos los procedimientos siguientes :

- *Procedimiento de asignación y cambio de contraseñas.*
- *Procedimiento de respaldo y recuperación.*
- *Procedimiento de gestión de soportes*

Se adjunta impreso de inventario de soportes y autorización de salida de soportes

INVENTARIO DE SOPORTES

Página nº _____

Fichero:	**NOMBRE DE FICHERO**				
ALTAS		BAJAS			
Nº de orden	Fecha de copia	Motivo			Fecha
		Reutilización	Destrucción	Otros	
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /

Los ficheros de datos se enviarán a los responsables de ficheros en sobre cerrado, por mensajero y con acuse de recibo para garantizar e identificar su recepción.

Cualquier salida de soportes deberá ser autorizada por el Responsable del fichero, de acuerdo con el siguiente documento:

Nº de inscripción	NOMBRE DE FICHERO

AUTORIZACIÓN DE SALIDA DE SOPORTES

Fecha de salida del soporte

SOPORTE	
Identificación	
Contenido	
Ficheros de donde proceden los datos	
Fecha de creación	

FINALIDAD Y DESTINO	
Finalidad	
Destino	
Destinatario	

FORMA DE ENVÍO	
Medio de envío	
Remitente	
Precauciones para el transporte	

AUTORIZACIÓN	
Persona que autoriza	
Cargo / Puesto	
Observaciones	
Firma	

Anexo H. Funciones y obligaciones del personal

FUNCIONES DEL RESPONSABLE DEL FICHERO

El responsable del fichero es el encargado jurídicamente de la seguridad del fichero y de las medidas establecidas en el presente documento, implantará las medidas de seguridad establecidas en él y adoptará las medidas necesarias para que el personal afectado por este documento conozca las normas que afecten al desarrollo de sus funciones.

Designará al responsable de seguridad que figura en el Anexo F.

FUNCIONES DEL RESPONSABLE DE SEGURIDAD

Es el encargado de coordinar y controlar las medidas definidas en el presente documento.

CLASIFICACIÓN DEL PERSONAL DE ADMINISTRACIÓN O PERSONAL INFORMÁTICO

Se distinguen dos situaciones diferentes, que condicionan el tipo de personal que tiene acceso al fichero en cada caso:

- Producción habitual, sin incidencias técnicas. Explotación diaria.
- Errores, cortes, incidencias técnicas de cualquier tipo que detienen la producción.

PERSONAL AUTORIZADO EN PRODUCCIÓN HABITUAL

En el primer caso, el acceso se limita a los siguientes perfiles

- Usuario/Administrador del sistema.

- Operador.

ADMINISTRADORES TÉCNICOS E INFORMÁTICOS GENERALES QUE INTERVIENEN EN SITUACIONES NO HABITUALES

Cuando no existe un personal técnico determinado que se pueda relacionar de forma directa con un fichero o sistema informático y que acceda habitualmente al mencionado fichero o sistema.

Siempre será posible conocer el personal que intervino con posterioridad a la intervención, dejando constancia de ello, identificando al personal técnico, anotándolo en le Registro de Incidencias.

FUNCIONES DE LOS ADMINISTRADORES O PERSONAL INFORMÁTICO

El personal que administra el sistema de acceso al Fichero se puede a su vez clasificar en varias categorías, que no necesariamente deberán estar presentes en todos los casos, siendo en algunas ocasiones asumidas por una misma persona o personas. Estas categorías son:

- Administradores (Red, Sistemas operativos y Bases de Datos). Serán los responsables de los máximos privilegios y por tanto de máximo riesgo de que una actuación errónea pueda afectar al sistema. Tendrán acceso al software (programas y datos) del sistema, a las herramientas necesarias para su trabajo y a los ficheros o bases de datos necesarios para resolver los problemas que surjan.

- Operadores (Red, Sistemas operativos, Bases de Datos y Aplicación). Sus actuaciones están limitadas a la operación de los equipos y redes utilizando las herramientas de gestión disponibles. No deben, en principio, tener

acceso directo a los datos del Fichero, ya que su actuación no precisa de dicho acceso.

- Mantenimiento de los sistemas y aplicaciones. Personal responsable de la resolución de incidencias que puedan surgir en el entono hardware/software de los sistemas informáticos o de la propia aplicación de acceso al Fichero.

- Cualquier otro que la organización establezca.

OBLIGACIONES DEL RESPONSABLE DEL FICHERO

Implantar las medidas de seguridad establecidas en este documento.

El responsable del Fichero deberá garantizar la difusión de este Documento entre todo el personal que vaya a utilizar.

Deberá mantenerlo actualizado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo, según los artículos 8 y 9 de la Normativa de Seguridad.

Deberá adecuar en todo momento el contenido del mismo a las disposiciones vigentes en materia de seguridad de datos.

Entorno de Sistema Operativo y de Comunicaciones

5.3.1 El responsable del Fichero aprobará o designará al administrador que se responsabilizará del sistema operativo y de comunicaciones que deberá estar relacionado en el Anexo F.

5.3.2 En el caso más simple, como es que el Fichero se encuentre ubicado en un ordenador personal y accedido mediante una aplicación local monopuesto, el administrador del sistema operativo podrá ser el mismo usuario que accede usualmente al Fichero.

Sistema Informático o aplicaciones de acceso al Fichero

5.4.1 El responsable del fichero se encargará de que los sistemas informáticos de acceso al Fichero tengan su acceso restringido mediante un código de usuario y una contraseña.

5.4.2 Asimismo cuidará que todos los usuarios autorizados para acceder al Fichero, relacionados en el Anexo F, tengan un código de usuario que será único, y que estará asociado a la contraseña correspondiente, que sólo será conocida por el propio usuario.

Salvaguarda y protección de las contraseñas personales

5.5.1 Sólo las personas relacionadas en el Anexo F, podrán tener acceso a los datos del Fichero.

Gestión de soportes

7.1.4 La salida de soportes informáticos que contengan datos del Fichero fuera de los locales donde está ubicado el Fichero deberá ser expresamente autorizada por el responsable del Fichero.

Procedimientos de respaldo y recuperación

El responsable del Fichero se encargará de verificar la definición y correcta aplicación de las copias de respaldo y recuperación de los datos.

OBLIGACIONES DEL RESPONSABLE DE SEGURIDAD

El responsable de seguridad coordinará la puesta en marcha de las medidas de seguridad, colaborará con el responsable del fichero en la difusión del Documento de seguridad y cooperará con el responsable del fichero controlando el cumplimiento de las mismas.

Gestión de incidencias

6.1.1 El responsable de seguridad habilitará un Libro de Incidencias a disposición de todos los usuarios y administradores del Fichero con el fin de que se registren en él cualquier incidencia que pueda suponer un peligro para la seguridad del mismo.

Analizara las incidencias registradas, tomando las medidas oportunas en colaboración con el responsable del Fichero.

OBLIGACIONES QUE AFECTAN A TODO EL PERSONAL

Puestos de trabajo

5.2.1 Los puestos de trabajo estarán bajo la responsabilidad de algún usuario autorizado que garantizará que la información que muestran no pueda ser visible por personas no autorizadas.

5.2.2 Esto implica que tanto las pantallas como las impresoras u otro tipo de dispositivos conectados al puesto de trabajo deberán estar físicamente ubicados en lugares que garanticen esa confidencialidad.

5.2.3 Cuando el responsable de un puesto de trabajo lo abandone, bien temporalmente o bien al finalizar su turno de trabajo, deberá dejarlo en un estado que impida la visualización de los datos protegidos. Esto podrá realizarse a través de un protector de pantalla que impida la visualización de los datos. La reanudación del

trabajo implicará la desactivación de la pantalla protectora con la introducción de la contraseña correspondiente.

5.2.4 En el caso de las impresoras deberá asegurarse de que no quedan documentos impresos en la bandeja de salida que contengan datos protegidos. Si las impresoras son compartidas con otros usuarios no autorizados para acceder a los datos de Fichero, los responsables de cada puesto deberán retirar los documentos conforme vayan siendo impresos.

5.2.5 Queda expresamente prohibida la conexión a redes o sistemas exteriores de los puestos de trabajo desde los que se realiza el acceso al fichero. La revocación de esta prohibición sera autorizada por el responsable del fichero, quedando constancia de esta modificación en el Libro de incidencias.

5.2.6 Los puestos de trabajo desde los que se tiene acceso al fichero tendrán una configuración fija en sus aplicaciones, sistemas operativos que solo podrá ser cambiada bajo al autorización del responsable de seguridad o por administradores autorizados del anexo F.

Salvaguarda y protección de las contraseñas personales

5.5.2 Cada usuario será responsable de la confidencialidad de su contraseña y, en caso de que la misma sea conocida fortuita o fraudulentamente por personas no autorizadas, deberá registrarlo como incidencia y proceder a su cambio.

Gestión de incidencias

6.1.1 Cualquier usuario que tenga conocimiento de una incidencia es responsable de la comunicación de la misma al administrador del sistema, o en su caso del registro de la misma en el sistema de registro de incidencias del Fichero.

6.1.2 El conocimiento y la no notificación de una incidencia por parte de un usuario será considerado como una falta contra la seguridad del Fichero por parte de ese usuario.

Gestión de soportes

7.1.1 Los soportes que contengan datos del Fichero, bien como consecuencia de operaciones intermedias propias de la aplicación que los trata, o bien como consecuencia de procesos periódicos de respaldo o cualquier otra operación esporádica, deberán estar claramente identificados con una etiqueta externa que indique de qué fichero se trata, que tipo de datos contiene, proceso que los ha originado y fecha de creación.

7.1.2 Aquellos medios que sean reutilizables, y que hayan contenido copias de datos del Fichero, deberán ser borrados físicamente antes de su reutilización, de forma que los datos que contenían no sean recuperables.

7.1.3 Los soportes que contengan datos del Fichero deberán ser almacenados en lugares a lo que no tengan acceso personas no autorizadas para el uso del Fichero que no estén por tanto relacionadas en el Anexo F.

OBLIGACIONES DE LOS ADMINISTRADORES Y PERSONAL INFORMÁTICO

Entorno de sistema operativo y de Comunicaciones

5.3.3 Ninguna herramienta o programa de utilidad que permita el acceso al Fichero deberá ser accesible a ningún usuario o administrador no autorizado en el Anexo F.

5.3.4 En la norma anterior se incluye cualquier medio de acceso en bruto, es decir no elaborado o editado, a los datos del Fichero, como los llamados "queries", editores universales, analizadores de ficheros, etc., que deberán estar bajo el control de los administradores autorizados relacionados en el Anexo F.

5.3.5 El administrador deberá responsabilizarse de guardar en lugar protegido las copias de seguridad y respaldo del Fichero,de forma que ninguna persona no autorizada tenga acceso a las mismas.

5.3.6 Si la aplicación o sistema de acceso al Fichero utilizase usualmente ficheros temporales, ficheros de "logging", o cualquier otro medio en el que pudiesen ser grabados copias de los datos protegidos, el administrador deberá asegurarse de que esos datos no son accesibles posteriormente por personal no autorizado.

5.3.7 Si el ordenador en el que está ubicado el fichero está integrado en una red de comunicaciones de forma que desde otros ordenadores conectados a la misma sea posible el acceso al Fichero, el administrador responsable del sistema deberá asegurarse de que este acceso no se permite a personas no autorizadas.

Sistema Informático o aplicaciones de acceso al Fichero

5.4.3 Si la aplicación informática que permite el acceso al Fichero no cuenta con un control de acceso, deberá ser el sistema operativo, donde se ejecuta esa aplicación, el que impida el acceso no autorizado, mediante el control de los citados códigos de usuario y contraseñas.

Salvaguarda y protección de las contraseñas personales

5.5.5 Las contraseñas se asignarán y se cambiarán mediante el mecanismo y periodicidad que se determina en el Anexo G. Este mecanismo de asignación y distribución de las contraseñas deberá garantizar la confidencialidad de las mismas, y será responsabilidad del administrador del sistema.

5.5.6 El archivo donde se almacenen las contraseñas deberá estar protegido y bajo la responsabilidad del administrador del sistema.

Procedimientos de respaldo y recuperación

8.1.1 Existirá una persona, bien sea el administrador o bien otro usuario expresamente designado, que será responsable de obtener periódicamente una copia de seguridad del fichero, a efectos de respaldo y posible recuperación en caso de fallo.

8.1.2 Estas copias deberán realizarse con una periodicidad, al menos, semanal, salvo en el caso de que no se haya producido ninguna actualización de los datos.

8.1.3 En caso de fallo del sistema con pérdida total o parcial de los datos del Fichero existirá un procedimiento, informático o manual, que partiendo de la última copia de respaldo y del registro de las operaciones realizadas desde el momento de la copia, reconstruya los datos del Fichero al estado en que se encontraban en el momento del fallo. Ese procedimiento está descrito en el Anexo G.

Anexo I. Procedimiento de Notificación y gestión de incidencias

Procedimiento de Notificación y gestión de incidencias

Se describira el procedimiento de notificación y gestión de incidencias

En la notificación se hará constar :

- *Tipo de incidencia*
- *Fecha y hora en que se produjo*
- *Persona que realiza la notificación*
- *Persona a quien se comunica*
- *Efectos que puede producir la incidencia*
- *Descipción detallada de la misma*

Se adjunta el impreso de notificación manual que podra ser utilizado para la notificación de incidencias

Cuando ocurra una incidencia, el usuario o administrador deberá registrarla en el Libro de Incidencias o comunicarla al Responsable de seguridad para que a su vez proceda a su registro.

Se mantendrán las incidencias registradas de los 12 últimos meses.

A continuación se adjunta el impreso de notificación manual que podrá ser utilizado para la notificación de incidencias.

Impreso de notificación de incidencias

Incidencia nº: **|_____|** (A ser rellenado por el Responsable de Seguridad)	
Fecha de notificación: /__/__/____/	
Tipo de incidencia: (Anotar todos los detalles de interés de la incidencia,	
Descripción detallada de la incidencia	
Fecha y hora en que se produjo la incidencia	
Persona(s) que realiza(n) la notificación: (Especificar si son usuarios o no del Fichero)	
Persona(s) a quien(es) se comunica:	
Efectos que puede producir: (En caso de no subsanación o incluso independientemente de ella)	
Persona que realiza la comunicación: **Fdo.:**_____	

Nº de inscripción NOMBRE DE FICHERO

8

Seguridad Física

Artículo 19. Control de acceso físico.

Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los locales donde se encuentren ubicados los sistemas de información con datos de carácter personal.

8.1 CONTROL DE ACCESO FÍSICO

Además de incluir todo el capítulo 3 habrá que obligar, por el artículo 19 del Reglamento, el control de acceso físico al sistema. Para ello habrá que cerrar al público los locales donde se ubiquen los sistemas con ficheros con datos personales.

Para poder permitir solamente el acceso a los locales a las personas autorizadas habrá diferentes soluciones. Aunque sería suficiente la explicada en el punto 8.2.1 nosotros recomendaremos al menos el 8.2.2 pero, lo ideal sería el 8.2.4.

8.1.1 LLAVE

Los locales podrán estar protegidos por cerraduras con llaves de uso común, pero teniendo la posesión de las llaves solamente el personal autorizado.

8.1.2 LLAVE MAGNÉTICA

Con este tipo de solución se podrá tener registros de las personas que entran en la sala en todo momento. Obviamente, la llave sólo podrá estar en posesión del personal autorizado.

Si en 8.1.1 y 8.1.2 se perdiese alguna de las llaves habría dar de alta en el registro de incidencias según el Art. 10 del Reglamento.

8.1.3 PERSONAL DE SEGURIDAD

Otra solución que puede ser bastante buena sería la contratación de personal de seguridad y que estos arbitren el acceso a la sala.

8.1.4 SENSORES BIOMÉTRICOS

Este método de acceso sería el ideal. Aunque parezca que su coste es muy elevado, en la actualidad ha bajado enormemente.

El acceso se basa en que nunca dos mediciones (huellas dactilares, iris, etc.) puedan ser iguales, excepto la del individuo que debe tener acceso. Estos sensores son muchos más seguros y no se corre el riesgo de pueda ser robada la llave.

8.1.5 MIXTOS

Este método se basa en el uso de dos métodos de acceso simultáneamente. Por ejemplo, usar los puntos 8.2.2 y 8.2.3.

8.2 GESTIÓN FÍSICA DE LOS SOPORTES

El artículo 20.3 dispone que cuando los soportes vayan a salir fuera de los locales donde se almacenan los ficheros se adoptarán las medidas necesarias para impedir cualquier recuperación indebida de la información almacenada en ellos. Además, en el caso de que un soporte vaya a ser desechado o reutilizado exige que se adopten medidas para evitar la recuperación posterior de información personal. Una medida aceptable es el formateo a bajo nivel del dispositivo de almacenamiento o su destrucción física o incineración.

9

Auditoria

Artículo 17. Auditoría.

1. Los sistemas de información e instalaciones de tratamiento de datos se someterán a una auditoría interna o externa, que verifique el cumplimiento del presente Reglamento, de los procedimientos e instrucciones vigentes en materia de seguridad de datos, al menos, cada dos años.

2. El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles al presente Reglamento, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias.

Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas.

3. Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia de Protección de Datos.

9.1 INTRODUCCIÓN

Una auditoria es una opinión profesional sobre si “los sistemas de información e instalaciones de tratamiento de datos” presentan adecuadamente la realidad que pretende reflejar y/o cumple las condiciones que han sido prescritas. Se van a encontrar dos tipos de auditorias claramente diferenciadas:

- ***EXTERNA***: se encarga a una persona o empresa ajena a la propia para que el estudio sea más independiente y objetivo.

- ***INTERNA***: por el contrario, este tipo de auditoria es realizada por el propio equipo que gestiona el sistema.

Para ambos se recomienda que los profesionales que lo realicen tengan formación tanto es aspectos legales como técnico.

En la siguiente tabla se muestra las ventajas y desventajas principales para ambos tipos:

TIPOS	VENTAJAS	DESVENTAJAS
EXTERNA	INDEPENDENCIA OBJETIVIDAD PROFESIONALIDAD	ALTO COSTE
INTERNA	COSTE CERO	DEPENDENCIA

9.2 FASES

Nos podremos encontrar según el punto de vista diferentes fases. Nosotros la dividiremos en las cuatro siguientes:

1. Análisis de ficheros.
2. Elaboración y supervisión de documentación.
3. Evaluación de la aplicación.
4. Formación ulterior.

La duración de cada fase puede variar entre una semana y un mes dependiendo del tamaño de la empresa u organización.

9.2.1 ANÁLISIS DE LOS FICHEROS

En esta primera fase, se comprobará el nivel de cumplimiento de la normativa sobre Protección de Datos Personales, tanto de la LOPD como del Reglamento sobre Medidas de Seguridad, en la empresa. Para ello, se realizaran reuniones con los responsables (asesoría jurídica y del sistema informático) para la realización de un cuestionario de seguridad[1] con la finalidad de obtener:

- Un análisis de las posibles bases de datos de la empresa, así como de su registro en la Agencia de Protección de Datos. Si fuera necesario, se inscribirán en el mencionado organismo.

- El nivel de seguridad aplicable para cada una de las bases de datos encontradas.

- Las medidas de seguridad que se cumplen, así como las que fuesen necesario implementar con el fin de lograr una correcta adaptación al Reglamento.

Además de las reuniones con los responsables, habrá que reunirse con los empleados, así como contrastar la información con la realidad. No es la primera vez ni la última que no se corresponden las reuniones con la realidad en la empresa. Por este motivo el auditor no deja de ser como un detective descubriendo los ficheros tratados.

9.2.2 ELABORACIÓN Y SUPERVISIÓN DE LA DOCUMENTACIÓN

En esta fase se procederá a elaborar los documentos que exige la ley. Para ello, se comprenden las siguientes acciones:

---

[1] Véase sección 9.3

- Redacción del Documento de Seguridad exigido por el Reglamento.

- Creación de un registro de incidencias, registro de soportes, registro de accesos.

- Relación de los usuarios autorizados (habrá que evaluar sobre la suficiencia o exceso en su grado de autorización).

- Elaboración de los escritos de autorización que deberá emitir el responsable para determinados procesos en su manipulación.

9.2.3 EVALUACIÓN DE LA APLICACIÓN

El objetivo en esta etapa será evaluar la ejecución de las medidas de adaptación a la normativa de seguridad. Para ello se deberá:

- Supervisar y asesorar jurídicamente en cuanto a las medidas de seguridad implementadas.

- Evaluación de las aplicaciones elaboradas por los técnicos de la empresa, así como de las modificaciones técnicas y organizativas efectuadas.

- Realización de un informe[2] de auditoria, en cumplimiento del artículo 17 del Reglamento.

9.2.4 FORMACIÓN ULTERIOR

[2] Véase sección 9.4

En esta última fase se formará a los empleados en los meses siguientes debido a la gran variedad de ofertas de mercado y a la evolución continua del mercado de trabajo.

9.3 CUESTIONARIO DE SEGURIDAD

La realización del cuestionario de seguridad que se efectúa en la fase primera deberá ser amplio, claro y conciso. Uno de los grandes problemas de este tipo de cuestionarios es que muchas veces lo que se pregunta y la respuesta no tienen nada que ver con el objetivo de la pregunta, debido a quien ha hecho el cuestionario no es la misma persona que va a la empresa a la reunión. Todo esto ocurría a no ser que se formase al entrevistador y se le explicase el objetivo de cada pregunta.

Aunque no hay ningún cuestionario tipo, a continuación mostramos un pequeño extracto de uno para que se vea qué puntos se deben tratar. Tenga en cuenta que un buen cuestionario es la base de una buena auditoria. Por ello, los cuestionarios deberán estar preparados con rigor de cara a sacar el máximo partido.

La finalidad de este formulario es la de recoger la mayor cantidad de información acerca de su empresa para determinar las necesidades en materia de seguridad de datos de acuerdo con la LOPD 15/1999 y el Reglamento de Medidas de Seguridad 994/1999, de forma que permita realizar una estimación fiable del tiempo y recursos necesarios para adecuar su empresa a la normativa vigente.

Empresa/ Organismo:

Domicilio:

Nombre del Responsable:

Fecha:

DATOS GENERALES

1. ¿En qué Hardware se basan sus Sistemas de Información?

   ☐ Ordenadores Personales
   ☐ Ordenador Personal en red
   ☐ Equipos medios
   ☐ Equipos grandes

2. ¿Cuántos Centros de Proceso de Datos tiene su organización y dónde están ubicados?

3. Plataformas instaladas

4. Número de PC's y de usuarios

5. Si es un holding de empresas, ¿qué empresas forman parte de este holding?

6. Los ficheros están distribuidos:

7. ¿Tiene dados de alta sus ficheros de datos personales en la Agencia de Protección de Datos (APD)?

8. ¿Se transfieren datos de carácter personal a otros países? En caso afirmativo indicar que paises

RESPONSABLE DE SEGURIDAD

1. ¿Existe Responsable de Fichero? En caso afirmativo, indicar quién es.

2. ¿El Responsable del Fichero ha designado Responsables de Seguridad para coordinar y controlar las medidas definidas en el Documento de Seguridad? En caso afirmativo, indicar

quiénes son.

FUNCIONES Y OBLIGACIONES DEL PERSONAL

1. ¿Están definidas y documentadas las funciones y obligaciones de cada una de las personas?

2. ¿Ha adoptado el Responsable del Fichero las medidas necesarias para que el personal conozca las normas de seguridad y las consecuencias en las que pueda incurrir en caso de incumplimiento?

CONTROL DE ACCESO FÍSICO

1. ¿El acceso físico a los locales donde se encuentran ubicados los sistemas de información están limitados al personal autorizado?

IDENTIFICACIÓN Y AUTENTIFICACIÓN

1. ¿Están actualizadas la lista de los usuarios que tienen acceso autorizado al sistema de información?

2. Existen procedimientos de identificación y autentificación ¿En qué están basados?

3. ¿Existen procedimientos de asignación, distribución y almacenamiento de los procedimientos de identificación y autentificación que garanticen su confidencialidad e integridad?

4. ¿Existe un mecanismo que permite la identificación de forma inequívoca y personalizada verificando la autenticación?

5. ¿ Está limitada la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información?

CONTROL DE ACCESO

1. ¿Tienen los usuarios acceso únicamente a aquellos datos y recursos que precisan para el desarrollo de sus funciones?

2. ¿Contiene la relación de usuarios autorizados, el tipo de acceso autorizado a cada uno de ellos?

3. ¿Son las personas expresamente autorizadas en el Documento de Seguridad las únicas que pueden conceder, alterar o anular el acceso autorizado a los usuarios del fichero?

COPIAS DE SEGURIDAD

1. ¿Se encarga el Responsable del Fichero de verificar la definición y correcta aplicación de los procedimientos de realización de copias de seguridad?

2. ¿Garantizan los procedimientos de realización de copias de seguridad de datos su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción?

3. ¿Se conserva una copia de las copias de seguridad en un lugar diferente al que se encuentran los equipos informáticos?

AUDITORÍA

1. ¿Con qué frecuencia se realiza?

2. ¿El informe de auditoria dictamina sobre la adecuación de las medidas y controles, identifica deficiencias y propone medidas correctoras o complementarias?

3. Los informes, ¿una vez analizados se adoptan las medidas adecuadas?

DATOS REALES

1. ¿Está asegurada la inexistencia de pruebas con datos reales anteriormente a la implantación o modificación de los sistemas de información, salvo que se asegure el nivel de seguridad correspondiente al fichero tratado?

DOCUMENTO DE SEGURIDAD

1. ¿Existe documento de seguridad?

2. ¿Está claramente definido el ámbito de aplicación del documento de seguridad?

3. ¿Contiene las medidas, normas, procedimientos y reglas estándar encaminadas a garantizar el nivel de seguridad exigido en el R.D.994/1999?

4. ¿Están descritas las funciones y obligaciones del personal?

5. ¿Describe los procedimientos de notificación, gestión y respuesta ante las incidencias?

6. ¿Describe los procedimientos de realización de las copias de seguridad?

7. ¿Está adecuado a las últimas disposiciones vigentes en materia de seguridad de datos de carácter personal?

8. ¿Contiene la identificación del Responsable de Seguridad?

9. ¿Contiene los controles periódicos que se deben realizar para verificar lo dispuesto en el propio documento?

10. ¿Describe las medidas que hay que adoptar cuando un soporte vaya a ser desechado o

reutilizado?

REGISTRO DE INCIDENCIAS

1. ¿Hay un registro de las incidencias en el que se hace constar el tipo, el momento en que se ha producido, la persona que la notifica, a quién se comunica y los efectos derivados de la misma?

2. ¿Se consignan los procedimientos de recuperación de datos, indicando la persona que ejecutó el proceso, los datos restaurados, y en su caso qué datos ha sido necesario grabar manualmente en el proceso de recuperación?

GESTIÓN DE SOPORTES

1. ¿Son inventariados y se almacenan en un lugar con acceso restringido al personal autorizado?

2. ¿Es el Responsable del Fichero el único que puede autorizar la salida de soportes informáticos, que contengan datos de carácter personal, fuera de los locales en los que está ubicado el fichero?

3. ¿Existe un sistema de registro de entrada de soportes informáticos que permita conocer el tipo, la fecha y hora, el emisor, el número de soportes, el tipo de información contenida, la forma de envío y el responsable de la recepción que deberá estar debidamente autorizado?

4. ¿Existe un sistema de registro de salida de soportes informáticos que permita conocer el tipo, la fecha y hora, el emisor, el número de soportes, el tipo de información contenida, la forma de envío y el responsable de la entrega que deberá estar debidamente autorizado?

5. ¿Qué medidas se realizan cuando un soporte va a ser desechado o reutilizado?

DISTRIBUCIÓN DE SOPORTES

1. ¿Se realiza la distribución de soportes cifrando los datos?

REGISTRO DE ACCESOS

1. ¿Se guarda, como mínimo, de cada acceso la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado?

2. ¿Se guarda la información que permite identificar el registro accedido?

3. ¿Cuál es el periodo de conservación de los datos registrados?

COMUNICACIONES

1. ¿La transmisión de datos a través de redes de telecomunicaciones, se realiza cifrando dichos datos?

9.4 REALIZACIÓN DE UN INFORME DE AUDITORIA

Nos vamos a encontrar diferentes maneras de realizar informes de auditorias, aunque todos ellos tienen en común los siguientes puntos:

1. *IDENTIFICACIÓN DEL INFORME*. El objetivo es poder diferenciarlo de otros informes.

2. *IDENTIFICACIÓN DE LAS PERSONAS QUE LO HAN ENCARGADO*.

3. *IDENTIFICACIÓN DE LA EMPRESA U ORGANISMO AUDITADO*.

4. *OBJETIVOS*. En este parte identificamos el propósito de la auditoria, así como de los objetivos incumplidos.

5. *NORMATIVA APLICADA*. Se identifica las normas legales aplicadas, así como de las posibles excepciones.

6. *ALCANCE*. Se deberá concretar la extensión de la auditoria: área organizativa, departamento, período de la misma.

7. *CONCLUSIONES*. En este punto se incluirán las diferentes opiniones, tanto si son favorables como si no.

8. *FECHA*.

9. *FIRMA*.

A continuación mostramos un ejemplo de un informe

Informe de auditoría LOPD

Empresa: RLSOFT

Responsable : Esper Rivas

Descripción del caso

Una empresa de servicios alberga las páginas web de otra. El servidor realiza una copia de seguridad total una vez a la semana. Las copias se ubican en la misma sala. Para las copias de seguridad se emplea el propio software incluido en el sistema operativo (LINUX) y usa cintas DAT cuyo lector está ubicado en la misma CPU. Para subir las nuevas páginas la empresa usa el servicio ftp. El servidor es un sistema Linux.

Objetivo, ámbito y alcance

Realizar una auditoria LOPD que determine el nivel de adaptación de la empresa de servicios RLSOFT a los requisitos marcados por la “LEY ORGÁNICA 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal” y el “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" , auditoria que se realizará únicamente en el ámbito que afecta a los servicios de Hosting que esta empresa presta a una tercera empresa de nombre JXJSA y que afectará, por lo tanto, a todas las áreas de la empresa que directa o indirectamente intervengan en el tratamiento de datos de carácter personal propiedad de JXJSA y en los que RLSOFT actúa como encargada del tratamiento.

No se realizará, por tanto, la auditoria de cualesquiera otros datos de carácter personal que RLSOFT pudiese tratar en el desarrollo de sus funciones.

El período para la realización de la auditoria será de 4 semanas.

Normativa aplicada, hechos observados y conclusiones

Normativa relativa al reglamento

Artículo 4.- ***Aplicación de los niveles de seguridad.***

1.- Todos los ficheros que contengan datos de carácter personal deberán adoptar las medidas de seguridad calificadas como de nivel básico.

Hechos observados

- ✓ Tras un análisis de los datos objeto del tratamiento se ha determinado que estos son de nivel básico.

Medias correctoras

- ✓ No detectadas.

Artículo 5.- ***Acceso a datos a través de redes de comunicaciones.***

Las medidas de seguridad exigibles a los accesos a datos de carácter personal a través

de redes de comunicaciones deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local.

Hechos observados

- ✓ Hay un acceso a los datos desde el cliente mediante ftp para actualizar los datos. Este mecanismo de conexión es inseguro, ya que no garantiza de forma razonable (es muy fácil interceptar la transmisión y obtener la contraseña) la confidencialidad de las contraseñas tal y como exige el articulo 11.2

Medias correctoras

- ✓ Modificar el método de transmisión de información usando un método con cifrado de datos.

Artículo 7.- *Ficheros temporales.*

1.- Los ficheros temporales deberán cumplir el nivel de seguridad que les corresponda con arreglo a los criterios establecidos en el presente Reglamento.

2.- Todo fichero temporal será borrado una vez que haya dejado de ser necesario para los fines que motivaron su creación.

Hechos observados

- ✓ El sistema informático en el que están almacenados los datos genera de forma automática ficheros temporales que se borran también automáticamente, salvo fallos en el sistema.
- ✓ No existe un procedimiento de revisión y eliminación de esos ficheros temporales que el sistema pueda haber dejado sin borrar.

Medias correctoras

- ✓ Desarrollar un procedimiento para la revisión y eliminación de los ficheros temporales generados por el sistema.

Artículo 8.- ***Documento de seguridad.***

1.- El responsable del fichero elaborará e implantará la normativa de seguridad, mediante un documento de obligado cumplimiento para el personal con acceso a los datos automatizados de carácter personal y a los sistemas de información.

Hechos observados

- ✓ Existe un documento de seguridad.

Medias correctoras

- ✓ No se observan.

Artículo 10.- ***Registro de incidencias.***

El procedimiento de notificación y gestión de incidencias contendrá necesariamente un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, la persona que realiza la notificación, a quién se comunica y los efectos que se hubieran derivado de la misma.

Hechos observados

- ✓ El único registro de incidencias esta constituido por los “log” del sistema. Sin embargo, estos no recogen toda la información exigible por el reglamento.

Medias correctoras

- ✓ Mantener un registro de incidencias en el que se reflejen todos los datos que indica el artículo 10.

Artículo 11.- ***Identificación y autenticación.***

2.- Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad

3.- Las contraseñas se cambiarán con la periodicidad que se determine en el documento de seguridad y mientras estén vigentes se almacenarán de forma ininteligible.

Hechos observados

- ✓ El sistema (LINUX sobre MySQL) provee los mecanismos de identificación y autenticación para los administradores del sistema, únicos usuarios con acceso a los datos, que satisfacen las exigencias del artículo 11.2.
- ✓ No se ha determinado la frecuencia de cambio de las contraseñas. Estas se modifican según el criterio de los administradores.

Medias correctoras

- ✓ Determinar una frecuencia de cambio de las contraseñas y registrarla en el documento.

Artículo 12.- ***Control de acceso.***

1.- Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.

2.- El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a datos o recursos con derechos distintos de los autorizados.

Hechos observados

- ✓ Solo los administradores y las personas autorizadas para el envío de datos por ftp desde la empresa RLSOFT tienen acceso autorizado a los datos de carácter personal. Ningún otro usuario que no esté autorizado puede acceder a los

mismos. Necesitan ese acceso para la administración y tratamiento de esos datos.

Medias correctoras

- ✓ No se observan.

Artículo 13.- ***Gestión de soportes.***

1.- Los soportes informáticos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y almacenarse en un lugar con acceso restringido al personal autorizado para ello en el documento de seguridad.

Hechos observados

- ✓ Los soportes con datos de carácter personal son las cintas que almacenan las copias de seguridad de los soportes que envía la empresa RLSOFT para la actualización de los datos. Estas cintas se etiquetan y almacenan en la sala de servidores que es de acceso restringido a los administradores, único personal autorizado para acceder a los datos.
- ✓ No existe un inventario de soportes.
- ✓ En la misma cinta de copias de seguridad se almacenan datos de todo el volumen lo que puede implicar que se almacenen datos de diferentes niveles de seguridad en una misma cinta. Este hecho origina un problema de seguridad a la hora de acceder a los datos (un usuario puede estar autorizado para acceder a unos datos y no a otros) y para el borrado de los datos cuando estos dejan de ser útiles para la finalidad con que estaban siendo tratados. Habrá que borrar del fichero unos datos, pero no los otros.

Medias correctoras

- ✓ Implementar un inventario de soportes.
- ✓ Revisar el hecho de que se graben en el mismo soporte datos de diferentes niveles de seguridad y verificar que los recursos técnicos y organizativos permiten tanto un control del acceso como un borrado selectivo de los datos si fuese necesario.

Artículo 14.- Copias de respaldo y recuperación

2.- Los procedimientos establecidos para la realización de copias de respaldo y para la recuperación de los datos deberá garantizar su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

3. Deberán realizarse copias de respaldo, al menos semanalmente, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.

Hechos observados

- ✓ Las copias se realizan una vez por semana. Esto no es suficiente para garantizar una recuperación adecuada de los datos ya que la frecuencia de actualización es variable, cuando el cliente lo solicita.

Medias correctoras

- ✓ Realizar además de las copias de seguridad planificadas una cada vez que los datos son actualizados.

Normativa relativa a la LOPD

Principios de la protección de datos

Artículo 4. *Calidad de los datos.*

Hechos observados

- ✓ Los datos de carácter personal son tratados de acuerdo a las instrucciones dadas por el responsable del tratamiento, con la finalidad que este ha determinado, no siendo usados para ningún otro fin.
- ✓ Son actualizados con la frecuencia que determina el responsable del tratamiento y

cancelados cuando dejan de ser necesarios para la prestación del servicio.

Medias correctoras

- ✓ No se estiman.

Artículo 12. ***Acceso a los datos por cuenta de terceros.***

2. La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar.

3. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

Hechos observados

- ✓ Aunque existe un contrato de prestación de servicios, este no recoge ningún aspecto relativo al tratamiento de los datos de carácter personal.
- ✓ Aunque los datos son eliminados o devueltos habitualmente al responsable del tratamiento una vez que ya no son útiles, no existe un procedimiento establecido por contrato para garantizar esa eliminación en todos los casos.

Medias correctoras

- ✓ Redactar el contrato de prestación de servicios recogiendo todos los aspectos exigidos en el articulo 12.2 y 12.3 de la LOPD, incluyendo la obligación de eliminar

los datos a la finalización del contrato o cuando estos ya no sean necesarios para la prestación del servicio.

Vigo, 12 de Mayo de 2002

Fdo: José Rodríguez López

10

Documento de Seguridad

Artículo 15. Documento de seguridad.

El documento de seguridad deberá contener, además de lo dispuesto en el artículo 8 del presente Reglamento, la identificación del responsable o responsables de seguridad, los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento y las medidas que sea necesario adoptar cuando un soporte vaya a ser desechado o reutilizado.

10.1 INTRODUCCIÓN

Para la realización del documento de seguridad de nivel medio, todo lo dicho en el capítulo 7 tiene la misma importancia en éste. Nos gustaría volver a comentar que los ejemplos de cómo debe ser un documento de seguridad no puede copiarse, si no que hay que hacer adaptaciones en cada caso. Con esto queremos explicar que cada sistema de información es diferente. Aunque parezca que sean similares, siempre habrá diferencias, a veces muy sutiles.

10.2 PUNTOS A TENER EN CUENTA

Además de los puntos descritos en la sección 7.2, deberá contener la identificación del responsable o responsables de seguridad, los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento y las medidas que sea necesario adoptar cuando un soporte vaya a ser desechado o reutilizado (artículo 15 del Reglamento de Medidas de Seguridad).

A continuación se muestra un ejemplo de un documento de seguridad que como en el capítulo 7 ha sido obtenido de la página web de la Agencia de Protección de Datos de la Comunidad de Madrid:

10. EJEMPLO

Documento de Seguridad para ficheros automatizados de datos de carácter personal con nivel de seguridad medio

Fichero

Nº inscripción	NOMBRE DE FICHERO	

NOMBRE EMPRESA

Dirección General / Órgano / Organismo / Entidad

Fecha versión del Borrador del Documento de Seguridad	7 de junio de 2000
Versión	
Sistema de Información	

ÍNDICE

ANEXOS

1. Objeto del documento

El presente documento responde a la obligación establecida en el artículo 8 del Real Decreto 994/1999 de 11 de Junio en el que se regulan las medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

El fichero de datos: **NOMBRE DE FICHERO**, en adelante el Fichero, descrito en el documento de Notificación a la Agencia de Protección de Datos de la NOMBRE DE LA EMPRESA, que se adjunta en el Anexo A, se encuentra oficialmente clasificado como de nivel de seguridad **medio**, atendiendo a las condiciones descritas en el artículo 4 del Real Decreto citado, siendo por tanto aplicable a él todas las medidas de seguridad de nivel **medio** que se establecen en el Capítulo II del citado decreto.

2. Ámbito de aplicación

Este documento ha sido elaborado bajo la responsabilidad de la persona descrita en el apartado (1) del documento adjunto en el Anexo A, quien, como responsable del Fichero, se compromete a implantar y actualizar ésta Normativa de Seguridad de obligado cumplimiento para todo el personal con acceso a los datos protegidos o a los sistemas de información que permiten al acceso a los mismos.

Todas las personas que tengan acceso a los datos del Fichero, bien a través del sistema informático **NOMBRE DEL SISTEMA INFORMÁTICO** habilitado para acceder al mismo, o bien a través de cualquier otro medio automatizado de acceso al Fichero, se encuentran obligadas por ley a cumplir lo establecido en este documento, y sujetas a las consecuencias que pudieran incurrir en caso de incumplimiento.

Una copia de este documento con la parte que le afecte será entregada, para su conocimiento, a cada persona autorizada a acceder a los datos del Fichero, siendo requisito obligatorio para poder acceder a esos datos el haber firmado la recepción del mismo.

3. Recursos protegidos

La protección de los datos del Fichero frente a accesos no autorizados se deberá realizar mediante el control, a su vez, de todas las vías por las que se pueda tener acceso a dicha información.

Los recursos que, por servir de medio directo o indirecto para acceder al Fichero, deberán ser controlados por esta normativa son:

1) Los centros de tratamiento y locales donde se encuentren ubicados los ficheros o se almacenen los soportes que los contengan, su descripción figura en el Anexo E.

2) Los puestos de trabajo, bien locales o remotos, desde los que se pueda tener acceso al Fichero. La relación de esos puestos de trabajo está descrita en el Anexo E.

3) Los servidores, si los hubiese, y el entorno de sistema operativo y de comunicaciones en el que se encuentra ubicado el Fichero, que está descrito en el Anexo D.

4) Los sistemas informáticos, o aplicaciones establecidos para acceder a los datos, descritos en el Anexo C.

4. Funciones y obligaciones del personal

El personal afectado por esta normativa se clasifica en dos categorías:

1) **Administradores del sistema**, encargados de administrar o mantener el entorno operativo del Fichero. Este personal deberá estar explícitamente relacionado en el Anexo F, ya que por sus funciones pueden utilizar

herramientas de administración que permitan el acceso a los datos protegidos saltándose las barreras de acceso de la Aplicación.

2) **Usuarios del Fichero**, o personal que usualmente utiliza el sistema informático de acceso al Fichero, y que también deben estar explícitamente relacionados en el Anexo F.

Además del personal anteriormente citado existirá un **Responsable de Seguridad del Fichero** cuyas funciones serán las de coordinar y controlar las medidas definidas en el documento, sirviendo al mismo tiempo de enlace con el **Responsable del Fichero**, sin que esto suponga en ningún caso una delegación de la responsabilidad que corresponde a éste último, de acuerdo con el R.D. 994/1999 de 11 de Junio.
Este documento es de obligado cumplimiento para todos ellos. Las funciones y obligaciones del personal están descritas en el Anexo H. Sin embargo, los administradores del sistema deberán además atenerse a aquellas normas, más extensas y estrictas, que se referencian en el Anexo G, y que atañen, entre otras, al tratamiento de los respaldos de seguridad, normas para el alta de usuarios y contraseñas, así como otras normas de obligado cumplimiento en la unidad administrativa a la que pertenece el Fichero.

5. Normas y procedimientos de seguridad

5.1 Centros de tratamiento y locales

Los locales donde se ubiquen los ordenadores que contienen el Fichero deben ser objeto de especial protección que garantice la disponibilidad y confidencialidad de los datos protegidos, especialmente en el caso de que el Fichero esté ubicado en un servidor accedido a través de una red.

5.1.1. Los locales deberán contar con los medios mínimos de seguridad que eviten los riesgos de indisponibilidad del Fichero que pudieran producirse como

consecuencia de incidencias fortuitas o intencionadas. La descripción de esos medios se encuentra en el Anexo E.

5.1.2. El acceso a los locales donde se encuentre el fichero deberá estar restringido exclusivamente a los administradores del sistema que deban realizar labores de mantenimiento para las que sean imprescindibles el acceso físico.

5.2 Puestos de trabajo

Son todos aquellos dispositivos desde los cuales se puede acceder a los datos del Fichero, como, por ejemplo, terminales u ordenadores personales.

Se consideran también puestos de trabajo aquellos terminales de administración del sistema, como, por ejemplo, las consolas de operación, donde en algunos casos también pueden aparecer los datos protegidos del Fichero.

5.2.1. Cada puesto de trabajo estará bajo la responsabilidad de una persona de las autorizadas en el Anexo F, que garantizará que la información que muestra no pueda ser vista por personas no autorizadas.

5.2.2. Esto implica que tanto las pantallas como las impresoras u otro tipo de dispositivos conectados al puesto de trabajo deberán estar físicamente ubicados en lugares que garanticen esa confidencialidad.

5.2.3. Cuando el responsable de un puesto de trabajo lo abandone, bien temporalmente o bien al finalizar su turno de trabajo, deberá dejarlo en un estado que impida la visualización de los datos protegidos. Esto podrá realizarse a través de un protector de pantalla que impida la visualización de los datos. La reanudación del trabajo implicará la desactivación de la pantalla protectora con la introducción de la contraseña correspondiente.

5.2.4. En el caso de las impresoras deberá asegurarse de que no quedan documentos impresos en la bandeja de salida que contengan datos protegidos. Si las impresoras son compartidas con otros usuarios no autorizados para acceder a los datos de Fichero, los responsables de cada puesto deberán retirar los documentos conforme vayan siendo impresos.

5.2.5. Queda expresamente prohibida la conexión a redes o sistemas exteriores de los puestos de trabajo desde los que se realiza el acceso al fichero. La revocación de esta prohibición será autorizada por el responsable del fichero, quedando constancia de esta modificación en el Libro de incidencias.

5.2.6. Los puestos de trabajo desde los que se tiene acceso al fichero tendrán una configuración fija en sus aplicaciones, sistemas operativos que solo podrá ser cambiada bajo al autorización del responsable de seguridad o por administradores autorizados del anexo F.

5.3 Entorno de Sistema Operativo y de Comunicaciones

Aunque el método establecido para acceder a los datos protegidos del Fichero es el sistema informático referenciado en el Anexo C, al estar el fichero ubicado en un ordenador con un sistema operativo determinado y poder contar con unas conexiones que le comunican con otro ordenadores, es posible, para las personas que conozcan estos entornos, acceder a los datos protegidos sin pasar por los procedimientos de control de acceso con los que pueda contar la aplicación.

Esta normativa debe, por tanto, regular el uso y acceso de las partes del sistema operativo, herramientas o programas de utilidad, o del entorno de comunicaciones, de forma que se impida el acceso no autorizado a los datos de Fichero.

5.3.1. El sistema operativo y de comunicaciones del Fichero deberá tener al menos un responsable, que, como administrador deberá estar relacionado en el Anexo F.

5.3.2. En el caso más simple, como es que el Fichero se encuentre ubicado en un ordenador personal y accedido mediante una aplicación local monopuesto, el

administrador del sistema operativo podrá ser el mismo usuario que accede usualmente al Fichero.

5.3.3. Ninguna herramienta o programa de utilidad que permita el acceso al Fichero deberá ser accesible a ningún usuario o administrador no autorizado en el Anexo F.

5.3.4. En la norma anterior se incluye cualquier medio de acceso en bruto, es decir no elaborado o editado, a los datos del Fichero, como los llamados "queries", editores universales, analizadores de ficheros, etc., que deberán estar bajo el control de los administradores autorizados relacionados en el Anexo F.

5.3.5. El administrador deberá responsabilizarse de guardar en lugar protegido las copias de seguridad y respaldo del Fichero, de forma que ninguna persona no autorizada tenga acceso a las mismas.

5.3.6. Si la aplicación o sistema de acceso al Fichero utilizase usualmente ficheros temporales, ficheros de "logging", o cualquier otro medio en el que pudiesen ser grabados copias de los datos protegidos, el administrador deberá asegurarse de que esos datos no son accesibles posteriormente por personal no autorizado.

5.3.7. Si el ordenador en el que está ubicado el fichero está integrado en una red de comunicaciones de forma que desde otros ordenadores conectados a la misma sea posible acceso al Fichero, el administrador responsable del sistema deberá asegurarse de que este acceso no se permite a personas no autorizadas.

5.4 Sistema Informático o aplicaciones de acceso al Fichero

Son todos aquellos sistemas informáticos, programas o aplicaciones con las que se puede acceder a los datos del Fichero, y que son usualmente utilizados por los usuarios para acceder a ellos.

Estos sistemas pueden ser aplicaciones informáticas expresamente diseñadas para acceder al Fichero, o sistemas preprogramados de uso general como aplicaciones o paquetes disponibles en el mercado informático.

5.4.1. Los sistemas informáticos de acceso al Fichero deberán tener su acceso restringido mediante un código de usuario y una contraseña.

5.4.2. Todos los usuarios autorizados para acceder al Fichero, relacionados en el Anexo F, deberán tener un código de usuario que será único, y que estará asociado a la contraseña correspondiente, que sólo será conocida por el propio usuario.

5.4.3. Si la aplicación informática que permite el acceso al Fichero no cuenta con un control de acceso, deberá ser el sistema operativo, donde se ejecuta esa aplicación, el que impida el acceso no autorizado, mediante el control de los citados códigos de usuario y contraseñas.

5.4.4. En cualquier caso se controlarán los intentos de acceso fraudulento al Fichero, limitando el
número máximo de intentos fallidos, y cuando sea técnicamente posible, guardando en un fichero auxiliar la fecha , hora, código y clave erróneas que se han introducido, así como otros datos relevantes que ayuden a descubrir la autoría de esos intentos de acceso fraudulentos.

5.4.5. Si durante las pruebas anteriores a la implantación o modificación de la aplicación de acceso al Fichero se utilizasen datos reales, se deberá aplicar a esos ficheros de prueba el mismo tratamiento de seguridad que se aplica al mismo Fichero, y se deberán relacionar esos ficheros de prueba en el Anexo B.

5.5 Salvaguarda y protección de las contraseñas personales

Las contraseñas personales constituyen uno de los componentes básicos de la seguridad de los datos, y deben por tanto estar especialmente protegidas. Como llaves de acceso al sistema, las contraseñas deberán ser estrictamente confidenciales y personales, y

cualquier incidencia que comprometa su confidencialidad deberá ser inmediatamente comunicada al administrador y subsanada en el menor plazo de tiempo posible.

5.5.1. Sólo las personas relacionadas en el Anexo F podrán tener acceso a los datos del Fichero.

5.5.2. Cada usuario será responsable de la confidencialidad de su contraseña y, en caso de que la misma sea conocida fortuita o fraudulentamente por personas no autorizadas, deberá registrarlo como incidencia y proceder inmediatamente a su cambio.

5.5.3. Las contraseñas se asignarán y se cambiarán mediante el mecanismo y periodicidad que se determina en el Anexo G.

5.5.4. El archivo donde se almacenen las contraseñas deberá estar protegido y bajo la responsabilidad del administrador del sistema.

6. Gestión de incidencias

Una incidencia es cualquier evento que pueda producirse esporádicamente y que pueda suponer un peligro para la seguridad del Fichero, entendida bajo sus tres vertientes de confidencialidad, integridad y disponibilidad de los datos.

El mantener un registro de las incidencias que comprometan la seguridad de un Fichero es una herramienta imprescindible para la prevención de posibles ataques a esa seguridad, así como para persecución de los responsables de los mismos.

6.1.1. El responsable de seguridad de Fichero habilitará un Libro de Incidencias a disposición de todos los usuarios y administradores del Fichero con el fin de que se registren en él cualquier incidencia que pueda suponer un peligro para la seguridad del mismo.

6.1.2. Cualquier usuario que tenga conocimiento de una incidencia es responsable del registro de la misma en el Libro de Incidencias del Fichero o en su caso de la comunicación por escrito al responsable de seguridad o al responsable del Fichero.

6.1.3. El conocimiento y la no notificación o registro de una incidencia por parte de un usuario será considerado como una falta contra la seguridad del Fichero por parte de ese usuario.

6.1.4. La notificación o registro de una incidencia deberá constar al menos de los siguientes datos: tipo de incidencia, fecha y hora en que se produjo, persona que realiza la notificación, persona a quien se comunica, efectos que puede producir, descripción detallada de la misma. El procedimiento está descrito en el Anexo I.

7. Gestión de soportes

Soportes informáticos son todos aquellos medios de grabación y recuperación de datos que se utilizan para realizar copias o pasos intermedios en los procesos de la aplicación que gestiona el Fichero.

Dado que la mayor parte de los soportes que hoy en día se utilizan, como disquetes o CD-ROMs, son fácilmente transportables, reproducibles y/o copiables, es evidente la importancia que para la seguridad de los datos del Fichero tiene el control de estos medios.

7.1.1. Los soportes que contengan datos del Fichero, bien como consecuencia de operaciones intermedias propias de la aplicación que los trata, o bien como consecuencia de procesos periódicos de respaldo o cualquier otra operación esporádica, deberán estar claramente identificados con una etiqueta externa que indique de qué fichero se trata, que tipo de datos contiene, proceso que los ha originado y fecha de creación.

7.1.2. Aquellos medios que sean reutilizables, y que hayan contenido copias de datos del Fichero, deberán ser borrados físicamente antes de su reutilización, de forma que los datos que contenían no sean recuperables.

7.1.3. Los soportes que contengan datos del Fichero deberán ser almacenados en lugares a lo que no tengan acceso personas no autorizadas para el uso del Fichero que no estén por tanto relacionadas en el Anexo F.

7.1.4. La salida de soportes informáticos que contengan datos del Fichero fuera de los locales donde está ubicado el Fichero deberá ser expresamente autorizada por el responsable del Fichero, utilizando para ello el documento adjunto en el anexo G.

7.1.5 El responsable del Fichero mantendrá un Libro de registro de entradas y salidas donde se guardarán los formularios de entradas y de salidas de soportes descritos en el anexo G, con indicación de tipo de soporte, fecha y hora, emisor, número de soportes, tipo de información que contienen, forma de envío, destinario, o persona responsable de la recepción que deberán estar debidamente autorizadas.

7.1.6 Cuando los soportes vayan a salir fuera de los locales en que se encuentren ubicados los ficheros como consecuencia de operaciones de mantenimiento, se adoptarán las medidas necesarias para impedir cualquier recuperación indebida de la información almacenada en ellos.

8. Entrada y salida de datos por red

La transmisión de datos por red, ya sea por medio de correo electrónico o mediante sistemas de transferencia de ficheros, se está convirtiendo en uno de los medios más utilizados para el envío de datos, hasta el punto de que está sustituyendo a los soportes físicos. Por ello merecen un tratamiento especial ya que, por sus características, pueden ser más vulnerables que los soportes físicos tradicionales.

8.1.1 Todas las entradas y salidas de datos del Fichero que se efectúen mediante correo electrónico se realizarán desde una única cuenta o dirección de correo controlada por un usuario especialmente autorizado por el responsable del Fichero. Igualmente si se realiza la entrada o salida de datos mediante sistemas de transferencia de ficheros por red, únicamente un usuario o administrador estará autorizado para realizar esas operaciones.

8.1.2 Se guardarán copias de todos los correos electrónicos que involucren entradas o salidas de datos del Fichero, en directorios protegidos y bajo el control del responsable citado. Se mantendrán copias de esos correos durante al menos dos años. También se guardará durante un mínimo de dos años, en directorios protegidos, una copia de los ficheros recibidos o transmitidos por sistemas de transferencia de ficheros por red, junto con un registro de la fecha y hora en que se realizó la operación y el destino del fichero enviado.

8.1.4 Cuando los datos del Fichero vayan a ser enviados por correo electrónico o por sistemas de transferencia de ficheros, a través de redes públicas o no protegidas, se recomienda que sean encriptados de forma que solo puedan ser leídos e interpretados por el destinatario.

9. Procedimientos de respaldo y recuperación

La seguridad de los datos personales del Fichero no sólo supone la confidencialidad de los mismos sino que también conlleva la integridad y la disponibilidad de esos datos.

Para garantizar estos dos aspectos fundamentales de la seguridad es necesario que existan unos procesos de respaldo y de recuperación que, en caso de fallo del sistema informático, permitan recuperar y en su caso reconstruir los datos del Fichero.

9.1.1. Existirá una persona, bien sea el administrador o bien otro usuario expresamente designado, que será responsable de obtener periódicamente una copia de seguridad del fichero, a efectos de respaldo y posible recuperación en caso de fallo.

9.1.2. Estas copias deberán realizarse con una periodicidad, al menos, semanal, salvo en el caso de que no se haya producido ninguna actualización de los datos.

9.1.3. En caso de fallo del sistema con pérdida total o parcial de los datos del Fichero existirá un procedimiento, informático o manual, que partiendo de la última copia de respaldo y del registro de las operaciones realizadas desde el momento de la copia, reconstruya los datos del Fichero al estado en que se encontraban en el momento del fallo. Ese procedimiento está descrito en el Anexo G.

9.1.4 Será necesaria la autorización por escrito del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos, y deberá dejarse constancia en el registro de incidencias de las manipulaciones que hayan debido realizarse para dichas recuperaciones,
incluyendo la persona que realizó el proceso, los datos restaurados y los datos que hayan debido ser grabados manualmente en el proceso de recuperación.

10. Controles periódicos de verificación del cumplimiento

La veracidad de los datos contenidos en los anexos de este documento, así como el cumplimiento de las normas que contiene deberán ser periódicamente comprobados, de forma que puedan detectarse y subsanarse anomalías.

10.1.1 El responsable de seguridad del Fichero comprobará, con una periodicidad al menos trimestral, que la lista de usuarios autorizados del Anexo F se corresponde con la lista de los usuarios realmente autorizados en la aplicación de acceso al Fichero, para lo que recabará la lista de usuarios y sus códigos de acceso al administrador o administradores del Fichero. Ademas de estas comprobaciones periódicas, el administrador comunicará al responsable de seguridad, en cuanto se produzca, cualquier alta o baja de usuarios con acceso autorizado al Fichero.

10.1.2 Se comprobará también al menos con periodicidad trimestral, la existencia de copias de respaldo que permitan la recuperación de Fichero según lo estipulado en el apartado 8 de este documento.

10.1.3 A su vez, y también con periodicidad al menos trimestral, los administradores del Fichero comunicaran al responsable de seguridad cualquier cambio que se haya realizado en los datos técnicos de los anexos, como por ejemplo cambios en el software o hardware, base de datos o aplicación de acceso al Fichero, procediendo igualmente a la actualización de dichos anexos.

10.1.4 El responsable de seguridad, verificará, con periodicidad al menos trimestral, el cumplimiento de lo previsto en los apartados 7 y 8 de este documento en relación con las entradas y salidas de datos, sean por red o en soporte magnético.

10.1.5 El responsable del fichero junto con el responsable de seguridad, analizaran con periodicidad al menos trimestral las incidencias registradas en el libro correspondiente, para independientemente de las medidas particulares que se hayan adoptado en el momento que se produjeron, adoptar las medidas correctoras que limiten esas incidencias en el futuro.

10.1.6 Al menos cada dos años, se realizará una auditoría, externa o interna que dictamine el correcto cumplimiento y la adecuación de las medidas del presente documento de seguridad o las exigencias del Reglamento de seguridad, identificando las deficiencias y proponiendo las media correctoras necesarias. Los informes de auditoría serán analizados por el responsable de seguridad, quien propondrá al responsable del Fichero las medidas correctoras correspondientes.

10.1.7 Los resultados de todos estos controles periódicos, así como de las auditorías serán adjuntadas a este documento de seguridad en el Anexo J.

Anexo A. Documentos de Notificación y Decretos

Documento de Notificación a la Agencia de Protección de Datos de Registro del Fichero.

Se adjuntará aquí una copia del documento de notificación de la creación, y en su caso de las posibles modificaciones del Fichero.

En este mismo apartado se recogerá una copia de la publicación de la disposición de creación, y si procede de las modificaciones.

Anexo B. Descripción detallada de la estructura del Fichero o la Base de Datos.

La descripción contendrá al menos los siguientes aspectos:

Ubicación física del Fichero, tipo de soporte, servidor, nombre del área o directorio etc…

Descripción lógica, archivos o tablas, registros o tuplas, campos o columnas, así como el formato, descripción y relaciones entre los mismos.

Si se realizan pruebas con datos reales , se relacionaran estos ficheros de prueba, indicando el nombre y descripción de los mismos y procedimiento previsto para el borrado físico de estos datos.

Gestor de base de datos, mecanismos de recuperación.

Anexo C. Descripción del sistema informático de acceso al fichero.

Descripción del Sistema Informático de acceso al Fichero

El sistema informático o aplicación de acceso al fichero es el conjunto de programas, específicamente diseñados para el caso o de propósito general, con los que normalmente se accede para consultar o actualizar los dato del Fichero.

La descripción deberá al menos contener los siguientes datos:

- *Nombre de la aplicación*
- *Si se trata de un paquete o producto estándar del mercado o de unos programas expresamente diseñados para ese propósito.*
- *Quién y en que fecha se programó.*
- *Responsables del mantenimiento.*
- *Tipo de control de acceso si lo tiene, indicando si se limita el numero de intentos fallidos de acceso al sistema y si se guarda en un fichero auxiliar la historia de estos intentos.*
- *Tipo de procedimientos de histórico de operaciones (logging) y de recuperación, si los tiene.*

Nº de inscripción	NOMBRE DE FICHERO

Anexo D. Entorno de Sistema Operativo y de Comunicaciones del Fichero

Entorno de Sistema Operativo y de Comunicaciones del Fichero
(a ser cumplimentado por el administrador del sistema)

Deberá contener al menos los siguientes datos y aspectos:

Sistema operativo

Nombre y versión
Fabricante
Características generales (monopuesto, multiusuario, compartición de ficheros u otros recursos, etc..)
Control de acceso, características
Archivos de logging y procedimientos de recuperación propios del sistema.
Responsables del mantenimiento

Entorno de comunicaciones (si lo tuviese)

Tipo de red local (Ethernet, otras), ámbito y extensión.
Si existe conexión con otras redes locales o WAN, indicar el tipo de conexión (permanente, esporádica, etcc..), a través de redes públicas como Internet o con conexiones
privadas etc..
Hay compartición de recursos y archivos ?. Si es así indicar que tipo de sistema de red es
utilizado, sus límites y alcance.
Controles de acceso desde la red al sistema del Fichero.

Anexo E. Locales y equipamiento

Locales y equipamiento de los centros de tratamiento

Locales

Descripción de la ubicación física
Tipo de acceso: Se especificara el tipo de control de acceso
Sistemas de continuidad
Equipamiento; armarios ignífugos, etc

Puestos de Trabajo

Descripción Equipos: Servidores, equipos, Impresoras
Relación de puestos de trabajo

Anexo F. Personal autorizado para acceder al Fichero

RESPONSABLE DEL FICHERO

Nombre y apellidos	Cargo	Alta	Baja

RESPONSABLE DE SEGURIDAD

Nombre y apellidos	Cargo	Alta	Baja

ADMINISTRADORES DEL SISTEMA

Nombre y apellidos	Organismo / Unidad Administrativa	Alta	Baja

Nº de inscripción NOMBRE DE FICHERO

USUARIOS DEL FICHERO

Nombre y apellidos	Unidad Administrativa	Nº inventario Puesto Trabajo	Alta	Baja

Anexo G. Procedimientos de control y seguridad

Contendrá al menos los procedimientos siguientes :

Procedimiento de asignación y cambio de contraseñas.

Procedimiento de respaldo y recuperación.

Procedimiento de gestión de soportes:

Constará al menos de los siguientes apartados

- *Identificación de etiquetas*
- *Inventario de soportes*
- *Lugar de almacenamiento*
- *En el caso de reutilización o eliminación de soportes grabados con datos del fichero se indicará el método utilizado para el borrado físico de estos datos.*

Se adjunta impreso de inventario de soportes y formularios de inscripción para registrar en el Libro de entradas y salida de soportes.

Entrada y salida de datos por red :

Se especificará

- *Cuenta de correo*
- *Responsable de transferencias electrónicas*

INVENTARIO DE SOPORTES

Página nº _____

Fichero: NOMBRE DE FICHERO					
ALTAS		BAJAS			
		Reutilización	Destrucción	MÉTODO	
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /

SALIDA DE SOPORTES

Cualquier salida de soportes fuera de los locales donde esta ubicado el fichero deberá ser autorizada por el responsable del fichero de acuerdo con el documento que se adjunta.

El responsable del fichero mantendrá un Libro en el que registrará las salidas de soportes, cuyos asientos estarán constituidos por los documentos de autorización de salida debidamente cumplimentados.

La persona responsable de la entrega de soportes estará debidamente autorizada por el responsable del fichero.

REGISTRO Y AUTORIZACIÓN DE SALIDA DE SOPORTES

Fecha y hora de salida del soporte	

SOPORTE	
Tipo de soporte y número	
Contenido	
Ficheros de donde proceden los datos	
Fecha de creación	

FINALIDAD Y DESTINO	
Finalidad	
Destino	
Destinatario	

Nº de inscripción NOMBRE DE FICHERO

FORMA DE ENVÍO	
Medio de envío	
Remitente	
Precauciones para el transporte	

AUTORIZACIÓN	
Persona responsable de la entrega	
Persona que autoriza	
Cargo / Puesto	
Observaciones	
Firma	

ENTRADA DE SOPORTES

El responsable del fichero mantendrá un Libro en el que registrará las entradas de soportes cuyos asientos estarán constituidos por los datos recogidos en el formulario que se adjunta.

La persona responsable de la recepción de soportes estará debidamente autorizada por el responsable del fichero.

REGISTRO DE ENTRADA DE SOPORTES

Fecha y hora de entrada de soporte	

SOPORTE	
Tipo de soporte y número	
Contenido	
Fecha de creación	

ORIGEN Y FINALIDAD	
Finalidad	
Origen	

FORMA DE ENVÍO	
Medio de envío	
Remitente	
Precauciones para el transporte	

Nº de inscripción NOMBRE DE FICHERO

AUTORIZACIÓN	
Persona responsable de la recepción	
Cargo / Puesto	
Observaciones	
Firma	

Anexo H. Funciones y obligaciones del personal

FUNCIONES DEL RESPONSABLE DEL FICHERO

El responsable del fichero es el encargado jurídicamente de la seguridad del fichero y de las medidas establecidas en el presente documento, implantará las medidas de seguridad establecidas en él y adoptará las medidas necesarias para que el personal afectado por este documento conozca las normas que afecten al desarrollo de sus funciones.

Designará al responsable de seguridad que figura en el Anexo F.

FUNCIONES DEL RESPONSABLE DE SEGURIDAD

Es el encargado de coordinar y controlar las medidas definidas en el presente documento.

CLASIFICACIÓN DEL PERSONAL DE ADMINISTRACIÓN O PERSONAL INFORMÁTICO

Se distinguen dos situaciones diferentes, que condicionan el tipo de personal que tiene acceso al fichero en cada caso:

- -Producción habitual, sin incidencias técnicas. Explotación diaria.
- -Errores, cortes, incidencias técnicas de cualquier tipo que detienen la producción.

PERSONAL AUTORIZADO EN PRODUCCIÓN HABITUAL

En el primer caso, el acceso se limita a los siguientes perfiles

- -Usuario/Administrador del sistema.
- -Operador.

ADMINISTRADORES TÉCNICOS E INFORMÁTICOS GENERALES QUE INTERVIENEN EN SITUACIONES NO HABITUALES

Cuando no existe un personal técnico determinado que se pueda relacionar de forma directa con un fichero o sistema informático y que acceda habitualmente al mencionado fichero o sistema.

Siempre será posible conocer el personal que intervino con posterioridad a la intervención, dejando constancia de ello, identificando al personal técnico, anotándolo en le Registro de Incidencias.

FUNCIONES DE LOS ADMINISTRADORES O PERSONAL INFORMÁTICO

El personal que administra el sistema de acceso al Fichero se puede a su vez clasificar en varias categorías, que no necesariamente deberán estar presentes en todos los casos, siendo en algunas ocasiones asumidas por una misma persona o personas. Estas categorías son:

- Administradores (Red, Sistemas operativos y Bases de Datos). Serán los responsables de los máximos privilegios y por tanto de máximo riesgo de que una actuación errónea pueda afectar al sistema. Tendrán acceso al software (programas y datos) del sistema, a las herramientas necesarias para su trabajo y a los ficheros o bases de datos necesarios para resolver los problemas que surjan.

- Operadores (Red, Sistemas operativos, Bases de Datos y Aplicación). Sus actuaciones están limitadas a la operación de los equipos y redes utilizando las herramientas de gestión disponibles. No deben, en principio, tener acceso directo a los datos del Fichero, ya que su actuación no precisa de dicho acceso.

- Mantenimiento de los sistemas y aplicaciones. Personal responsable de la resolución de incidencias que puedan surgir en el entono hardware/software de los sistemas informáticos o de la propia aplicación de acceso al Fichero.

- Cualquier otro que la organización establezca.

OBLIGACIONES DEL RESPONSABLE DEL FICHERO

Implantar las medidas de seguridad establecidas en este documento.

El responsable del Fichero deberá garantizar la difusión de este Documento entre todo el personal que vaya a utilizar.

Deberá mantenerlo actualizado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo, según los artículos 8 y 9 de la Normativa de Seguridad.

Deberá adecuar en todo momento el contenido del mismo a las disposiciones vigentes en materia de seguridad de datos.

Deberá designar uno o varios responsables de seguridad.

Entorno de Sistema Operativo y de Comunicaciones

5.3.1 El responsable del Fichero aprobará o designará al administrador que se responsabilizará del sistema operativo y de comunicaciones que deberá estar relacionado en el Anexo F.

5.3.2 En el caso más simple, como es que el Fichero se encuentre ubicado en un ordenador personal y accedido mediante una aplicación local monopuesto, el administrador del sistema operativo podrá ser el mismo usuario que accede usualmente al Fichero.

Sistema Informático o aplicaciones de acceso al Fichero

5.4.1 El responsable del fichero se encargará de que los sistemas informáticos de acceso al Fichero tengan su acceso restringido mediante un código de usuario y una contraseña.

5.4.2 Asimismo cuidará que todos los usuarios autorizados para acceder al Fichero, relacionados en el Anexo F, tengan un código de usuario que será único, y que estará asociado a la contraseña correspondiente, que sólo será conocida por el propio usuario.

Salvaguarda y protección de las contraseñas personales

5.5.1 Sólo las personas relacionadas en el Anexo F, podrán tener acceso a los datos del Fichero.

Gestión de soportes

7.1.4 La salida de soportes informáticos que contengan datos del Fichero fuera de los locales donde está ubicado el Fichero deberá ser expresamente autorizada por el responsable del Fichero.

Entrada y salida de datos por red

8.1.1 Todas las entradas y salidas de datos del Fichero que se efectúen mediante correo electrónico se realizarán desde una única cuenta o dirección de correo controlada por un usuario especialmente autorizado por el responsable del Fichero. Igualmente si se realiza la entrada o salida de datos mediante sistemas de transferencia de ficheros por red, únicamente un usuario o administrador estará autorizado para realizar esas operaciones.

Procedimientos de respaldo y recuperación

El responsable del Fichero se encargará de verificar la definición y correcta aplicación de las copias de respaldo y recuperación de los datos.

9.1.4 Será necesaria la autorización por escrito del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos, y deberá dejarse constancia en el registro de incidencias de las manipulaciones que hayan debido realizarse para dichas recuperaciones,
incluyendo la persona que realizó el proceso, los datos restaurados y los datos que hayan debido ser grabados manualmente en el proceso de recuperación.

Controles periódicos de verificación del cumplimiento

9.1.5 El responsable del fichero junto con el responsable de seguridad, analizaran con periodicidad
al menos trimestral las incidencias registradas en el libro correspondiente, para independientemente de las medidas particulares que se hayan adoptado en el momento que se produjeron, poner las medidas correctoras que limiten esas incidencias en el futuro.

9.1.6 Al menos cada dos años, se realizará una auditoría, externa o interna que dictamine el correcto cumplimiento y la adecuación de las medidas del presente documento de seguridad o las exigencias del Reglamento de seguridad,

identificando las deficiencias y proponiendo las media correctoras necesarias. Los informes de auditoria serán analizados por el responsable de seguridad, quien propondrá al responsable del Fichero las medidas correctoras correspondientes.

9.1.7 Los resultados de todos estos controles periódicos, así como de las auditorias serán adjuntadas a este documento de seguridad en el Anexo J.

OBLIGACIONES DEL RESPONSABLE DE SEGURIDAD

El responsable de seguridad coordinará la puesta en marcha de las medidas de seguridad, colaborará con el responsable del fichero en la difusión del Documento de seguridad y cooperará con el responsable del fichero controlando el cumplimiento de las mismas.

Gestión de incidencias

6.1.1 El responsable de seguridad habilitará un Libro de Incidencias a disposición de todos los usuarios y administradores del Fichero con el fin de que se registren en él cualquier incidencia que pueda suponer un peligro para la seguridad del mismo.

Analizara las incidencias registradas, tomando las medidas oportunas en colaboración con el responsable del Fichero.

Controles periódicos de verificación del cumplimiento

9.1.1. El responsable de seguridad del Fichero comprobará, con una periodicidad al menos trimestral, que la lista de usuarios autorizados del Anexo F se corresponde con la lista de los usuarios realmente autorizados en la aplicación de acceso al Fichero, para lo que recabará la lista de usuarios y sus códigos de acceso al administrador o administradores del Fichero. Ademas de estas comprobaciones periódicas, el administrador comunicará al responsable de seguridad, en cuanto se produzca, cualquier alta o baja de usuarios con acceso autorizado al Fichero.

9.1.2 Se comprobará también al menos con periodicidad trimestral, la existencia de copias de respaldo que permitan la recuperación de Fichero según lo estipulado en el apartado 8 de este documento.

9.1.3 A su vez, y también con periodicidad al menos trimestral, los administradores del Fichero comunicaran al responsable de seguridad cualquier cambio que se haya realizado en los datos técnicos de los anexos, como por ejemplo cambios en el software o hardware, base de datos o aplicación de acceso al Fichero, procediendo igualmente a la actualización de dichos anexos.

9.1.4 El responsable de seguridad, verificará, con periodicidad al menos trimestral, el cumplimiento de lo previsto en los apartados 7 y 8 de este documento en relación con las entradas y salidas de datos, sean por red o en soporte magnético.

9.1.5 El responsable del fichero junto con el responsable de seguridad, analizaran con periodicidad al menos trimestral las incidencias registradas en el libro correspondiente, para independientemente de las medidas particulares que se hayan adoptado en el momento que se produjeron, poner las medidas correctoras que limiten esas incidencias en el futuro.

9.1.6 Al menos cada dos años, se realizará una auditoria, externa o interna que dictamine el correcto cumplimiento y la adecuación de las medidas del presente documento de seguridad o las exigencias del Reglamento de seguridad, identificando las deficiencias y proponiendo las media correctoras necesarias. Los informes de auditoria serán analizados por el responsable de seguridad, quien propondrá al responsable del Fichero las medidas correctoras correspondientes.

9.1.7 Los resultados de todos estos controles periódicos, así como de las auditorias serán adjuntadas a este documento de seguridad en el Anexo J.

OBLIGACIONES QUE AFECTAN A TODO EL PERSONAL

Puestos de trabajo

5.2.1 Los puestos de trabajo estarán bajo la responsabilidad de algún usuario autorizado que garantizará que la información que muestran no pueda ser visible por personas no autorizadas.

5.2.2 Esto implica que tanto las pantallas como las impresoras u otro tipo de dispositivos conectados al puesto de trabajo deberán estar físicamente ubicados en lugares que garanticen esa confidencialidad.

5.2.3 Cuando el responsable de un puesto de trabajo lo abandone, bien temporalmente o bien al finalizar su turno de trabajo, deberá dejarlo en un estado que impida la visualización de los datos protegidos. Esto podrá realizarse a través de un protector de pantalla que impida la visualización de los datos. La reanudación del trabajo implicará la desactivación de la pantalla protectora con la introducción de la contraseña correspondiente.

5.2.4 En el caso de las impresoras deberá asegurarse de que no quedan documentos impresos en la bandeja de salida que contengan datos protegidos. Si las impresoras son compartidas con otros usuarios no autorizados para acceder a los datos de Fichero, los responsables de cada puesto deberán retirar los documentos conforme vayan siendo impresos.

5.2.5 Queda expresamente prohibida la conexión a redes o sistemas exteriores de los puestos de trabajo desde los que se realiza el acceso al fichero. La revocación de esta prohibición será autorizada por el responsable del fichero, quedando constancia de esta modificación en el Libro de incidencias.

5.2.6 Los puestos de trabajo desde los que se tiene acceso al fichero tendrán una configuración fija en sus aplicaciones, sistemas operativos que solo podrá ser

cambiada bajo al autorización del responsable de seguridad o por administradores autorizados del anexo F.

Salvaguarda y protección de las contraseñas personales

5.5.2 Cada usuario será responsable de la confidencialidad de su contraseña y, en caso de que la misma sea conocida fortuita o fraudulentamente por personas no autorizadas, deberá registrarlo como incidencia y proceder a su cambio.

Gestión de incidencias

6.1.1 Cualquier usuario que tenga conocimiento de una incidencia es responsable de la comunicación de la misma al administrador del sistema, o en su caso del registro de la misma en el sistema de registro de incidencias del Fichero.

6.1.2 El conocimiento y la no notificación de una incidencia por parte de un usuario será considerado como una falta contra la seguridad del Fichero por parte de ese usuario.

Gestión de soportes

7.1.1 Los soportes que contengan datos del Fichero, bien como consecuencia de operaciones intermedias propias de la aplicación que los trata, o bien como consecuencia de procesos periódicos de respaldo o cualquier otra operación esporádica, deberán estar claramente identificados con una etiqueta externa que indique de qué fichero se trata, que tipo de datos contiene, proceso que los ha originado y fecha de creación.

7.1.2 Aquellos medios que sean reutilizables, y que hayan contenido copias de datos del Fichero, deberán ser borrados físicamente antes de su reutilización, de forma que los datos que contenían no sean recuperables.

7.1.3 Los soportes que contengan datos del Fichero deberán ser almacenados en lugares a lo que no tengan acceso personas no autorizadas para el uso del Fichero que no estén por tanto relacionadas en el Anexo F.

7.1.5. Cuando la salida de datos del Fichero se realice por medio de correo electrónico los envíos se realizaran, siempre y únicamente, desde una dirección de correo controlada por el administrador de seguridad, dejando constancia de estos envíos en el directorio histórico de esa dirección de correo o en algún otro sistema de registro de salidas que permita conocer en cualquier momento los envios realizados, a quien iban dirigidos y la información enviada.

7.1.6. Cuando los datos del Fichero deban ser enviados fuera del recinto físicamente protegido donde se encuentra ubicado el Fichero, bien sea mediante un soporte físico de grabación de datos o bien sea mediante correo electrónico, deberán ser encriptados de forma que solo puedan ser leídos e interpretados por el destinatario.

7.1.8. Se deberán registrar mediante correo electrónico o transferencia de datos por red, de forma que se pueda siempre identificar su origen, tipo de datos , formato, fecha y hora del envío y destinatario de los mismos.

OBLIGACIONES DE LOS ADMINISTRADORES Y PERSONAL INFORMÁTICO

Entorno de sistema operativo y de Comunicaciones

5.3.3 Ninguna herramienta o programa de utilidad que permita el acceso al Fichero deberá ser accesible a ningún usuario o administrador no autorizado en el Anexo F.

5.3.4 En la norma anterior se incluye cualquier medio de acceso en bruto, es decir no elaborado o editado, a los datos del Fichero, como los llamados "queries", editores universales, analizadores de ficheros, etc., que deberán estar bajo el control de los administradores autorizados relacionados en el Anexo F.

5.3.5 El administrador deberá responsabilizarse de guardar en lugar protegido las copias de seguridad y respaldo del Fichero, de forma que ninguna persona no autorizada tenga acceso a las mismas.

5.3.6 Si la aplicación o sistema de acceso al Fichero utilizase usualmente ficheros temporales, ficheros de "logging", o cualquier otro medio en el que pudiesen ser grabados copias de los datos protegidos, el administrador deberá asegurarse de que esos datos no son accesibles posteriormente por personal no autorizado.

5.3.7 Si el ordenador en el que está ubicado el fichero está integrado en una red de comunicaciones de forma que desde otros ordenadores conectados a la misma sea posible el acceso al Fichero, el administrador responsable del sistema deberá asegurarse de que este acceso no se permite a personas no autorizadas.

Sistema Informático o aplicaciones de acceso al Fichero

5.4.3 Si la aplicación informática que permite el acceso al Fichero no cuenta con un control de acceso, deberá ser el sistema operativo, donde se ejecuta esa aplicación, el que impida el acceso no autorizado, mediante el control de los citados códigos de usuario y contraseñas.

5.4.4. En cualquier caso se controlarán los intentos de acceso fraudulento al Fichero, limitando el

número máximo de intentos fallidos, y, cuando sea técnicamente posible, guardando en un fichero auxiliar la fecha , hora, código y clave erróneas que se han introducido, así como otros datos relevantes que ayuden a descubrir la autoría de esos intentos de acceso fraudulentos.

5.4.5. Si durante las pruebas anteriores a la implantación o modificación de la aplicación de acceso al Fichero se utilizasen datos reales, se deberá aplicar a esos ficheros de prueba el mismo tratamiento de seguridad que se aplica al mismo Fichero, y se deberán relacionar esos ficheros de prueba en el Anexo B.

Salvaguarda y protección de las contraseñas personales

5.5.5 Las contraseñas se asignarán y se cambiarán mediante el mecanismo y periodicidad que se determina en el Anexo G. Este mecanismo de asignación y distribución de las contraseñas deberá garantizar la confidencialidad de las mismas, y será responsabilidad del administrador del sistema.

5.5.6 El archivo donde se almacenen las contraseñas deberá estar protegido y bajo la responsabilidad del administrador del sistema.

Procedimientos de respaldo y recuperación

8.1.1 Existirá una persona, bien sea el administrador o bien otro usuario expresamente designado, que será responsable de obtener periódicamente una copia de seguridad del fichero, a efectos de respaldo y posible recuperación en caso de fallo.

8.1.2 Estas copias deberán realizarse con una periodicidad, al menos, semanal, salvo en el caso de que no se haya producido ninguna actualización de los datos.

8.1.3 En caso de fallo del sistema con pérdida total o parcial de los datos del Fichero existirá un procedimiento, informático o manual, que partiendo de la última copia de respaldo y del registro de las operaciones realizadas desde el momento de la copia, reconstruya los datos del Fichero al estado en que se encontraban en el momento del fallo. Ese procedimiento está descrito en el Anexo G.

8.1.4 Será necesaria la autorización por escrito del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos, y deberá dejarse

constancia en el registro de incidencias de las manipulaciones que hayan debido realizarse para dichas recuperaciones,
incluyendo la persona que realizó el proceso, los datos restaurados y los datos que hayan debido ser grabados manualmente en el proceso de recuperación.

Controles periódicos de verificación del cumplimiento

9.1.1. El responsable de seguridad del Fichero comprobará, con una periodicidad al menos trimestral, que la lista de usuarios autorizados del Anexo F se corresponde con la lista de los usuarios realmente autorizados en la aplicación de acceso al Fichero, para lo que recabará la lista de usuarios y sus códigos de acceso al administrador o administradores del Fichero. Ademas de estas comprobaciones periódicas, el administrador comunicará al responsable de seguridad, en cuanto se produzca, cualquier alta o baja de usuarios con acceso autorizado al Fichero.

9.1.2 Se comprobará también al menos con periodicidad trimestral, la existencia de copias de respaldo que permitan la recuperación de Fichero según lo estipulado en el apartado 8 de este documento.

9.1.3 A su vez, y también con periodicidad al menos trimestral, los administradores del Fichero comunicaran al responsable de seguridad cualquier cambio que se haya realizado en los datos técnicos de los anexos, como por ejemplo cambios en el software o hardware, base de datos o aplicación de acceso al Fichero, procediendo igualmente a la actualización de dichos anexos.

9.1.4 El responsable de seguridad, verificará, con periodicidad al menos trimestral, el cumplimiento de lo previsto en los apartados 7 y 8 de este documento en relación con las entradas y salidas de datos, sean por red o en soporte magnético.

9.1.6 Al menos cada dos años, se realizará una auditoria, externa o interna que dictamine el correcto cumplimiento y la adecuación de las medidas del presente documento de seguridad o las exigencias del Reglamento de seguridad,

identificando las deficiencias y proponiendo las media correctoras necesarias. Los informes de auditoria serán analizados por el responsable de seguridad, quien propondrá al responsable del Fichero las medidas correctoras correspondientes.

9.1.7 Los resultados de todos estos controles periódicos, así como de las auditorias serán adjuntadas a este documento de seguridad en el Anexo J.

Anexo I. Procedimiento de Notificación y gestión de incidencias

Procedimiento de Notificación y gestión de incidencias

Se describirá el procedimiento de notificación y gestión de incidencias

En la notificación se hará constar :

- *Tipo de incidencia*
- *Fecha y hora en que se produjo*
- *Persona que realiza la notificación*
- *Persona a quien se comunica*
- *Efectos que puede producir la incidencia*
- *Descripción detallada de la misma*

Si se trata de una recuperación de datos se incluirá además :

- *Autorización del responsable del fichero*
- *Procedimientos realizados*
- *Persona que realizó el proceso*
- *Datos restaurados*
- *Datos grabados manualmente*

Se adjunta el impreso de notificación manual que podra ser utilizado para la notificación de incidencias

Cuando ocurra una incidencia, el usuario o administrador deberá registrarla en el Libro de Incidencias o comunicarla al Responsable de seguridad para que a su vez proceda a su registro.

Se mantendrán las incidencias registradas de los 12 últimos meses.

A continuación se adjunta el impreso de notificación manual que podrá ser utilizado para la notificación de incidencias.

Impreso de notificación de incidencias

Incidencia Nº: |_____| (Este número será rellenado por el Responsable de seguridad)	
Fecha de notificación: /__/__/____/	
Tipo de incidencia:	
Descripción detallada de la incidencia:	
Fecha y hora en que se produjo la incidencia:	
Persona(s) a quien(es) se comunica:	
Efectos que puede producir: (En caso de no subsanación o incluso independientemente de ella)	
Recuperación de Datos :(A rellenar sólo si la incidencia es de este tipo) Procedimiento realizado: Datos restaurados: Datos grabados manualmente: Persona que ejecutó el proceso: Firma del Responsable del fichero: Fdo _____	
Persona que realiza la comunicación: Fdo.:_____	

Nº de inscripción NOMBRE DE FICHERO

Anexo J. Controles periódicos y auditorias

Contendrá los resultados de los controles periódicos descritos en el apartado 10 y de las auditorias realizadas

11

Copia de Seguridad

Artículo 25. Copias de respaldo y recuperación.

Deberá conservarse una copia de respaldo y de los procedimientos de recuperación de los datos en un lugar diferente de aquél en que se encuentren los equipos informáticos que los tratan cumpliendo en todo caso, las medidas de seguridad exigidas en este Reglamento.

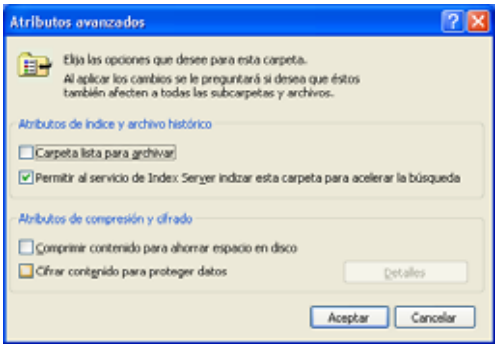
11.1 UBICACIÓN

El artículo 25 del Reglamento de Medidas de Seguridad de la LOPD exige que tanto las copias de seguridad como los procedimientos para su recuperación se almacenen en un lugar distinto al de los equipos informáticos donde se traten datos personales. Además dicho lugar tendrá que cumplir las mismas medidas de seguridad que el nivel alto, en particular, acceso físico.

11.2 DISTRIBUCCIÓN DE LOS SOPORTES

En lo que respecta a la distribución de soportes con datos personales de nivel alto de seguridad, el artículo 23 del Reglamento exige que se cifren o encripten dichos datos, o bien que se utilice un sistema similar que garantice la ininteligibilidad de la información y que la misma no pueda ser manipulada durante su transporte.

Para poder encriptar las copias de seguridad algunas de las aplicaciones mencionadas en el capítulo 6 se pueden usar como: Kbackup, Legato, etc. Las propias que vienen con los sistemas operativos como por ejemplo: dump & restore, copia de seguridad NT, etc. no permiten cifrar las copias de seguridad, por lo que tendremos que instalar otros programas, aunque en las versiones de Windows 2000 y Windows XP permiten cifrar una carpeta o archivo individualmente. Con lo que podríamos realizar la copia de seguridad con los programas anteriormente y luego basta cifrar el archivo que se ha creado en la realización de la copia de seguridad. Para ello, haga clic con el botón derecho sobre el nombre del archivo que se quiera cifrar, con lo que saldrá un menú emergente y pulse propiedades. Una vez hecho esto haga clic sobre opciones avanzadas y saldrá el siguiente cuadro de dialogo.



Para terminar active *Cifrar contenido para proteger datos*.[1]

[1] Es el mismo proceder para Windows 2000 y Windows XP

12

Transmisión de la información

Artículo 26. Telecomunicaciones.

La transmisión de datos de carácter personal a través de redes de telecomunicaciones se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

12.1 CONCEPTOS GENERALES

El concepto de transmisión segura de la información surge hace muchísimos años, conocida como escritura secreta. Uno de los primeros testimonios se remontan al siglo V A.C cuando había los conflictos entre griegos y persas. Según Herodoto[1] fue este arte, escritura secreta, el que salvó a Grecia de ser ocupada. Antiguamente se basaba en la ocultación de la existencia del mensaje, en nuestro días los algoritmos son públicos y se basan en una buena clave. De hecho los algoritmos de encriptados no son el problema si no la implementación de ellos. Muchas veces las implementaciones están mal lo que hace que sea vulnerable la información.

En la actualidad nos encontraremos fundamentalmente con dos tipos de cifrado:

12.1.1 CLAVE SIMÉTRICA

Este sistema emplea una sola clave, tanto para el cifrado como el descifrado de los datos. Por tanto, la seguridad reside en el secreto de dicha clave. Una de sus principales ventajas es su rapidez. Algunos de los más conocidos algoritmos son:

- **DES** (**Data Encryption Standard, Estándar de Encriptación de Información**) se convirtió en un estándar de los Estados Unidos en 1997. Se considera un *"cifrado de bloque"*, ya que la información se encripta normalmente en bloques de 64 bits. La clave es de una longitud de 56 bits. Dicha clave actualmente se considera corta para la mayor parte de los algoritmos de encriptación.

- **RC2** se utiliza normalmente en los Estados Unidos, siendo su cifrado también en bloque. Lo desarrolló RSA Data Security y, a diferencia de otros sistemas de cifrado, su algoritmo es confidencial. RC2. La clave que emplea es de de 128 bits, pudiendo ser implementado con claves de distintas longitudes.

- **RC4** fue desarrollado por RSA Data Security. Se considera un *"cifrado de secuencia"*, debido a que encripta un mensaje bit a bit en vez del bloque entero. RC4 se parece a RC2 en que el algoritmo se puede implementar con claves de distintas longitudes.

12.1.2 CLAVE PÚBLICA Ó ASIMÉTRICA

Este sistema, a diferencia del anterior, emplea dos claves diferentes:

- *Clave pública*, que como su nombre indica se encuentra a disposición del público.

- *Clave privada*, que la guarda en secreto el propietario del par de claves.

Se empleará una clave para cifrar la información y otra distinta para descifrarla. Este tipo de claves permite dos maneras de uso:

12.1.2.1 CIFRADO

A posee un mensaje en claro que quiere enviar a ***B*** y sin que nadie mas que el destinatario lea su contenido. Para ello tendrá que:

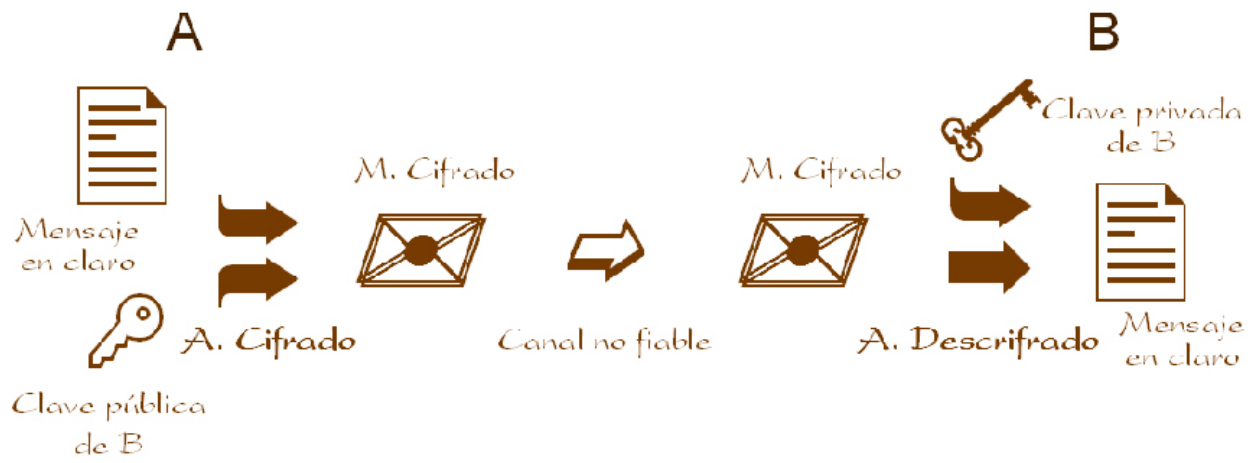
1) ***A*** cifra el mensaje con la clave pública de ***B*** y se lo envía.

2) ***B*** lo recibe y lo descrifra con su clave privada para poder acceder a su contenido y así obtener el mensaje en claro que le envía ***A***.

En este caso, la privacidad está garantizada, ya que la obtención del mensaje en claro, necesita la clave privada, y sólo el destinatario está en posesión de ella. A continuación se muestra una figura que describe el proceso explicado.

---

[1] El padre de la historia según Cicerón.

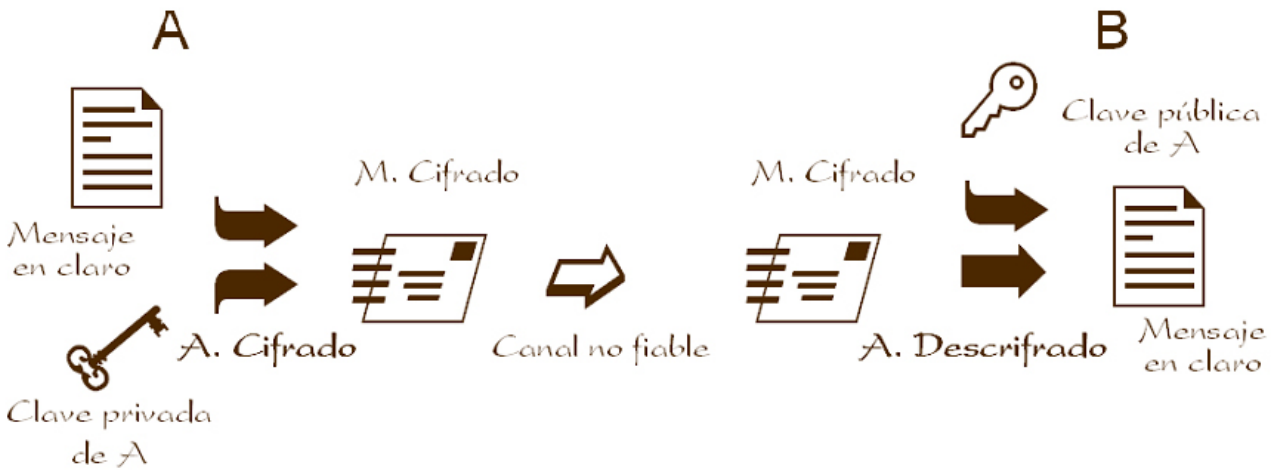


12.1.2.2 AUTENTIFICADO

El otro modo de empleo es el que se describe a continuación:

1) ***A*** encripta el mensaje con la clave privada de ***A***. Fíjese que todo el mundo que esté en posesión de la clave pública ***A*** tendrá acceso al mensaje en claro.

2) ***B*** desencripta el contenido del mensaje con la pública de ***A***. Por tanto, sabrá que el mensaje venía de ***A***.



12.1.3 FIRMA DIGITAL

Como se ha visto en apartados anteriores la encriptación de clave pública se puede utilizar para identificar a un usuario. La *firma digital* es una rama de ese mecanismo de autentificación, es decir, permitirá identificar el autor del mensaje y dará prueba de la integridad de los datos. Pero no se podrá añadir simplemente al final de un documento y esperar que este sea seguro. Para que una firma sea valida deberá indicar de alguna forma que se corresponde con el documento. Para implementar esto se utiliza la función resumen o HASH.

12.1.3.1 FUNCIÓN RESUMEN

La *función resumen* va a ser una función con una entrada de longitud arbitraria que produce una salida de longitud fija, conocida con el nombre de *resumen*. Dicha salida deberá cumplir que:

1) Será imposible determinar el mensaje original a partir del resumen.

2) Nunca podrá haber dos resúmenes iguales.

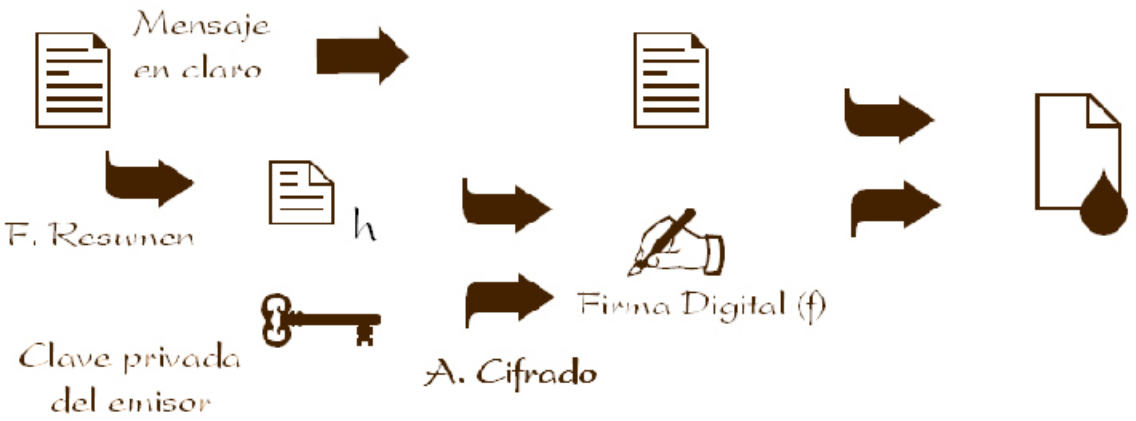
12.1.3.2 OBTENCIÓN DE LA FIRMA DIGITAL

El emisor deberá seguir el siguiente proceso:

1) Aplicar la función resumen al mensaje en claro con lo que obtiene un resumen que recibe el nombre de *h*.

2) La firma digital de este documento entonces se obtendrá como el resultado de cifrar *f* con la clave privada del emisor.

3) Enviar la firma digital añadida al final del documento en claro.



12.1.3.3 VERIFICACIÓN DE LA FIRMA DIGITAL

El receptor del documento firmado deberá seguir los siguientes pasos:

1) Aplicar al mensaje en claro la misma función resumen que el emisor, con lo que obtendrá un resumen denominado *h'*.

2) Deberá desencriptar la firma digital recibida con la clave pública de emisor para obtener el resumen de emisor *h*.

3) Comparar *h* y *h'*. Si *h* y *h'* coinciden entonces el receptor tiene la certeza de que el documento recibido no se ha corrompido en el camino y que el emisor es quién dice ser. Es decir, la firma es válida. Si no coincidiesen, entonces la firma no sería válida y el documento tampoco se consideraría como tal.

12.2 CERTIFICADOS

Los *certificados* surgen para paliar el problema de la clave pública. Este problema se basaba en cómo asegurar que una clave utilizada pertenece a la persona que nosotros pensamos que pertenece. Para solucionarlo, los *certificados* están compuestos por una clave pública de usuario que está firmado por una autoridad de certificación (CA).

Los *certificados* deberán tener al menos los siguientes campos:

- *Versión de certificado:* La versión de especificación de certificado que sigue el certificado.

- *Número de serie:* Un número único para cada certificado firmado por la autoridad de certificado.

- *Firma:* Especifica el esquema de encriptación de clave pública de algoritmo de mezcla. La firma se agrega al final del certificado.

- *Nombre del emisor:* El nombre distintivo X.500 de la autoridad de certificado que firma el certificado.

- *Período de validez:* Las fechas de inicio y finalización que marcan el intervalo de validez de un certificado.

- *Nombre:* El nombre distintivo X.500 del individuo cuya clave pública está contenida en el certificado. Los Nombres Distinguidos son universalmente únicos.

- *Clave pública:* La clave pública verdadera del individuo especificado en el campo de nombre. En la práctica, este campo normalmente contiene dos claves públicas: una utilizada para llevar a cabo los intercambios de clave de sesión y otra que se utiliza para firmar documentos.

12.2.1 AUTORIDADES DE CERTIFICACIÓN

Las *autoridades de certificación*, *CA*, son las encargadas de distribuir las claves públicas y de verificar toda la información contenida en un certificado antes de firmarlo. Para verificar los certificados habrá que:

- Verificar que el período de validez sea el adecuado.
- Verificar la firma digital del certificado utilizando la clave pública de la autoridad de certificado.
- Verificar que el número de serie de certificado no está en una lista de certificados revocados publicada por la autoridad de certificado.
- Verificar que el nombre de sujeto sea el nombre del individuo deseado.

12.3 SECURE SOCKETS LAYER

Secure Sockets Layer, *SSL*, es un protocolo que se utiliza para establecer comunicaciones entre usuarios. *SSL*, además de encriptar contenidos, identifica inequívocamente a los usuarios haciendo uso de lo explicado anteriormente. *SSL* realizará también cualquier tipo de comunicación sobre TCP-IP, por tanto, sobre Internet.

Este protocolo tendrá dos estados básicos:

1) Fase de saludo: establece la conexión segura. Para ello, los algoritmos se ponen de acuerdo, se intercambian las claves y se identifican los puntos finales.

2) Fase de transferencia de datos: En ésta, la información se pasa a SSL y se entrega una entidad de un nivel superior. La transferencia de información es como si la encriptación no se llevase a cabo.

12.4 POSIBLES SOLUCIONES

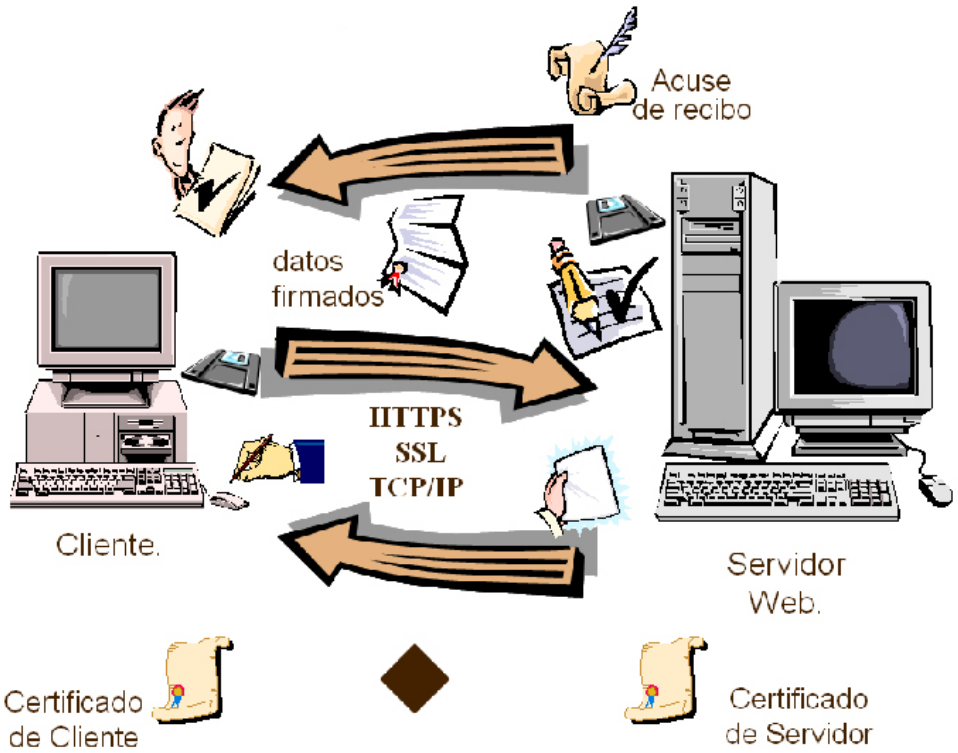
A continuación comentaremos dos posibles soluciones para la transferencia de información sensible.

12.4.1 TRANSFERENCIA SENCILLA

Cuando se pretende acceder a ficheros con datos personales con aplicaciones como telnet, FTP, etc. es necesario tanto tomar las medidas de seguridad oportunas como la utilización de otras aplicaciones que tengan las mismas funcionalidades, pero que añadan el encriptado en la comunicación. Por ejemplo el ssh[2], SSLFTP[3], IPSec, etc.

12.4.2 TRANSFERENCIA CON APLICACIÓN

A continuación, se muestra una posible solución para obtener una aplicación segura por internet.



[2] http:://www.ssh.com/

[3] ftp://ftp.psy.oz.au/pub/crypto/SSLapps

Tal como se ha explicado anteriormente, tanto el cliente como el servidor tendrán un certificado que avale su identidad. Estos certificados serán intercambiados por ambas partes cuando el cliente intente recuperar la información sensible. Como no sólo se autentica el servidor ante el cliente, sino que éste también lo hace frente al servidor, este proceso recibe el nombre de autenticación mutua.

Si el proceso de autenticación se realiza satisfactoriamente el cliente recuperará la información sensible. Una vez cumplimentados los datos necesarios se procederá a su firma y posterior almacenamiento en disco. Estos datos, junto con la firma aplicada sobre ellos, son remitidos al servidor, que efectuará la verificación oportuna y su almacenamiento[4].

Para terminar el proceso, sólo queda que el servidor genere el acuse de recibo, haga el tratamiento de los datos solicitados y se los envíe al cliente para que este tenga constancia de que sus datos han sido recibidos correctamente. Este acuse de recibo no es más que la firma digital del servidor. De esta forma, cuando el cliente verifica dicha firma y la almacena, está en situación de probar en cualquier momento que la comunicación efectivamente ha sido realizada.

[4] Dicho almacenamiento es debido a que se debe tener un registro de los datos solicitados así como quién los ha solicitado.

13

Documento de Seguridad

En este capitulo veremos, como en el 7 y en el 10, cómo se debe escribir un documento de seguridad. Aunque no existe ningún artículo específico para el nivel alto como hay en los niveles anteriores, no se puede utilizar el documento que hacíamos referencia en el capítulo 10.

Por tanto, en este capítulo veremos como en capítulos anteriores qué puntos habrá que tener en cuenta a mayores a la hora de redactar dicho documento.

13.1 INTRODUCCIÓN

Para la realización del documento de seguridad del nivel alto habrá que tener en cuenta todo lo dicho en capítulos anteriores. Recuerde el capítulo 1 en donde explicábamos que las medidas de seguridad se aplican de forma acumulativa, así el nivel alto deberá cumplir también las reguladas para el nivel medio y el nivel bajo de seguridad.

13.2 PUNTOS A TENER EN CUENTA

Tendrá que tener en cuenta los puntos descritos en las secciones 7.2 y 10.2. Además, en las normas y procedimientos de seguridad tendrá que hacer referencia a qué información guardan los logs, así como su periodo de conservación. En las gestión de soportes habrá que añadir que su distribución se hace cifrándolos para que la información contenida en ella sea inteligible durante su transporte. Otros de los puntos que habrá que describir es en la entrada y salida de datos por red si la hubiese que tiene que estar cifrada. En los procedimientos de respaldo y recuperación se tendrá que hacer referencia que se guarda en lugar diferente en el que se encuentren los equipos informáticos y que estos cumplirán las medidas del nivel alto. Por último, en el punto de controles periódicos de verificación del cumplimento habrá que comentar los mecanismos que permiten el registro de accesos.

A continuación, se muestra un ejemplo de un documento de seguridad que como en los capítulos 7 y 10 están sacados de la web de la Agencia de Protección de Datos de la Comunidad de Madrid:

13.3 EJEMPLO

Documento de Seguridad para ficheros automatizados de datos de carácter personal con nivel de seguridad alto

Fichero

Nº inscripción	NOMBRE DE FICHERO	

NOMBRE EMPRESA

Dirección General / Órgano / Organismo / Entidad

Fecha versión del Borrador del Documento de Seguridad	15 de septiembre de 2000
Versión	
Sistema de Información	

ÍNDICE

ANEXOS

Nº de inscripción	NOMBRE DE FICHERO

1. Objeto del documento

El presente documento responde a la obligación establecida en el artículo 8 del Real Decreto 994/1999 de 11 de Junio en el que se regulan las medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

El fichero de datos: **NOMBRE DE FICHERO**, en adelante el Fichero, descrito en el documento de Notificación a la Agencia de Protección de Datos de la Comunidad de Madrid, que se adjunta en el Anexo A, se encuentra oficialmente clasificado como de nivel de seguridad **alto**, atendiendo a las condiciones descritas en el artículo 4 del Real Decreto citado, siendo por tanto aplicable a él todas las medidas de seguridad de nivel **alto** que se establecen en el Capítulo III del citado decreto.

2. Ámbito de aplicación

Este documento ha sido elaborado bajo la responsabilidad de la persona descrita en el apartado (1) del documento adjunto en el Anexo A, quien, como responsable del Fichero, se compromete a implantar y actualizar ésta Normativa de Seguridad de obligado cumplimiento para todo el personal con acceso a los datos protegidos o a los sistemas de información que permiten al acceso a los mismos.

Todas las personas que tengan acceso a los datos del Fichero, bien a través del sistema informático **NOMBRE DEL SISTEMA INFORMÁTICO** habilitado para acceder al mismo, o bien a través de cualquier otro medio automatizado de acceso al Fichero, se encuentran obligadas por ley a cumplir lo establecido en este documento, y sujetas a las consecuencias que pudieran incurrir en caso de incumplimiento.

Una copia de este documento con la parte que le afecte será entregada, para su conocimiento, a cada persona autorizada a acceder a los datos del Fichero, siendo

requisito obligatorio para poder acceder a esos datos el haber firmado la recepción del mismo.

3. Recursos protegidos

La protección de los datos del Fichero frente a accesos no autorizados se deberá realizar mediante el control, a su vez, de todas las vías por las que se pueda tener acceso a dicha información.

Los recursos que, por servir de medio directo o indirecto para acceder al Fichero, deberán ser controlados por esta normativa son:

1) Los centros de tratamiento y locales donde se encuentren ubicados los ficheros o se almacenen los soportes que los contengan, su descripción figura en el Anexo E.

2) Los puestos de trabajo, bien locales o remotos, desde los que se pueda tener acceso al Fichero. La relación de esos puestos de trabajo está descrita en el Anexo E.

3) Los servidores, si los hubiese, y el entorno de sistema operativo y de comunicaciones en el que se encuentra ubicado el Fichero, que está descrito en el Anexo D.

4) Los sistemas informáticos, o aplicaciones establecidos para acceder a los datos, descritos en el Anexo C.

4. Funciones y obligaciones del personal

El personal afectado por esta normativa se clasifica en dos categorías:

1) **Administradores del sistema**, encargados de administrar o mantener el entorno operativo del Fichero. Este personal deberá estar explícitamente relacionado en el Anexo F, ya que por sus funciones pueden utilizar herramientas de administración que permitan el acceso a los datos protegidos sáltandose las barreras de acceso de la Aplicación.

2) **Usuarios del Fichero**, o personal que usualmente utiliza el sistema informático de acceso al Fichero, y que también deben estar explícitamente relacionados en el Anexo F.

Además del personal anteriormente citado existirá un **Responsable de Seguridad del Fichero** cuyas funciones serán las de coordinar y controlar las medidas definidas en el documento, sirviendo al mismo tiempo de enlace con el **Responsable del Fichero**, sin que esto suponga en ningún caso una delegación de la responsabilidad que corresponde a éste último, de acuerdo con el R.D. 994/1999 de 11 de Junio.
Este documento es de obligado cumplimiento para todos ellos. Las funciones y obligaciones del personal están descritas en el Anexo H. Sin embargo, los administradores del sistema deberán además atenerse a aquellas normas, más extensas y estrictas, que se referencian en el Anexo G, y que atañen, entre otras, al tratamiento de los respaldos de seguridad, normas para el alta de usuarios y contraseñas, así como otras normas de obligado cumplimiento en la unidad administrativa a la que pertenece el Fichero.

5. Normas y procedimientos de seguridad

5.1 Centros de tratamiento y locales

Los locales donde se ubiquen los ordenadores que contienen el Fichero deben ser objeto de especial protección que garantice la disponibilidad y confidencialidad de los datos protegidos, especialmente en el caso de que el Fichero esté ubicado en un servidor accedido a través de una red.

5.1.1. Los locales deberán contar con los medios mínimos de seguridad que eviten los riesgos de indisponibilidad del Fichero que pudieran producirse como consecuencia de incidencias fortuitas o intencionadas. La descripción de esos medios se encuentra en el Anexo E.

5.1.2. El acceso a los locales donde se encuentre el fichero deberá estar restringido exclusivamente a los administradores del sistema que deban realizar labores de mantenimiento para las que sean imprescindibles el acceso físico.

5.2 Puestos de trabajo

Son todos aquellos dispositivos desde los cuales se puede acceder a los datos del Fichero, como, por ejemplo, terminales u ordenadores personales.

Se consideran también puestos de trabajo aquellos terminales de administración del sistema, como, por ejemplo, las consolas de operación, donde en algunos casos también pueden aparecer los datos protegidos del Fichero.

5.2.1. Cada puesto de trabajo estará bajo la responsabilidad de una persona de las autorizadas en el Anexo F, que garantizará que la información que muestra no pueda ser vista por personas no autorizadas.

5.2.2. Esto implica que tanto las pantallas como las impresoras u otro tipo de dispositivos conectados al puesto de trabajo deberán estar físicamente ubicados en lugares que garanticen esa confidencialidad.

5.2.3. Cuando el responsable de un puesto de trabajo lo abandone, bien temporalmente o bien al finalizar su turno de trabajo, deberá dejarlo en un estado que impida la visualización de los datos protegidos. Esto podrá realizarse a través de un

protector de pantalla que impida la visualización de los datos. La reanudación del trabajo implicará la desactivación de la pantalla protectora con la introducción de la contraseña correspondiente.

5.2.4. En el caso de las impresoras deberá asegurarse de que no quedan documentos impresos en la bandeja de salida que contengan datos protegidos. Si las impresoras son compartidas con otros usuarios no autorizados para acceder a los datos de Fichero, los responsables de cada puesto deberán retirar los documentos conforme vayan siendo impresos.

5.2.5. Queda expresamente prohibida la conexión a redes o sistemas exteriores de los puestos de trabajo desde los que se realiza el acceso al fichero. La revocación de esta prohibición sera autorizada por el responsable del fichero, quedando constancia de esta modificación en el Libro de incidencias.

5.2.6. Los puestos de trabajo desde los que se tiene acceso al fichero tendrán una configuración fija en sus aplicaciones, sistemas operativos que solo podrá ser cambiada bajo al autorización del responsable de seguridad o por administradores autorizados del anexo F.

5.3 Entorno de Sistema Operativo y de Comunicaciones

Aunque el método establecido para acceder a los datos protegidos del Fichero es el sistema informático referenciado en el Anexo C, al estar el fichero ubicado en un ordenador con un sistema operativo determinado y poder contar con unas conexiones que le comunican con otro ordenadores, es posible, para las personas que conozcan estos entornos, acceder a los datos protegidos sin pasar por los procedimientos de control de acceso con los que pueda contar la aplicación.

Esta normativa debe, por tanto, regular el uso y acceso de las partes del sistema operativo, herramientas o programas de utilidad, o del entorno de comunicaciones, de forma que se impida el acceso no autorizado a los datos de Fichero.

5.3.1. El sistema operativo y de comunicaciones del Fichero deberá tener al menos un responsable, que, como administrador deberá estar relacionado en el Anexo F.

5.3.2. En el caso más simple, como es que el Fichero se encuentre ubicado en un ordenador personal y accedido mediante una aplicación local monopuesto, el administrador del sistema operativo podrá ser el mismo usuario que accede usualmente al Fichero.

5.3.3. Ninguna herramienta o programa de utilidad que permita el acceso al Fichero deberá ser accesible a ningún usuario o administrador no autorizado en el Anexo F.

5.3.4. En la norma anterior se incluye cualquier medio de acceso en bruto, es decir no elaborado o editado, a los datos del Fichero, como los llamados "queries", editores universales, analizadores de ficheros, etc., que deberán estar bajo el control de los administradores autorizados relacionados en el Anexo F.

5.3.5. El administrador deberá responsabilizarse de guardar en lugar protegido las copias de seguridad y respaldo del Fichero, de forma que ninguna persona no autorizada tenga acceso a las mismas.

5.3.6. Si la aplicación o sistema de acceso al Fichero utilizase usualmente ficheros temporales, ficheros de "logging", o cualquier otro medio en el que pudiesen ser grabados copias de los datos protegidos, el administrador deberá asegurarse de que esos datos no son accesibles posteriormente por personal no autorizado.

5.3.7. Si el ordenador en el que está ubicado el fichero está integrado en una red de comunicaciones de forma que desde otros ordenadores conectados a la misma sea posible acceso al Fichero, el administrador responsable del sistema deberá asegurarse de que este acceso no se permite a personas no autorizadas.

5.4 Sistema Informático o aplicaciones de acceso al Fichero

Son todos aquellos sistemas informáticos, programas o aplicaciones con las que se puede acceder a los datos del Fichero, y que son usualmente utilizados por los usuarios para acceder a ellos.

Estos sistemas pueden ser aplicaciones informáticas expresamente diseñadas para acceder al Fichero, o sistemas preprogramados de uso general como aplicaciones o paquetes disponibles en el mercado informático.

5.4.1. Los sistemas informáticos de acceso al Fichero deberán tener su acceso restringido mediante un código de usuario y una contraseña.

5.4.2. Todos los usuarios autorizados para acceder al Fichero, relacionados en el Anexo F, deberán tener un código de usuario que será único, y que estará asociado a la contraseña correspondiente, que sólo será conocida por el propio usuario.

5.4.3. Si la aplicación informática que permite el acceso al Fichero no cuenta con un control de acceso, deberá ser el sistema operativo, donde se ejecuta esa aplicación, el que impida el acceso no autorizado, mediante el control de los citados códigos de usuario y contraseñas.

5.4.4. En cualquier caso se controlarán los intentos de acceso fraudulento al Fichero, limitando el

número máximo de intentos fallidos, y cuando sea técnicamente posible, guardando en un fichero auxiliar la fecha , hora, código y clave erróneas que se han introducido, así como otros datos relevantes que ayuden a descubrir la autoría de esos intentos de acceso fraudulentos.

5.4.5. Si durante las pruebas anteriores a la implantación o modificación de la aplicación de acceso al Fichero se utilizasen datos reales, se deberá aplicar a esos ficheros de prueba el mismo tratamiento de seguridad que se aplica al mismo Fichero, y se deberán relacionar esos ficheros de prueba en el Anexo B.

5.4.6 De cada acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.Si se trata de un accesso autorizado, se guardara la clave del registro o bien la información que permita identificar el registro accedido.

5.4.7 El periódo mínimo de conservación de los datos registrados será de dos años.

5.5 Salvaguarda y protección de las contraseñas personales

Las contraseñas personales constituyen uno de los componentes básicos de la seguridad de los datos, y deben por tanto estar especialmente protegidas. Como llaves de acceso al sistema, las contraseñas deberán ser estrictamente confidenciales y personales, y cualquier incidencia que comprometa su confidencialidad deberá ser inmediatamente comunicada al administrador y subsanada en el menor plazo de tiempo posible.

5.5.1. Sólo las personas relacionadas en el Anexo F podrán tener acceso a los datos del Fichero.

5.5.2. Cada usuario será responsable de la confidencialidad de su contraseña y, en caso de que la misma sea conocida fortuita o fraudulentamente por personas no

autorizadas, deberá registrarlo como incidencia y proceder inmediatamente a su cambio.

5.5.3. Las contraseñas se asignarán y se cambiarán mediante el mecanismo y periodicidad que se determina en el Anexo G.

5.5.4. El archivo donde se almacenen las contraseñas deberá estar protegido y bajo la responsabilidad del administrador del sistema.

6. Gestión de incidencias

Una incidencia es cualquier evento que pueda producirse esporádicamente y que pueda suponer un peligro para la seguridad del Fichero, entendida bajo sus tres vertientes de confidencialidad, integridad y disponibilidad de los datos.

El mantener un registro de las incidencias que comprometan la seguridad de un Fichero es una herramienta imprescindible para la prevención de posibles ataques a esa seguridad, así como para persecución de los responsables de los mismos.

6.1.1. El responsable de seguridad de Fichero habilitará un Libro de Incidencias a disposición de todos los usuarios y administradores del Fichero con el fin de que se registren en él cualquier incidencia que pueda suponer un peligro para la seguridad del mismo.

6.1.2. Cualquier usuario que tenga conocimiento de una incidencia es responsable del registro de la misma en el Libro de Incidencias del Fichero o en su caso de la comunicación por escrito al responsable de seguridad o al responsable del Fichero.

6.1.3. El conocimiento y la no notificación o registro de una incidencia por parte de un usuario será considerado como una falta contra la seguridad del Fichero por parte de ese usuario.

6.1.4. La notificación o registro de una incidencia deberá constar al menos de los siguientes datos: tipo de incidencia, fecha y hora en que se produjo, persona que realiza la notificación, persona a quien se comunica, efectos que puede producir, descripción detallada de la misma. El procedimiento está descrito en el Anexo I.

7. Gestión de soportes

Soportes informáticos son todos aquellos medios de grabación y recuperación de datos que se utilizan para realizar copias o pasos intermedios en los procesos de la aplicación que gestiona el Fichero.

Dado que la mayor parte de los soportes que hoy en día se utilizan, como disquetes o CD-ROMs, son fácilmente transportables, reproducibles y/o copiables, es evidente la importancia que para la seguridad de los datos del Fichero tiene el control de estos medios.

7.1.1. Los soportes que contengan datos del Fichero, bien como consecuencia de operaciones intermedias propias de la aplicación que los trata, o bien como consecuencia de procesos periódicos de respaldo o cualquier otra operación esporádica, deberán estar claramente identificados con una etiqueta externa que indique de qué fichero se trata, que tipo de datos contiene, proceso que los ha originado y fecha de creación.

7.1.2. Aquellos medios que sean reutilizables, y que hayan contenido copias de datos del Fichero, deberán ser borrados físicamente antes de su reutilización, de forma que los datos que contenían no sean recuperables.

7.1.3. Los soportes que contengan datos del Fichero deberán ser almacenados en lugares a lo que no tengan acceso personas no autorizadas para el uso del Fichero que no estén por tanto relacionadas en el Anexo F.

7.1.4. La salida de soportes informáticos que contengan datos del Fichero fuera de los locales donde está ubicado el Fichero deberá ser expresamente autorizada por el responsable del Fichero, utilizando para ello el documento adjunto en el anexo G.

7.1.5 El responsable del Fichero mantendrá un Libro de registro de entradas y salidas donde se guardarán los formularios de entradas y de salidas de soportes descritos en el anexo G, con indicación de tipo de soporte, fecha y hora, emisor, número de soportes, tipo de información que contienen, forma de envío, destinario, o persona responsable de la recepción que deberán estar debidamente autorizadas.

7.1.6 Cuando los soportes vayan a salir fuera de los locales en que se encuentren ubicados los ficheros como consecuencia de operaciones de mantenimiento, se adoptarán las medidas necesarias para impedir cualquier recuperación indebida de la información almacenada en ellos.

7.1.8 La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su transporte.

8. Entrada/salida de datos por red y Telecomunicaciones

La transmisión de datos por red, ya sea por medio de correo electrónico o mediante sistemas de transferencia de ficheros, se está convirtiendo en uno de los medios más

utilizados para el envío de datos, hasta el punto de que está sustituyendo a los soportes físicos. Por ello merecen un tratamiento especial ya que, por sus características, pueden ser más vulnerables que los soportes físicos tradicionales.

8.1.1 Todas las entradas y salidas de datos del Fichero que se efectúen mediante correo electrónico se realizarán desde una única cuenta o dirección de correo controlada por un usuario especialmente autorizado por el responsable del Fichero. Igualmente si se realiza la entrada o salida de datos mediante sistemas de transferencia de ficheros por red, únicamente un usuario o administrador estará autorizado para realizar esas operaciones.

8.1.2 Se guardarán copias de todos los correos electrónicos que involucren entradas o salidas de datos del Fichero, en directorios protegidos y bajo el control del responsable citado. Se mantendrán copias de esos correos durante al menos dos años. También se guardará durante un mínimo de dos años, en directorios protegidos, una copia de los ficheros recibidos o transmitidos por sistemas de transferencia de ficheros por red, junto con un registro de la fecha y hora en que se realizó la operación y el destino del fichero enviado.

8.1.4 Cuando los datos del Fichero vayan a ser enviados por correo electrónico o por sistemas de transferencia de ficheros, a través de redes públicas o no protegidas, se recomienda que sean encriptados de forma que solo puedan ser leídos e interpretados por el destinatario.

8.1.5 La transmisión de datos de carácter personal a través de redes de telecomunicaciones se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

9. Procedimientos de respaldo y recuperación

La seguridad de los datos personales del Fichero no sólo supone la confidencialidad de los mismos sino que también conlleva la integridad y la disponibilidad de esos datos.

Para garantizar estos dos aspectos fundamentales de la seguridad es necesario que existan unos procesos de respaldo y de recuperación que, en caso de fallo del sistema informático, permitan recuperar y en su caso reconstruir los datos del Fichero.

9.1.1. Existirá una persona, bien sea el administrador o bien otro usuario expresamente designado, que será responsable de obtener periódicamente una copia de seguridad del fichero, a efectos de respaldo y posible recuperación en caso de fallo.

9.1.2. Estas copias deberán realizarse con una periodicidad, al menos, semanal, salvo en el caso de que no se haya producido ninguna actualización de los datos.

9.1.3. En caso de fallo del sistema con pérdida total o parcial de los datos del Fichero existirá un procedimiento, informático o manual, que partiendo de la última copia de respaldo y del registro de las operaciones realizadas desde el momento de la copia, reconstruya los datos del Fichero al estado en que se encontraban en el momento del fallo. Ese procedimiento está descrito en el Anexo G.

9.1.4 Será necesaria la autorización por escrito del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos, y deberá dejarse constancia en el registro de incidencias de las manipulaciones que hayan debido realizarse para dichas recuperaciones, incluyendo la persona que realizó el proceso, los datos restaurados y los datos que hayan debido ser grabados manualmente en el proceso de recuperación.

9.1.5. Deberá conservarse una copia de respaldo y de los procedimientos de recuperación de los datos en un lugar diferente de aquél en que se encuentren los equipos informáticos que los tratan cumpliendo en todo caso, las medidas de seguridad exigidas en el Reglamento.

10. Controles periódicos de verificación del cumplimiento

La veracidad de los datos contenidos en los anexos de este documento, así como el cumplimiento de las normas que contiene deberán ser periódicamente comprobados, de forma que puedan detectarse y subsanarse anomalías.

10.1.1. El responsable de seguridad del Fichero comprobará, con una periodicidad al menos trimestral, que la lista de usuarios autorizados del Anexo F se corresponde con la lista de los usuarios realmente autorizados en la aplicación de acceso al Fichero, para lo que recabará la lista de usuarios y sus códigos de acceso al administrador o administradores del Fichero. Ademas de estas comprobaciones periódicas, el administrador comunicará al responsable de seguridad, en cuanto se produzca, cualquier alta o baja de usuarios con acceso autorizado al Fichero.

10.1.2 Se comprobará también al menos con periodicidad trimestral, la existencia de copias de respaldo que permitan la recuperación de Fichero según lo estipulado en el apartado 8 de este documento.

10.1.3 A su vez, y también con periodicidad al menos trimestral, los administradores del Fichero comunicaran al responsable de seguridad cualquier cambio que se haya realizado en los datos técnicos de los anexos, como por ejemplo cambios en el software o hardware, base de datos o aplicación de acceso al Fichero, procediendo igualmente a la actualización de dichos anexos.

10.1.4 El responsable de seguridad, verificará, con periodicidad al menos trimestral, el cumplimiento de lo previsto en los apartados 7 y 8 de este documento en relación con las entradas y salidas de datos, sean por red o en soporte magnético.

10.1.5 El responsable del fichero junto con el responsable de seguridad, analizaran con periodicidad al menos trimestral las incidencias registradas en el libro correspondiente, para independientemente de las medidas particulares que se hayan adoptado en el momento que se produjeron, adoptar las medidas correctoras que limiten esas incidencias en el futuro.

10.1.6 Al menos cada dos años, se realizará una auditoría, externa o interna que dictamine el correcto cumplimiento y la adecuación de las medidas del presente documento de seguridad o las exigencias del Reglamento de seguridad, identificando las deficiencias y proponiendo las media correctoras necesarias. Los informes de auditoría serán analizados por el responsable de seguridad, quien propondrá al responsable del Fichero las medidas correctoras correspondientes.

10.1.7 Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad sin que se deba permitir , en ningun caso la desactivación de los mismos.

10.1.8 El reponsable de seguridad se encargará de revisar periodicamente la información de control registrada y eleborará un informe de las revisiones relaizadas y los problemas detectados al menos una vez al mes.

10.1.9 Los resultados de todos estos controles periódicos, así como de las auditorías serán adjuntadas a este documento de seguridad en el Anexo J.

Anexo A. Documentos de Notificación y Decretos

Documento de Notificación a la Agencia de Protección de Datos de Registro del Fichero.

Se adjuntará aquí una copia del documento de notificación de la creación, y en su caso de las posibles modificaciones del Fichero.

En este mismo apartado se recojerá una copia de la publicación de la disposición de creación, y si procede de las modificaciónes.

Nº de inscripción	NOMBRE DE FICHERO

Anexo B. Descripción detallada de la estructura del Fichero o la Base de Datos.

La descripción contendrá al menos los siguientes aspectos:

Ubicación física del Fichero, tipo de soporte, servidor, nombre del área o directorio etcΨ

Descripción lógica, archivos o tablas, registros o tuplas, campos o columnas, así como el formato, descripción y relaciones entre los mismos.

Si se realizan pruebas con datos reales , se relacionaran estos ficheros de prueba, indicando el nombre y descripción de los mismos y procedimiento previsto para el borrado físico de estos datos.

Gestor de base de datos, mecanismos de recuperación Y mecanismos del registro de accesos.

Nº de inscripción	NOMBRE DE FICHERO

Anexo C.Descripción del sistema informático de acceso al fichero.

Descripción del Sistema Informático de acceso al Fichero

El sistema informático o aplicación de acceso al fichero es el conjunto de programas, específicamente diseñados para el caso o de propósito general, con los que normalmente se accede para consultar o actualizar los dato del Fichero.

La descripción deberá al menos contener los siguientes datos:

- Nombre de la aplicación
- Si se trata de un paquete o producto estándar del mercado o de unos programas expresamente diseñados para ese propósito.
- Quién y en que fecha se programó.
- Responsables del mantenimiento.
- Tipo de control de acceso si lo tiene, indicando si se limita el numero de intentos fallidos de acceso al sistema y si se guarda en un fichero auxiliar la historia de estos intentos.
- Tipo de procedimientos de histórico de operaciones (logging) y de recuperación, si los tiene.

Nº de inscripción	NOMBRE DE FICHERO

Anexo D.Entorno de Sistema Operativo y de Comunicaciones del Fichero

Entorno de Sistema Operativo y de Comunicaciones del Fichero
(a ser cumplimentado por el administrador del sistema)

Deberá contener al menos los siguientes datos y aspectos:

Sistema operativo

Nombre y versión
Fabricante
Características generales (monopuesto, multiusuario, compartición de ficheros u otros recursos, etc..)
Control de acceso, características
Archivos de logging y procedimientos de recuperación propios del sistema.
Responsables del mantenimiento

Entorno de comunicaciones (si lo tuviese)

Tipo de red local (Ethernet, otras), ámbito y extensión.
Si existe conexión con otras redes locales o WAN, indicar el tipo de conexión (permanente, esporádica, etcc..), a través de redes públicas como Internet o con conexiones privadas etc..
Hay compartición de recursos y archivos ?. Si es así indicar que tipo de sistema de red es utilizado, sus límites y alcance.
Controles de acceso desde la red al sistema del Fichero.

Sistema de cifrado utilizado en la transmisión de datos

Nº de inscripción	NOMBRE DE FICHERO

Anexo E. Locales y equipamiento

Locales y equipamiento de los centros de tratamiento y almacenamiento de las copias de respaldo y recuperación.

Locales

Descripción de la ubicación física
Tipo de acceso: Se especificara el tipo de control de acceso
Sistemas de continuidad
Equipamiento; armarios ignífugos, etc

Puestos de Trabajo

Descripción Equipos: Servidores, equipos, Impresoras
Relación de puestos de trabajo

Anexo F. Personal autorizado para acceder al Fichero

RESPONSABLE DEL FICHERO

Nombre y apellidos	Cargo	Alta	Baja

RESPONSABLE DE SEGURIDAD

Nombre y apellidos	Cargo	Alta	Baja

Nº de inscripción NOMBRE DE FICHERO

ADMINISTRADORES DEL SISTEMA

Nombre y apellidos	Organismo / Unidad Administrativa	Alta	Baja

Nº de inscripción NOMBRE DE FICHERO

USUARIOS DEL FICHERO

Nombre y apellidos	Unidad Administrativa	N1 inventario Puesto Trabajo	Alta	Baja

Nº de inscripción NOMBRE DE FICHERO

Nº de inscripción NOMBRE DE FICHERO

Anexo G. Procedimientos de control y seguridad

Contendrá al menos los procedimientos siguientes :

Procedimiento de asignación y cambio de contraseñas.

Procedimiento de respaldo y recuperación.

Procedimiento de gestión de soportes:

Constará al menos de los siguientes apartados

- Identificación de etiquetas
- Inventario de soportes
- Lugar de almacenamiento
- En el caso de reutilización o eliminación de soportes grabados con datos del fichero se indicará el método utilizado para el borrado físico de estos datos.

Se adjunta impreso de inventario de soportes y formularios de inscripción para registrar en el Libro de entradas y salida de soportes.

Entrada y salida de datos por red :

Se especificará

Nº de inscripción	NOMBRE DE FICHERO

- Cuenta de correo

- Responsable de transferencias electrónicas

Procedimiento de distribución de soportes.

Se describirá el sistema utilizado para el cifrado de datos.

INVENTARIO DE SOPORTES

Página nº _____

Fichero: NOMBRE DE FICHERO					
ALTAS		**BAJAS**			
		Reutilización	**Destrucción**	**MÉTODO**	
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /

Nº de inscripción NOMBRE DE FICHERO

SALIDA DE SOPORTES

Cualquier salida de soportes fuera de los locales donde esta ubicado el fichero deberá ser autorizada por el responsable del fichero de acuerdo con el documento que se adjunta.

El responsable del fichero mantendrá un Libro en el que registrará las salidas de soportes, cuyos asientos estarán constituidos por los documentos de autorización de salida debidamente cumplimentados.

La persona responsable de la entrega de soportes estará debidamente autorizada por el responsable del fichero.

REGISTRO Y AUTORIZACIÓN DE SALIDA DE SOPORTES

Fecha y hora de salida del soporte	

SOPORTE	
Tipo de soporte y número	
Contenido	
Ficheros de donde proceden los datos	
Fecha de creación	

FINALIDAD Y DESTINO	
Finalidad	
Destino	
Destinatario	

FORMA DE ENVÍO	
Medio de envío	
Remitente	
Precauciones para	

Nº de inscripción NOMBRE DE FICHERO

el transporte	

AUTORIZACIÓN	
Persona responsable de la entrega	
Persona que autoriza	
Cargo / Puesto	
Observaciones	
Firma	

Nº de inscripción NOMBRE DE FICHERO

ENTRADA DE SOPORTES

El responsable del fichero mantendrá un Libro en el que registrará las entradas de soportes cuyos asientos estarán constituidos por los datos recogidos en el formulario que se adjunta.

La persona responsable de la recepción de soportes estará debidamente autorizada por el responsable del fichero.

Nº de inscripción NOMBRE DE FICHERO

REGISTRO DE ENTRADA DE SOPORTES

Fecha y hora de entrada de soporte	

SOPORTE	
Tipo de soporte y número	
Contenido	
Fecha de creación	

ORIGEN Y FINALIDAD	
Finalidad	
Origen	

FORMA DE ENVÍO	
Medio de envío	
Remitente	
Precauciones para el transporte	

Nº de inscripción NOMBRE DE FICHERO

AUTORIZACIÓN	
Persona responsable de la recepción	
Cargo / Puesto	
Observaciones	
Firma	

Nº de inscripción NOMBRE DE FICHERO

Anexo H. Funciones y obligaciones del personal

FUNCIONES DEL RESPONSABLE DEL FICHERO

El responsable del fichero es el encargado jurídicamente de la seguridad del fichero y de las medidas establecidas en el presente documento, implantará las medidas de seguridad establecidas en él y adoptará las medidas necesarias para que el personal afectado por este documento conozca las normas que afecten al desarrollo de sus funciones.

Designará al responsable de seguridad que figura en el Anexo F.

FUNCIONES DEL RESPONSABLE DE SEGURIDAD

Es el encargado de coordinar y controlar las medidas definidas en el presente documento.

CLASIFICACIÓN DEL PERSONAL DE ADMINISTRACIÓN O PERSONAL INFORMÁTICO

Se distinguen dos situaciones diferentes, que condicionan el tipo de personal que tiene acceso al fichero en cada caso:

- -Producción habitual, sin incidencias técnicas. Explotación diaria.
- -Errores, cortes, incidencias técnicas de cualquier tipo que detienen la producción.

PERSONAL AUTORIZADO EN PRODUCCIÓN HABITUAL

En el primer caso, el acceso se limita a los siguientes perfiles

- -Usuario/Administrador del sistema.
- -Operador.

ADMINISTRADORES TÉCNICOS E INFORMÁTICOS GENERALES QUE INTERVIENEN EN SITUACIONES NO HABITUALES

Cuando no existe un personal técnico determinado que se pueda relacionar de forma directa con un fichero o sistema informático y que acceda habitualmente al mencionado fichero o sistema.

Siempre será posible conocer el personal que intervino con posterioridad a la intervención, dejando constancia de ello, identificando al personal técnico, anotándolo en le Registro de Incidencias.

FUNCIONES DE LOS ADMINISTRADORES O PERSONAL INFORMÁTICO

El personal que administra el sistema de acceso al Fichero se puede a su vez clasificar en varias categorías, que no necesariamente deberán estar presentes en todos los casos, siendo en algunas ocasiones asumidas por una misma persona o personas. Estas categorías son:

- Administradores (Red, Sistemas operativos y Bases de Datos). Serán los responsables de los máximos privilegios y por tanto de máximo riesgo de que una actuación errónea pueda afectar al sistema. Tendrán acceso al

software (programas y datos) del sistema, a las herramientas necesarias para su trabajo y a los ficheros o bases de datos necesarios para resolver los problemas que surjan.

- Operadores (Red, Sistemas operativos, Bases de Datos y Aplicación). Sus actuaciones están limitadas a la operación de los equipos y redes utilizando las herramientas de gestión disponibles. No deben, en principio, tener acceso directo a los datos del Fichero, ya que su actuación no precisa de dicho acceso.

- Mantenimiento de los sistemas y aplicaciones. Personal responsable de la resolución de incidencias que puedan surgir en el entono hardware/software de los sistemas informáticos o de la propia aplicación de acceso al Fichero.

- Cualquier otro que la organización establezca.

OBLIGACIONES DEL RESPONSABLE DEL FICHERO

Implantar las medidas de seguridad establecidas en este documento.

El responsable del Fichero deberá garantizar la difusión de este Documento entre todo el personal que vaya a utilizar.

Deberá mantenerlo actualizado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo, según los artículos 8 y 9 de la Normativa de Seguridad.

Deberá adecuar en todo momento el contenido del mismo a las disposiciones vigentes en materia de seguridad de datos.

Deberá designar uno o varios responsables de seguridad.

Entorno de Sistema Operativo y de Comunicaciones

5.3.1 El responsable del Fichero aprobará o designará al administrador que se responsabilizará del sistema operativo y de comunicaciones que deberá estar relacionado en el Anexo F.

5.3.2 En el caso más simple, como es que el Fichero se encuentre ubicado en un ordenador personal y accedido mediante una aplicación local monopuesto, el administrador del sistema operativo podrá ser el mismo usuario que accede usualmente al Fichero.

Sistema Informático o aplicaciones de acceso al Fichero

5.4.1 El responsable del fichero se encargará de que los sistemas informáticos de acceso al Fichero tengan su acceso restringido mediante un código de usuario y una contraseña.

5.4.2 Asimismo cuidará que todos los usuarios autorizados para acceder al Fichero, relacionados en el Anexo F, tengan un código de usuario que será único, y que estará asociado a la contraseña correspondiente, que sólo será conocida por el propio usuario.

Salvaguarda y protección de las contraseñas personales

5.5.1 Sólo las personas relacionadas en el Anexo F, podrán tener acceso a los datos del Fichero.

Gestión de soportes

7.1.4 La salida de soportes informáticos que contengan datos del Fichero fuera de los locales donde está ubicado el Fichero deberá ser expresamente autorizada por el responsable del Fichero.

Entrada y salida de datos por red

8.1.1 Todas las entradas y salidas de datos del Fichero que se efectúen mediante correo electrónico se realizarán desde una única cuenta o dirección de correo controlada por un usuario especialmente autorizado por el responsable del Fichero. Igualmente si se realiza la entrada o salida de datos mediante sistemas de transferencia de ficheros por red, únicamente un usuario o administrador estará autorizado para realizar esas operaciones.

Procedimientos de respaldo y recuperación

El responsable del Fichero se encargará de verificar la definición y correcta aplicación de las copias de respaldo y recuperación de los datos.

9.1.4 Será necesaria la autorización por escrito del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos, y deberá dejarse constancia en el registro de incidencias de las manipulaciones que hayan debido realizarse para dichas recuperaciones, incluyendo la persona que realizó el proceso, los datos restaurados y los datos que hayan debido ser grabados manualmente en el proceso de recuperación.

Controles periódicos de verificación del cumplimiento

10.1.5 El responsable del fichero junto con el responsable de seguridad, analizaran con periodicidad al menos trimestral las incidencias registradas en el libro correspondiente, para independientemente de las medidas particulares que se hayan adoptado en el momento que se produjeron, poner las medidas correctoras que limiten esas incidencias en el futuro.

10.1.6 Al menos cada dos años, se realizará una auditoría, externa o interna que dictamine el correcto cumplimiento y la adecuación de las medidas del presente documento de seguridad o las exigencias del Reglamento de seguridad, identificando las deficiencias y proponiendo las media correctoras necesarias. Los informes de auditoría serán analizados por el responsable de seguridad, quien propondrá al responsable del Fichero las medidas correctoras correspondientes.

10.1.9Los resultados de todos estos controles periódicos, así como de las auditorías serán adjuntadas a este documento de seguridad en el Anexo J.

OBLIGACIONES DEL RESPONSABLE DE SEGURIDAD

El responsable de seguridad coordinará la puesta en marcha de las medidas de seguridad, colaborará con el responsable del fichero en la difusión del Documento de seguridad y cooperará con el responsable del fichero controlando el cumplimiento de las mismas.

Gestión de incidencias

6.1.1 El responsable de seguridad habilitará un Libro de Incidencias a disposición de todos los usuarios y administradores del Fichero con el fin de que se registren en él cualquier incidencia que pueda suponer un peligro para la seguridad del mismo.

Analizara las incidencias registradas, tomando las medidas oportunas en colaboración con el responsable del Fichero.

Controles periódicos de verificación del cumplimiento

10.1.1. El responsable de seguridad del Fichero comprobará, con una periodicidad al menos trimestral, que la lista de usuarios autorizados del Anexo F se corresponde con la lista de los usuarios realmente autorizados en la aplicación de acceso al Fichero, para lo que recabará la lista de usuarios y sus códigos de acceso al administrador o administradores del Fichero. Ademas de estas comprobaciones periódicas, el administrador comunicará al responsable de seguridad, en cuanto se produzca, cualquier alta o baja de usuarios con acceso autorizado al Fichero.

10.1.2 Se comprobará también al menos con periodicidad trimestral, la existencia de copias de respaldo que permitan la recuperación de Fichero según lo estipulado en el apartado 8 de este documento.

10.1.3 A su vez, y también con periodicidad al menos trimestral, los administradores del Fichero comunicaran al responsable de seguridad cualquier cambio que se haya realizado en los datos técnicos de los anexos, como por ejemplo cambios en el software o hardware, base de datos o aplicación de acceso al Fichero, procediendo igualmente a la actualización de dichos anexos.

10.14 El responsable de seguridad, verificará, con periodicidad al menos trimestral, el cumplimiento de lo previsto en los apartados 7 y 8 de este documento en relación con las entradas y salidas de datos, sean por red o en soporte magnético.

10.15 El responsable del fichero junto con el responsable de seguridad, analizaran con periodicidad

al menos trimestral las incidencias registradas en el libro correspondiente, para independientemente de las medidas particulares que se hayan adoptado en el momento que se produjeron, poner las medidas correctoras que limiten esas incidencias en el futuro.

10.1.6 Al menos cada dos años, se realizará una auditoría, externa o interna que dictamine el correcto cumplimiento y la adecuación de las medidas del presente documento de seguridad o las exigencias del Reglamento de seguridad, identificando las deficiencias y proponiendo las media correctoras necesarias. Los informes de auditoría serán analizados por el responsable de seguridad, quien propondrá al responsable del Fichero las medidas correctoras correspondientes.

10.1.7 Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad sin que se deba permitir , en ningun caso la desactivación de los mismos.

10.1.8 El reponsable de seguridad se encargará de revisar periodicamente la información de control registrada,

10.1.9 Los resultados de todos estos controles periódicos, así como de las auditorías serán adjuntadas a este documento de seguridad en el Anexo J.

OBLIGACIONES QUE AFECTAN A TODO EL PERSONAL

Puestos de trabajo

5.2.1 Los puestos de trabajo estarán bajo la responsabilidad de algún usuario autorizado que garantizará que la información que muestran no pueda ser visible por personas no autorizadas.

5.2.2 Esto implica que tanto las pantallas como las impresoras u otro tipo de dispositivos conectados al puesto de trabajo deberán estar físicamente ubicados en lugares que garanticen esa confidencialidad.

5.2.3 Cuando el responsable de un puesto de trabajo lo abandone, bien temporalmente o bien al finalizar su turno de trabajo, deberá dejarlo en un estado que impida la visualización de los datos protegidos. Esto podrá realizarse a través de un protector de pantalla que impida la visualización de los datos. La reanudación del trabajo implicará la desactivación de la pantalla protectora con la introducción de la contraseña correspondiente.

5.2.4 En el caso de las impresoras deberá asegurarse de que no quedan documentos impresos en la bandeja de salida que contengan datos protegidos. Si las impresoras son compartidas con otros usuarios no autorizados para acceder a los datos de Fichero, los responsables de cada puesto deberán retirar los documentos conforme vayan siendo impresos.

5.2.5 Queda expresamente prohibida la conexión a redes o sistemas exteriores de los puestos de trabajo desde los que se realiza el acceso al fichero. La revocación de esta prohibición sera autorizada por el responsable del fichero, quedando constancia de esta modificación en el Libro de incidencias.

5.2.6 Los puestos de trabajo desde los que se tiene acceso al fichero tendrán una configuración fija en sus aplicaciones, sistemas operativos que solo podrá ser cambiada bajo al autorización del responsable de seguridad o por administradores autorizados del anexo F.

Salvaguarda y protección de las contraseñas personales

5.5.2 Cada usuario será responsable de la confidencialidad de su contraseña y, en caso de que la misma sea conocida fortuita o fraudulentamente por personas no autorizadas, deberá registrarlo como incidencia y proceder a su cambio.

Gestión de incidencias

6.1.1 Cualquier usuario que tenga conocimiento de una incidencia es responsable de la comunicación de la misma al administrador del sistema, o en su caso del registro de la misma en el sistema de registro de incidencias del Fichero.

6.1.2 El conocimiento y la no notificación de una incidencia por parte de un usuario será considerado como una falta contra la seguridad del Fichero por parte de ese usuario.

Gestión de soportes

7.1.1 Los soportes que contengan datos del Fichero, bien como consecuencia de operaciones intermedias propias de la aplicación que los trata, o bien como consecuencia de procesos periódicos de respaldo o cualquier otra operación esporádica, deberán estar claramente identificados con una etiqueta externa que indique de qué fichero se trata, que tipo de datos contiene, proceso que los ha originado y fecha de creación.

7.1.2 Aquellos medios que sean reutilizables, y que hayan contenido copias de datos del Fichero, deberán ser borrados físicamente antes de su reutilización, de forma que los datos que contenían no sean recuperables.

7.1.3 Los soportes que contengan datos del Fichero deberán ser almacenados en lugares a lo que no tengan acceso personas no autorizadas para el uso del Fichero que no estén por tanto relacionadas en el Anexo F.

7.1.5. Cuando la salida de datos del Fichero se realice por medio de correo electrónico los envíos se realizaran, siempre y únicamente, desde una dirección de correo controlada por el administrador de seguridad, dejando constancia de estos envíos en el directorio histórico de esa dirección de correo o en algún otro sistema de registro de salidas que permita conocer en cualquier momento los envios realizados, a quien iban dirigidos y la información enviada.

7.1.6. Cuando los datos del Fichero deban ser enviados fuera del recinto físicamente protegido donde se encuentra ubicado el Fichero, bien sea mediante un soporte físico de grabación de datos o bien sea mediante correo electrónico, deberán ser encriptados de forma que solo puedan ser leídos e interpretados por el destinatario.

7.1.8. Se deberán registrar mediante correo electrónico o transferencia de datos por red, de forma que se pueda siempre identificar su origen, tipo de datos , formato, fecha y hora del envío y destinatario de los mismos.

OBLIGACIONES DE LOS ADMINISTRADORES Y PERSONAL INFORMÁTICO

Entorno de sistema operativo y de Comunicaciones

5.3.3 Ninguna herramienta o programa de utilidad que permita el acceso al Fichero deberá ser accesible a ningún usuario o administrador no autorizado en el Anexo F.

5.3.4 En la norma anterior se incluye cualquier medio de acceso en bruto, es decir no elaborado o editado, a los datos del Fichero, como los llamados "queries", editores universales, analizadores de ficheros, etc., que deberán estar bajo el control de los administradores autorizados relacionados en el Anexo F.

5.3.5 El administrador deberá responsabilizarse de guardar en lugar protegido las copias de seguridad y respaldo del Fichero,de forma que ninguna persona no autorizada tenga acceso a las mismas.

5.3.6 Si la aplicación o sistema de acceso al Fichero utilizase usualmente ficheros temporales, ficheros de "logging", o cualquier otro medio en el que pudiesen ser grabados copias de los datos protegidos, el administrador deberá asegurarse de que esos datos no son accesibles posteriormente por personal no autorizado.

5.3.7 Si el ordenador en el que está ubicado el fichero está integrado en una red de comunicaciones de forma que desde otros ordenadores conectados a la misma sea posible el acceso al Fichero, el administrador responsable del sistema deberá asegurarse de que este acceso no se permite a personas no autorizadas.

Sistema Informático o aplicaciones de acceso al Fichero

5.4.3 Si la aplicación informática que permite el acceso al Fichero no cuenta con un control de acceso, deberá ser el sistema operativo, donde se ejecuta esa aplicación, el que impida el acceso no autorizado, mediante el control de los citados códigos de usuario y contraseñas.

5.4.4. En cualquier caso se controlarán los intentos de acceso fraudulento al Fichero, limitando el

número máximo de intentos fallidos, y, cuando sea técnicamente posible, guardando en un fichero auxiliar la fecha , hora, código y clave erróneas que se han introducido, así como otros datos relevantes que ayuden a descubrir la autoría de esos intentos de acceso fraudulentos.

5.4.5. Si durante las pruebas anteriores a la implantación o modificación de la aplicación de acceso al Fichero se utilizasen datos reales, se deberá aplicar a esos ficheros de prueba el mismo tratamiento de seguridad que se aplica al mismo Fichero, y se deberán relacionar esos ficheros de prueba en el Anexo B.

Salvaguarda y protección de las contraseñas personales

5.5.5 Las contraseñas se asignarán y se cambiarán mediante el mecanismo y periodicidad que se determina en el Anexo G. Este mecanismo de asignación y distribución de las contraseñas deberá garantizar la confidencialidad de las mismas, y será responsabilidad del administrador del sistema.

5.5.6 El archivo donde se almacenen las contraseñas deberá estar protegido y bajo la responsabilidad del administrador del sistema.

Procedimientos de respaldo y recuperación

8.1.1 Existirá una persona, bien sea el administrador o bien otro usuario expresamente designado, que será responsable de obtener periódicamente una copia de seguridad del fichero, a efectos de respaldo y posible recuperación en caso de fallo.

8.1.2 Estas copias deberán realizarse con una periodicidad, al menos, semanal, salvo en el caso de que no se haya producido ninguna actualización de los datos.

8.1.3 En caso de fallo del sistema con pérdida total o parcial de los datos del Fichero existirá un procedimiento, informático o manual, que partiendo de la última copia de respaldo y del registro de las operaciones realizadas desde el momento de la copia, reconstruya los datos del Fichero al estado en que se encontraban en el momento del fallo. Ese procedimiento está descrito en el Anexo G.

8.1.4 Será necesaria la autorización por escrito del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos, y deberá dejarse constancia en el registro de incidencias de las manipulaciones que hayan debido realizarse para dichas recuperaciones,
incluyendo la persona que realizó el proceso, los datos restaurados y los datos que hayan debido ser grabados manualmente en el proceso de recuperación.

Controles periódicos de verificación del cumplimiento

10.1.1. El responsable de seguridad del Fichero comprobará, con una periodicidad al menos trimestral, que la lista de usuarios autorizados del Anexo F se corresponde con la lista de los usuarios realmente autorizados en la aplicación de acceso al Fichero, para lo que recabará la lista de usuarios y sus códigos de acceso al administrador o administradores del Fichero. Ademas de estas comprobaciones periódicas, el administrador comunicará al responsable de seguridad, en cuanto se produzca, cualquier alta o baja de usuarios con acceso autorizado al Fichero.

10.1.2 Se comprobará también al menos con periodicidad trimestral, la existencia de copias de respaldo que permitan la recuperación de Fichero según lo estipulado en el apartado 8 de este documento.

10.1.3 A su vez, y también con periodicidad al menos trimestral, los administradores del Fichero comunicaran al responsable de seguridad cualquier cambio que se haya realizado en los datos técnicos de los anexos, como por ejemplo cambios en

el software o hardware, base de datos o aplicación de acceso al Fichero, procediendo igualmente a la actualización de dichos anexos.

10.1.4 El responsable de seguridad, verificará, con periodicidad al menos trimestral, el cumplimiento de lo previsto en los apartados 7 y 8 de este documento en relación con las entradas y salidas de datos, sean por red o en soporte magnético.

10.1.6 Al menos cada dos años, se realizará una auditoría, externa o interna que dictamine el correcto cumplimiento y la adecuación de las medidas del presente documento de seguridad o las exigencias del Reglamento de seguridad, identificando las deficiencias y proponiendo las media correctoras necesarias. Los informes de auditoría serán analizados por el responsable de seguridad, quien propondrá al responsable del Fichero las medidas correctoras correspondientes.

10.1.7 Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad sin que se deba permitir , en ningun caso la desactivación de los mismos.

10.1.8 El reponsable de seguridad se encargará de revisar periodicamente la información de control registrada,

10.1.9 Los resultados de todos estos controles periódicos, así como de las auditorías serán adjuntadas a este documento de seguridad en el Anexo J.

Anexo I. Procedimiento de Notificación y gestión de incidencias

Procedimiento de Notificación y gestión de incidencias

Se describirá el procedimiento de notificación y gestión de incidencias

<u>En la notificación se hará constar :</u>

- Tipo de incidencia
- Fecha y hora en que se produjo
- Persona que realiza la notificación
- Persona a quien se comunica
- Efectos que puede producir la incidencia
- Descripción detallada de la misma

<u>Si se trata de una recuperación de datos se incluirá además :</u>

- Autorización del responsable del fichero
- Procedimientos realizados
- Persona que realizó el proceso
- Datos restaurados
- Datos grabados manualmente

Se adjunta el impreso de notificación manual que podra ser utilizado para la notificación de incidencias

Cuando ocurra una incidencia, el usuario o administrador deberá registrarla en el Libro de Incidencias o comunicarla al Responsable de seguridad para que a su vez proceda a su registro.

Se mantendrán las incidencias registradas de los 12 últimos meses.

A continuación se adjunta el impreso de notificación manual que podrá ser utilizado para la notificación de incidencias.

Nº de inscripción	NOMBRE DE FICHERO

Impreso de notificación de incidencias

Incidencia N1: |_____| **(Este número será rellenado por el Responsable de seguridad)**	
Fecha de notificación: /__/__/_____/	
Tipo de incidencia:	
Descripción detallada de la incidencia:	
Fecha y hora en que se produjo la incidencia:	
Persona(s) a quien(es) se comunica:	
Efectos que puede producir: **(En caso de no subsanación o incluso independientemente de ella)**	

Nº de inscripción NOMBRE DE FICHERO

Recuperación de Datos :(A rellenar sólo si la incidencia es de este tipo)

Procedimiento realizado:

Datos restaurados:

Datos grabados manualmente:

Persona que ejecutó el proceso:

Firma del Responsable del fichero:

Fdo _____

Persona que realiza la comunicación:

Fdo.:_____

Nº de inscripción NOMBRE DE FICHERO

Anexo J. Controles periódicos y auditorías

Contendrá los resultados de los controles periódicos descritos en el apartado 10 y de las auditorías realizadas

a

Adaptación a la LOPD

A.1 INTRODUCCIÓN

En este apéndice 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.

A.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.

A.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.

A.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.

A.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.

A.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.

A.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.

A.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.

A.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.

A.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.

b

Posibles sanciones

B.1 INTRODUCCIÓN

La cuantía de las sanciones dependerá atendiendo a:

- La naturaleza de los derechos personales afectados.
- La cantidad de los afectados.
- Los beneficios obtenidos.
- Grado de intencionalidad.
- Reincidencia.
- Daños a terceras personas.
- Cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora.

Las sanciones dependiendo de su naturaleza podrán ser:

- **Leves**: de 601,01 € a 60.101,21 €.
- **Graves**: de 60.101,21 € a 300.506,05 €.
- **Muy graves**: de 300.506,05 € a 601.012,10 €.

En caso de utilización o cesión ilícita de datos que atenten contra los derechos fundamentales, el Director de la A.P.D. podría requerir a los responsables de los ficheros la cesación de la utilización o cesión ilícita de los datos. Si se desatendiese el requerimiento, se podrían inmovilizar los ficheros mediante una resolución motivada.

El director de la Agencia podrá proponer la iniciación de actuaciones disciplinarias, si procedieran cuando se trate de ficheros de los que sean responsables las Administraciones Públicas. El procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario de las Administraciones Públicas.

B.2 INFRACCIONES LEVES

Las infracciones leves prescriben al año y serán todas aquellas que:

- No atender, por motivos formales la solicitud del interesado de rectificación o cancelación de los datos personales objeto de tratamiento cuando legalmente proceda.

- No proporcionar la información que solicite la Agencia de Protección de Datos en el ejercicio de las competencias que tiene legalmente atribuidas, en relación con aspectos no sustantivos de la protección de datos.

- No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando no sea constitutivo de infracción grave.

- Proceder a la recogida de datos de carácter personal de los propios afectados, sin proporcionarles la información que señala el artículo 5 de la presente Ley.

- Incumplir el deber de secreto establecido en el artículo 10 de esta Ley, salvo que constituya infracción grave.

B.3 INFRACCIONES GRAVES

Por el contrario, las infracciones graves prescriben a los dos años y serán todas aquellas que:

- Proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general, publicada en el “Boletín Oficial del Estado” o diario oficial correspondiente.

- Proceder a la creación de ficheros de titularidad privada o iniciar la recogida de datos de carácter personal para los mismos con finalidades distintas de las que constituyen el objeto legítimo de la empresa o entidad.

- Proceder a la recogida de datos de carácter personal sin recabar el consentimiento expreso de las personas afectadas, en los casos en que éste sea exigible.

- Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la presente Ley o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción muy grave.

- El impedimento o la obstaculización del ejercicio de los derechos de acceso y oposición y la negativa a facilitar la información que sea solicitada.

- Mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de las personas que la presente Ley ampara.

- La vulneración del deber de guardar secreto sobre los datos de carácter personal incorporados a ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, prestación de servicios de solvencia patrimonial y crédito, así como aquellos otros ficheros que contengan un conjunto de

datos de carácter personal suficientes para obtener una evaluación de la personalidad del individuo.

- Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen.

- No remitir a la Agencia de Protección de Datos las notificaciones previstas en esta Ley o en sus disposiciones de desarrollo, así como no proporcionar en plazo a la misma cuantos documentos e informaciones deba recibir o sean requeridos por aquél a tales efectos.

- La obstrucción al ejercicio de la función inspectora.

- No inscribir el fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando haya sido requerido para ello por el Director de la Agencia de Protección de Datos.

- Incumplir el deber de información que se establece en los artículos 5, 28 y 29 de esta Ley, cuando los datos hayan sido recabados de persona distinta del afectado.

B.4 INFRACCIONES MUY GRAVES

Por último, las infracciones muy graves prescriben a los tres años serán todas aquellas que:

- La recogida de datos en forma engañosa y fraudulenta.

- La comunicación o cesión de los datos de carácter personal, fuera de los casos en que estén permitidas.

- Recabar y tratar los datos de carácter personal a los que se refiere el apartado 2 del artículo 7 cuando no medie el consentimiento expreso del afectado; recabar y tratar los datos referidos en el apartado 3 del artículo 7 cuando no lo disponga una Ley o el afectado no haya consentido expresamente, o violentar la prohibición contenida en el apartado 4 del artículo 7.

- No cesar en el uso ilegítimo de los tratamientos de datos de carácter personal cuando sea requerido para ello por el Director de la Agencia de Protección de Datos o por las personas titulares del derecho de acceso.

- La transferencia temporal o definitiva de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento, con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia de Protección de Datos.

- Tratar los datos de carácter personal de forma ilegítima o con menosprecio de los principios y garantías que les sean de aplicación, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales. La vulneración del deber de guardar secreto sobre los datos de carácter personal a que hacen referencia los apartados 2 y 3 del artículo 7, así como los que hayan sido recabados para fines policiales sin consentimiento de las personas afectadas.

- No atender u obstaculizar de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación u oposición.

- No atender de forma sistemática el deber legal de notificación de la inclusión de datos de carácter personal en un fichero.

C

FAQ

1 INTRODUCCIÓN

En este apéndice veremos algunas de las preguntas que se nos formulan cada vez que damos seminarios, cursos, talleres sobre la implantación de la LOPD. Algunas de ellas ya han sido respondidas por la Agencia de Protección de Datos, por lo que las respuestas serán las mismas, pero otras aun las han resuelto. Por tanto, algunas de las preguntas con sus respuestas podrán ser vistas en la página web de la Agencia.

2 ¿CUÁNDO SE DEBE DE PROCEDER A DECLARAR UN FICHERO DE DATOS?

El articulo 2.1 de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal establece que:

" 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."

Por datos de carácter personal hay que entender de acuerdo con la definición contenida en el artículo 3 a) de la LOPD, "cualquier información concerniente a personas físicas identificadas o indentificables".

El articulo 25 de la LOPD permite que cuando resulte necesario para el logro de la actividad de la persona, o empresa en cuestión, se podrán crear ficheros que contengan datos de carácter personal, y será necesario de conformidad con el articulo 26 la declaración de los mismos ante el Registro General de Protección de Datos de esta Agencia, quedando sometidos a la regulación contenida en la referida Ley orgánica y demás normas de desarrollo.

3 ¿CÓMO SE DEBE DECLARAR UN FICHERO O TRATAMIENTO DE DATOS? *¿SE PUEDE REALIZAR A TRAVÉS DE INTERNET?*

En primer lugar se indica que el criterio determinante para proceder a la inscripción de un fichero es el tratamiento de los datos relativos a personas físicas; por lo que si

tienen cualquier fichero que contenga datos de esta clase deberán proceder a su declaración ante el Registro General de Protección de Datos de la Agencia.

Para proceder a la declaración se deberá de utilizar necesariamente el formulario aprobado y publicado en el BOE num. 153 de 27 de junio de 2000, en la parte correspondiente a ficheros de titularidad privada.

Se le indica que la declaración la 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 nuestra página Web 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 las páginas 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, 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 91 4483680 o bien, a través del correo ordinario.

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

Por lo tanto, será indiferente a los efectos de inscripción en el Registro General de Protección de Datos, los ficheros (en terminología técnica) o tablas que incluyan los diseños informáticos de los sistemas de información. Se tendrá que notificar por cada declaración de ficheros la información que corresponda con el conjunto de datos

asociados a un tratamiento o uso de los mismos, con una finalidad o finalidades compatibles y determinadas.

Finalmente se informa que de conformidad con el Reglamento aprobado por Real Decreto 994/1999, de 11 de junio (BOE 25-6-1999) deberán de adoptar en sus ficheros el nivel de seguridad básico medio o alto en función del tipo de datos que manejen (art. 4) y redactar el documento de seguridad regulado en el articulo 8 del referido Reglamento no teniendo la obligación de presentarlo en la Agencia, sino tan sólo tenerlo disponible por si les fuera requerido. Al propio tiempo se le informa que la Agencia no ha elaborado ningún modelo de este documento de seguridad.

Toda la normativa en materia de protección de datos se encuentra disponible en nuestra página Web dentro del apartado legislación.

4 ¿SE DEBE DE DECLARAR ANTE LA AGENCIA DE PROTECCIÓN DE DATOS EL DOCUMENTO DE SEGURIDAD DE LOS FICHEROS AUTOMATIZADOS DE DATOS DE CARÁCTER PERSONAL?

Se informa que, de conformidad con el Reglamento aprobado por Real Decreto 994/1999, de 11 de junio (BOE 25-6-1999), deberán de adoptar en sus ficheros el nivel de seguridad básico medio o alto en función del tipo de datos que manejen (art. 4) y redactar el documento de seguridad regulado en el articulo 8 del referido Reglamento no teniendo la obligación de presentarlo en la Agencia, sino tan sólo tenerlo disponible por si les fuera requerido. Al propio tiempo se le informa que la Agencia no ha elaborado ningún modelo de este documento de seguridad.

5 ¿EN EL FICHERO DE NÓMINAS DE LOS EMPLEADOS DE MI EMPRESA, QUE TIPO DE MEDIDAS DE SEGURIDAD DEBO DE ADOPTAR?

Se informa que, para establecer el nivel de protección que tienen que tener los ficheros de nóminas, habrá que acudir a lo establecido en el artículo 4 del Reglamento de Medidas de Seguridad en donde se regula los niveles de seguridad. Este Precepto señala que, como norma general, todos los ficheros que contengan datos de carácter personal

deberán adoptar las medidas de seguridad calificadas como de nivel básico, añadiendo en su punto 3 que, cuando los ficheros contengan datos de ideología, religión, creencias, origen racial, salud o vida sexual….. de las personas afectadas deberán reunir, además de las medidas de nivel básico y medio, las calificadas como de nivel alto.

En consecuencia y a la vista de la normativa anterior si en un fichero de nóminas no se contienen datos que hagan referencia a datos especialmente protegidos se aplicarán las medidas de nivel básico, pero si se contemplan datos de salud, como podría ser el caso de reflejar minusvalías a los efectos de la declaración de la renta, o datos de ideología sindical cuando se aplica el descuento de la cuota sindical, se le aplicarán las medidas de nivel alto.

6 ¿HE TENIDO CONOCIMIENTO DE QUE EL TRIBUNAL CONSTITUCIONAL HA DICTADO UNA SENTENCIA POR LA QUE SE DECLARAN CONTRARIOS A LA CONSTITUCIÓN ALGUNOS PRECEPTOS DE LA LEY ORGÁNICA 15/1999 DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL. ME PODRÍAN INDICAR QUE IMPLICACIONES TIENE ESTA SENTENCIA?

En primer lugar se informa que, efectivamente el Tribunal Constitucional con fecha 30/11/2000 ha procedido a dictar sentencia en el recurso de inconstitucionalidad 1563-2000, interpuesto por el Defensor del Pueblo contra los artículos 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal, habiéndose publicado en el Boletín Oficial del Estado de fecha 4/01/2001.

Una de las cuestiones mas importantes a destacar de la referida sentencia, es que el T.C. establece el derecho a la protección de datos como derecho fundamental autónomo, configurando su contenido con los principios y derechos que se contemplan en la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal, y en virtud del cual, el ciudadano, con carácter general, puede decidir sobre sus propios datos.

Al ciudadano se le ha de informar para qué finalidad se obtienen los datos y así consentir sobre la entrega de los mismos para finalidades explícitas.

El ciudadano tendrá derecho, no obstante, de acceder a los datos que tanto empresas, particulares, como Administraciones tengan recabados del mismo y poder rectificarlos y cancelarlos.

El T.C. ha estimado el recurso de inconstitucionalidad y procede a declarar contrario a la Constitución y nulo el inciso "cuando la comunicación hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso" del apartado 1ºdel artículo 21 de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal.

Igualmente declara 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 artículo 24, y todo su apartado 2, de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal.

Las consecuencias que dicha sentencia tiene son:

- De un lado y respecto de la cesión de datos, independientemente de la regulación general contenida en el artículo 11 de la LOPD que evidentemente le es y le era de aplicación a las Administraciones Publicas con anterioridad a la sentencia, la regulación especifica contenida en el artículo 21.1 restringe la posibilidad de cesión de datos entre las Administraciones Publicas, al ejercicio de la mismas competencias o al tratamiento posterior con fines históricos, estadísticos o científicos. Es por ello, que fuera de las excepciones contempladas con carácter general en los artículos 11.2 LOPD y con carácter especifico en el artículo 21.1 y 2 LOPD, será siempre necesario el consentimiento de las personas afectadas por los datos, para que las Administraciones Públicas se los puedan ceder entre si, salvo que expresamente lo excepcione una norma con rango de ley.

- Por otro lado y con la declaración de inconstitucionalidad de los incisos del apartado 1 del artículo 24, lo que se desprende es, que el derecho de información al ciudadano reconocido en el artículo 5.1 y 2 LOPD

únicamente podrá ser excepcionado por las Administraciones Públicas, cuando dicha información pueda afectar, a la Defensa Nacional, a la seguridad publica, o a la persecución de una infracción de tipo penal.

- Se suprime igualmente todo el apartado 2 del artículo 24, por lo que las únicas excepciones especificas que la Administraciones Publicas podrán alegar para el ejercicio de los derechos de acceso, rectificación y cancelación por lo ciudadanos, serán las reguladas en el artículo 23 LOPD.

7 ¿QUIÉN ES EL ENCARGADO DEL TRATAMIENTO, CUANDO NO HAY CESIÓN DE LOS DATOS A UN TERCERO PARA NINGÚN TIPO DE FINALIDAD? ¿PUEDE SER LA MISMA PERSONA JURÍDICA RESPONSABLE DEL FICHERO?

Cuando no hay acceso a los datos por cuenta de ningún tercero, no existe ningún encargado del tratamiento. En este caso es el propio responsable del fichero el que efectúa directamente dicho tratamiento.

8 SI LOS DATOS QUE SE INCLUYEN EN LAS LIBRETAS DE DIRECCIONES PERSONALES DE MS OUTLOOK SE CORRESPONDEN CON DATOS DE LAS PERSONAS DE LAS EMPRESAS QUE TIENES ALGUNA ACTIVIDAD CONTRACTUAL, TENEMOS QUE DECLARAR ESTE TIPO DE FICHERO?

Por supuesto que sí. El hecho de tener dichos datos sólo exime de la obligación de obtener el consentimiento de dichas personas para tratar sus datos pero no exime de la obligación de inscribir dicho fichero en la Agencia de Protección de Datos ni de cumplir con el resto de las obligaciones contempladas en la LOPD y en el Reglamento de Medidas de Seguridad.

9 SE DEBE DE PONER EN LOS CORREOS ALGUNA APARTE (POR DEFECTO COMO FIRMA) INDICANDO QUE SI EL DESTINATARIO NO QUIERE RECIBIR CORREOS NOS LO HAGA SABER Y ALGO QUE

HAGA REFERENCIA A LA RESPONSABILIDAD DE LA EMPRESA POR EL CONTENIDO DEL CORREO.

En base a la LOPD, cuando se realiza la primera comunicación por correo electrónico con una persona que no hemos contactado anteriormente y de la cual no hemos obtenido su consentimiento para tratar sus datos, es necesario comunicarle quienes somos, donde estamos, cómo hemos obtenido sus datos, en qué fichero los hemos incluido, con qué finalidad e informarle de la posibilidad de que se oponga a su tratamiento así como de ejercer sus derechos de acceso, rectificación y cancelación sobre los mismos.

En cuanto a la cláusula de responsabilidad por el contenido del correo, no es algo exigido por la LOPD pero es una práctica cada vez más extendida y recomendable en algunos casos aunque, repito, no se exige.

10 ¿UN FICHERO CON DATOS PERSONALES QUE CONTENGA ENTRE OTROS FECHA DE BAJA(ENFERMEDAD / ACCIDENTE) Y FECHA DE ALTA SE PUEDE CONSIDERAR DE NIVEL ALTO?

Entendemos que un fichero que contenga tales datos debe cumplir con el nivel alto de seguridad ya que, son indicativos de que, entre dichas fechas, una persona ha estado enferma o afectada por un accidente y, por tanto, que no ha estado sana durante dicho período lo cual, aunque genérico, es un dato sobre su salud.

11 ME GUSTARÍA DISPONER DE UN GUIÓN / ÍNDICE DE LOS PASOS A SEGUIR PARA PODER EMPEZAR A CUMPLIR LA LEY DENTRO DE NUESTRA ORGANIZACIÓN (SABER POR DONDE EMPEZAR, EL CAMINO A SEGUIR....)

Los pasos fundamentales a seguir, de modo general y sin ánimo de ser exhaustivos, son los siguientes:

1º- Detectar los posibles ficheros con datos personales de la empresa que entren en dicho concepto con arreglo a la LOPD. Delimitar en cada caso sus

finalidades, estructura, usos, tratamientos y personal con acceso a los mismos y la legalidad de todos estos elementos.

2º- Comprobar si dichos ficheros están inscritos correctamente en la Agencia de Protección de Datos y, en caso negativo, realizar dicha inscripción.

3º- Comprobar si hemos recabado el consentimiento de los titulares de los datos o entran en alguna excepción legal que exima de ello.

4º- Comprobar si hemos informado correctamente en su recogida o en la primera comunicación a sus titulares.

5º- Ver si se han comunicado o cedido a terceras personas o se prevé hacerlo en el futuro. En el caso de que exista un encargado del tratamiento, elaborar un contrato con arreglo a l artículo 12 LOPD.

6º- Eliminar datos erróneos, excesivos u obsoletos.

7º- Arbitrar mecanismos para permitir el ejercicio de los derechos de acceso, rectificación y cancelación de los titulares de los datos.

8º- En función del tipo de datos, determinar su nivel de Seguridad exigible con arreglo al artículo 4 del Real decreto 994/1999 y las medidas concretas a implementar.

9º- Redactar un Documento de Seguridad y el resto de la documentación, modelos y registros exigibles y, a partir del nivel medio de seguridad, elaborar o encargar un Informe de Auditoría.

10º- Implementar las medidas de seguridad técnicas y organizativas contempladas en el Reglamento y desarrolladas específicamente en el Documento de Seguridad así como formar a nuestro personal en su cumplimiento.

12 ¿CUANTO TIEMPO HAY QUE DEJAR LAS COPIAS DE SEGURIDAD DE LOS LOGS DE LAS MÁQUINAS?

En base al artículo 24.4 del Reglamento (Nivel Alto) el plazo mínimo de conservación del registro de accesos es de 2 años.

13 ¿COMO DEBERÁN SER O QUE CARACTERÍSTICA DEBERÁN TENER ESAS COPIAS DE LOS LOGS PARA QUE SEAN VALIDAS JUDICIALMENTE?, HAY QUE TENER EN CUENTA QUE ESTOS DATOS PUEDEN ESTAR SUJETOS A MODIFICACIONES HORARIAS, ETC.

De cualquier forma, aquí también entra en juego el tema de la autenficación NTP, es decir, que la hora de los servidores sea obtenida correctamente de los servidores de NTP (hora), sin que nadie pueda alterar esta información, lo cual por las características del protocolo NTP se puede lograr hacer.

Respecto al NTP, es un tema importante pero no necesario a efectos de la Protección de Datos (aunque sí para el tema de prueba en juicio)

d

Real Decreto 994

Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad de la LORTAD

El artículo 18.4 de la Constitución Española establece 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».

La Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos de carácter personal, prevé en su artículo 9, la obligación del responsable del fichero de adoptar las medidas de índole técnica y organizativas 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 estén expuestos, ya provengan de la acción humana o del medio físico o natural, estableciéndose en el artículo 43.3.h) que mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen constituye infracción grave en los términos previstos en la propia Ley.

Sin embargo, la falta de desarrollo reglamentario ha impedido disponer de un marco de referencia para que los responsables promovieran las adecuadas medidas de seguridad y, en consecuencia, ha determinado la imposibilidad de hacer cumplir uno de los más importantes principios de la Ley Orgánica.

El presente Reglamento tiene por objeto el desarrollo de lo dispuesto en los artículos 9 y 43.3.h) de la Ley Orgánica 5/1992. El Reglamento determina las medidas de índole técnica y organizativa que garanticen la confidencialidad e integridad de la información con la finalidad de preservar el honor, la intimidad personal y familiar y el pleno ejercicio de los derechos personales frente a su alteración, pérdida, tratamiento o acceso no autorizado.

Las medidas de seguridad que se establecen se configuran como las básicas de seguridad que han de cumplir todos los ficheros que contengan datos de carácter personal, sin perjuicio de establecer medidas especiales para aquellos ficheros que por la especial naturaleza de los datos que contienen o por las propias características de los mismos exigen un grado de protección mayor.

En su virtud, a propuesta de la Ministra de Justicia, de acuerdo con el Consejo de Estado, y previa deliberación del Consejo de Ministros en su reunión del día 11 de junio de 1999, DISPONGO:

Artículo único. Aprobación del Reglamento.
Se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, cuyo texto se inserta a continuación.
Disposición final única. Entrada en vigor.
El presente Real Decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

Dado en Madrid a 11 de junio de 1999.
JUAN CARLOS R.
La Ministra de Justicia,
MARGARITA MARISCAL DE GANTE Y MIRÓN

REGLAMENTO DE MEDIDAS DE SEGURIDAD DE LOS FICHEROS AUTOMATIZADOS QUE CONTENGAN DATOS DE CARÁCTER PERSONAL

CAPÍTULO I

Disposiciones generales

Artículo 1. Ámbito de aplicación y fines.
El presente Reglamento tiene por objeto establecer las medidas de índole técnica y organizativas necesarias para garantizar la seguridad que deben reunir los ficheros automatizados, los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento automatizado de los datos de carácter personal sujetos al régimen de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal.

Artículo 2. Definiciones.

A efectos de este Reglamento, se entenderá por:

1. Sistemas de información: conjunto de ficheros automatizados, programas, soportes y equipos empleados para el almacenamiento y tratamiento de datos de carácter personal.

2. Usuario: sujeto o proceso autorizado para acceder a datos o recursos.

3. Recurso: cualquier parte componente de un sistema de información.

4. Accesos autorizados: autorizaciones concedidas a un usuario para la utilización de los diversos recursos.

5. Identificación: procedimiento de reconocimiento de la identidad de un usuario.

6. Autenticación: procedimiento de comprobación de la identidad de un usuario.

7. Control de acceso: mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.

8. Contraseña: información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario.

9. Incidencia: cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.

10. Soporte: objeto físico susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar o recuperar datos.

11. Responsable de seguridad: persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.

12. Copia del respaldo: copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.

Artículo 3. Niveles de seguridad.

1. Las medidas de seguridad exigibles se clasifican en tres niveles: básico, medio y alto.

2. Dichos niveles se establecen atendiendo a la naturaleza de la información tratada, en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información.

Artículo 4. Aplicación de los niveles de seguridad.

1. Todos los ficheros que contengan datos de carácter personal deberán adoptar las medidas de seguridad calificadas como de nivel básico.

2. Los ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros y aquellos ficheros

cuyo funcionamiento se rija por el artículo 28 de la Ley Orgánica 5/1992, deberán reunir, además de las medidas de nivel básico, las calificadas como de nivel medio.
3. Los ficheros que contengan 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 deberán reunir, además de las medidas de nivel básico y medio, las calificadas de nivel alto.
4. Cuando los ficheros contengan un conjunto de datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo deberán garantizar las medidas de nivel medio establecidas en los artículos 17, 18, 19 y 20.
5. Cada uno de los niveles descritos anteriormente tienen la condición de mínimos exigibles, sin perjuicio de las disposiciones legales o reglamentarias específicas vigentes.

Artículo 5. Acceso a datos a través de redes de comunicaciones.
Las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local.

Artículo 6. Régimen de trabajo fuera de los locales de la ubicación del fichero.
La ejecución de tratamiento de datos de carácter personal fuera de los locales de la ubicación del fichero deberá ser autorizada expresamente por el responsable del fichero y, en todo caso, deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.

Artículo 7. Ficheros temporales.
1. Los ficheros temporales deberán cumplir el nivel de seguridad que les corresponda con arreglo a los criterios establecidos en el presente Reglamento.
2. Todo fichero temporal será borrado una vez que haya dejado de ser necesario para los fines que motivaron su creación.

CAPÍTULO II

Medidas de seguridad de nivel básico

Artículo 8. Documento de seguridad.

1. El responsable del fichero elaborará e implantará la normativa de seguridad mediante un documento de obligado cumplimiento para el personal con acceso a los datos automatizados de carácter personal y a los sistemas de información.
2. El documento deberá contener, como mínimo, los siguientes aspectos:
a) Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.
b) Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este Reglamento.
c) Funciones y obligaciones del personal.
d) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.
e) Procedimiento de notificación, gestión y respuesta ante las incidencias.
f) Los procedimientos de realización de copias de respaldo y de recuperación de los datos.
3. El documento deberá mantenerse en todo momento actualizado y deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo.
4. El contenido del documento deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

Artículo 9. Funciones y obligaciones del personal.
1. Las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas, de acuerdo con lo previsto en el artículo 8.2.c).
2. El responsable del fichero adoptará las medidas necesarias para que el personal conozca las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

Artículo 10. Registro de incidencias.
El procedimiento de notificación y gestión de incidencias contendrá necesariamente un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, la persona que realiza la notificación, a quién se le comunica y los efectos que se hubieran derivado de la misma.

Artículo 11. Identificación y autenticación.

1. El responsable del fichero se encargará de que exista una relación actualizada de usuarios que tengan acceso autorizado al sistema de información y de establecer procedimientos de identificación y autenticación para dicho acceso.

2. Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.

3. Las contraseñas se cambiarán con la periodicidad que se determine en el documento de seguridad y mientras estén vigentes se almacenarán de forma ininteligible.

Artículo 12. Control de acceso.

1. Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.

2. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a datos o recursos con derechos distintos de los autorizados.

3. La relación de usuarios a la que se refiere el artículo 11.1 de este Reglamento contendrá el acceso autorizado para cada uno de ellos.

4. Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los datos y recursos, conforme a los criterios establecidos por el responsable del fichero.

Artículo 13. Gestión de soportes.

1. Los soportes informáticos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y almacenarse en un lugar con acceso restringido al personal autorizado para ello en el documento de seguridad.

2. La salida de soportes informáticos que contengan datos de carácter personal, fuera de los locales en los que esté ubicado el fichero, únicamente podrá ser autorizada por el responsable del fichero.

Artículo 14. Copias de respaldo y recuperación.

1. El responsable de fichero se encargará de verificar la definición y correcta aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

2. Los procedimientos establecidos para la realización de copias de respaldo y para la recuperación de los datos deberá garantizar su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.
3. Deberán realizarse copias de respaldo, al menos semanalmente, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.

CAPÍTULO III

Medidas de seguridad de nivel medio

Artículo 15. Documento de seguridad.
El documento de seguridad deberá contener, además de lo dispuesto en el artículo 8 del presente Reglamento, la identificación del responsable o responsables de seguridad, los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento y las medidas que sea necesario adoptar cuando un soporte vaya a ser desechado o reutilizado.

Artículo 16. Responsable de seguridad.
El responsable del fichero designará uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el documento de seguridad. En ningún caso esta designación supone una delegación de la responsabilidad que corresponde al responsable del fichero de acuerdo con este Reglamento.

Artículo 17. Auditoría.
1. Los sistemas de información e instalaciones de tratamiento de datos se someterán a una auditoría interna o externa, que verifique el cumplimiento del presente Reglamento, de los procedimientos e instrucciones vigentes en materia de seguridad de datos, al menos, cada dos años.
2. El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles al presente Reglamento, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias.
Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas.

3. Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia de Protección de Datos.

Artículo 18. Identificación y autenticación.

1. El responsable del fichero establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.

2. Se limitará la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

Artículo 19. Control de acceso físico.

Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los locales donde se encuentren ubicados los sistemas de información con datos de carácter personal.

Artículo 20. Gestión de soportes.

1. Deberá establecerse un sistema de registro de entrada de soportes informáticos que permita, directa o indirectamente, conocer el tipo de soporte, la fecha y hora, el emisor, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.

2. Igualmente, se dispondrá de un sistema de registro de salida de soportes informáticos que permita, directa o indirectamente, conocer el tipo de soporte, la fecha y hora, el destinatario, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada.

3. Cuando un soporte vaya a ser desechado o reutilizado, se adoptarán las medidas necesarias para impedir cualquier recuperación posterior de la información almacenada en él, previamente a que se proceda a su baja en el inventario.

4. Cuando los soportes vayan a salir fuera de los locales en que se encuentren ubicados los ficheros como consecuencia de operaciones de mantenimiento, se adoptarán las medidas necesarias para impedir cualquier recuperación indebida de la información almacenada en ellos.

Artículo 21. Registro de incidencias.

1. En el registro regulado en el artículo 10 deberán consignarse, además, los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.

2. Será necesaria la autorización por escrito del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos.

Artículo 22. Pruebas con datos reales.

Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tipo de fichero tratado.

CAPÍTULO IV

Medidas de seguridad de nivel alto

Artículo 23. Distribución de soportes.

La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su transporte.

Artículo 24. Registro de accesos.

1. De cada acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.

2. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.

3. Los mecanismos que permiten el registro de los datos detallados en los párrafos anteriores estarán bajo el control directo del responsable de seguridad competente sin que se deba permitir, en ningún caso, la desactivación de los mismos.

4. El período mínimo de conservación de los datos registrados será de dos años.

5. El responsable de seguridad competente se encargará de revisar periódicamente la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados al menos una vez al mes.

Artículo 25. Copias de respaldo y recuperación.
Deberá conservarse una copia de respaldo y de los procedimientos de recuperación de los datos en un lugar diferente de aquél en que se encuentren los equipos informáticos que los tratan cumpliendo en todo caso, las medidas de seguridad exigidas en este Reglamento.

Artículo 26. Telecomunicaciones.
La transmisión de datos de carácter personal a través de redes de telecomunicaciones se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

CAPÍTULO V

Infracciones y sanciones

Artículo 27. Infracciones y sanciones.
1. El incumplimiento de las medidas de seguridad descritas en el presente Reglamento será sancionado de acuerdo con lo establecido en los artículos 43 y 44 de la Ley Orgánica 5/1992, cuando se trate de ficheros de titularidad privada.
El procedimiento a seguir para la imposición de la sanción a la que se refiere el párrafo anterior será el establecido en el Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal.
2. Cuando se trate de ficheros de los que sean responsables las Administraciones públicas se estará, en cuanto al procedimiento y a las sanciones, a lo dispuesto en el artículo 45 de la Ley Orgánica 5/1992.

Artículo 28. Responsables.
Los responsables de los ficheros, sujetos al régimen sancionador de la Ley Orgánica 5/1992, deberán adoptar las medidas de índole técnica y organizativas necesarias que

garanticen la seguridad de los datos de carácter personal en los términos establecidos en el presente Reglamento.

CAPÍTULO VI

Competencias del Director de la Agencia de Protección de Datos

Artículo 29. Competencias del Director de la Agencia de Protección de Datos.

El Director de la Agencia de Protección de Datos podrá, de conformidad con lo establecido en el artículo 36 de la Ley Orgánica 5/1992:

1. Dictar, en su caso y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos automatizados a los principios de la Ley Orgánica 5/1992.

2. Ordenar la cesación de los tratamientos de datos de carácter personal y la cancelación de los ficheros cuando no se cumplan las medidas de seguridad previstas en el presente Reglamento.

Disposición transitoria única. Plazos de implantación de las medidas.

En el caso de sistemas de información que se encuentren en funcionamiento a la entrada en vigor del presente Reglamento, las medidas de seguridad de nivel básico previstas en el presente Reglamento deberán implantarse en el plazo de seis meses desde su entrada en vigor, las de nivel medio en el plazo de un año y las de nivel alto en el plazo de dos años.

Cuando los sistemas de información que se encuentren en funcionamiento no permitan tecnológicamente la implantación de alguna de las medidas de seguridad previstas en el presente Reglamento, la adecuación de dichos sistemas y la implantación de las medidas de seguridad deberán realizarse en el plazo máximo de tres años a contar desde la entrada en vigor del presente Reglamento.

e

LOPD

LEY ORGÁNICA 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal

JUAN CARLOS I

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente Ley Orgánica.

TÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

Artículo *2. Ámbito de aplicación.*

1. 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.

Se regirá por la presente Ley Orgánica todo tratamiento de datos de carácter personal:

a) Cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento.

b) Cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española en aplicación de normas de Derecho Internacional público.

c) Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito.

2. El régimen de protección de los datos de carácter personal que se establece en la presente Ley Orgánica no será de aplicación:

a) A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.

b) A los ficheros sometidos a la normativa sobre protección de materias clasificadas.

c) 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.

3. Se regirán por sus disposiciones específicas, y por lo especialmente previsto, en su caso, por esta Ley Orgánica los siguientes tratamientos de datos personales:

a) Los ficheros regulados por la legislación de régimen electoral.

b) Los que sirvan a fines exclusivamente estadísticos, y estén amparados por la legislación estatal o autonómica sobre la función estadística pública.

c) Los que tengan por objeto el almacenamiento de los datos contenidos en los informes personales de calificación a que se refiere la legislación del régimen del personal de las Fuerzas Armadas.

d) Los derivados del Registro Civil y del Registro Central de penados y rebeldes.

e) Los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por lasFuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia.

Artículo 3. Definiciones.

A los efectos de la presente Ley Orgánica se entenderá por:

a) Datos de carácter personal: cualquier información concerniente a personas físicas identificadas o identificables.

b) Fichero: todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

c) Tratamiento de datos: 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,

d) Responsable del fichero o tratamiento: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.

e) Afectado o interesado: persona física titular de los datos que sean objeto del tratamiento a que se refiere el apartado c) del presente artículo.

f) Procedimiento de disociación: todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.

g) Encargado del tratamiento: 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.

h) Consentimiento del interesado: toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.

i) Cesión o comunicación de datos: toda revelación de datos realizada a una persona distinta del interesado.

j) Fuentes accesibles al público: aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación.

TÍTULO II

Principios de la protección de datos

Artículo 4. Calidad de los datos.

1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.

3. Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado.

4. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que a los afectados reconoce el artículo 16.

5. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados.

Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos.

6. Los datos de carácter personal serán almacenados de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados.

7. Se prohibe la recogida de datos por medios fraudulentos, desleales o ilícitos.

Artículo 5. Derecho de información en la recogida de datos.

1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.

b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de trámite, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.

2. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior.

3. No será necesaria la información a que se refieren las letras b), c) y d) del apartado 1 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.

4. Cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras a), d) y e) del apartado 1 del presente artículo.

5. No será de aplicación lo dispuesto en el apartado anterior, cuando expresamente una ley lo prevea, cuando el tratamiento tenga fines históricos, estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia de Protección de Datos o del organismo

autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias.

Asimismo, tampoco regirá lo dispuesto en el apartado anterior cuando los datos procedan de fuentes accesibles al público y, se destinen a la actividad de publicidad o prospección comercial, en cuyo caso, en cada comunicación que se dirija al interesado se le informará del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten.

Artículo 6. Consentimiento del afectado.

1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa.
2. No será preciso el consentimiento 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; 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; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o 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.

3. El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos.

4. En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado.

Artículo 7. Datos especialmente protegidos.

1. De acuerdo con lo establecido do en el apartado 2 del artículo 16 de la Constitución, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias.

Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo.

2. Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical: en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado.

3. Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente.

4. Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual.

5. Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras.

6. No obstante lo dispuesto en los apartados anteriores, podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos' se realice por un profesional

sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.

También podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.

Artículo 8. Datos relativos a la salud.

Sin perjuicio de lo que se dispone en el artículo 11 respecto de la cesión, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad.

Artículo 9. Seguridad de los datos.

1. 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 0 del medio físico o natural.

2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por. vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley.

Artículo 10. Deber de secreto.

El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

Artículo 11. Comunicación de datos.

1. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.

2. El consentimiento exigido en el apartado anterior no será preciso:

a) Cuando la cesión está autorizada en una ley.

b) Cuando se trate de datos recogidos de fuentes accesibles al público.

c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.

d) Cuando la comunicación que deba efectuarse tenga por, destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.

e) Cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios

epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

3. Será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero, cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretenden comunicar.

4. El consentimiento para la comunicación de los datos de carácter personal tiene también un carácter de revocable.

5. Aquel a quien se comuniquen los datos de carácter personal se obliga, por el solo hecho de la comunicación, a la observancia de las disposiciones de la presente Ley.

6. Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores.

Artículo 12. Acceso a los datos por cuenta de terceros.

1. No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento,

2. La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar.

3. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

4. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

TÍTULO III

Derechos de las personas

Artículo 13. Impugnación de valoraciones.

1. Los ciudadanos tienen derecho a no verse sometidos a una decisión con efectos jurídicos, sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad.

2. El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad.

3. En este caso, el afectado tendrá derecho a obtener información del responsable del fichero sobre los criterios de valoración y el programa utilizados en el tratamiento que sirvió para adoptar la decisión en que consistió el acto.

4. La valoración sobre el comportamiento de los ciudadanos, basada en un tratamiento de datos, únicamente podrá tener valor probatorio a petición del afectado.

Artículo 14. Derecho de consulta al Registro General de Protección de Datos.

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. El Registro General será de consulta pública y gratuita.

Artículo 15. Derecho de acceso.

1. El interesado tendrá derecho a 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.

2. La información podrá obtenerse mediante la mera consulta de los datos por medio de su visualización, o la indicación de los datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos.

3. El derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrán ejercitarlo antes.

Artículo 16. Derecho de rectificación y cancelación.

1. El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días.

2. Serán rectificados o cancelados, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la presente Ley y, en particular, cuando tales datos resulten inexactos o incompletos.

3. La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión.

4. Si los datos rectificados o cancelados hubieran sido comunicados previamente, el responsable del tratamiento deberá notificar la rectificación o cancelación efectuada a

quien se hayan comunicado, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la cancelación.

5. 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.

Artículo 17. Procedimiento de oposición, acceso, rectificación o cancelación.

1. Los procedimientos para ejercitar el derecho de oposición, acceso, así como los de rectificación y cancelación serán establecidos reglamentariamente.

2. No se exigirá contra prestación alguna por el ejercicio de los derechos de oposición, acceso, rectificación o cancelación.

Artículo 18. Tutela de los derechos.

1. Las actuaciones contrarias a lo dispuesto en la presente Ley pueden ser objeto de reclamación por los interesados ante la Agencia de Protección de Datos, en la forma que reglamentariamente se determine.

2. El interesado al que se deniegue, total o parcialmente, el ejercicio de los derechos de oposición, acceso, rectificación o cancelación, podrá ponerlo en conocimiento de la Agencia de Protección de Datos o, en su caso, del organismo competente de cada Comunidad Autónoma, que deberá asegurarse de la procedencia o improcedencia de la denegación.

3. El plazo máximo en que debe dictarse la resolución expresa de tutela de derechos será de seis meses.

4. Contra las resoluciones de la Agencia de Protección de Datos procederá recurso contencioso-administrativo.

Artículo 19. Derecho a indemnización.

1. Los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados.

2. Cuando se trate de ficheros de titularidad pública, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones públicas.

3. En el caso de los ficheros de titularidad privada, la acción se ejercitará ante los órganos de la jurisdicción ordinaria.

TÍTULO IV

Disposiciones sectoriales

CAPÍTULO I

Ficheros de titularidad pública

Artículo 20. Creación, modificación o supresión.

1. La creación, modificación o supresión de los ficheros de las Administraciones públicas sólo podrán hacerse por medio de disposición general publicada en el «Boletín Oficial del Estado» o Diario oficial correspondiente.

2. Las disposiciones de creación o de modificación de ficheros deberán indicar:

a) La finalidad del fichero y los usos previstos para el mismo.

b) Las personas o colectivos sobré los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.

c) El procedimiento de recogida de los datos de carácter personal.

d) La estructura básica del fichero y la descripción de los tipos de datos de carácter personal incluidos en el mismo.

e) Las cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a países terceros.

f) Los órganos de las Administraciones responsables del fichero.

g) Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.

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

3. En las disposiciones que se dicten para la supresión de los ficheros. se establecerá el destino de los mismos o, en su caso, las previsiones que se adopten para su destrucción

Artículo 21. Comunicación de datos entre Administraciones públicas

1. Los datos de carácter personal recogidos o elaborados por las Administraciones públicas para el desempeño de sus atribuciones no serán comunicados a otras Administraciones públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, salvo cuando la comunicación hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso, o cuando la comunicación tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

2. Podrán, en todo caso, ser objeto de comunicación los datos de carácter personal que una Administración pública obtenga o elabore con destino a otra.

3. No obstante lo establecido en el artículo 11.2.b), la comunicación de datos recogidos de fuentes accesibles al público no podrá efectuarse a ficheros de titularidad privada, sino con el consentimiento del interesado o cuando una ley prevea otra cosa.

4. En los supuestos previstos en los apartados 1 y 2 del presente artículo no será necesario el consentimiento del afectado a que se refiere el artículo 11 de la presente Ley.

Artículo 22. Ficheros de las Fuerzas y Cuerpos de Seguridad.

1. Los ficheros creados por las Fuerzas y Cuerpos de Seguridad que contengan datos de carácter personal que, por haberse recogido para fines administrativos, deban ser objeto de registro permanente, estarán sujetos al régimen general de la presente Ley.

2. La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad.

3. La recogida y tratamiento por las Fuerzas y Cuerpos de Seguridad de los datos, a que hacen referencia los apartados 2 y 3 del artículo 7, podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas en su caso por los interesados que corresponden a los órganos jurisdiccionales.

4. Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento.

A estos efectos, se considerará especialmente la edad del afectado y el carácter de los datos almacenados, la necesidad de mantener los datos hasta la conclusión de una investigación o procedimiento concreto, la resolución judicial firme, en especial la absolutoria, el indulto, la rehabilitación y la prescripción de responsabilidad.

Artículo 23. Excepciones a los derechos de acceso, rectificación y cancelación.

1. Los responsables de los ficheros que contengan los datos a que se refieren los apartados 2, 3 y 4 del artículo anterior podrán denegar el acceso, la rectificación o cancelación en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando.

2. Los responsables de los ficheros de la Hacienda Pública podrán, igualmente, denegar el ejercicio de los derechos a que se refiere el apartado anterior cuando el mismo obstaculice las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado esté siendo objeto de actuaciones inspectoras.

3. El afectado al que se deniegue, total o parcialmente, el ejercicio de los derechos mencionados en los apartados anteriores podrá ponerlo en conocimiento del Director de la Agencia de Protección de Datos o del organismo competente de cada Comunidad Autónoma en el caso de ficheros mantenidos por Cuerpos de Policía propios de éstas, o por las Administraciones tributarías autonómicas, quienes deberán asegurarse de la procedencia o improcedencia de la denegación.

Artículo 24. Otras excepciones a los derechos de los afectados.

1. Lo dispuesto en los apartados 1 y 2 del artículo 5 no será aplicable a la recogida de datos cuando la información al afectado impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones públicas o cuando afecte a la Defensa Nacional. a la seguridad pública o a la persecución de infracciones penales o administrativas.

2. Lo dispuesto en el artículo 15 y en el apartado 1 del artículo 16 no será de aplicación si, ponderados los intereses en presencia, resultase que los derechos que dichos preceptos conceden al afectado hubieran de ceder ante razones de interés público o ante intereses de terceros más dignos de protección. Si el órgano administrativo responsable del fichero invocase lo dispuesto en este apartado, dictará resolución motivada e instruirá al afectado del derecho que le asiste a poner la negativa en conocimiento del Director de

la Agencia de Protección de Datos o, en su caso, del órgano equivalente de las Comunidades Autónomas.

CAPÍTULO II

Ficheros de titularidad privada

Artículo 25. Creación.

Podrán crearse ficheros de titularidad privada que contengan datos de carácter personal cuando resulte necesario para el logro de la actividad u objeto legítimos de la persona, empresa o entidad titular y se respeten las garantías que esta Ley establece para la protección de las personas.

Artículo 26. *Notificación e* inscripción registral.

1. Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia de Protección de Datos.

2. Por vía reglamentaria se procederá ala regulación detallada de los distintos extremos que debe contener la notificación, entre los cuales figurarán necesariamente el responsable del fichero, la finalidad del mismo, su ubicación, el tipo de datos de carácter personal que contiene, las medidas de seguridad, con indicación del nivel básico. medio o alto exigible y las cesiones de datos de carácter personal que se prevean realizar y, en su caso, las transferencias de datos que se prevean a países terceros.

3. Deberán comunicarse a la Agencia de Protección de Datos los cambios que se produzcan en la finalidad del fichero automatizado, en su responsable y en la dirección de su ubicación.

4. El Registro General de Protección de Datos inscribirá el fichero si la notificación se ajusta a los requisitos exigibles.

En caso contrario podrá pedir que se completen los datos que falten o se proceda a su subsanación.

5. Transcurrido un mes desde la presentación de la solicitud. de inscripción sin que la Agencia de Protección de Datos hubiera resuelto sobre la misma. se entenderá inscrito el fichero automatizado a todos los efectos.

Artículo 27. *Comunicación de* la *cesión de datos*.

1. El responsable del fichero, en el momento en que se efectúe la primera cesión de datos, deberá informar de ello a los afectados, indicando, asimismo. la finalidad del fichero, la naturaleza de los datos que han sido cedidos y el nombre y dirección del cesionario.

2. La obligación establecida en el apartado anterior no existirá en el supuesto previsto en los apartados 2, letras c), d), e) y 6 del artículo 11, ni cuando la cesión venga impuesta por ley.

Artículo 28. *Datos incluidos en las fuentes de acceso público.*

1. Los datos personales que figuren en el censo promocional, o las listas de personas pertenecientes a grupos de profesionales a que se refiere el artículo 3, j) de esta Ley deberán limitarse a los que sean estrictamente necesarios para cumplir la finalidad a que se destina cada listado. La inclusión de datos adicionales por las entidades responsables del mantenimiento de dichas fuentes requerirá el consentimiento del interesado, que podrá ser revocado en cualquier momento.

2. Los interesados tendrán derecho a que la entidad responsable del mantenimiento de los listados de los Colegios profesionales indique gratuitamente que sus datos personales no pueden utilizarse para fines de publicidad o prospección comercial

Los interesados tendrán derecho a exigir gratuitamente la exclusión de la totalidad de sus datos personales que consten en el censo promocional por las entidades encargadas del mantenimiento de dichas fuentes.

La atención a la solicitud de exclusión de la información innecesaria o de inclusión de la objeción al uso de los datos para fines de publicidad o venta a distancia deberá realizarse en el plazo de diez días respecto de las informaciones que se realicen mediante consulta o comunicación telemática y en la siguiente edición del listado cualquiera que sea el soporte en que se edite.

3. Las fuentes de acceso público que se editen en forma de libro o algún otro soporte físico, perderán el carácter de fuente accesible con la nueva edición que se publique.

En el caso de que se obtenga telemáticamente una copia de la lista en formato electrónico, ésta perderá el carácter de fuente de acceso público en el plazo de un año, contado desde el momento de su obtención.

4. Los datos que figuren en las guías de servicios de telecomunicaciones disponibles al público se regirán por su normativa específica.

Artículo 29. *Prestación de servicios de información sobre solvencia patrimonial y crédito.*

1. Quienes se dediquen a la prestación de servicios de información sobre la solvencia patrimonial y el crédito sólo podrán tratar datos de carácter personal obtenidos de los registros y las fuentes accesibles al público establecidos al efecto o procedentes de informaciones facilitadas por el interesado o con su consentimiento.

2. Podrán tratarse también datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés. En estos casos se notificará a los interesados respecto de los que hayan registrado datos de carácter personal en ficheros, en el plazo de treinta días desde dicho registro, una referencia de los que hubiesen sido incluidos y se les informará de su derecho a recabar información de la totalidad de ellos, en los términos establecidos por la presente Ley.

3. En los supuestos a que se refieren los dos apartados anteriores, cuando el interesado lo solicite, el responsable de¡ tratamiento le comunicará los datos, así como las evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los

últimos seis meses y el nombre y dirección de la persona o entidad a quien se hayan revelado los datos,

4. Sólo se podrán registrar y ceder los datos de carácter personal que sean determinantes para enjuiciar la solvencia económica de los interesados y que no se refieran, cuando sean adversos, a más de seis años, siempre que respondan con veracidad a la situación actual de aquéllos.

Artículo 30. *Tratamientos con fines de publicidad y de prospección comercial.*

1. Quienes se dediquen a la recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial y otras actividades análogas, utilizarán nombres y direcciones u otros datos de carácter personal cuando los mismos figuren en fuentes accesibles al público o cuando hayan sido facilitados por los propios interesados u obtenidos con su consentimiento.

2. Cuando los datos procedan de fuentes accesibles al público, de conformidad con lo establecido en el párrafo segundo del artículo 5.5 de esta Ley, en cada comunicación que se dirija al interesado se informará del origen de los datos y de la identidad del responsable del tratamiento, así como de los derechos que le asisten.

3. En el ejercicio del derecho de acceso los interesados tendrán derecho a conocer el origen de sus datos de carácter personal, así como del resto de información a que se refiere el artículo 15.

4. Los interesados tendrán derecho a oponerse, previa petición y sin gastos, al tratamiento de los datos que les conciernan, en cuyo caso serán dados de baja del tratamiento, cancelándose las informaciones que sobre ellos figuren en aquél, a su simple solicitud.

Artículo 31. *Censo promocional.*

1. Quienes pretendan realizar permanente o esporádicamente la actividad de recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección

comercial u otras actividades análogas, podrán solicitar del Instituto Nacional de Estadística o de los órganos equivalentes de las Comunidades Autónomas una copia del censo promocional, formado con los datos de nombre, apellidos y domicilio que constan en el censo electoral.

2. El uso de cada lista de censo promocional tendrá un plazo de vigencia de un año. Transcurrido el plazo citado, la lista perderá su carácter de fuente de acceso público.

3. Los procedimientos mediante los que los interesados podrán solicitar no aparecer en el censo promocional se regularán reglamentariamente. Entre estos

procedimientos, que serán gratuitos para los interesados, se incluirá el documento de empadronamiento. Trimestralmente se editará una lista actualizada del censo promocional, excluyendo los nombres y domicilios de los que así lo hayan solicitado.

4. Se podrá exigir una contra prestación por la facilitación de la citada lista en soporte informático.

Artículo 32. *Códigos tipo.*

1. Mediante acuerdos sectoriales, convenios administrativos o decisiones de empresa, los responsables de tratamientos de titularidad pública y privada, así como las organizaciones en que se agrupen, podrán formular códigos tipo que establezcan las condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad del entorno, programas o equipos, obligaciones de los implicados en el tratamiento y uso de la información personal, así como las garantías, en su ámbito, para el ejercicio de los derechos de las personas con pleno respeto a los principios y disposiciones de la presente Ley y sus normas de desarrollo.

2. Los citados códigos podrán contener o no reglas operacionales detalladas de cada sistema particular y estándares técnicos de aplicación.

En el supuesto de que tales reglas o estándares no se incorporen directamente al código, las instrucciones u órdenes que los establecieran deberán respetar los principios fijados en aquél.

3, Los códigos tipo tendrán el carácter de códigos deontológicos o de buena práctica profesional, debiendo ser depositados o inscritos en el Registro General de Protección de Datos y, cuando corresponda, en los creados a estos efectos por las Comunidades Autónomas, de acuerdo con el artículo 41. El Registro General de Protección de Datos podrá denegar la inscripción cuando considere que no se ajusta a las disposiciones legales y reglamentarias sobre la materia, debiendo, en este caso, el Director de la Agencia de Protección de Datos requerir a los solicitantes para que efectúen las correcciones oportunas.

TÍTULO V

Movimiento internacional de datos

Artículo 33. Norma general.

1. No podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas.

2. El carácter adecuado del nivel de protección que ofrece el país de destino se evaluará por la Agencia de Protección de Datos atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento 0 de los tratamientos previstos, el país de origen y el país de destino final, las normas de derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

Artículo 34. *Excepciones.*

Lo dispuesto en el artículo anterior no será de aplicación:

a) Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España.

b) Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional.

c) Cuando la transferencia sea necesaria para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento médicos o la gestión de servicios sanitarios.

d) Cuando se refiera a transferencias dinerarias conforme a su legislación específica.

e) Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista.

f) Cuando la transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado.

g) Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero.

h) Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público. Tendrá esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias.

i) Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

j) Cuando la transferencia se efectúe, a petición de persona con interés legítimo, desde un Registro público y aquélla sea acorde con la finalidad del mismo.

k) Cuando la transferencia tenga como destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado.

TÍTULO VI

Agencia de Protección de Datos

Artículo 35. Naturaleza y régimen jurídico.

1. La Agencia de Protección de Datos es un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones públicas en el ejercicio de sus funciones. Se regirá por lo dispuesto en la presente Ley y en un Estatuto propio, que será aprobado por el Gobierno.

2. En el ejercicio de sus funciones públicas, y en defecto de lo que disponga la presente Ley y sus disposiciones de desarrollo, la Agencia de Protección de Datos actuará de conformidad con la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. En sus adquisiciones patrimoniales y contratación estará sujeta al derecho privado.

3. Los puestos de trabajo de los órganos y servicios que integren la Agencia de Protección de Datos serán desempeñados por funcionarios de las Administraciones públicas y por personal contratado al efecto, según la naturaleza de las funciones asignadas a cada puesto de trabajo. Este personal está obligado a guardar secreto de los datos de carácter personal de que conozca en el desarrollo de su función.

4. La Agencia de Protección de Datos contará, para el cumplimiento de sus fines, con los siguientes bienes y medios económicos,

a) Las asignaciones que se establezcan anualmente con cargo a los Presupuestos Generales del Estado.

b) Los bienes y valores que constituyan su patrimonio, así como los productos y rentas del mismo.

c) Cualesquiera otros que legalmente puedan serie atribuidos.

5. La Agencia de Protección de Datos elaborará y aprobará con carácter anual el correspondiente anteproyecto de presupuesto y lo remitirá al Gobierno para que sea integrado, con la debida independencia, en los Presupuestos Generales del Estado.

Artículo 36. El Director.

1. El Director de la Agencia de Protección de Datos dirige la Agencia y ostenta su representación. Será nombrado, de entre quienes componen el Consejo Consultivo, mediante Real Decreto, por un período de cuatro años.

2. Ejercerá sus funciones con plena independencia y objetividad y no estará sujeto a instrucción alguna en el desempeño de aquéllas.

En todo caso, el Director deberá oír al Consejo Consultivo en aquellas propuestas que éste le realice en el ejercicio de sus funciones.

3. El Director de la Agencia de Protección de Datos sólo cesará antes de la expiración del período a que se refiere el apartado 1, a petición propia o por separación acordada por el Gobierno, previa instrucción de expediente, en el que necesariamente serán oídos los restantes miembros del Consejo Consultivo, por incumplimiento grave de sus obligaciones, incapacidad sobrevenida para el ejercicio de su función, incompatibilidad o condena por delito doloso.

4. El Director de la Agencia de Protección de Datos tendrá la consideración de alto cargo y quedará en la situación de servicios especiales si con anterioridad estuviera desempeñando una función pública. En el supuesto de que sea nombrado para el cargo

algún miembro de la carrera judicial o fiscal, pasará asimismo a la situación administrativa de servicios especiales.

Artículo 37. Funciones.

Son funciones de la Agencia de Protección de Datos:

a) Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.

b) Emitir las autorizaciones previstas en la Ley o en sus disposiciones reglamentarias.

c) Dictar, en su caso, y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos a los principios de la presente Ley.

d) Atender las peticiones y reclamaciones formuladas por las personas afectadas.

e) Proporcionar información a las personas acerca de sus derechos en materia de tratamiento de los datos de carácter personal.

f) Requerir a los responsables y los encargados de los tratamientos, previa audiencia de éstos, la adopción de las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones de esta Ley y, en su caso, ordenar la cesación de los tratamientos y la cancelación de los ficheros, cuando no se ajuste a sus disposiciones.

g) Ejercer la potestad sancionadora en los términos previstos por el Título VII de la presente Ley.

h) Informar, con carácter preceptivo, los proyectos de disposiciones generales que desarrollen esta Ley.

i) Recabar de los responsables de los ficheros cuanta ayuda e información estime necesaria para el desempeño de sus funciones.

j) Velar por la publicidad de la existencia de los ficheros de datos con carácter personal, a cuyo efecto publicará periódicamente una relación de dichos ficheros con la información adicional que el Director de la Agencia determine.

k) Redactar una memoria anual y remitirla al Ministerio de Justicia.

l) Ejercer el control y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos, así como desempeñar las funciones de cooperación internacional en materia de protección de datos personales.

m) Velar por el cumplimiento de las disposiciones que la Ley de la Función Estadística Pública establece respecto a la recogida de datos estadísticos y al secreto estadístico, así como dictar las instrucciones precisas, dictaminar sobre las condiciones de seguridad de los ficheros constituidos con fines exclusivamente estadísticos y ejercer la potestad a la que se refiere el artículo 46.

n) Cuantas otras le sean atribuidas por normas legales o reglamentarias.

Artículo 38. Consejo Consultivo.

El Director de la Agencia de Protección de Datos estará asesorado por un Consejo Consultivo compuesto por los siguientes miembros:

Un Diputado, propuesto por el Congreso de los Diputados.

Un Senador, propuesto por el Senado.

Un representante de la Administración Central, designado por el Gobierno.

Un representante de la Administración Local, propuesto por la Federación, Española de Municipios y Provincias.

Un miembro de la Real Academia de la Historia, propuesto por la misma.

Un experto en la materia, propuesto por el Consejo Superior de Universidades.

Un representante de los usuarios y consumidores, seleccionado del modo que se prevea reglamentariamente.

Un representante de cada Comunidad Autónoma que haya creado una agencia de protección de datos en su ámbito territorial, propuesto de acuerdo con el procedimiento que establezca la respectiva Comunidad Autónoma,

Un representante del sector de ficheros privados, para cuya propuesta se seguirá el procedimiento que se regule regla menta ría mente.

El funcionamiento del Consejo Consultivo se regirá por las normas reglamentarias que al efecto se establezcan.

Artículo 39. El Registro General de Protección de Datos.

1. El Registro General de Protección de Datos es un órgano integrado en la Agencia de Protección de Datos.

2. Serán objeto de inscripción en el Registro General de Protección de Datos:

a) Los ficheros de que sean titulares las Administraciones públicas.

b) Los ficheros 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.

3. Por vía reglamentaria se regulará el procedimiento de inscripción de los ficheros, tanto de titularidad pública como de titularidad privada, en el Registro General de Protección de Datos, el contenido de la inscripción, su modificación, cancelación, reclamaciones y recursos contra las resoluciones correspondientes y demás extremos pertinentes.

Artículo 40. Potestad de inspección.

1. Las autoridades de control podrán inspeccionar los ficheros a que hace referencia la presente Ley, recabando cuantas informaciones precisen para el cumplimiento de sus cometidos.

A tal efecto, podrán solicitar la exhibición o el envío de documentos y datos y examinarlos en el lugar en que se encuentren depositados, así como inspeccionar los equipos físicos y lógicos utilizados para el tratamiento de los datos, accediendo a los locales donde se hallen instalados.

2. Los funcionarios que ejerzan la inspección a que se refiere el apartado anterior tendrán la consideración de autoridad pública en el desempeño de sus cometidos.

Estarán obligados a guardar secreto sobre las informaciones que conozcan en el ejercicio de las mencionadas funciones, incluso después de haber cesado en las mismas.

Artículo 41. Órganos correspondientes de las Comunidades Autónomas.

1. Las funciones de la Agencia de Protección de Datos reguladas en el artículo 37, a excepción de las mencionadas en los apartados j), k) y l), y en los apartados f) y g) en lo que se refiere a las transferencias internacionales de datos, así como en los artículos 46 y 49, en relación con sus específicas competencias serán ejercidas, cuando afecten a ficheros de datos de carácter personal creados o gestionados por las Comunidades Autónomas y por la Administración Local de su ámbito territorial, por los órganos correspondientes de cada Comunidad, que tendrán la consideración de autoridades de control, a los que garantizarán plena independencia y objetividad en el ejercicio de su cometido.

2. Las Comunidades Autónomas podrán crear y mantener sus propios registros de ficheros para el ejercicio de las competencias que se les reconoce sobre los mismos.

3. El Director de la Agencia de Protección de Datos podrá convocar regularmente a los órganos correspondientes de las Comunidades Autónomas a efectos de cooperación institucional y coordinación de criterios o procedimientos de actuación. El Director de la Agencia de Protección de Datos y los órganos correspondientes de las Comunidades Autónomas podrán solicitarse mutuamente la información necesaria para el cumplimiento de sus funciones.

Artículo 42. Ficheros de las Comunidades Autónomas en materia de su exclusiva competencia.

1. Cuando el Director de la Agencia de Protección de Datos constate que el mantenimiento o uso de un determinado fichero de las Comunidades Autónomas contraviene algún precepto de esta Ley en materia de su exclusiva competencia podrá requerir a la Administración correspondiente que se adopten las medidas correctoras que determine en el plazo que expresamente se fije en el requerimiento.

2. Si la Administración pública correspondiente no cumpliera el requerimiento formulado, el Director de la Agencia de Protección de Datos podrá impugnar la resolución adoptada por aquella Administración.

TÍTULO VII

Infracciones y sanciones

Artículo 43. Responsables.

1. Los responsables de los ficheros y los encargados de los tratamientos estarán sujetos al régimen sancionador establecido en la presente Ley.

2. Cuando se trate de ficheros de los que sean responsables las Administraciones públicas se estará, en cuanto al procedimiento y a las sanciones, a lo dispuesto en el artículo 46, apartado 2.

Artículo 44. Tipos de infracciones.

1. Las infracciones se calificarán como leves, graves o muy graves.

2. Son infracciones leves:

a) No atender, por motivos formales, la solicitud del interesado de rectificación o cancelación de los datos personales objeto de tratamiento cuando legalmente proceda.

b) No proporcionar la información que solicite la Agencia de Protección de Datos en el ejercicio de las competencias que tiene legalmente atribuidas, en relación con aspectos no sustantivos de la protección de datos.

c) No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando no sea constitutivo de infracción grave.

d) Proceder a la recogida de datos de carácter personal de los propios afectados sin proporcionarles la información que señala el artículo 5 de la presente Ley.

e) Incumplir el deber de secreto establecido en el artículo 10 de esta Ley, salvo que constituya infracción grave.

3. Son infracciones graves:

a) Proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general, publicada en el «Boletín Oficial del Estado» o Diario oficial correspondiente.

b) Proceder a la creación de ficheros de titularidad privada o iniciar la recogida de datos de carácter personal para los mismos con finalidades distintas de las que constituyen el objeto legítimo de la empresa o entidad.

c) Proceder a la recogida de datos de carácter personal sin recabar el consentimiento expreso de las personas afectadas, en los casos en que éste sea exigible.

d) Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la presente Ley o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción muy grave.

e) El impedimento o la obstaculización del ejercicio de los derechos de acceso y oposición y la negativa a facilitar la información que sea solicitada.

f) Mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de las personas que la presente Ley ampara.

g) La vulneración del deber de guardar secreto sobre los datos de carácter personal incorporados a ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, prestación de servicios de solvencia patrimonial y crédito, así como aquellos otros ficheros que contengan un conjunto de datos de carácter personal suficientes para obtener una evaluación de la personalidad del individuo.

h) Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen.

i) No remitir a la Agencia de Protección de Datos las notificaciones previstas en esta Ley o en sus disposiciones de desarrollo, así como no proporcionar en plazo a la misma cuantos documentos e informaciones deba recibir o sean requeridos por aquél a tales efectos.

j) La obstrucción al ejercicio de la función inspectora. .

k) No inscribir el fichero de datos de carácter personal en el Registro General de Protección Datos, cuando haya sido requerido para ello por el Director de la Agencia de Protección de Datos.

l) Incumplir el deber de información que se establece en los artículos 5, 28 y 29 de esta Ley, cuando los datos hayan sido recabados de persona distinta del afectado.

4. Son infracciones muy graves:

a) La recogida de datos en forma engañosa y fraudulenta.

b) La comunicación o cesión de los datos de carácter personal, fuera de los casos en que estén permitidas.

c) Recabar y tratar los datos de carácter personal a los que se refiere el apartado 2 del artículo 7 cuando no medie el consentimiento expreso del afectado; recabar y tratar los datos referidos en el apartado 3 del artículo 7 cuando no lo disponga una ley o el afectado no haya consentido expresamente, o violentar la prohibición contenida en el apartado 4 del artículo 7.

d) No cesar en el uso ilegítimo de los tratamientos de datos de carácter personal cuando sea requerido para ello por el Director de la Agencia de Protección de Datos o por las personas titulares del derecho de acceso.

e) La transferencia temporal o definitiva de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento, con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia de Protección de Datos.

f) Tratar los datos de carácter personal de forma ilegítima o con menosprecio de los principios y garantías que les sean de aplicación, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales.

g) La vulneración del deber de guardar secreto sobre los datos de carácter personal a que hacen referencia los apartados 2 y 3 del artículo 7, así como los que hayan sido recabados para fines policiales sin consentimiento de las personas afectadas.

h) No atender, u obstaculizar de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación u oposición.

i) No atender de forma sistemática el deber legal de notificación de la inclusión de datos de carácter personal en un fichero.

Artículo 45. Tipo de sanciones.

1. Las infracciones leves serán sancionadas con multa de 100.000 a 10.000.000 de pesetas.

2. Las infracciones graves serán sancionadas con multa de 10.000.000 a 50.000.000 de pesetas.

3. Las infracciones muy graves serán sancionadas con multa de 50.000.000 a 100.000.000 de pesetas.

4. La cuantía de las sanciones se graduará atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a terceras personas, y a cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora.

5. Si, en razón de las circunstancias concurrentes se apreciara una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad M hecho, el órgano sancionador establecerá la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate.

6. En ningún caso podrá imponerse una sanción más grave que la fijada en la Ley para la clase de infracción en la que se integre la que se pretenda sancionar.

7. El Gobierno actualizará periódicamente la cuantía de las sanciones de acuerdo con las variaciones que experimenten los índices de precios.

Artículo 46. Infracciones de las Administraciones públicas.

1. Cuando las infracciones a que se refiere el artículo 44 fuesen cometidas en ficheros de los que sean responsables las Administraciones públicas, el Director de la Agencia de Protección de Datos dictará una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción. Esta resolución se notificará al responsable del fichero, al órgano del que dependa jerárquicamente y a los afectados si los hubiera.

2. El Director de la Agencia podrá proponer también la iniciación de actuaciones disciplinarias, si procedieran. El procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario de las Administraciones públicas.

3. Se deberán comunicar a la Agencia las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores,

4. El Director de la Agencia comunicará al Defensor del Pueblo las actuaciones que efectúe y las resoluciones que dicte al amparo de los apartados anteriores.

Artículo 47. Prescripción.

1. Las infracciones muy graves prescribirán a los tres años, las graves a los dos años y las leves al año.

2. El plazo de prescripción comenzará a contarse desde el día en que la infracción se hubiera cometido.

3. Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento sancionador, reanudándose el plazo de prescripción si el expediente sancionador estuviere paralizado durante más de seis meses por causas no imputables al presunto infractor.

4. Las sanciones impuestas por faltas muy graves prescribirán a los tres años, las impuestas por faltas graves a los dos años y las impuestas por faltas leves al año.

S. El plazo de prescripción de las sanciones comenzará a contarse desde el día siguiente a aquel en que adquiera firmeza la resolución por la que se impone la sanción.

6. La Prescripción se interrumpirá por la iniciación, con conocimiento del interesado, del procedimiento de ejecución, volviendo a transcurrir el plazo si el mismo está paralizado durante más de seis meses por causa no imputable al infractor.

Artículo 48. Procedimiento sancionador.

1. Por vía reglamentaria se establecerá el procedimiento a seguir para la determinación de las infracciones y la imposición de las sanciones a que hace referencia el presente Título.

2. Las resoluciones de la Agencia de Protección de Datos u órgano correspondiente de la Comunidad Autónoma agotan la vía administrativa.

Artículo 49. Potestad de inmovilización de ficheros.

En los supuestos, constitutivos de infracción muy grave, de utilización o cesión ilícita de los datos de carácter personal en que se impida gravemente o se atente de igual modo contra el ejercicio de los derechos de los ciudadanos y el libre desarrollo de la personalidad que la Constitución y las leyes garantizan, el Director de la Agencia de Protección de Datos podrá, además de ejercer la potestad sancionadora, requerir a los responsables de ficheros de datos de carácter personal, tanto de titularidad pública como privada, la cesación en la utilización o cesión ilícita de los datos. Si el requerimiento fuera desatendido, la Agencia de Protección de Datos podrá, mediante resolución motivada,

inmovilizar tales ficheros a los solos efectos de restaurar los derechos de las personas afectadas.

Disposición adicional primera. Ficheros preexistentes.

Los ficheros y tratamientos automatizados inscritos o no en el Registro General de Protección de Datos deberán adecuarse a la presente Ley Orgánica dentro M plazo de tres años, a contar desde su entrada en vigor. En dicho plazo, los ficheros de titularidad privada deberán ser comunicados a la Agencia de Protección de Datos y las Administraciones públicas, responsables de ficheros de titularidad pública, deberán aprobar la pertinente disposición de regulación M fichero o adaptar la existente.

En el supuesto de ficheros y tratamientos no automatizados, su adecuación a la presente Ley Orgánica, y la obligación prevista en el párrafo anterior deberán cumplimentarse en el plazo de doce años a contar desde el 24 de octubre de 1995, sin perjuicio del ejercicio de los derechos de acceso, rectificación y cancelación por parte de los afectados.

Disposición adicional segunda. Ficheros y Registro de

Población de las Administraciones públicas.

1. La Administración General del Estado y las Administraciones de las Comunidades Autónomas podrán solicitar al Instituto Nacional de Estadística, sin consentimiento del interesado, una copia actualizada del fichero formado con los datos del nombre, apellidos, domicilio, sexo y fecha de nacimiento que constan en los padrones municipales de habitantes y en el censo electoral correspondientes a los territorios donde ejerzan sus competencias, para la creación de ficheros o registros de población.

2. Los ficheros o registros de población tendrán como finalidad la comunicación de los distintos órganos de cada Administración pública con los interesados residentes en los respectivos territorios, respecto a las relaciones jurídico administrativas derivadas de las competencias respectivas de las Administraciones públicas.

Disposición adicional tercera. Tratamiento de los expedientes de las derogadas Leyes de Vagos y Maleantes y de Peligrosidad y Rehabilitación Social.

Los expedientes específicamente instruidos al amparo de las derogadas Leyes de Vagos y Maleantes, y de Peligrosidad y Rehabilitación Social, que contengan datos de cualquier índole susceptibles de afectar a la seguridad, al honor, a la intimidad o a la imagen de las personas, no podrán ser consultados sin que medie consentimiento expreso de los afectados, o hayan transcurrido cincuenta años desde la fecha de aquéllos.

En este último supuesto, la Administración General del Estado, salvo que haya constancia expresa del fallecimiento de los afectados, pondrá a disposición del solicitante la documentación, suprimiendo de la misma los datos aludidos en el párrafo anterior, mediante la utilización de los procedimientos técnicos pertinentes en cada caso.

Disposición adicional cuarta. Modificación del artículo 112.4 de la Ley General Tributaria.

El apartado cuarto del artículo 112 de la Ley General Tributaría pasa a tener la siguiente redacción:

«4. La cesión de aquellos datos de carácter personal, objeto de tratamiento, que se debe efectuar a la Administración tributaría conforme a lo dispuesto en el artículo 111, en los apartados anteriores de este artículo o en otra norma de rango legal, no requerirá el consentimiento del afectado. En este ámbito tampoco será de aplicación lo que respecto a las Administraciones públicas establece el apartado 1 del artículo 21 de la Ley Orgánica de Protección de Datos de carácter personal.»

Disposición adicional quinta. Competencias del Defensor del Pueblo y órganos autonómicos semejantes.

Lo dispuesto en la presente Ley Orgánica se entiende sin perjuicio de las competencias del Defensor del Pueblo y de los órganos análogos de las Comunidades Autónomas.

Disposición adicional sexta. Modificación del artículo 24.3 de la Ley de Ordenación y Supervisión de los Seguros Privados.

Se modifica el artículo 24.3, párrafo 2º de la Ley 30/1995, de 8 de noviembre, de Ordenación y Supervisión de los Seguros Privados, con la siguiente redacción:

«Las entidades aseguradoras podrán establecer ficheros comunes que contengan datos de carácter personal para la liquidación de siniestros y la colaboración estadístico actuarial con la finalidad de permitir la tarificación y selección de riesgos y la elaboración de estudios de técnica aseguradora. La cesión de datos a los citados ficheros no requerirá el consentimiento previo del afectado, pero sí la comunicación al mismo de la posible cesión de sus datos personales a ficheros comunes para los fines señalados con expresa indicación del responsable para que se puedan ejercitar los derechos de acceso, rectificación y cancelación previstos en la ley.

También podrán establecerse ficheros comunes cuya finalidad sea prevenir el fraude en el seguro sin que sea necesario el consentimiento del afectado. No obstante, será necesaria en estos casos la comunicación al afectado, en la primera introducción de sus datos, de quién sea el responsable

del fichero y de las formas de ejercicio de los derechos de acceso, rectificación y cancelación.

En todo caso, los datos relativos a la salud sólo podrán ser objeto de tratamiento con el consentimiento expreso del afectado.»

Disposición transitoria primera. Tratamientos creados por Convenios internacionales.

La Agencia de Protección de Datos será el organismo competente para la protección de las personas físicas en lo que respecta al tratamiento de datos de carácter personal respecto de los tratamientos establecidos en cualquier Convenio Internacional del que sea parte España que atribuya a una autoridad nacional de control esta competencia, mientras no se cree una autoridad diferente para este cometido en desarrollo del Convenio.

Disposición transitoria segunda. Utilización del censo promocional

Reglamentariamente se desarrollarán los procedimientos de formación del censo promocional, de oposición a aparecer en el mismo, de puesta a disposición de sus solicitantes, y de control de las listas difundidas. El Reglamento establecerá los plazos para la puesta en operación del censo promocional,

Disposición transitoria tercera. preexistentes.

Subsistencia de normas

Hasta tanto se lleven a efectos las previsiones de la disposición final primera de esta Ley, continuarán en vigor, con su propio rango, las normas reglamentarias existentes y, en especial, los Reales Decretos 428/1993, de 26 de marzo; 1332/1994, de 20 de junio, y 994/1999, de 11 de junio, en cuanto no se opongan a la presente Ley.

Disposición derogatoria única. Derogación normativa.

Queda derogada la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del tratamiento automatizado de los datos de carácter personal.

Disposición final primera. Habilitación para el desarrollo reglamentario.

El Gobierno aprobará, o modificará, las disposiciones reglamentarias necesarias para la aplicación y desarrollo de la presente Ley.

Disposición final segunda. Preceptos con carácter de Ley ordinaria

Los Títulos IV, VI excepto el último inciso del párrafo 4 del artículo 36 y VII de la presente Ley, la disposición adicional cuarta, la disposición transitoria primera y la final primera tienen el carácter de Ley ordinaria.

Disposición final tercera. Entrada en vigor.

La presente Ley entrará en vigor en el plazo de un mes, contado desde su publicación en el «Boletín Oficial del Estado».

Por tanto,

Mando a todos los españoles, particulares y autoridades, que guarden y hagan guardar esta Ley Orgánica.

Madrid, 13 de diciembre de 1999.

JUAN CARLOS R.

El Presidente del Gobierno.
JOSÉ MARÍA AZNAR LÓPEZ

f

Bibliografía

Http://www.madrid.org/apdcm/

Http://www.agenciaprotecciondedatos/

Http://www.portaley.com/protecciondatos/

Http://www.delitosinformaticos.com/protecciondatos/ auditoriaprotecciondatos.shtml

Http://www.leydatos.com/

Http://www.hispasec.com/

Http://www.rediris.es/

Http://SecurityPortal.com/

Http://www.w3.org/Security/

Http://www.redhat.com/corp/support/errata/

Http://security.debian.rog/

Http://www.suse.de/e/patches/

Http://sunslove.sun.com/

Http://www.virtualey.com/

Http://www.pintos-salgado.com/

Http://www.ipf.uvigo.es/

Http://www.cert.org/

Http://www.cs.purdue.edu/coast/coast.html

ALVAREZ-CIENFUEGOS SUÁREZ, José María: *"Los delitos de falsedad y los documentos generados electrónicamente. Concepto procesal y material de documento: nuevas técnicas"*. Cuadernos de Derecho Judicial. La nueva delincuencia II. Consejo General del Poder Judicial. Madrid, 1993.

ANONYMOUS: "*Maximum Linux Security*". Ed SAMS, 2000.

ASSOCIATED PRESS: *"Hackers: Pentagon archives vulnerables".* Mercury Center, 17 de abril de 1998: http://spyglass1.sjmercury.com/breaking/docs/077466.htm

BLACK, Uyless: "*Internet Security Protocols*". Ed. Prentice Hall, 2000.

BRELSFORD, Harry M.: "*Windows 2000 Server*", 1ª Edición. Ed. Anaya, 2000

BRENTON, Chris: "*Mastering Network Security*". Ed. Sybex, 1999.

CORRERA, Michele M. y MARTUCCI, Pierpaolo: *I Reati Comessi con l'uso del computer. Banche dei dati e tutela della persona.* CEDAM (Casa Editrice Dott. Antonio Milani). Padova, 1986.

DAVARA RODRÍGUEZ, M. A.: *"El documento electrónico, informático y telemático y la firma electrónica"*. Actualidad Informática Aranzadi, nº24, Navarra, julio de 1997.

DAVARA RODRÍGUEZ, Miguel Ángel: *"Derecho Informático"*. Ed. Aranzadi. Navarra, 1993.

DEL PESO, Emilio, PIATTINI, Mario G.: "*Auditoría Informática*", 2ª Edición. Ed. RA-MA, 2000

DRAGO, Mirta: *"Hispahack: tres «cerebros» desactivados"*. El Mundo del siglo XXI. Madrid, 4 de abril de 1998.

GARFINKEL, Simson y SPAFFORD, Gene: "*Practical Unix & Internet Security*", 2ª Edición. Ed. O'Reilly & Associates, Inc. 1996.

HANCE, Olivier: *Leyes y Negocios en Internet*, McGraw-Hill, México 1996.

HILLEY, Valda: " Los secretos de Windows NT 4.0", 1ª Edición. Ed. Anaya, 1997

JUMES, James G., COOPER, N. F.: "Windows NT 4.0 Seguridad, auditoria y control", 1ª Edición. Ed. Microsoft Press, 1999.

KAEO, Merike: "*Designing Network Security*". Cisco Press, 1999.

LOPES ROCHA, Manuel y MACEDO, Mario: *Direito no Ciberespaço*, Ediçoes Cosmos, Lisboa 1996.

McCLURE, Stuart, SCAMBRAY, Joel y KURTZ, George: "*Hackers Secretos y soluciones para la seguridad de redes*", 1ª Edición. Ed. Osborne McGraw-Hill, 2000.

MOHR, James: "*Linux: Recursos para el usuario*". Ed. Prentice Hall, 1999.

MOYNA MÉNGUEZ, José y otros: *"Código Penal"*. 2ª Edición. Ed. Colex. Madrid, 1996.

PÉREZ LUÑO, A. E.: *Manual de Informática y Derecho*, Ariel, Barcelona 1996.

PÉREZ LUÑO, A. E.: *Nuevas tecnologías, sociedad y Derecho. El impacto sociojurídico de las N. T. de la información*, Fundesco, Madrid 1987.

PIETTE-COUDOL, Thierry et BERTRAND, André: *Internet et la Loi*, Dalloz, Paris 1997.

QUINTERO OLIVARES, Gonzalo y otros: *"Comentarios al Nuevo Código Penal"*. Ed. Aranzadi. Navarra, 1996.

RAYA, José Luis, RAYA, Elena: "*Windows NT Server Versión 4*", 1ª Edición. Ed. RA-MA, 1997.

RIVAS LÓPEZ, José Luis, ARES GÓMEZ, José Enrique y PÉREZ RODRÍGUEZ, Judith Mª: "*Linux Servidor NT*". Ed. PrensaTécnica. Revista Mas PC nº7, 1999.

RIVAS LÓPEZ, José Luis, ARES GÓMEZ, José Enrique y PÉREZ RODRÍGUEZ, Judith Mª: "*Proceso para convertir Unix en un PDC*". Ed. PrensaTécnica. Revista Sólo Linux nº16, 2001.

RIVAS LÓPEZ, José Luis, ARES GÓMEZ, José Enrique, SALGADO SEGUÍN, Victor A. y CONDE RODRÍGUEZ, Laura Elena: "*Situaciones de Hackeo [II]: penalización y medidas de seguridad*". Ed. PrensaTécnica. Revista Linux Actual nº15, 2000.

RIVAS LÓPEZ, José Luis, ARES GÓMEZ, José Enrique, SALGADO SEGUÍN, Victor A. y CONDE RODRÍGUEZ, Laura Elena: "*Situaciones de Hackeo [I]: pasos habituales del hacker*". Ed. PrensaTécnica. Revista Linux Actual nº14, 2000.

RIVAS LÓPEZ, José Luis, ARES GÓMEZ, José Enrique, SALGADO SEGUÍN, Victor A. y PÉREZ RODRIGUEZ, Judith: "*Linux: Seguridad técnica y legal*".

RUSSEL, Charlie, CRAWFORD, Sharon: "*Running Windows NT Server 4.0*", 1ª Edición. Ed. Microsoft Press, 1997

SANZ LARRUGA, F.J.: *El Derecho ante las nuevas tecnologías de la Información*, nº1 del Anuario de la Facultad de Derecho da Universidade da Coruña (1997), pp. 499-516.

SEMINARA, Sergio: *La pirateria su Internet e il diritto penale.* AIDA, 1996.

SHELDON, Tom, COX, Philip: "Windows 2000 *Manual de seguridad*". Ed. Osborne McGraw-Hill, 2002.

SHELDON, Tom: "*Manual de seguridad de Windows NT*". Ed. Osborne McGraw-Hill, 1997.

TACKETT & GUNTER: "*Utilizando Linux*", 2ª Edición. Ed. Prentice Hall, 1996.

TANENBAUM, Andrew S.: "*Redes de Computadoras*", 3ª Edición. Ed. Prentice Hall, 1997.

VARIOS: "*Seguridad en Windows 2000 Referencia técnica*". 1ª Edicción. Ed. Microsoft Press, 2001.

ZWICKY, Elizabeth, COOPER, Simon y CHAPMAN, D. Brent: "*Building Internet Firewalls*", 2ª Edición. Ed. O'Reilly, 2000.