Microsoft

LA PROTECCIÓN DE DATOS PERSONALES

SOLUCIONES EN ENTORNOS MICROSOFT®

Legister ABOGADOS

ipsCA

Gonzalo Gallo
Iñigo Coello de Portugal
Fernando Parrondo
Héctor Sánchez

La Protección de Datos Personales: Soluciones en Entornos Microsoft®

Autores

D. Gonzalo Gallo Ruiz. Responsable del Departamento Jurídico de IPS Certification Authority, S.L. Es Licenciado en Derecho por la Universidad del País Vasco y posee diversos Masters y Cursos Postgrado sobre Derecho Informático.

D. Iñigo Coello de Portugal Martínez del Peral. Director del Servicio Jurídico de Legister Abogados, Abogado del Estado y Letrado del Consejo de Estado. Es Doctor en Derecho por la Universidad de Navarra.

D. Fernando Parrondo García. Consultor Senior de Microsoft Consulting Services de Microsoft Iberica, S.R.L. Desarrolla su labor como Consultor Senior en la División de Servicios. Su misión es ayudar a las empresas a establecer la definición de los procesos que integran el ciclo de vida de las tecnologías de la información.

D. Héctor Sánchez Montenegro. Responsable de Seguridad de Microsoft Ibérica y Supervisor de ingeniería de Preventa de Enterprise and Partner Group . Anteriormente fue responsable del ISP y del Área de Servicios de seguridad de empresas como DINSA y Level Data. Es licenciado en Ciencias Físicas por la Universidad Autónoma de Madrid.

La Protección de Datos Personales: Soluciones en Entornos Microsoft®

Gonzalo Gallo Ruiz

Iñigo Coello de Portugal Martínez del Peral

Fernando Parrondo García

Héctor Sánchez Montenegro

ipsCA

Microsoft®

Legister ABOGADOS

Publicado por:
Microsoft Ibérica S.R.L.
C/ Ronda de Poniente, 10
28760 Tres Cantos (Madrid)

Depósito legal: M-8025-2003

Coordinador editorial: Juan Costa. Microsoft Press.
Diseño y maquetación: Susana Albalá. Newcomlab, S.L.L.
Revisión técnica: Newcomlab, S.L.L.
Imprime: Gráficas Marcar, S.A.
Impreso en España - Printed in Spain
Realizado en papel reciclado.

Índice de contenidos

Agradecimientos

Los autores desean agradecer a las siguientes personas, quienes sin su inestimable colaboración, hubiera resultado imposible la edición de este libro:

- Rodolfo Lomascolo Szittyay, Director General de IPS Certification Authority, S.L. (ipsCA)
- Olvido Nicolás, TechNet Program Manager Enterprise Marketing de Microsoft Ibérica S.R.L.
- Jesús Pintado, Enterprise Marketing Program Manager de Microsoft Ibérica S.R.L.
- Juan Costa, Business Development Manager Microsoft Press para España, Portugal y Latinoamérica de Microsoft Ibérica S.R.L.
- Mónica Pujadó Coll, Directora Financiera de IPS Certification Authority, S.L. (ipsCA).
- Eduardo Azanza, Technology Specialist Enterprise Solutions Group de Microsoft Ibérica S.R.L.
- Francisco Serrano, Technology Specialist Enterprise Solutions Group de Microsoft Ibérica S.R.L.
- Susana Juan, Technology Specialist Enterprise Solutions Group de Microsoft Ibérica S.R.L.
- Miguel Vega Martín, Director Comercial de IPS Certification Authority, S.L. (ipsCA)
- Eva María Corral, Technology Specialist Enterprise Solutions Group de Microsoft Ibérica S.R.L.
- Juan Carlos Pascual Chichón, Director Técnico de IPS Certification Authority, S.L. (ipsCA)
- Alberto Pecci Suárez, Director Técnico de Internet Publishing Services, S.L. (IPS).
- Mar Bastida, Product Manager de Microsoft Windows XP de Microsoft Ibérica S.R.L.
- Germán Díaz, Servers Product Manager de Microsoft Ibérica S.R.L.

Prólogo

La automatización de los procesos de tratamiento de datos nos ha proporcionado evidentes ventajas que han mejorado y aumentado tanto la productividad personal como la de las empresas. La tecnología está para aumentar nuestra capacidad de desarrollo tanto personal como profesional, permitiéndonos alcanzar metas impensables tan solo hace unos años. Los beneficios que nos reporta su uso exceden con mucho los problemas, como los derivados de la impersonalización en el tratamiento de los datos que manejamos. Por eso debemos poner límite al grado de intrusión en nuestra privacidad que el tratamiento automatizado de datos puede generar.

Desde una doble perspectiva, reconocemos que es nuestro derecho como ciudadanos la protección adecuada de nuestra privacidad y nuestro deber como suministradores de tecnología, facilitar el acceso a las tecnologías que ayuden en la consecución de este derecho.

¿Quién no se ha preguntado alguna vez si aquellos que tratan sus datos personales no tendrán demasiada información sobre su vida privada y cotidiana? Es obvio que debe existir un control sobre nuestros datos personales para que podamos sentirnos protegidos.

La Ley sobre Protección de Datos de Carácter Personal (LOPD) establece un límite sobre la tenencia y utilización de este tipo de datos así como sobre el tráfico de los mismos. De esta manera, la Agencia de Protección de Datos se encarga de facilitar al ciudadano el derecho a conocer quién está utilizando sus datos personales y para qué, y negar el permiso sobre el uso de sus datos a quien considere oportuno.

El planteamiento de este libro es bastante sencillo. No existen pretensiones técnicas ni legales ambiciosas. Para eso ya están los manuales especializados al respecto. El objetivo es doble: concordar la tecnología de seguridad implícita a la plataforma Microsoft con determinados requerimientos tecnológicos derivados del cumplimiento de la ley y, en segundo lugar (pero no menos importante), acercar al lector el conocimiento necesario sobre una ley que, como ciudadano protege nuestros derechos de privacidad, y que como responsable del proceso de datos ajenos necesito conocer para proteger eficazmente los derechos de los demás.

Fdo. Rosa García
Consejera Delegada de Microsoft Ibérica S.R.L.

1

Introducción

Como en casi todos los ámbitos de la vida la cuestión del tratamiento de los datos personales por terceros se encuentra en una situación de tensión. Esta tensión deriva de que los ficheros que reflejan circunstancias y perfiles de personas concretas han llegado a ser de tal maleabilidad y magnitud que ostentan un indudable valor económico. Una base de datos de personas puede ser "filtrada" en términos tales que recoja sólo la lista de las personas que "dan el perfil" correcto para un negocio. Tener esos datos es por tanto valioso para cualquier actividad de márketing, y por tanto objeto de comercio.

Pero por otro lado estamos hablando de datos de personas, que no son cosas, y que tienen una natural dignidad[1]. Y por tanto tienen derecho a ser tratadas como tales: a que se respete su condición, a saber qué se está haciendo con su nombre, a saber qué se está haciendo con sus datos personales... en una palabra, a la intimidad. Vamos a desarrollar estas ideas.

1.1 Ficheros y "bases de datos"

Los "ficheros" que afectan a la vida de las personas, y que "tratan" información de carácter personal, han existido desde siempre, sólo que en papel. El cambio que opera la informática es que multiplica para cualquier organización o persona la posibilidad de realizar un tratamiento automático y racional de la información. Ésta se encuentra recogida en archivos informáticos llamados "bases de datos", que sustituyen a los antiguos ficheros de papel. Estos archivos

[1] Hay ficheros informáticos de datos que son cosas (químicos, programas, etc.) que también son valiosos, y están protegidos. Pero por otras reglas no menos estrictas pero distintas.

informáticos, las bases de datos, son también ficheros. Lo único que cambia es el formato: son ficheros (archivos) informáticos.

La mayor potencia de los ordenadores sobre el papel a la hora de "tratar" la información que suministran las bases de datos, y la generalización de su uso por cualquiera que tenga un PC, ha obligado a los gobiernos a publicar normas jurídicas que regulen el tratamiento de la información. Ya en 1951 se creó en Estados Unidos la "Oficina Intergubernamental para la informática" (I.B.I). Este organismo ya ponía de manifiesto la influencia que tiene la Informática en la sociedad y que los países deberían de disponer de mecanismos para facilitar el uso de la misma y contribuir al bienestar de la humanidad en su contexto cultural, económico y social.

Estas normas jurídicas nuevas son de extraordinaria importancia, porque afectan a los derechos fundamentales de la persona. Son los mismos derechos fundamentales que la persona tenía antes de que la informática se introdujera en la vida cotidiana, pero ahora más protegidos, en la medida en que las nuevas tecnologías permiten un abuso mayor y más extendido.

1.2 La intimidad, un Derecho

La intimidad es un valor que se reconoce unánimemente en todo el mundo civilizado desde el Siglo XX. La intimidad ya fue recogida como uno de los derechos humanos en el artículo 12 de la Declaración Universal de Derechos Humanos (1944) al señalar 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."

Centrándonos en España, este derecho viene reconocido en el artículo 18 de la Constitución (1978) que señala lo siguiente:

1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.
2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.
3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.
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.

Vemos, por lo tanto, que la intimidad es uno de los derechos fundamentales que se recoge en el ordenamiento jurídico español, además de ser uno de los derechos humanos reconocidos internacionalmente.

1.3 El concepto de "intimidad"

La pregunta en este punto es qué se entiende por "intimidad". Aunque caben muchas interpretaciones, podemos definir el derecho a la intimidad, hablando en general, como el derecho que poseen las personas de poder excluir a las demás personas del conocimiento de su vida personal, es decir, de sus sentimientos, de sus emociones, de sus datos biográficos y personales y de su imagen. En términos técnico-jurídicos, puede hacerse una distinción bastante clara entre el derecho al honor, el derecho a la intimidad personal y el derecho a la propia imagen. Pero se trata de sutilezas que en este momento no interesa detallar.

El derecho a la intimidad abarca muchas circunstancias de la vida personal. Últimamente, con el desarrollo de la informática, la intimidad ha expandido el ámbito a que ella misma se refiere y se ha ido observando que las nuevas herramientas informáticas pueden suponer una intromisión en la vida privada de las personas. Por ello, el concepto de intimidad ha ido aproximando al de "privacidad". Es más que nada una cuestión de palabras. Lo que se denomina correctamente en castellano "intimidad" muchas veces la gente, empleando un anglicismo, lo llama "privacidad". El anglicismo trae causa de que los británicos denominan "private" a lo que no es "public", esto es, a aquellos ámbitos de la vida en los que los demás no tienen derecho a inmiscuirse, a lo íntimo.[2] Así se han ido mezclando los conceptos de "intimidad" y "privacidad", de tal suerte que por privacidad se entiende no sólo a la facultad que una persona tiene para poder excluir a cualquier persona o ente del conocimiento de su vida personal sino que, además, se incluye la posibilidad de controlar que aspectos de esta vida personal, puedan ser conocidos por otras personas. La intimidad ha ido ampliando y mezclando su concepto, incluye la definición de privacidad y ofrece una doble faceta:

- Por un lado, será el derecho que poseen las personas de poder excluir a las demás personas del conocimiento de su vida personal, es decir, sus sentimientos, sus emociones, sus datos biográficos y personales y su imagen.

2 Muchas veces puede verse escrito en las puertas: "privado". Éste es el uso anglosajón de la palabra, importado al castellano. "Privado" es el lugar o el ámbito de la vida al que la gente no tiene derecho a acceder, porque uno mismo lo impide. El ámbito de la "privacidad" en la que uno exige "intimidad" es, por tanto, personal y variable, pues unos exigen más intimidad que otros, pero dentro de ciertos límites objetivos, que son los que configuran el *derecho a la intimidad.*

- Por otro lado, además, será la facultad de determinar en qué medida esas dimensiones de la vida personal pueden ser legítimamente comunicadas o conocidas por otras personas.

Lo novedoso de esta nueva concepción de lo que es la intimidad viene dado por el hecho de que una persona tiene el derecho al control sobre cuándo y quién puede percibir diferentes aspectos de su vida personal, aspecto que, lógicamente, se concretan en la información o en sus datos personales.

Ya sabemos que la intimidad supone la no injerencia de terceros en la vida privada de una persona y el control que esa persona tiene para que determinados aspectos de su vida privada puedan ser conocidos por terceros. Ahora sólo hace falta saber como se hace efectivo este derecho.

La primera ley sobre protección de datos se redacta por el "Land" Alemán de Hesse el 7 de Octubre de 1.970. En cambio, el primer país que posee una legislación específica sobre protección de datos será Suecia, en 1973. En Estados Unidos se dictó la "Privacy Act" (Ley de Privacidad) en 1974.

En un rango normativo superior, la Constitución portuguesa de 1976 fue la primera Constitución en el mundo que limitó el uso de la informática para salvaguardar la intimidad: en su artículo 35 establece no solamente el derecho de acceso de los ciudadanos a los registros mecanográficos y la petición de su rectificación y actualización, sino que excluye la posibilidad de usar la informática para tratamiento de datos referentes a las convicciones políticas, fe religiosa o vida privada excepto cuando se tratare un de proceso de datos no identificables para fines estadísticos.

Muy poco más tarde, en 1978, la Constitución española también limitó el uso de la informática para preservar la intimidad de sus ciudadanos en el artículo 18.4 (el referido a intimidad y que ya recogimos antes): "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 a la que se refiere este apartado de nuestra Constitución se previó en la misma pero no se dictó hasta que no hizo falta. Lo que ocurrió cuando la informática, por la fuerza de la tecnología y el abaratamiento de los sistemas de proceso de la información (hardware y software) resultó tan potente que se hizo un peligro[3]. Esto sucedió en 1992, año en que se dictó la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de

3 Hay incluso películas, que hoy podemos considerar antiguas, antes consideradas de "ciencia ficción" y hoy auténticos clásicos del cine de profecía, que reflejan esta realidad. Así "2001, una odisea en el espacio", de Stanley Kubrick, y "La Red", sobre internet.

Carácter Personal ("LORTAD") que en su día fue muy contestada y recurrida ante el Tribunal Constitucional. Esta Ley ha sido sustituida por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal ("LOPD")[4], dictada con el 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[5].

También en el seno de la Unión Europea existen varias normas relativas a la protección de datos personales, entre las que podemos citar 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 (Directiva de Protección de Datos), y la Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones. Recientemente se ha aprobado la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas, (DOCE 201/2002 de 31-07-2002).

4 El Tribunal Constitucional se pronunció sólo parcialmente sobre la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal porque para cuando dictó sentencia estaba ya en vigor la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Fue en la sentencia 290/2000, de 30 de noviembre.

5 Artículo 1 de la Ley.

2

Datos de “Carácter Personal”

Hasta ahora hemos hablado de información en un concepto muy amplio y genérico. Pero debemos concretar qué se entiende por información. Podemos convenir que información es todo dato o conjunto de datos que transmiten un conocimiento en un proceso de comunicación entre un emisor y un receptor.

La noción sobre la que se basa el concepto de información es el dato (o conjunto de datos), y ello es lógico ya que la información, de una u otra manera, está en el dato (o conjunto de datos) que hace perceptible el concepto.

Por ello definiremos “dato” como aquel hecho o valor a partir del cual se puede inferir una conclusión o, como se define por la Real Academia de la Lengua Española, será el antecedente necesario para llegar al conocimiento exacto de una cosa o para deducir las consecuencias legítimas de un hecho.

Los datos informáticos constituyen uno de los valores más importantes de las empresas hoy en día debido a la generalización en el uso de los instrumentos informáticos. Las empresas deben inventariar estos activos y dotarlos de ciertas medidas de protección y seguridad, no sólo para el cumplimiento legal de ciertos requisitos sino también para asegurar accesos deliberados no consentidos de terceros. Siguiendo a D. Emilio del Peso Navarro, podemos clasificar los datos informáticos de la siguiente manera:

- Datos confidenciales: Son aquellos datos de difusión no autorizada. Su uso puede suponer un importante daño a la organización.
- Datos restringidos: Son aquellos datos de difusión no autorizada. Su utilización iría contra los intereses de la organización y/o sus clientes.

- Datos de uso interno: Son aquellos datos que no necesitan ningún grado de protección para su difusión dentro de la organización.
- Datos no clasificados: Son aquellos datos que no necesitan ningún grado de protección para su difusión.
- Datos de carácter personal: Son aquellos datos relacionados con la intimidad de las personas y son un tipo de datos específicos que legalmente deben ser protegidos.

2.1 Los datos "de carácter personal" y sus tipos

No entraremos a analizar los primeros cuatro tipos de datos expuestos al final del apartado anterior. Por el contrario, nos vamos a detener en lo que se entiende por dato de carácter personal o dato personal.

En líneas generales se entenderá por dato personal aquel dato inherente de una persona determinada, es decir, cualquier tipo de dato que permita conocer las características personales, en el sentido más amplio, de alguien.

Aparte de las opiniones particulares, la definición importante, no obstante, es la definición legal.

El artículo 2.a de 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 esos datos (en adelante "Directiva de 1995"), define el dato personal como:

> "*toda información sobre una persona identificada o identificable (...) se considerará identificable toda persona, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social*".

Este mismo concepto es el recogido por la legislación española sobre protección de datos y, así, en el artículo 3.a de la LOPD se define al dato personal como:

> "*cualquier información concerniente a personas físicas identificadas o identificables*".

2.2 Diversos tipos de datos personales

Conocido lo que es un dato personal nos parece conveniente señalar en este punto que, legalmente, hay varios tipos de datos personales y la clasificación se puede llevar a cabo según dos criterios:

- Según su importancia.
- Según su seguridad.

El primer criterio (según su importancia) clasifica a los datos personales en función de la relación que tienen esos datos personales con el derecho a la intimidad. Hay datos personales especialmente protegidos.

La relación de cuáles son esos datos especialmente protegidos está en los artículos 7 y 8 de la LOPD. Son precisamente a los que nos referíamos hace un instante, es decir, son los datos que tienen mayor relación con los aspectos más importantes del derecho a la intimidad. Así, "datos personales" son todos los datos personales que no están especialmente protegidos. Y "datos personales especialmente protegidos" son los referidos a la ideología, religión, creencias, afiliación sindical, salud, vida sexual, origen racial o étnico y comisión de infracciones penales o administrativas [(6)].

---

6 El artículo 7 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, dice así:

"1. De acuerdo con lo establecido en el apartado 2 del art. 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."

El segundo criterio de clasificación de los datos personales (según su seguridad), está basado en las medidas de seguridad que se deben cumplir cuando se posean datos personales.

Estas medidas de seguridad se encuentran previstas en el artículo 9 de la LOPD y se desarrollan en 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 (en adelante, Reglamento de Seguridad), del que posteriormente realizaremos una exposición más detenida, porque tiene una gran importancia práctica.

- Datos de nivel básico: Son aquellos datos personales que no se clasifiquen como de nivel medio atenuado, de nivel medio o de nivel alto.
- Datos de nivel medio atenuado: Aquellos datos personales que permitan obtener una evaluación de la personalidad del individuo.
- Datos de nivel medio: Aquellos datos personales relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros y prestación de servicios de información sobre solvencia patrimonial y crédito.
- Datos de nivel alto: Aquellos datos personales relativos a la ideología, religión, creencias, origen racial, salud, vida sexual y datos recabados para fines policiales sin consentimiento del interesado.

Es importante saber que los datos personales están altamente protegidos por la Ley. La utilización, no ya abusiva o fraudulenta, sino incluso negligente, de dichos datos es sancionable administrativamente con importantes multas y otro tipo de sanciones y está castigada como delito.

Para la protección del derecho a la intimidad en relación a los datos personales, en España, como en los demás estados del mundo occidental civilizado, es obligatorio el cumplimiento de una serie de requisitos legales que las entidades (públicas o privadas) que gestionan estos datos personales deben cumplir (sobre todo, medidas de seguridad para proteger dichos datos), y existen órganos administrativos especializados dedicados exclusivamente a velar por el cumplimiento de las normas protectoras al Derecho a la Intimidad en materia de datos personales. En España este órgano es la Agencia de Protección de Datos, a la que haremos referencia más adelante.

El Artículo 8 (“Datos relativos a la salud”) dice lo siguiente: “Sin perjuicio de lo que se dispone en el art. 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.”

3

La Ley Orgánica de Protección de Datos de Carácter Personal

3.1 ¿Cuándo se aplica la LOPD?

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, se aplica 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. Como ya hemos dicho, la Ley considera "dato de carácter personal" a cualquier información concerniente a personas físicas identificadas o identificables. Y protege estos datos en orden a su "tratamiento", que no es otra cosa que las operaciones y procedimientos técnicos de carácter automatizado o no que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

3.2 ¿Son iguales todos los datos de carácter personal?

No, como ya mencionamos en el apartado anterior, también en esto hay categorías. De entre todo el elenco de datos personales sobresalen un tipo de datos que la LOPD califica de "especialmente protegidos". Bajo nuestro punto de vista, son los más cercanos al derecho fundamental a la intimidad, en el sentido de que son los que más se aproximan al concepto de zona reservada de los individuos (puede no ser relativamente importante en relación a la intimidad que una entidad conozca el nombre de una persona, pero sí que es importante el que conozca que esa persona tiene una enfermedad crónica). Estos datos, como ya señaláramos anteriormente son los que se refieren a la ideología, religión,

creencias, afiliación sindical, salud, vida sexual, origen racial o étnico y comisión de infracciones penales o administrativas. El legislador trata a este tipo de datos de forma diferenciada ya que entiende que, en principio, todos los datos personales no deberían ser conocidos por nadie si el interesado no lo desea, pero estos datos aún en menor medida deben ser conocidos (a no ser que exista consentimiento del interesado o exista una necesidad de conocerlos para preservar otro derecho de nivel superior al de la intimidad, como pudiera ser el derecho a la vida en una situación médica urgente). Estos datos especialmente protegidos tienen un régimen jurídico especial que explicaremos en cada apartado de este libro, señalando las especialidades que les afectan.

3.3 ¿Se aplica la LOPD a todos los ficheros?

La LOPD considera "Fichero" todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso. Respecto de éstos, cualquier tratamiento de datos está limitado.

Pero no son "fichero" a estos efectos los ficheros que posean personas físicas en el ejercicio de actividades "exclusivamente personales o domésticas" (por ejemplo, los de una agenda electrónica o PDA), ni los "sometidos a la normativa sobre protección de materias clasificadas" (por ejemplo, los secretos del CESID). Tampoco entran dentro del ámbito de la LOPD los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada, aunque el Ministerio del Interior debe comunicar su existencia y su finalidad a la Agencia de Protección de Datos.

Tampoco entran dentro del ámbito de la LOPD, aunque se encuentran protegidos por otro tipo de legislación, muchos ficheros de las Administraciones Públicas: los ficheros regulados por la legislación de régimen electoral (sobre todo, el censo), los que se utilicen para fines estadísticos y están amparados por la legislación sobre la función estadística pública, los que almacenen datos en informes personales de calificación que se encuentran amparados por la legislación del Régimen del personal de las Fuerzas Armadas, los del Registro Civil, el Registro Central de penados y rebeldes, los que contengan imágenes y sonidos obtenidos de videocámaras de las Fuerzas y Cuerpos de Seguridad del Estado y se encuentren amparados por su legislación específica, etc.

Para los efectos de este libro, estos ficheros dan igual porque este libro se refiere al público en general, no a las Administraciones Públicas y, por tanto, no tratamos el régimen jurídico de los ficheros de titularidad pública.

3.4 ¿Qué tipo de soportes? ¿También a los ficheros en papel?

En teoría, la LOPD se aplica tanto a los datos personales registrados en soporte físico que los haga susceptible de tratamiento como a toda modalidad de uso posterior de los datos personales llevados a cabo por los sectores público y privado. Una de las grandes diferencias con la anterior legislación (LORTAD) era que únicamente era de aplicación al tratamiento automatizado (informático) de datos personales. La LOPD es de aplicación a todo tipo de tratamiento (no sólo informático), aunque en la práctica no es del todo así, como podrá verse en el apartado siguiente.

3.5 ¿Desde qué día es obligatoria?

Sin embargo, la obligatoriedad de declarar los "ficheros en papel" es inexistente en la práctica, porque los ficheros no automatizados deben adaptarse a la LOPD para el 24 de octubre del 2007[7].

Para los efectos de lo que ahora importa, procede señalar que los ficheros automatizados (en soporte informático) creados con anterioridad al 14 de enero del 2000 (que es la fecha de entrada en vigor de la LOPD), deben adecuarse a la LOPD antes del 14 de enero del 2003.

7 Según la Disposición Final Primera de la LOPD

4

La Legítima Toma de Posesión de los Datos

4.1 La recogida de los datos

No se pueden recoger datos personales "porque sí". Sólo se pueden recoger datos personales *mediando determinadas circunstancias*. La primera de todas, que es una declaración de principios establecida por la Ley, es que sólo se pueden recoger para su tratamiento datos "de calidad": datos que sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido[8]. Es éste un criterio muy general pero que sirve para conocer los criterios en que la Ley se basa. Los datos no se pueden obtener indiscriminadamente por el puro placer de obtenerlos, por mero comercio. Pueden recabarse, sí, pero en un contexto adecuado, mediando buena fe por parte de quien los obtiene.

Piénsese el caso, por ejemplo, de recoger los datos de "Nombre", "Apellido", "Domicilio", "Número de Identificación Fiscal", "Cuenta Bancaria" y "Estado Civil" de una persona cuando esa persona decide comprar un electrodoméstico. La finalidad de recoger estos datos personales en este supuesto parece claro, es decir, pueden ser útiles para la entrega del electrodoméstico comprado en el domicilio de la persona, también pueden ser adecuados para la realización de la factura o como datos contables para el vendedor. No obstante, existe un dato ("Estado Civil") que no tiene relación alguna con las finalidades expuestas, por lo que consideramos que este datos es inadecuado, no pertinente y excesivo en relación con la finalidad de la recogida.

8 Artículo 4 de la LOPD.

4.1.1 La información a los interesados durante la recogida de datos

Se considera "afectado" o "interesado" a la persona física titular de los datos personales que sean objeto del tratamiento.

Los interesados a los que se soliciten datos personales deben ser previamente informados de modo expreso, preciso e inequívoco, 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.

Por ejemplo, es lo más habitual advertir de que los datos que se dan en una encuesta serán incorporados a un fichero de carácter personal, y de que, por tanto, pueden responder o no responder.

Debe informarse del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas y las consecuencias de la obtención de los datos o de la negativa a suministrarlos[9].

En la www esto suele tener lugar señalando en rojo, o en otro color, qué datos son imprescindibles en la contestación, indicándose por ejemplo que, de no suministrarse el dato del número de la tarjeta de crédito, no se admite otro medio de pago, y por tanto no hay contrato.

También se debe dar a conocer la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición, de los que nos ocuparemos más adelante, así como de la identidad y dirección del responsable del tratamiento o, en su caso, de su representante[10].

Es de notar que normalmente este último requisito (identificar al responsable del fichero) es algo que se olvida.

En los cuestionarios u otros impresos debe hacerse figurar, en forma claramente legible, las mencionadas advertencias.

Si los datos de carácter personal no se obtienen directamente del interesado sino de otra fuente, el interesado debe ser informado de forma expresa, precisa e inequívoca por el responsable del fichero o su representante, dentro de los tres

---

9 Como se prevé en la Ley que no es necesario informar del derecho de rectificación y otros 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, a veces hay quien omite este trámite. No es aconsejable.

10 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, se debe designar, salvo que tales medios se utilicen con fines de trámite, un representante en España. Todo ello sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.

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 y de todo lo demás que hemos señalado, salvo que 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.

En la práctica, esto obliga a consultar a la Agencia de Protección de Datos. No se puede soslayar esta obligación.

Tampoco hay obligación de comunicar cuando los datos proceden de fuentes accesibles al público y se destinan 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.

4.1.2 El consentimiento del afectado

Vale como consentimiento manifestado por el interesado toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.

Para que se pueda realizar el tratamiento de los datos de carácter personal se requiere el consentimiento inequívoco del afectado. No es preciso, sin embargo, cuando se refieran a las partes de un contrato o precontrato de una relación negocial o laboral y sean necesarios para su mantenimiento o cumplimiento, 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.

El consentimiento puede ser revocado por el interesado cuando exista causa justificada para ello, sin efectos retroactivos. Y además éste, 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, puede oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero está obligado a excluir del tratamiento los datos relativos al afectado.

4.1.3 Recogidas prohibidas

Está prohibida la recogida de datos por medios fraudulentos, desleales o ilícitos. Es una prohibición muy general pero que con un poco de sentido común resulta fácil de concretar.

Por ejemplo, está prohibido recoger datos personales obligando al interesado por la fuerza a prestarlos: "sugiriendo" a los trabajadores de una empresa que los cedan revistiendo el hecho de "recogida de firmas" contra el SIDA, etc.

Pero hay una cosa clara: determinados datos están además **especialmente protegidos, también para su recogida**. Cuando se trata de solicitar datos que puedan tener cualquier relación, por remota que sea, con la ideología, religión o creencias, o afiliación sindical, es una obligación legal recabar de modo expreso y por escrito el consentimiento del afectado para el tratamiento de sus datos[11], y además debe advertirse igualmente de modo expreso que tiene derecho a no prestar su consentimiento.

Por ejemplo, cuando se solicita para una encuesta para la venta de libros de texto si prefiere tal o cual marca por motivos ideológicos, deben hacerse constar las referidas circunstancias.

Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo pueden ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley, que para las empresas no existe, o el afectado consienta expresamente.

Por tanto, si una empresa dedicada a la venta de medicamentos realiza una encuesta a sus pacientes de cuáles son sus enfermedades y desea que esos datos formen parte de un fichero informático, deberá solicitar a éstos el consentimiento expreso y por escrito. De otra forma, no podrá tratar esos datos.

En fin, los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo pueden ser incluidos en ficheros de las Administraciones Públicas competentes y, aún así, sólo en los supuestos previstos en las respectivas normas reguladoras.

Por ejemplo, una aseguradora, aunque tenga interés en saber cuáles de sus asegurados han sido condenados por alcoholemia al volante, no puede incluir estos datos en sus ficheros ya que es un delito. Tendrá que aprenderlo de memoria.

Hay una excepción. Entre todos los datos antes mencionados pueden ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias, origen racial, salud y vida sexual, cuando sea necesario para la prevención o para el diagnóstico médicos, la prestación de

11. 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.*

asistencia sanitaria o tratamientos médicos, o la gestión de servicios sanitarios[12]. Pero aun entonces hay una limitación: 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[13].

Nadie sabe qué es "profesional sanitario" ni quien tiene una "obligación equivalente" de guardar secreto. En nuestra opinión, puede ser un licenciado, un ATS o un auxiliar de enfermería, porque todos están obligados a guardar secreto. Es ésta una de las inconcreciones sublimes de la Ley.

4.2 La creación de ficheros

Pueden crearse todos los ficheros privados que contengan datos de carácter personal que sean necesarios para el logro de la actividad u objeto legítimos de la persona, empresa o entidad titular, siempre que se respeten las garantías que vamos a mencionar. Pero está prohibido crear ficheros 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.

Para la creación del fichero debe seguirse este procedimiento: toda persona o entidad que quiera crear un fichero que contenga datos de carácter personal debe notificarlo previamente a la Agencia de Protección de Datos, cuyo Registro General inscribe el fichero. Si falta algún dato en la solicitud, se pide al interesado que complete los datos que faltan o subsane lo que proceda. Transcurrido un mes desde la presentación de la solicitud de inscripción sin que la Agencia de Protección de Datos haya resuelto, el fichero queda inscrito a todos los efectos.

12 Los datos sobre la salud no son tan secretos, cuando quien accede al dato o su tratamiento es un médico, en pro de la salud del enfermo o de la sanidad general. Las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes pueden tratar 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.*

13 Lo que también vale para cuando el dato 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. En este caso no se necesita que el tratamiento lo realice "profesional sanitario".

5

Durante la Posesión de los Datos

5.1 Obligaciones del responsable

El "responsable del fichero", también llamado "responsable del tratamiento", es la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decide sobre la finalidad, contenido y uso del tratamiento.

5.1.1 Obligación de seguridad

El responsable del fichero y, en su caso, el encargado del tratamiento,[14] tienen que velar por la seguridad de los datos. Para ello deben 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.

En la práctica, esta obligación da lugar a que no se puedan registrar datos de carácter personal en ficheros que no reúnan las condiciones que se han determinado por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas. Por Reglamento se han establecido además requisitos y condiciones ulteriores que deben reunir los ficheros de clase "A" y las personas que intervengan en el tratamiento de los datos, en particular los datos .

14 Es "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.

5.1.2 Deber de secreto y de utilización legítima

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**. Estas obligaciones no terminan con el "borrado" del fichero, sino que subsisten aún después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo. Además, los datos de carácter personal objeto de tratamiento no pueden usarse para fines incompatibles con aquéllos para los que los datos hubieran sido recogidos[15]. El uso que la entidad que gestiona con datos personales da a los mismos es otra de las cuestiones fundamentales. Ya dijimos que los datos deben ser adecuados, pertinentes y no excesivos en relación a las finalidades concretas para los que se hayan obtenido. Por tanto, si se desean recoger datos personales, se debe informar que éstos son para unas determinadas finalidades y no recogerlos para una y utilizarlos para otra. Además, queremos recordar que esta actuación (tratar los datos con una finalidad diferente a la inicial) podría considerarse una infracción muy grave por "recoger los datos en forma engañosa y fraudulenta" que lleva aparejada una sanción de 300.000 a 600.000 euros, aproximadamente.

En nuestro ejemplo anterior de la compra del electrodoméstico supóngase que los datos recogidos, con las finalidades antes expuestas, son utilizados para el envío de publicidad no solicitada al domicilio del comprador. Es decir, se solicitaron unos datos con una finalidad lícita y posteriormente son utilizados con otra finalidad.

5.1.3 Permitir el derecho de acceso de los interesados a sus datos y a su rectificación

Una vez creado el fichero y obtenidos los datos, incluso si ha mediado consentimiento del interesado para el tratamiento, los interesados tienen derecho a acceder a sus propios datos. Por eso, los datos de carácter personal deben almacenarse de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados. Los interesados tienen derecho a solicitar y obtener *gratuitamente* información de sus datos de carácter personal sometidos a tratamiento; sobre cuál sea el origen de dichos datos y sobre las comunicaciones realizadas o que se prevén hacer de los mismos. Repetimos que esta actividad es gratuita: no se puede exigir contraprestación alguna por el ejercicio de los derechos de oposición, acceso, rectificación o cancelación. Esta información puede obtenerse mediante la mera consulta de los datos, por medio de su visualización, o mediante la indicación de los datos que son objeto de tratamiento por medio

15 No se considera incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.

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.

Para que los interesados no se pasen la vida interfiriendo en las organizaciones, este derecho de acceso sólo puede ser ejercitado a intervalos que no sean inferiores a doce meses, salvo que se acredite un interés legítimo al efecto, en cuyo caso podrán ejercitarlo antes.

Además de los interesados, cualquier persona puede conocer la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento, recabando a tal fin la información oportuna del Registro General de Protección de Datos de la Agencia de Protección de Datos. Este Registro es de consulta pública y gratuita.

El interesado, como dueño de los datos, puede obligar al responsable del tratamiento a que haga efectivo el derecho de rectificación o cancelación en el plazo de diez días si su tratamiento no se ajusta a lo dispuesto en la LORTAD; en particular, cuando resulten *inexactos o incompletos*. La cancelación da lugar al bloqueo de los datos, conservándose éstos 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. Si los datos rectificados o cancelados hubieran sido comunicados previamente a un tercero, el responsable del tratamiento debe notificar la rectificación o cancelación ya efectuada a quien se hayan comunicado, en el caso de que éste mantenga el tratamiento deberá también proceder a la cancelación.

Para ejercitar el derecho de oposición, acceso, así como los de rectificación y cancelación, el procedimiento ha sido establecido reglamentariamente. Se recoge en una Instrucción de la Agencia de Protección de Datos antes señalada. Así, el procedimiento será el siguiente:

- Se deberá remitir una solicitud al responsable del fichero en la que contenga lo siguiente:
    - Nombre, apellidos y fotocopia del DNI del interesado.
    - Petición en que se concreta la solicitud, en este caso ejercitar el derecho de acceso.
    - Domicilio del solicitante a efectos de notificaciones.
    - Fecha.
    - Firma del solicitante.

- Respecto a la forma de acreditar el envío de la solicitud del derecho de acceso, el interesado deberá utilizar cualquier medio que permita acreditar el envío y la recepción de la solicitud. Respecto a este medio, el que mejor cumple este requisito es el bureau-fax, aunque una carta certificada también podría entenderse que cumple con este mandato.

- En cualquier caso, el responsable del fichero deberá contestar a esta solicitud y le indicará qué datos personales posee del solicitante o, por el contrario, si no posee datos personales de él. Esta contestación deberá producirse en un mes desde la recepción de la solicitud. No obstante, en el caso de que se estime el derecho de acceso (es decir, el responsable posee datos del solicitante), éste se deberá materializar en diez días desde que se notifica la solicitud.

Si por la razón que fuere, el interesado y el responsable del fichero no se ponen de acuerdo, el interesado puede presentar reclamación ante la Agencia de Protección de Datos en la forma que estudiamos más adelante. En síntesis, el interesado al que se deniegue total o parcialmente el ejercicio de los derechos de oposición, acceso, rectificación o cancelación, puede ponerlo en conocimiento de la Agencia de Protección de Datos que debe asegurarse de la procedencia o improcedencia de la denegación, dictando resolución expresa de tutela de derechos en el plazo de seis meses. Contra las resoluciones de la Agencia de Protección de Datos cabe recurso ante los tribunales.

Los interesados que sean objeto de un tratamiento de sus datos que incumpla la LOPD y además sufran daño o lesión en sus bienes o derechos, tendrán derecho a ser indemnizados, ejercitándose la acción ante los órganos de la jurisdicción ordinaria.

5.1.4 Deber de conservación y puesta al día de los datos

Los datos de carácter personal deben 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.

El responsable del fichero no sólo está obligado a conservarlos sino también a que éstos sean exactos y estén puestos al día de forma que respondan con veracidad a la situación actual del afectado.

Cómo debe cumplirse esta obligación es una cuestión muy discutible. En realidad el primer interesado es el titular del fichero puesto que no colecciona datos por placer, sino porque los necesita para su actividad o trabajo. Por tanto, como toda otra herramienta, si no está afilada no tiene utilidad.

En nuestro ejemplo, piénsese el caso que nuestro comprador vuelve a comprar otro electrodoméstico al día siguiente pero informa al vendedor que su domicilio ha cambiado. El vendedor deberá cambiar el dato "Domicilio" ya que, según está recogido en su fichero, no es exacto.

Los datos no pueden ser conservados de forma que se permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados.[16]

Si los datos de carácter personal registrados resultaran ser inexactos en todo o en parte o incompletos, deben ser cancelados y sustituidos por el propio responable del fichero desde el momento en que tenga noticia del error, incorporando los correspondientes datos rectificados o completados. Sin perjuicio del derecho del propio interesado a promover la rectificación.

En el ejemplo del electrodoméstico suponemos que la finalidad para la recogida de los datos es el envío del bien al domicilio del comprador. Una vez que éste haya recibido su compra, en principio, la finalidad que motivó el envío del electrodoméstico ha concluido por lo que deberían ser cancelados.

Se han de cancelar ("borrar") los datos que hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

5.1.5 Cómo conservar y tratar los datos

La conservación y tratamiento de los datos depende del tipo de datos de que se trate. Los datos pueden ser de nivel básico, medio atenuado, medio y alto. Señalamos a continuación las medidas que deben adoptarse.

Medidas de nivel básico

El artículo 4.1 del Reglamento de Seguridad establece que **todos** los ficheros que contengan datos de carácter personal deberán adoptar las medidas de seguridad calificadas como de nivel básico. Con ello se pretende que cualquier dato de carácter personal esté protegido con ciertas medidas de seguridad. Las de nivel básico se encuentran recogidas en el Capítulo II del Reglamento de Seguridad (artículos 8-14) y en el artículo 7. En concreto estas medidas de seguridad son las siguientes:

16 Reglamentariamente se ha determinado el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos, se puede llegar a decidir el mantenimiento íntegro de determinados datos.

Ficheros temporales

Los Ficheros temporales deben cumplir el nivel de seguridad que les corresponda con arreglo a los demás criterios señalados en el Reglamento, y deben ser borrados una vez que hayan dejado de ser necesarios para los fines que motivaron su creación. Vulgarmente se entiende por "fichero temporal" aquel fichero, distinto del original y creado por la aplicación informática que lo gestiona, cuya finalidad es un procesamiento paralelo de los datos originales sin afectar al fichero original, y/o con la finalidad de copia de seguridad temporal ante una parada anormal del sistema. Es lo que denominamos fichero temporal creado por la aplicación. Usualmente, los programadores los apellidan "tmp". Pero la acepción legal, viene dada por el mencionado artículo 7 del Reglamento de Seguridad y por el artículo 3.b de la LOPD que definen el fichero temporal como todo conjunto organizado de datos, independientemente de su forma o modalidad de creación, almacenamiento, organización o acceso, y que fue creado para un espacio determinado de tiempo que variará en función de la finalidad para la que se creó ese fichero. Parece obvio que un fichero temporal creado por la aplicación caería dentro del ámbito conceptual de fichero temporal legal. Por lo mismo, cuando un programa se utiliza para tratar datos personales debe proceder también al borrado del fichero temporal una vez que haya cesado el fin que motivó su creación. Hecho que, generalmente ocurre automáticamente. Pero dentro del concepto de fichero temporal en su versión legal, entendemos que también cabría incluir un fichero creado manualmente para una concreta finalidad y que contiene datos que han sido obtenidos de un fichero matriz. Una vez terminada esa finalidad, se procedería al borrado, también manual, de ese fichero.

En definitiva, con la medida de seguridad del artículo 7 del Reglamento de Seguridad se pretende *que no exista una gestión paralela, a través de un fichero temporal, de datos personales, obtenidos de un fichero original o matriz.* En caso de que exista la mencionada gestión paralela, ésta únicamente podría ser llevada a cabo para una finalidad concreta dentro de un espacio determinado de tiempo y siempre cumpliendo las medidas de seguridad definidas para el fichero original o matriz. Además, tenemos que señalar que dentro de las gestiones que se pueden realizar con ese fichero temporal, únicamente se permitiría la consulta de datos ya que, por ejemplo, si se introdujeran nuevos datos que no provinieran del fichero original o matriz, ello implicaría que ese fichero temporal fuera considerado como un nuevo fichero y, por tanto, sujeto a todos los requisitos legales, no sólo en cuanto a medidas de seguridad, que se establecen en la LOPD.

Los "Documentos de seguridad"

Es un punto fundamental. Se trata de un documento privado pero de acceso público en el que se señalan las políticas de seguridad que se seguirán por quienes traten datos personales. No debe confundirse con un documento "informático". Aquí se utiliza la palabra "documento" en el sentido más clásico de la expresión.

La idea es que el responsable del fichero, normalmente una empresa, esté obligada a personalizar el uso que va a hacer de los datos personales elaborando e implantando un documento que, una vez asumido, será de obligado cumplimiento para el personal con acceso a los datos automatizados de carácter personal y a los sistemas de información. Este documento deberá contener los "mínimos" que se seguirán en la política de seguridad de la empresa, y por tanto al menos los siguientes aspectos:

a) Ámbito de aplicación del propio 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 incidencias.

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

Este documento debe mantenerse en todo momento actualizado y ha de revisarse siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo. Su contenido debe adecuarse en todo momento a los cambios normativos en materia de seguridad de los datos de carácter personal.

Responsable del fichero

Es la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decide sobre la finalidad, contenido y uso del tratamiento. En definitiva, la entidad que gestiona datos personales.

El responsable del fichero tiene la obligación de realizar un documento llamado "Documento de seguridad" en el que se establecerán diferentes medidas de seguridad. Estas medidas de seguridad tienen que ser cumplidas obligatoriamente por las personas que acceden a datos personales y por los sistemas informáticos que gestionan estos datos.

Personas con acceso a los datos de carácter personal

Las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y a los sistemas de información deben estar claramente definidas y documentadas en el documento de seguridad.

El responsable del fichero debe adoptar 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.

Como ya hemos señalado, el instrumento donde deben recogerse las funciones y obligaciones es el documento de seguridad. Respecto a cómo deben ser conocidas por el personal, el Reglamento de Seguridad no se pronuncia al respecto. Se otorga libertad a la entidad que posee datos personales para que establezca un mecanismo de conocimiento. En la práctica hay varias opciones, desde la firma de un documento por parte del personal en el que se recojan sus funciones y obligaciones respecto al tratamiento de datos personales y su acatamiento a las mismas, hasta la disposición del documento de seguridad (en el que se incluyen estas funciones y obligaciones) en un lugar de libre acceso al personal de la empresa. Aunque lo cierto es que, a nuestro entender, cualquier mecanismo sería válido siempre y cuando permitiera conocer estas funciones y obligaciones. Nos parece que la firma de un documento por parte del personal (vía contrato laboral o vía acuerdo de confidencialidad autónomo), es el mecanismo más correcto para permitir conocer las funciones y obligaciones relativas a los datos personales.

Para finalizar, hemos de señalar que ésta es una medida eminentemente jurídica que intenta evitar, en la medida de lo posible, un incorrecto o ilegal tratamiento o gestión de los datos personales por parte de la plantilla de la empresa que posee datos de carácter personal.

Registro de incidencias

Esta medida se encuentra en el artículo 10 del Reglamento de Seguridad que establece que “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.”

Antes de señalar los aspectos más característicos de esta medida hemos de indicar que por incidencia, según el artículo 2.9 del Reglamento de Seguridad, se entiende “cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos”. Vemos por tanto que el legislador ha optado por un concepto amplio de incidencia, dejando la descripción de la misma abierta a las empresas. Por otro lado, debemos señalar que este concepto de incidencia no se refiere únicamente a cuestiones informáticas (malfuncionamiento de sistemas, por ejemplo), sino que también a otras cuestiones reflejadas en el documento de seguridad (pérdida de contraseñas, por ejemplo).

Esta medida viene a reflejar lo siguiente:

- Deberá existir un procedimiento de notificación de incidencias relativo a los datos de carácter personal. La descripción del procedimiento estará en manos de cada entidad en concreto. No obstante, habrá una serie de cuestiones que son obligatorias:
    - Tipo de incidencia.
    - Momento en que se ha producido.
    - Persona que la notifica.
    - A quien se comunica.
    - Efectos derivados de la incidencia.
- Deberá existir un registro de las incidencias que se han producido. En el registro deberán recogerse obligatoriamente las mismas cuestiones señaladas en el párrafo anterior.

A continuación procederemos a comentar algunos aspectos de esta medida. En primer lugar, y por lo que se refiere a los tipos de incidencia, el Reglamento de Seguridad no define los tipos de incidencia que se pueden detectar. Así, bajo nuestro punto de vista, los entes que gestionen datos personales deberán identificar las incidencias que pudieran surgir con mayor habitualidad y, de este modo, clasificarlas. No obstante, creemos necesario no cerrar el campo de las incidencias y dejar una de tipo abierto para cualquier otra incidencia que pudiera surgir y que no se encuentre clasificada. Por ejemplo, se podría clasificar este tipo de incidencia abierta como “Otras incidencias”.

Respecto al momento en que se ha producido la incidencia, entendemos que lo que realmente ha deseado el legislador es señalar el momento en que se ha detectado.

Para terminar con el análisis de esta medida y en lo relativo a los efectos derivados de la incidencia, entendemos que no sólo se deben especificar los aspectos negativos de la misma, sino también, y en caso de ser posible preverlos, los efectos correctores que se han implantado para solucionar la mencionada incidencia.

En definitiva, con esta medida se pretende, bajo nuestro punto de vista, reflejar los posibles defectos que se detecten en la implantación y el funcionamiento de las medidas de seguridad para su correcta solución y, en su caso, puesta en marcha.

Identificación y autenticación

La presente medida de seguridad viene establecida por el artículo 11 del Reglamento de Seguridad que señala lo que a continuación procedemos a reproducir:

"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 en forma ininteligible."

Por lo tanto, el examen que podemos realizar de esta medida es el siguiente:

- Los usuarios que accedan al sistema de información deben estar claramente identificados. Al respecto, se entiende por sistema de información, en virtud del artículo 2.1 del Reglamento de Seguridad, al "conjunto de ficheros automatizados, programas, soportes y equipos empleados para el almacenamiento y tratamiento de datos de carácter personal". El listado de estos usuarios se deberá contener en el documento de seguridad.
- Se prevé la existencia del sistema tradicional de identificación y autenticación. Así, la identificación se haría por "Nombre de usuario" y la autenticación por contraseña. Este sistema no es obligatorio y podrían implantarse otros, como por ejemplo, la identificación y autenticación mediante tarjeta criptográfica, mediante tarjeta con banda magnética o basada en parámetros biométricos.
- Si se opta por la identificación y autenticación tradicional (Nombre de usuario y Contraseña) se deberá especificar un mecanismo, que se recogerá en el documento de seguridad, de asignación, distribución y almacenamiento ininteligible de las contraseñas. Además, las contraseñas deberán ser cambiadas con la periodicidad que se recoja en el documento de seguridad.

De lo recogido en esta medida de seguridad, lo que a nuestro entender es más complejo de determinar es el concepto del almacenamiento de forma ininteligible. Este último concepto significa que se debe almacenar las

contraseñas de tal forma que no se puedan entender. Y esto puede ser llevado a cabo por medios informáticos, lo que parece lo más lógico hoy en día, o por medio no informáticos (piénsese en un almacenamiento de las contraseñas en un sobre lacrado y guardado en una caja de seguridad).

En definitiva, con esta medida se pretende tener identificados claramente a los usuarios que acceden, tratan o gestionan datos personales y evitar, asimismo, el acceso no autorizado por parte de terceros a datos de carácter personal del ente que los gestiona.

Control de acceso:

La presente medida de seguridad legal viene definida por el artículo 12 del Reglamento de Seguridad que establece lo siguiente:

"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 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 datos y recursos, conforme a los criterios establecidos por el responsable del fichero."

Los aspectos más significativos de esta medida son los siguientes:

- El personal que acceda a datos personales sólo podrá acceder a aquellos datos que sean necesarios en el ejercicio de sus funciones. (Por ejemplo, una persona del área de Recursos Humanos no tendría derecho a acceder a datos personales contables concernientes a clientes de su compañía).

- Se deben establecer mecanismos que eviten que un usuario pueda acceder a datos a los que no debería tener acceso. Estos mecanismos deben recogerse en el documento y generalmente son elementos informáticos, tales como control de acceso directo, grupos de usuarios o perfiles, en definitiva, son técnicas de administración de sistemas.

- En el listado de usuarios que señalábamos en la medida anterior, se deben especificar, por cada usuario, los datos personales a los que accede. Esta medida puede ser llevada a cabo, bajo nuestra perspectiva, de diferentes maneras, desde señalar específicamente los datos a los que accede el usuario, hasta especificar el tipo de perfil, por ejemplo, que posee un usuario.

- Cada usuario tendrá el derecho a consultar, alterar o anular los datos a los que tiene acceso, en función de las directrices marcadas en el documento de seguridad sobre esta materia. En este sentido también existen herramientas informáticas, para establecer los derechos de consulta, alteración o anulación de datos personales. Estas técnicas son las mismas que administran el acceso a los datos personales, es decir, son las técnicas de administración de sistemas.

En definitiva, con esta medida, como su nombre indica, se pretende controlar y gestionar el acceso al sistema de información que contiene los datos de carácter personal.

Gestión de soportes

La penúltima medida de seguridad de nivel básico se encuentra recogida en el artículo 13 del Reglamento que, a continuación, procedemos a transcribir:

"*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."

Previamente a examinar lo que señala este artículo hemos de realizar una serie de aclaraciones. Por soporte informático, según el artículo 2.10 del Reglamento de Seguridad se entiende a cualquier "objeto físico susceptible de ser tratado en un sistema de información y sobre el cual se puedan grabar o recuperar datos". Con esta definición legal parece claro que un CD- ROM, una cinta de back-up o un disquete, entre otros, son soportes informáticos. La pregunta que en este punto nos realizamos es si un ordenador, un servidor o un portátil se consideran un soporte informático. En un sentido estricto y fijándonos en la definición anterior parece que la respuesta es negativa ya que, en si mismos, no serían soportes sino más bien los sistemas que los tratan. No obstante, en un ordenador, en un servidor o en un portátil si que existe un soporte, su disco duro, sobre el que se pueden grabar o recuperar datos. En definitiva, desde nuestro punto de vista y, según lo expresado en el presente párrafo, soporte será tanto un CD-ROM, una cinta de back-up o un disquete, como un ordenador, un servidor o un portátil.

Lo característico de esta medida de seguridad es lo siguiente:

- Los soportes que contengan datos personales deberán permitir especificar el tipo de información que contienen. Creemos que la mejor forma de identificación de estos soportes será a través de etiquetas identificativas que, si bien no nos van a permitir conocer directamente cuáles son los datos concretos que se contienen en ellos, si que nos van a permitir conocer indirectamente estos datos. Por ejemplo si una cinta de back-up posee una etiqueta que señala "Copia de la BBDD XXXX del día 01-01-2002", indirectamente sabremos que el mencionado soporte contiene los datos de la BBDD XXXX.

- Los soportes que contienen datos personales deberán estar inventariados correctamente.

- Los soportes que contienen datos personales deberán ser almacenados en un lugar en el que únicamente las personas que se especifiquen en el documento de seguridad puedan tener acceso. Este lugar, por ejemplo, puede ser un armario cerrado con llave que es controlado por un número determinado de personas o una habitación cerrada con llave a la que únicamente tendrá acceso un número determinado de personas.

- La salida de soportes informáticos fuera del lugar habitual donde se ubique el fichero que contiene esos datos personales deberá ser debidamente autorizada. Con esta medida lo que se pretende es establecer un procedimiento o un régimen de salidas de soportes para evitar una cesión no consentida de datos personales.

Copias de respaldo y recuperación

La última medida de nivel básico se encuentra recogida en el artículo 14 del Reglamento de Seguridad que señala lo siguiente:

"1. El responsable del fichero se encargará de verificar la definición y correcta aplicación de los procedimientos de realización de copias de respaldo y de recuperación de 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 periodo no se hubiera producido ninguna actualización de los datos."

Las cuestiones más características de este apartados son las siguientes:

- Se debe establecer a través del documento de seguridad un procedimiento de realización de copias de respaldo y de recuperación de los datos.
- Estos procedimientos señalados en el punto anterior deberán garantizar la reconstrucción de los datos en el estado en el que se encontraban los mismos en el momento en que se perdieron o destruyeron por cualquier motivo.
- Las copias de respaldo deberán realizarse periódicamente. En principio, existe libertad para especificar cada cuanto se deben realizar estas copias. No obstante, se ha establecido que una vez semanalmente se tienen que realizar copias de seguridad, excepto en el caso de que no hayan sido actualizados datos del fichero.

En relación con esta medida de seguridad y con la referida al procedimiento de notificación, gestión y registro de incidencias, debemos establecer que, cuando sea necesaria la restauración de datos, es preciso iniciar el procedimiento de gestión ante incidencias recogido en el documento de seguridad.

En definitiva, con esta medida se pretende tener en todo momento los datos personales actualizados y adecuados a la realidad.

Medidas de nivel medio atenuado

Estas medidas de seguridad no se encuentran específicamente reguladas en el Reglamento de Seguridad, sino que se hayan recogidas dentro del epígrafe que regula las medidas de seguridad de nivel medio.

El artículo 4.4 del Reglamento de Seguridad establece lo siguiente:

"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."

Por tanto, podemos observar que este nivel de seguridad se aplicará a datos personales que permitan obtener una evaluación de la personalidad del titular legítimo de esos datos. Un ejemplo de este tipo de datos se encontraría en los ficheros de los departamentos de Recursos Humanos que alberguen diferentes informaciones personales provenientes de entrevistas.

Por último, y antes de entrar a analizar las medidas de seguridad específicas, debemos recordar que este tipo de datos personales (los que permiten

obtener una evaluación de la personalidad del individuo), no sólo deben cumplir con las medidas de seguridad que vamos a proceder a exponer a continuación, sino también con las medidas de nivel básico.

Auditoría

El artículo 17 del Reglamento de Seguridad señala lo siguiente:

"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 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."

Los aspectos mas relevantes de esta medida de seguridad son los siguientes:

- Al menos bianualmente deberá realizarse una auditoría de seguridad que analice las siguientes cuestiones:
    - El cumplimiento que la entidad que posee datos personales realiza de las medidas descritas en el Reglamento de Seguridad.
    - La adecuación a la realidad de las diferentes normas y procedimientos recogidos en el documento de seguridad.
- La auditoría, como no podía ser de otra manera, finalizará con un informe que abarque al menos los siguientes puntos:
    - Adecuación de las medidas y de los controles implantados en la entidad referidos a la seguridad de los datos personales, respecto al Reglamento de Seguridad.
    - Identificar las deficiencias encontradas en la labor auditora y, en su caso, proponer las medidas necesarias para paliar las mencionadas deficiencias.
    - Especificar las diferentes evidencias derivadas de la labor auditora sobre las que se basen los dictámenes y recomendaciones propuestas.

- El informe de auditoría deberá ser analizado por la compañía, quien deberá adoptar las medidas correctoras de las deficiencias encontradas.

- El informe de auditoría deberá estar disponible a la Agencia de Protección de Datos (entidad administrativa que se encarga de la vigilancia de la Legislación sobre Protección de Datos de la que más adelante haremos mención).

En definitiva, hemos de señalar que la inclusión de esta medida de seguridad en el Reglamento de Seguridad viene motivada dado que no sólo se deben implementar las diferentes medidas de seguridad en el ente que gestiona los datos personales, sino que también debe establecerse una serie de medidas de control (a través de la auditoría) que reflejen la adecuación de las medidas implantadas respecto a la seguridad de los datos personales.

Medidas adicionales de identificación y autenticación

El artículo 18 del Reglamento de Seguridad establece lo que a continuación procedemos a reproducir:

"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."

Esta medida, intenta reforzar la medida de identificación y autentificación recogida para el nivel básico. A lo dicho en aquel apartado debemos añadir lo siguiente:

- Todo usuario que acceda al sistema de información que gestiona los datos, deberá estar identificado personal e inequívocamente, además de verificar que está autorizado para acceder a dicho sistema. La diferencia o, reflejado de otra manera, lo adicional de esta medida con respecto a su análoga del nivel básico, es que mientras que ésta última sólo exigía el establecimiento de mecanismos de identificación sin especificar cuáles así como tener un listado actualizado de personas que acceden a los datos (por ello, sería posible, por ejemplo, establecer un "Nombre de usuario" a un grupo determinado de personas), en la medida de seguridad de nivel medio atenuado se exige que cada persona que acceda al sistema de información se encuentre individualmente identificada, es decir, en el caso de implantar la regla de "Nombre de usuario" como método de identificación, ya no cabría establecer uno para un grupo de usuarios sino que cada usuario debería poseer su propio "Nombre de usuario".

- Se tienen que limitar los accesos reiterados fallidos al sistema de información que trata los datos personales. El Reglamento de Seguridad no señala cuál es el número máximo de estos accesos reiterados fallidos sino que otorga libertad a las entidades para señalar este número máximo. No obstante, hemos de especificar que, por cuestiones de lógica, el número máximo no puede ser muy elevado (pongamos el caso que el número máximo de intentos fallidos se limite a 100), ni tampoco limitar el número máximo de accesos fallidos a uno. En la práctica, se suele limitar este acceso a un numero máximo de entre 3 y 5 intentos fallidos.

En definitiva, con esta medida se pretende tener controlados en todo momento a los usuarios que acceden al sistema, así como evitar, aún más, la posibilidad de un acceso no autorizado a los datos de carácter personal que posee una entidad que gestiona este tipo de datos.

Control de acceso físico

La presente medida viene regulada en el artículo 19 del Reglamento de Seguridad que establece lo siguiente:

"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."

Esta medida la podemos calificar como medida adicional de su análoga del nivel básico. Con ella se pretende establecer que no sólo se deben implantar mecanismos informáticos de control de acceso, sino también medidas físicas para garantizar un control de acceso a los lugares donde se ubiquen los sistemas de información con datos personales. Además, los usuarios que pueden acceder físicamente a estos locales deberán estar identificados en el documento de seguridad.

Medidas adicionales en la gestión de soportes

El artículo 20 del Reglamento de Seguridad señala lo siguiente:

"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."

Esta medida, al igual que las tres anteriores, establece una serie de cuestiones adicionales con respecto a otra medida análoga de nivel básico como es la gestión de soportes. En concreto, las señaladas medidas adicionales son las siguientes:

- Se debe implantar un registro de entrada de soportes informáticos que al menos contenga las siguientes cuestiones:
    - Tipo de soporte.
    - Fecha y hora de entrada del soporte.
    - Emisor del soporte.
    - Número de soportes.
    - Tipo de información que contienen los soportes.
    - Forma de envío de los soportes.
    - Persona que se encarga de la recepción del soporte. Esta persona debe estar autorizada para ello y así debe señalarse en el documento de seguridad.
- Se debe implantar un registro de salida de soportes informáticos que al menos contenga las siguientes cuestiones:
    - Tipo de soporte.
    - Fecha y hora de salida del soporte.
    - Destinatario del soporte.
    - Número de soportes.
    - Tipo de información que contienen los soportes.
    - Forma de envío de los soportes.

- Persona que se encarga de la emisión del soporte. Esta persona debe estar autorizada para ello y así debe señalarse en el documento de seguridad.
- En el caso de que se decida que un soporte se deseche o se reutilice deben adoptarse las medidas adecuadas para impedir que la información que contiene (datos personales) sea recuperada por terceros no autorizados. Estas medidas deberán detallarse en el documento de seguridad.
- En el caso de que se decida que un soporte se deseche o se reutilice, además de las medidas del punto anterior, debe darse de baja del inventario de soportes.
- Cuando se realicen operaciones de mantenimiento y, para ello, los soportes deban de salir fuera de donde habitualmente se encuentren (recordar que este lugar es de acceso restringido), deberán implantarse las medidas adecuadas que impidan el acceso a la información que se contiene en ellos por terceros no autorizados.

En resumen, lo que el legislador ha pretendido recoger en esta medida adicional es señalar una serie de cuestiones adicionales para reforzar la finalidad principal de una medida como es la gestión de soportes, es decir, ha pretendido reforzar el control que debe poseer un ente con respecto a los datos personales que gestiona.

Medidas de nivel medio

Estas medidas se encuentran en un lugar específico del Reglamento de Seguridad (capítulo III). En el señalado capítulo se recogen tanto las medidas de nivel medio en sentido estricto y que van a ser analizadas en el presente epígrafe, así como las medidas de nivel medio atenuado que han sido analizadas en el epígrafe anterior.

El artículo 4.2 del Reglamento de Seguridad señala lo siguiente:

"*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.*"

A este respecto debemos precisar que la mención "aquellos ficheros cuyo funcionamiento se rija por el artículo 28 de la Ley Orgánica 5/1992" debería entenderse como aquellos ficheros que se rijan por el artículo 29 de la Ley Orgánica 15/1999, ya que la Ley Orgánica a la que se refiere el artículo trascrito, fue sustituida por la Ley Orgánica 15/1999 (LOPD) y, en su artículo 29, hace mención a los ficheros que se recogían en el artículo 28 de la anterior Ley. Estos ficheros son los de solvencia patrimonial y de crédito.

En definitiva, se deberán implantar las medidas de nivel medio (que incluyen a las de nivel medio atenuado) junto con las medidas de nivel básico cuando se posean los siguientes tipos de datos personales:

- Datos referidos a la comisión de infracciones administrativas o penales.
- Datos referidos a Hacienda Pública.
- Datos referidos a servicios financieros.
- Datos referidos a solvencia patrimonial y de crédito.

Como ya señalamos hace un momento, el capítulo II del Reglamento de Seguridad recoge tanto las medidas de nivel medio, en sentido estricto, como las medidas de nivel medio atenuado. Estas últimas fueron analizadas en el epígrafe anterior y lo que vamos a analizar a continuación son las medidas de nivel medio.

Contenido adicional del documento de seguridad

El artículo 15 del Reglamento de Seguridad establece lo siguiente:

"El documento de seguridad deberá contener, además de lo dispuesto en el articulo 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."

Lo característico de la medida analizada en este apartado es lo siguiente:

- El contenido que legalmente debe poseer un documento de seguridad cuando se gestionen datos de nivel medio es el siguiente:
  - Su ámbito de aplicación.
  - Descripción de las medidas de seguridad implantadas en la empresa. Se entiende por medidas de seguridad las normas, procedimientos, reglas y estándares implantados.
  - Funciones y obligaciones del personal.
  - Estructura y descripción de los ficheros que contienen los datos personales.
  - Estructura y descripción de los sistemas informáticos que gestionan las aplicaciones que tratan los datos personales.
  - Descripción de un procedimiento de notificación, gestión y respuesta ante incidencias.

- Descripción de un procedimiento de realización de copias de respaldo y recuperación.
- Identificación del responsable de seguridad (esta figura será analizada posteriormente).
- Especificación de los controles periódicos que se realizan para comprobar las medidas implantadas y detalladas en el documento de seguridad.
- Definición de las medidas que se deben adoptar cuando se proceda al desecho o reutilización de un soporte informático.

Responsable de Seguridad

El artículo 16 del Reglamento de Seguridad establece lo que a continuación procedemos a señalar:

"*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 de fichero de acuerdo con este Reglamento.*"

Lo característico de esta medida es lo siguiente:

- Deberá existir la figura del responsable de seguridad. Este cargo podrá ser llevado a cabo por una o varias personas. La identificación de la/las personas que realizan esta labor deberá recogerse en el documento de seguridad.
- La función básica y principal del responsable de seguridad será la de controlar todas medidas implantadas en la entidad que gestiona datos personales y que han sido definidas y especificadas en el documento de seguridad.

Lo que se pretende con esta medida de seguridad es que todos los procedimientos y normas detallados en el documento de seguridad e implantados en la entidad que trata datos personales, sean centralizadas a través de esta figura. Además, hay que advertir que este cargo no supone ninguna asunción de la responsabilidades que posee el responsable del fichero (entidad que gestiona datos personales).

Medidas adicionales en el registro de incidencias

La medida que vamos a comentar en este momento se encuentra recogida en el artículo 21 del Reglamento de Seguridad que señala lo siguiente:

"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."

Como podemos observar, en este artículo se recogen una serie de contenidos adicionales con respecto a lo que se señalaba para esta medida en el nivel básico. Así, lo más específico de la señalada medida será:

- El procedimiento para la gestión incidencias se deberán establecer una serie de cuestiones adicionales cuando se gestionen datos de nivel medio. En concreto, este registro deberá detallar e implantar las siguientes cuestiones cuando se estén tratando datos de nivel medio:
    - Tipo de incidencia.
    - Momento en que se ha producido.
    - Persona que la notifica.
    - A quien se comunica.
    - Efectos derivados de la incidencia.
    - Cuando la incidencia haya motivado una recuperación de datos el registro también deberá contener lo siguiente:
        - Procedimientos realizados para la recuperación de los datos.
        - Persona que se encargo de realizar el proceso de recuperación de datos.
        - Los datos que han tenido que ser restaurados.
        - Los datos que han tenido que ser grabados manualmente.
- Cuando de una incidencia se derive un procedimiento de recuperación de datos será necesaria la autorización por escrito del responsable del fichero para ejecutar el mencionado procedimiento.

Pruebas con datos reales

El artículo 22 del Reglamento de Seguridad señala lo que, a continuación, se refleja:

"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."

Esta medida de seguridad viene a señalar que las pruebas que se realicen en la entidad, siempre que se utilicen datos personales reales para la implantación de los sistemas que gestionen esos datos, deberán llevar consigo las medidas de seguridad que debieran poseer en caso de no ser pruebas.

Medidas de nivel alto

Estas medidas se ubican dentro del capítulo IV del Reglamento de Seguridad. Estas medidas deberán ser previstas en el documento de seguridad e implantadas por la entidad que gestione datos personales siempre que sean de nivel alto, es decir, los datos personales que se reflejan en el artículo 4.3 del Reglamento de Seguridad:

> *"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."*

Además, debemos recordar que, cuando se gestionen datos de nivel alto, no sólo se deberán establecer estas medidas que vamos a analizar a continuación sino también las medidas precedentes, es decir, las medidas de nivel básico, las medidas de nivel medio atenuado y las medidas de nivel medio.

Distribución de soportes

El artículo 23 del Reglamento de Seguridad señala lo siguiente:

> *"La distribución de los soportes que contengan datos de carácter personal se realizará cifrando los datos o bien utilizando cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su transporte."*

A nuestro entender, lo más característico del este artículo es lo siguiente:

- Siempre que exista una distribución de soportes que contengan datos personales (de nivel alto) deberá cifrarse la información que se contiene en los mencionados soportes.
- No obstante, se podrá utilizar cualquier otro mecanismo diferente al cifrado siempre que garantice la ininteligibilidad y la no manipulación de la misma cuando se transporte.
- A pesar de la libertad de elección del mecanismo para evitar la no inteligibilidad y la no manipulación, estimamos que es más conveniente utilizar técnicas de cifrado para evitar estas cuestiones ya que son técnicas se encuentran hoy en día muy estandarizadas y generalizadas.

Esta medida pretende evitar el acceso no autorizado de terceros a lo contenido en los soportes cuando deban ser distribuidos.

Registros de accesos

El artículo 24 del Reglamento de Seguridad establece lo que a continuación procedemos a especificar:

"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 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 periodo 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."

Esta medida pretende potenciar, aun más, las medidas de identificación y autenticación y de control de accesos de los niveles básico y medio atenuado. Lo más característico de la medida señalada es lo que a continuación reflejamos:

- Cuando un usuario acceda a un sistema que contiene datos personales de nivel alto se deberá realizar un registro en el que se contengan al menos los siguientes conceptos:
    - Identificación del usuario que ha accedido.
    - La fecha y la hora en que se ha realizado el acceso.
    - El fichero al que se ha accedido.
    - Si el acceso ha sido autorizado o denegado. En el caso de haber sido autorizado se deben registrar en el mencionado registro de accesos las informaciones necesarias para identificar el dato o datos a los que se ha accedido.

- El tipo de acceso. Respecto a este concepto entendemos que el tipo de acceso se refiere a:
  - Acceso para consultar datos.
  - Acceso para modificar datos.
  - Acceso para suprimir datos.
  - Acceso para introducir datos.

- Las informaciones que se contienen en el registro de accesos deben ser guardadas por un período mínimo de dos años.
- El responsable de seguridad posee tres funciones en relación al registro de accesos:
  - Debe tener el control directo del registro de accesos que hemos señalado.
  - Debe revisar periódicamente las informaciones contenidas en el registro de accesos. El periodo de revisión mínimo lo fija el legislador en un mes.
  - Elaboración de un informe al menos mensual de las revisiones que se han realizado y de los problemas que se hayan producido.

Para concluir, podemos señalar que posiblemente esta medida de seguridad, tal y como se encuentra planteada en el Reglamento de Seguridad, es una de las más costosas tanto en el sentido económico como en el sentido de dedicación de recursos y ello básicamente por los siguientes motivos:

- La información que debe contener el registro de accesos es muy amplia.
- El tiempo que se debe conservar esa información es excesivo.

No obstante, lo cierto es que es una medida de seguridad que debe ser implantada y su no observación pude considerarse como una infracción grave con una sanción económica de hasta 300.000 euros.

Medidas adicionales en las copias de respaldo y recuperación

El artículo 25 del Reglamento de Seguridad establece lo siguiente:

"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."

Esta disposición pretende potenciar aun más las medidas de copias de respaldo y de recuperación de nivel básico. En ella se establece que estas copias deben ser almacenadas en un lugar de acceso restringido que debe ser diferente al lugar donde se encuentran los equipos informáticos (servidores) que contienen esos datos de nivel alto. En todo caso, ese lugar de almacenamiento de las copias debe cumplir con las medidas de seguridad recogidas en el Reglamento de Seguridad que les sean aplicables.

Telecomunicaciones

El artículo 26 del Reglamento de Seguridad establece lo que a continuación reproducimos:

> "*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.*"

Antes de analizar lo recogido en este artículo debemos señalar que se entiende por red de telecomunicaciones. Según la Ley 11/1998, de 24 de abril, General de Telecomunicaciones se entiende por Telecomunicaciones "toda transmisión, emisión o recepción de signos, señales, escritos, imágenes, sonidos o informaciones de cualquier naturaleza por hilo, radioelectricidad, medios ópticos u otros sistemas electromagnéticos". Esta misma Ley define a la Red de Telecomunicaciones como "los sistemas de transmisión y, cuando proceda, los equipos de conmutación y demás recursos que permitan la transmisión de señales entre puntos de terminación definidos mediante cable, o medios ópticos o de otra índole".

En definitiva, con las dos definiciones señaladas parece claro que red de telecomunicaciones es una red que permite la transmisión de información a través de dos puntos definidos en esa red. El problema radica en si todo tipo de red es considerada como "Red de Telecomunicaciones" porque, en ese caso, una red LAN sería una red de telecomunicaciones. Morfológicamente, la palabra telecomunicaciones está formado por el prefijo "tele-" (del griego τηλε) que significa "a distancia". Por lo tanto, entendemos que una red de telecomunicaciones será una red que permite la transmisión a distancia de información a través de dos puntos definidos en esa red. Es por ello que la idea de distancia es muy importante en este concepto y así, una red LAN dentro de un edificio, no entendemos que sea una red de telecomunicaciones, sino de comunicaciones, mientras que una red WAN, GAN o Internet, sí que las entendemos como red de telecomunicaciones.

Definido el concepto de telecomunicaciones ahora procederemos a analizar la medida recogida en este artículo:

- Siempre que exista una transmisión de datos personales de nivel alto deberá cifrarse la información que se envíe.
- No obstante, se podrá utilizar cualquier otro mecanismo diferente al cifrado siempre que garantice la ininteligibilidad y la no manipulación de los datos durante su transmisión.
- A pesar de la libertad de elección del mecanismo para evitar la no inteligibilidad y la no manipulación, estimamos que es más conveniente utilizar técnicas de cifrado para evitar estas cuestiones ya que son técnicas se encuentran hoy en día muy estandarizadas y generalizadas.

5.2 Derechos del responsable: utilización de y comercio con los datos de carácter personal

La toma de datos de carácter personal tiene un objetivo comercial y de márketing de primera magnitud. En el márketing directo su utilidad es tan grande que permite reducir considerablemente el coste por impacto de la publicidad (hacen falta menos "hits"), adecuarse al medio publicitario más conveniente y, al mismo tiempo, obtener mejores resultados en el esfuerzo de ventas. Así que el titular del fichero adquiere *derechos* sobre el mismo.

Aunque, como hemos visto, los datos de carácter personal objeto de tratamiento no pueden usarse para finalidades *incompatibles* con aquellas para las que los datos hubieran sido recogidos, sí pueden usarse para muchas actividades *compatibles*. Surge así la figura de la cesión de los datos y la figura del acceso de terceros a los datos

5.2.1 Cesión de datos

Es cesión o comunicación de datos toda revelación de los mismos realizada a una persona distinta del interesado.

Los datos de carácter personal sólo pueden 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.

Pero esto es muy amplio. "Funciones legítimas" del cedente y del cesionario pueden ser muchas. Por ejemplo: los datos recabados por una tienda de venta de artículos de marroquinería de lujo pueden ser utilizados por una tienda de artículos de pañuelos de lujo.

Este consentimiento se presta por escrito al mismo tiempo que se aportan los datos. Debe tenerse en cuenta que es *nulo* el consentimiento para la comunicación de los datos de carácter personal a un tercero cuando la información que se

facilite al interesado no permita al cedente conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretenden comunicar. El consentimiento es además revocable.

Es frecuente observar este fenómeno en el comercio. Al tiempo que se dan los datos, el cedente tiene la opción de conceder al cesionario el derecho a utilizar estos datos para otra finalidad.

No obstante, el consentimiento del cedente no es preciso cuando se trate de datos recogidos de fuentes accesibles al público o 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.

En teoría, el responsable del fichero en el momento en que se efectúe la primera cesión de datos debe 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. Pero en la práctica esta obligación muchas veces no existe 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. Tampoco será aplicable lo establecido en los apartados anteriores si la comunicación se efectúa previo procedimiento de disociación.[17]

La comunicación o cesión de datos personales, sin observar los requisitos legales que se establecen, supone una infracción muy grave y, por lo tanto, podría acarrear una sanción de 300.000 a 600.000 euros aproximadamente.

5.2.2 Acceso de terceros a los datos

Los datos son para el responsable del fichero, no para terceros. Por tanto, los terceros no pueden tener acceso legítimo a los datos, si no median las circunstancias que prevé la Ley. Por eso, la realización de tratamientos por cuenta de terceros debe consignarse en un contrato por escrito, 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,

17 Se llama “procedimiento de disociación” a todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.

ni siquiera para su conservación, a otras personas. Deben recogerse asimismo las medidas de seguridad que el encargado del tratamiento está obligado a implementar.(18)

Una vez cumplida la prestación contractual, los datos de carácter personal que obtenga el tercero deben 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. Si no lo hace y el encargado del tratamiento destina los datos a otra finalidad, los comunica o los utiliza incumpliendo las estipulaciones del contrato, es considerado también responsable del tratamiento y responde de las infracciones en que hubiera incurrido personalmente.

5.2.3 Utilización de datos incluidos en fuentes de acceso público

Son "fuentes accesibles al público" aquellos ficheros cuya consulta puede ser realizada por cualquier persona 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, los diarios y boletines oficiales y los medios de comunicación.

Los datos personales que figuren en el censo promocional o las listas de personas pertenecientes a grupos de profesionales deben limitarse a los estrictamente necesarios para cumplir la finalidad a que se destina cada listado. Sólo pueden contener los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo en cuestión. La inclusión de datos adicionales por las entidades responsables del mantenimiento de dichas fuentes *requiere el consentimiento del interesado*, que puede ser revocado en cualquier momento.

Estos datos, aunque son de público acceso, no pueden utilizarse para fines de publicidad o prospección comercial. Los interesados tienen derecho a que la entidad responsable del mantenimiento de los listados de los colegios profesionales indique gratuitamente la existencia de esta prohibición. Los interesados también tienen derecho a exigir gratuitamente la exclusión de la

18 No se considera 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. Por ejemplo, cuando una empresa subcontratista tiene que reparar el equipo informático del responsable del fichero.

totalidad de sus datos personales que consten en el censo promocional por las entidades encargadas del mantenimiento de dichas fuentes. La solicitud de exclusión debe atenderse 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.

Las fuentes de acceso público que se editan en forma de libro o algún otro soporte físico pierden el carácter de fuente accesible con la nueva edición que se publique. Si la lista se obtiene telemáticamente en formato electrónico, el carácter de fuente de acceso público se pierde en el plazo de un año contado desde el momento de su obtención.

O sea, sólo la última "Guía del Colegio de Procuradores", por poner un ejemplo, tiene la condición de "fuente de acceso público". El fichero "bajado de Internet" con el listado de los Procuradores tiene una validez de un año desde la publicación del fichero en Internet (no desde el día que se lo bajó el tercero).

5.2.4 En especial, los servicios de información sobre solvencia patrimonial y crédito

Las empresas que se dedican a la prestación de servicios de información sobre la solvencia patrimonial y el crédito de las personas físicas sólo pueden 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.

Existe la duda de si esto mismo puede aplicarse a las personas jurídicas, en particular a las compañías mercantiles.

Pueden 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, pero en estos casos se ha de notificar 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 ha de informar específicamente del derecho que tienen a recabar información de la totalidad de ellos. Cuando el interesado lo solicite, el responsable del tratamiento le debe comunicar 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.

Sólo se pueden registrar y ceder los datos de carácter personal que sean determinantes para enjuiciar la solvencia económica de los interesados y siempre que no se refieran, cuando sean adversos, a más de seis años y respondan con veracidad a la situación actual de aquéllos.

5.2.5 Tratamientos con fines de publicidad y de prospección comercial

Son los más comunes: los departamentos de márketing.

Quienes se dedican a la recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial y otras actividades análogas, pueden utilizar nombres y direcciones u otros datos de carácter personal cuando figuren en fuentes accesibles al público o cuando hayan sido facilitados por los propios interesados u obtenidos con su consentimiento.

Cuando los datos procedan de fuentes accesibles al público, 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. 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.

5.2.6 El Censo promocional

En particular 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 pueden 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. El uso de cada lista de censo promocional tiene un plazo de vigencia de un año. Transcurrido éste la lista pierde su carácter de fuente de acceso público.

5.2.7 Códigos tipo

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, pueden 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. Estos códigos pueden contener (o no contener) 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 deben respetar los principios fijados en aquél.

Estos "códigos-tipo" tienen el carácter de códigos deontológicos o de buena práctica profesional y deben 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. El Registro General de Protección de Datos puede 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.

5.2.8 Movimiento internacional de datos

No pueden 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 LOPD, 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. No obstante, la transferencia puede hacerse siempre cuando 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.

Quien señala si el nivel de protección que ofrece el país de destino es adecuado es la Agencia de Protección de Datos, no el responsable del fichero. Una de las mayores preocupaciones, a nuestro entender, de la Agencia de Protección de Datos es la vigilancia sobre la cesión de datos personales. Para evaluar el criterio del "Nivel de protección equiparable al que presta la LOPD" se tendrán en cuenta las siguientes cuestiones: la naturaleza y finalidad de los datos, la duración del tratamiento, los países de destino o de origen, las normas legales vigentes en el país tercero, el contenido de las informes de la Comisión de la Unión Europea y las normas de seguridad que se aplican en esos países.

Es de notar que los Estados Unidos de América no tienen un nivel equiparable a la LOPD, por lo que, al menos por el momento, no se pueden prestar datos a ese país.

No obstante, pueden realizarse transferencias internacionales de datos en los siguientes casos, entre otros aplicables a la Administraciones Públicas:

- Cuando resulte de la aplicación de tratados o convenios en los que sea parte España.
- Cuando se refiera a transferencias dinerarias (pero entonces se aplica la legislación específica de este sector).

- Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista. Por ejemplo, cuando al solicitar los datos se hace constar expresamente que los datos pueden cederse a ficheros sometidos a otras legislaciones.

- Cuando la transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero. Típicamente los ficheros que se refieren a materias de personal de una empresa multinacional. En este punto hemos de mencionar que, aunque la cesión se realice entre empresas dentro de un mismo grupo, se deben seguir las pautas marcadas por la LOPD en materia de cesión de datos ya que las empresas (cedentes y cesionarias) ***son dos entidades jurídicas diferentes*** y, por lo tanto, dos responsables de ficheros diferentes. Hemos querido señalar esta advertencia porque son varias las sanciones que ha impuesto la Agencia de Protección de Datos por cesión de datos entre empresas del grupo.

- 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.

- Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial. Lo que abre una enorme brecha para el caso de que los datos sean pedidos por un Juez de otro estado sin causa suficiente.

- 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.

5.2.9 Procedimiento de autorización

A continuación vamos a recoger el procedimiento por el cual el Director otorga autorización para realizar la transferencia internacional de datos. Este procedimiento se encuentra regulado en la Instrucción 1/2000 antes mencionada:

- El responsable del fichero, que es quien realiza la cesión, deberá aportar un contrato (con el cesionario) en el que se recojan los siguientes apartados:
    - La identificación del transmitente y el destinatario de los datos.
    - La finalidad de la transmisión.
    - Los datos que se ceden.
    - La obligación del transmitente de cumplimiento con la LOPD y, en especial, lo relativo a la inscripción del fichero.

- La obligación del que recibe los datos de cumplir con los principios de la LOPD, de no ceder los datos a un tercero y de cumplir con la finalidad recogida en el contrato.
- La obligación de que el destinatario adopte las medidas de seguridad reflejadas en la legislación española (Reglamento de Seguridad).
- La obligación de que ambas partes responderán solidariamente por el incumplimiento del contrato ante la Agencia de Protección de Datos si del mencionado incumplimiento deriva algún tipo de infracción de la LOPD.
- La obligación de que ambas partes indemnizarán a los afectados en caso de incumplimiento de la LOPD.
- El compromiso que el afectado pueda ejercer sus derechos de acceso, rectificación, cancelación y oposición y que, en caso de no ser atendido en el ejercicio de estos derechos, podrá reclamar tutela de la Agencia de Protección de Datos.
- El compromiso de que el destinatario autorizará a miembros de la Agencia de Protección de Datos el acceso a los locales donde se traten los datos y a la documentación necesaria con la finalidad de comprobar el cumplimiento de las obligaciones derivadas del contrato.
- La obligación de devolver o destruir los datos una vez expirado el contrato.
- El compromiso que los afectados puedan exigir lo estipulado en el contrato con respecto a aquellas cuestiones que les sean beneficiosas.

- Recibido el contrato la Agencia podrá señalar aquellas cuestiones que considere que se deben cambiar en él. Estas modificaciones deberán realizarse en el plazo de diez días.
- Si no se aporta el contrato con los requisitos expuestos o no se realizan las modificaciones que señale la Agencia de Protección de Datos, el Director de la misma denegará la transferencia de los datos.
- En caso de autorizar la transferencia, ésta será inscrita en el Registro General de Protección de Datos y será comunicada a la Comisión de las Comunidades Europeas.

6

Infracciones y Sanciones

6.1 Introducción

Hemos señalado en apartados anteriores del presente libro que los estados, para proteger el derecho a la intimidad de las personas, han decidido dictar diferentes leyes sobre protección de datos de carácter personal.

Además, con el ánimo de preservar la intimidad de sus ciudadanos, han creado diferentes organismos públicos para que lleven a cabo esta función. Los diferentes países europeos cuentan con instituciones de este tipo. Así, por ejemplo, en Alemania nos encontramos con la "Datenschutz", en Francia con la "Commission Nattionale de l'Informatique et des Libertés" o la "Comisión Nacional de Protección de Datos" en Portugal.

Las funciones de estas autoridades públicas, que la Directiva de Protección de Datos denomina Autoridades de Control, son diversas. Así estás Autoridades de Control, según el artículo 28 de la Directiva de Protección de datos, dispondrán, en líneas generales, de las siguientes potestades y funciones:

- Potestad de vigilancia sobre la aplicación de las normas de protección de datos.
- Potestad de consulta a la hora de elaboración de normas sobre protección de datos.
- Potestad de investigación para acceder a los datos personales y recabar la información necesaria para ejercitar su función de control.

- Potestad de intervención en el tratamiento de datos personales.
- Funciones procesales para las infracciones que se prevean en las legislaciones sobre protección de datos.
- Función protectora ante reclamaciones sobre protección de datos personales.

En España esta autoridad de control es la Agencia de Protección de Datos. La regulación de este organismo se encuentra en diferentes normas jurídicas de diferente rango:

- El Título VI de la LOPD.
- El Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos, modificado por el Real Decreto 156/1996, de 2 de febrero.
- Las normas que desarrollen la LOPD.
- La Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.
- Los preceptos de la Ley General Presupuestaria, texto refundido aprobado por Real Decreto legislativo 1091/1988, de 23 de septiembre, que resulten de aplicación.

Lo que a continuación vamos a reflejar será un breve examen de la estructura orgánica de la Agencia de Protección de Datos española, así como sus funciones más importantes, los procedimientos que ante ella se desarrollan y sus actuaciones más relevantes. En el caso de que desee profundizar sobre este epígrafe, se aconseja recurrir a las normas señaladas anteriormente.

6.1.1 Estructura orgánica

La Agencia de Protección de Datos se configura como un Ente de Derecho Público, con personalidad jurídica propia y que actúa con independencia respecto de cualquier Administración Pública.

La estructura de la Agencia es jerárquica. Así, con la máxima potestad de dirección de la Agencia y de representación se sitúa el Director. Bajo él, se encuentran tres Subdirecciones generales que son las siguiente:

- Subdirección General del Registro General de Protección De Datos.
- Subdirección General de Inspección de Datos.
- Subdirección General de Secretaria General.

Además de los órganos señalados, existe un Consejo Consultivo presidido por el director de la Agencia de Protección de Datos, con nueve vocales nombrados por el gobierno a propuesta de diferentes instituciones públicas y privadas. Los vocales son los siguientes:

- Un diputado.
- Un senador.
- Un vocal propuesto por el Ministerio de Justicia.
- Un vocal propuesto por las Comunidades Autónomas.
- Un vocal propuesto por la Federación Española de Municipios y Provincias.
- Un miembro de la Real Academia de la Historia.
- Un vocal propuesto por el Consejo de Universidades.
- Un vocal propuesto por el Consejo de Consumidores y Usuarios.
- Un vocal propuesto por el Consejo Superior de Cámaras de Comercio, Industria y Navegación.

6.1.2 Funciones

Las funciones de la Agencia de Protección de Datos, de manera genérica, se exponen en el artículo 37 de la LOPD. Estas funciones se desarrollan en el Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos, modificado por el Real Decreto 156/1996, de 2 de febrero.

Estas funciones son las siguientes:

- Vigilar en el territorio español del cumplimiento de la legislación sobre protección de datos.
- Controlar la aplicación de la legislación sobre protección de datos y, especialmente, lo relativo a los derechos de acceso, rectificación, oposición y cancelación, a los que anteriormente nos referimos.
- Dictar instrucciones sobre determinados aspectos de la protección de datos de carácter personal. A día de hoy estas instrucciones son las siguientes:
    - Instrucción 1/95, de 1 de marzo de la Agencia de Protección de Datos relativa a prestación de servicios de información sobre solvencia patrimonial y crédito.

  - 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.
  - 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.
  - 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.
  - Instrucción 1/98, de 19 de Enero, de La Agencia de Protección de Datos relativa al ejercicio de los derechos de acceso, rectificación y cancelación.
  - Instrucción 1/2000, de 1 de diciembre, de la Agencia de Protección de Datos relativa a las normas por las que se rigen los movimientos internacionales de datos.

- Atender a las peticiones, reclamaciones y consultas que formulen los titulares de los datos personales.
- Proporcionar información a los titulares de datos personales sobre sus legítimos derechos en materia de protección de datos personales.
- Señalar a las entidades que gestionen datos personales las medidas que deberían implantar para la adecuación de sus actuaciones con la legislación sobre protección de datos personales.
- Ordenar a las entidades que gestionen datos personales, el cese de determinadas actuaciones que no se ajustan a la legislación sobre protección de datos.
- Ejercer la potestad inspectora. Esta función se recoge en el artículo 40 de la LOPD. Los aspectos más significativos de esta función son los siguientes:
  - La Agencia de Protección de Datos podrá inspeccionar los ficheros con datos personales de las entidades que gestionan dichos tipos de datos.
  - Podrá solicitar e inspeccionar documentación, equipos físicos, lógicos y locales relacionados con datos personales.
  - Los funcionarios que actúen bajo esta función se consideran Autoridad Pública y poseen, como obligación, deber de secreto.

- Ejercer la potestad sancionadora de acuerdo con el Título VII de la LOPD. Al hilo de esta función debemos señalar que la Agencia de Protección de Datos debe seguir un procedimiento sancionador, al que posteriormente haremos referencia, que se encuentra recogido en el Capítulo V (artículos 18 y 19) del Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan algunos preceptos de la Ley Orgánica.
- Informar previamente los proyectos de disposiciones generales sobre protección de datos personales.
- Recabar de las entidades que gestionan datos personales la ayuda e información que necesite para el ejercicio de sus funciones.
- Comprobar la publicidad de los ficheros con datos personales. En este sentido, deberá publicar periódicamente la relación de ficheros con datos personales inscritos en ella.
- Redactar una memoria anual y remitirla al Ministerio de Justicia.
- Controlar y autorizar movimientos internacionales de datos personales.
- Cooperar internacionalmente en materia de protección de datos personales.
- Velar por determinados aspectos de la Ley de la Función Estadística.
- Otras funciones que sean atribuidas a la Agencia por vía legal o por vía reglamentaria.

6.1.3 Procedimientos

La Agencia de Protección de Datos lleva a cabo diferentes procedimientos administrativos en relación a los datos de carácter personal. En definitiva, la Agencia de Protección de Datos va a llevar a cabo tres grandes procedimientos que vamos reflejar a continuación:

- Procedimiento de notificación e inscripción de ficheros.
- Procedimiento de tutela de derechos.
- Procedimiento sancionador.

Procedimiento de notificación e inscripción de ficheros

Este procedimiento se encuentra recogido en los artículos 20, 25 y 26 de la LOPD y en el Capítulo III del Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan algunos preceptos de la Ley Orgánica.

En primer lugar hemos de señalar que cualquier fichero con datos personales, sea gestionado por una entidad pública o por una entidad privada, deberá estar inscrito en el Registro General de Protección de Datos, así como cualquier modificación del mismo o su cancelación.

Hemos de señalar, asimismo, que este procedimiento varía para la ficheros que son de titularidad pública y los ficheros de titularidad privada:

Ficheros de titularidad pública

- Previamente a la creación, modificación o supresión del ficheros de titularidad pública, deberá existir una disposición general publicada en el correspondiente Boletín Oficial en el que se recojan determinados aspectos especificados en los artículos 20.2 (caso de creación o modificación) y 20.3 (caso de supresión) de la LOPD.

- Creación de ficheros:

    - Una vez publicada la disposición general de creación deberá notificarse este hecho, a través de los formularios que reglamentariamente están establecidos, a la Agencia de Protección de Datos a través de dos vías:

        - Envío del formulario de creación a través de medios tradicionales.

        - Envío del formulario de creación a través de Internet.

    - Una vez recibido el formulario de inscripción, la Agencia de Protección de Datos inscribirá de oficio el fichero creado.

    - Una vez inscrito, el Registro General comunicará tal hecho al responsable del fichero inscrito

- Modificación y supresión de ficheros:

    - La disposición general publicada de modificación o cancelación será remitida a la Agencia de Protección de Datos.

    - La Agencia de Protección de Datos procederá a modificar o cancelar de oficio la inscripción del fichero.

Ficheros de titularidad privada

- Previamente a la creación de un fichero con datos personales o hasta un mes después de la modificación o supresión de un fichero con datos de carácter personal, deberá comunicarse a la Agencia de Protección de Datos a través del formulario creado reglamentariamente, cualquiera de estos hechos (creación, modificación o supresión) a través de dos vías :

    - Envío del formulario de creación, modificación o supresión a través de medios tradicionales.

- Envío del formulario de creación, modificación o supresión a través de Internet.

- Una vez recibida esta comunicación, la Agencia procederá a la inscripción del fichero en el Registro General de Protección de Datos siempre y cuando no haya encontrado defectos subsanables.

- Si se encuentran defectos subsanables, la Agencia comunicará éstos para su subsanación en el plazo de diez días. De no subsanarse no se procederá a la inscripción o, en su caso, la modificación o la supresión de la misma.

- La inscripción o, en su caso, la modificación o la supresión de la misma se comunicará al responsable del fichero inscrito, modificado o suprimido.

- En el caso de la inscripción, si la Agencia de Protección de Datos no hubiera resuelto sobre la misma en un plazo de un mes desde que se recibe el formulario de inscripción, se entenderá inscrito el fichero.

Procedimiento de tutela de derechos

Este procedimiento viene especificado en el artículo 18 de la LOPD y en el artículo 17 del Real Decreto 1332/1994. Lo que se pretende con este procedimiento es garantizar el ejercicio efectivo de los derecho de acceso, rectificación, cancelación y oposición, de los que anteriormente hemos hecho mención.

Las cuestiones más importantes de este procedimiento son las siguientes:

- Se podrá acudir a este procedimiento cuando a una persona física se le hayan denegado injustificadamente, sus legítimos derechos de oposición, acceso, rectificación o cancelación.

- El procedimiento se inicia exclusivamente con un escrito de esta persona a la Agencia de Protección de Datos expresando claramente el contenido de su reclamación así como, a su entender, los preceptos de la LOPD que han sido vulnerados.

- Recibido el escrito, la Agencia de Protección de Datos comunicará al ente presuntamente infractor para que en un plazo de quince días formule las alegaciones que estime oportunas.

- Transcurridos el plazo de quince días o recibidas esta alegaciones, la Agencia de Protección de Datos realizará cuantas actuaciones legales estime oportunas.

- Realizadas estas actuaciones, el director de la Agencia de Protección de Datos dictará una resolución en un plazo de seis meses y notificará su decisión tanto a la persona afectada como a la entidad investigada.

- Contra esta resolución cabe interponer recurso contencioso-administrativo (recurso por la vía judicial) sin perjuicio de los recursos administrativos que pudieran existir (recurso de reposición).

Procedimiento sancionador

Se encuentra regulado en el artículo 48 de la LOPD y en los artículos 18 y 19 del Real Decreto 1332/1994 además de por la Ley Orgánica 5/1992.

Las cuestiones básicas en este procedimiento son las que a continuación vamos a proceder a especificar:

- El procedimiento se inicia de oficio por acuerdo del director de la Agencia de Protección de Datos y puede ser por su propia iniciativa o por recibir una denuncia de uno o varios afectados.
- El acuerdo del director de la Agencia de Protección de Datos indicará el instructor del procedimiento y, en su caso, el secretario que podrán ser recusados según la legislación administrativa.
- En el mismo acuerdo se indicará lo siguiente:
  - La persona presuntamente responsable.
  - Los hechos imputados.
  - La infracción presuntamente cometida.
  - Las medidas provisionales que se adopten.
  - La sanción que pudiera imponerse.
- Este acuerdo se le notificará al presunto responsable de los hechos imputados.
- En un plazo máximo de quince días después de esta notificación, el instructor ordenará cuantas actuaciones legales estime oportunas y adecuadas con el ánimo de esclarecer los hechos imputados y determinará las responsabilidades que se deriven de esos hechos.
- En el mismo plazo de quince días después de la notificación, el presunto responsable podrá realizar cuantas alegaciones estime oportunas así como la proposición de las pruebas que considere útiles.
- Después de transcurridos estos quince días, el instructor ordenará la práctica de las pruebas que estime pertinentes en los treinta días siguientes.
- Practicadas las pruebas se enviará el expediente de las misma al presunto responsable para que un plazo máximo de quince días formule alegaciones.

- Transcurridos estos últimos quince días el instructor formulará propuesta de resolución (que deberá estar fundamentada jurídicamente) y señalará la sanción a imponer o la no existencia de responsabilidad.

- La propuesta de resolución se enviará al presunto responsable para que en un plazo máximo de quince días formule las alegaciones pertinentes.

- Transcurrido el plazo anterior, el instructor elevará el expediente completo (propuesta de resolución, pruebas practicadas, alegaciones formuladas, etc.) al director de la Agencia de Protección de Datos.

- Potestativamente, el director de la Agencia de Protección de Datos, podrá otorgar un plazo de quince días adicionales para que el instructor realice cuantas actuaciones considere necesarias.

- Una vez que el director de la Agencia de Protección de Datos posea el expediente o, en su caso, hayan transcurridos el plazo de quince días para la práctica de nuevas actuaciones, tendrá un plazo de diez días para dictar una resolución.

- La resolución podrá indicar una de las siguientes cuestiones:

    - Los hechos imputados, la infracción cometida, el responsable de la misma y sanción impuesta.
    - La declaración de no existencia de responsabilidad.

- La resolución será notificada al responsable o al presunto responsable que contará con el derecho a interponer recurso contencioso-administrativo (recurso por la vía judicial) sin perjuicio de los recursos administrativos que pudieran existir (recurso de reposición).

- Si el procedimiento se hubiera iniciado como consecuencia de una denuncia, la Resolución deberá ser notificada al denunciante.

6.1.4 Actuaciones más relevantes

Según la memoria de 2001 de la Agencia de Protección de Datos, durante el año 2001, y por lo que respecta al Registro de Protección de Datos, se han producido 36.690 resoluciones de inscripción, de las cuales 26.113 han sido para la creación de ficheros, 7.402 han sido de modificación y 5.175 han sido de supresión.

Por lo que respecta al procedimiento de tutela de derechos y según la misma fuente indicada en el párrafo anterior, en el año 2001 se han iniciado 363 procedimientos de este tipo de los han quedado pendientes de concluir 99.

Por lo que respecta al procedimiento sancionador, en el mismo año y, según la memoria de 2001 de la Agencia de Protección de Datos, se han iniciado 218 de este tipo de procedimientos.

Quizás los procedimientos más importantes son los sancionadores ya que a través de sus resoluciones y, especialmente de resoluciones que impongan sanciones, se podrá observar cómo la Agencia de Protección de Datos ejerce su función básica, como es velar por el cumplimiento sobre protección de datos personales y controlar su aplicación. Por ello, vamos a señalar en este apartado las resoluciones sancionadores más relevantes de los últimos años:

Primera sanción en protección de datos por un correo electrónico no deseado

La primera resolución de la Agencia de Protección de Datos en defensa de la intimidad a través de Internet concluyó con una sanción de 10.000.001 pesetas (poco más de 60.100 euros). El infractor insistió en remitir un correo electrónico a un particular, después de haber advertido éste que no deseaba recibir este tipo de correos electrónicos.

Según los hechos imputados en la resolución, el infractor contestó al particular con un nuevo e-mail publicitario dirigido a la persona que había manifestado su voluntad de no recibirlos, acompañado con expresiones como que le iba a "partir las piernas". La infracción que se cometió en este caso fue calificada como grave (este tipo de infracciones acarrea entre 60.000 a 300.000 euros). La resolución fue dictada por conculcación del artículo 43.3.d de la LORTAD (antigua legislación existente en España y que ha sido derogada por la LOPD). La falta grave aplicada consiste en el tratamiento de datos personales sin el consentimiento del interesado. Según explicó el director de la Agencia de Protección de Datos "enviar mensajes a una dirección de correo electrónico equivale a la introducción de publicidad en los buzones de una casa, actividad que no está sancionada hasta que los mensajes, vinculados a una persona, se envían contra la voluntad del destinatario". La novedad de esta sanción consiste en que es la primera que se impone en España contra una vulneración del derecho a la intimidad a través de correo electrónico.

Sanción por acceso de terceros a datos personales

La Agencia de Protección de Datos multó a principios del año 2001 con 180.000.000 de pesetas (alrededor de 1.080.000 euros) a una productora de televisión por permitir el acceso de terceros a datos de los futuros participantes en un concurso televisivo.

La Agencia de Protección de Datos consideró en su resolución que la productora había incumplido los artículos 5, 6, 9 y 11 de la LOPD referidos al

derecho de información previa al consentimiento del afectado, a la seguridad de los datos y a la comunicación de datos, respectivamente y que posteriormente examinaremos.

Por un lado, la Agencia de Protección de Datos multó con 5.000.000 de pesetas (aproximadamente 30.000 euros) a la mencionada productora por incumplimiento del artículo 5 de la LOPD que establece que la obligatoriedad de informar a los interesados de forma "expresa, precisa e inequívoca" de la existencia de un fichero o tratamiento de datos de carácter personal, así como la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación de dichos datos.

Asimismo, esta productora fue multada con 75.000.000 de pesetas (aproximadamente 450.000 euros) por infringir el artículo 6 de la LOPD que hace mención al "consentimiento inequívoco" del afectado para cualquier tratamiento de los datos por parte de la empresa.

La misma multa le fue impuesta por incumplimiento del artículo 11 de la LOPD que recoge que los datos 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".

La última infracción, que supuso una multa de 25.000.000 de pesetas (aproximadamente 150.000 euros), es del artículo 9 que obliga al responsable del fichero a adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos a través de lo establecido en el Reglamento de Seguridad ya analizado.

Sanción de la Agencia de Protección de Datos por la utilización de webcams

La Agencia de Protección de Datos multó a una empresa editorial con 1.000.000 de pesetas (aproximadamente 6.000 euros) por colocar en las oficinas de un periódico, propiedad de esta empresa, cámaras fotográficas que recogían las actividades de los trabajadores que podían ser seguidas a través de Internet.

Las cámaras recogían imágenes de la actividad de los trabajadores, que, posteriormente, se podían ver en Internet siendo renovadas cada quince segundos. Esta práctica tuvo lugar sin que ningún empleado del periódico hubiera sido consultado previamente.

La Agencia de Protección de Datos consideró que, aunque el hecho supone un tratamiento de datos ya que supone recogida y grabación de datos personales, éste no conlleva intencionalidad de crear un fichero con los datos personales de

los trabajadores debido al corto tiempo que se conservaban las imágenes, hecho que se consideró como atenuante por la Agencia de Protección de Datos.

La infracción cometida por la empresa editorial, según la Agencia de Protección de Datos, fue la no observancia del artículo 6 de la LOPD se refiere al consentimiento del afectado y establece que el tratamiento de datos de carácter personal requerirá el consentimiento "inequívoco del afectado, salvo en los casos que la Ley disponga otra cosa."

Sanción por cesión de datos

La Agencia de Protección de Datos sancionó a un grupo de telecomunicaciones con una multa de 140.000.000 de pesetas (aproximadamente 840.000 euros) porque dos de sus filiales intercambiaban los datos de sus clientes sin su consentimiento, además de tratar los datos con una finalidad distinta para la que fueron recogidos.

Una de las filiales empleaba los datos de sus clientes para promocionar productos de la otra filial. Según la resolución de la Agencia de Protección de Datos, la primera filial cedía ficheros de datos de sus clientes a la segunda quien, tras una selección, los cedía de nuevo a la primera filial para que ésta promocionase los servicios de la segunda filial.

El procedimiento sancionador de la Agencia de Protección de Datos se inició de oficio por parte de la Agencia de Protección de Datos en octubre del año 2000 en virtud de una denuncia de un particular, cliente de la primera filial del grupo.

En su día, este particular solicitó la cancelación de sus datos personales pero se mantuvieron sus referencias en el fichero. Además, solicitó que no se utilizase los datos con otro fin que no fuera con el relacionado a la finalidad para la que se recogieron los datos que era, básicamente, la facturación del servicio de telefonía contratado por el particular. Todas estas solicitudes constaban en un bureau-fax que el particular remitió en su día a la filial en el que prohibía expresamente que se utilizasen sus datos para un uso distinto a la finalidad señalada anteriormente.

Las filiales de la empresa de telecomunicaciones infringieron, según la Agencia de protección de Datos, el artículo 6 de la LOPD relativo al consentimiento, el artículo 11 de la LOPD relativo al uso y la cesión de datos personales sin consentimiento del afectado y el artículo 16 relativo al derecho de rectificación y cancelación.

La sanción para la primera de las filiales fue una multa de 70.000.000 de pesetas (unos 420.000 euros), de los cuales 50.000.000 de pesetas (300.000 euros) se debe a una infracción muy grave debido a una cesión no consentida de datos

personales, otros 10.000.000 de pesetas (60.000 euros) por una infracción grave al haber utilizado la información con un fin para el que no fue recopilada y otros 10.000.000 de pesetas (60.000 euros) también por una infracción grave por tratar los datos del afectado sin su consentimiento previo. Por su parte, la segunda filial fue sancionada con una multa de 70.000.000 de pesetas (unos 420.000 euros) de los cuales, 50.000.000 de pesetas (300.000 euros) fueron por ceder ficheros a la primera filial, 10.000.000 de pesetas (60.000 euros) se debieron por tratar la información sin consentimiento del afectado y el resto fue motivado por no atender al derecho de cancelación de datos.

6.2 Infracciones

Las infracciones se agrupan en el artículo 44 y 47 de la LOPD dentro del Título VII que lleva por nombre "Infracciones y Sanciones". La LOPD distingue tres tipos de sanciones: leves, graves y muy graves.

6.2.1 Leves

La prescripción de las infracciones leves es de un año desde que se comete el hecho supuestamente infractor. Las infracciones leves son las siguientes:

- No atender la solicitud de rectificación o cancelación.
- No facilitar a la Agencia de Protección de Datos la información que ésta solicite.
- No solicitar la inscripción de un fichero con datos personales.
- Recoger datos personales contraviniendo el derecho de información en la recogida de datos (artículo 5 LOPD).
- Incumplir el deber de secreto recogido en el artículo 10 de la LOPD.

6.2.2 Graves

La prescripción de las infracciones graves es de dos años desde que se comete el hecho supuestamente infractor. Las infracciones graves son las siguientes:

- Crear un fichero de titularidad pública o proceder a la recogida de datos personales sin autorización de "disposición general" publicada en un Boletín Oficial.
- Crear un fichero de titularidad privada o proceder a la recogida de datos con una finalidad distinta al objeto legítimo de la entidad que los recaba.
- Recoger datos sin el consentimiento expreso de los afectados (siempre y cuando este sea exigible).

- Tratar los datos personales en contra de los principios y las garantías recogidos en la LOPD.
- El impedimento del ejercicio de los derechos de acceso o de oposición y la negativa a facilitar la información requerida.
- Mantener los datos de forma inexacta o no efectuar las rectificaciones o cancelaciones de los datos cuando legalmente haya que realizarlas.
- Infringir del deber de secreto sobre datos de nivel medio atenuado o de nivel medio (según el Reglamento de Seguridad).
- No implantar las medidas que se correspondan según el Reglamento de Seguridad.
- No remitir a la Agencia de Protección de Datos las notificaciones que sean solicitadas o no proporcionarlas en el plazo requerido.
- La obstrucción del ejercicio de la función inspectora de la Agencia de Protección de Datos.
- No inscribir el fichero en el Registro General de Protección de Datos, cuando sea requerido por el director de la Agencia de Protección de Datos.
- Incumplir el deber de información cuando los datos hayan sido recabados de persona distinta del afectado.

6.2.3 Muy graves

La prescripción de las infracciones muy graves es de tres años desde que se comete el hecho supuestamente infractor. Las infracciones muy graves son las siguientes:

- Recoger datos personales de forma engañosa y fraudulenta.
- Ceder datos personales fuera de los casos en los que está permitido.
- Recabar y tratar datos especialmente protegidos sin el consentimiento expreso del afectado, cuando no lo disponga una ley o cuando se recaben con la única finalidad de poseer este tipo de datos.
- No cesar en el uso ilegítimo de un tratamiento de datos personal cuando así sea requerido por el director de la Agencia de Protección de Datos.
- No recabar la autorización del director de la Agencia de Protección de Datos para realizar una transferencia internacional de datos cuando aquella sea necesaria.

- Tratar los datos personales de manera ilegítima o contra los principios y las garantías aplicables, siempre que ello impida o vaya en contra de derechos fundamentales.
- Vulnerar el deber de secreto (artículo 10 de la LOPD) de los datos especialmente protegidos.
- No atender u obstaculizar sistemáticamente el ejercicio de los derechos de acceso, rectificación, cancelación u oposición.
- No atender sistemáticamente el derecho de información en la recogida de datos personales.

6.3 Sanciones

Las sanciones, al igual que las infracciones, vienen recogidas dentro del Título VII de la LOPD, pero, en este caso, en los artículos 45, 46, 47 y 49. El tipo de sanciones varía en función de la naturaleza jurídica del responsable del fichero. Así, en caso de que este responsable sea una entidad privada, las sanciones serán multas administrativas y, en su caso, la inmovilización del fichero; si es una entidad pública, las sanciones son diversas y relacionadas con el régimen disciplinario de las Administraciones, así como, en su caso, la inmovilización del fichero.

6.3.1 Sanciones para las entidades privadas

En el caso de las multas administrativas, éstas variarán en función del tipo de infracción que se cometa:

- Las infracciones leves llevan aparejadas una multa administrativa que varía de los 601,01 euros a los 60.101,21 euros (de 100.000 pesetas a 10.000.000 de pesetas).
- Las infracciones graves llevan consigo una multa administrativa de 60.101,21 euros a 300.506,05 euros (de 10.000.000 de pesetas a 50.000.000 de pesetas).
- Las infracciones muy graves llevan aparejadas una multa administrativa de 300.506,05 euros a 601.012,10 euros (de 50.000.000 de pesetas a 100.000.000 de pesetas). Además, en este caso, en virtud del artículo 49 de la LOPD, el director de la Agencia de Protección de Datos, cuando la infracción muy grave sea por ceder o utilizar los datos personales y siempre y cuando se atente contra los derechos fundamentales de las personas, podrá requerir al responsable del fichero sancionado para que cese en su actuación. Si este requerimiento no es atendido, el director de la Agencia de Protección de Datos podrá dictar una resolución en la ordene inmovilizar los ficheros.

Respecto a las multas administrativas, la cuantía concreta de las mismas se impondrá atendiendo a "la naturaleza de los derechos personales afectados, el volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia y perjuicios causados a las personas interesadas y a terceras personas, y a cualquier otra circunstancia que sea relevante (...)" (Artículo 45.4 de la LOPD).

6.3.2 Sanciones para las entidades públicas

En este caso no existe la multa administrativa. Así, cuando se cometa una infracción, el director de la Agencia de Protección de Datos resolverá estableciendo las medidas a adoptar para que cesen los hechos infractores o para que se corrijan los efectos derivados de la infracción.

Otro tipo de sanción que también puede imponer el director de la Agencia de Protección de Datos es la iniciación del procedimiento sancionador. El resto de este procedimiento y las sanciones a aplicar serán las recogidas en la legislación sobre régimen disciplinario de las Administraciones Públicas. En líneas generales y sin querer entrar en profundidad en esta materia, las sanciones que se pueden imponer, en función del Real Decreto 33/1986, de 10 de enero, por el que se aprueba el Reglamento de Régimen Disciplinario de los Funcionarios de la Administración del Estado, son la separación del servicio, la suspensión de funciones, el traslado con cambio de residencia y el apercibimiento.

Por último, otro tipo de sanciones para las entidades públicas es la que hace mención a la inmovilización de los ficheros (artículo 49 de la LOPD) y que ya expusimos cuando nos referíamos a las sanciones para las entidades privadas.

7

Conclusión

Analizados los aspectos más importantes en la legislación española sobre protección de datos personales estamos en la disposición de llevar a cabo una serie de conclusiones que expondremos a continuación.

En primer lugar hemos de señalar que hemos podido apreciar como la generalización en el uso de la informática ha hecho que los estados tengan que reaccionar para salvaguardar la intimidad de sus ciudadanos. Esta reacción ha venido encabezada por los países europeos (España se unió tarde a esta reacción) y, en este contexto, se ha reflejado en dos directivas sobre protección de datos personales.

Nuestro país, según los mandatos de las directivas europeas, ha legislado en esta materia y lo ha hecho, en líneas generales, imponiendo estrictos requisitos, principalmente en materia de seguridad.

Mientras que otros países europeos optaron por una mayor libertad a la hora de regular la seguridad de los datos y sólo recogieron los principios en los que se deberían basar las medidas de seguridad, en España se optó por una fórmula totalmente opuesta y de ello derivó el Reglamento de Seguridad, al que podemos calificar como una norma jurídica eminentemente técnica.

En segundo y último lugar podemos señalar como conclusión que esa reacción que han tenido los Estados a través de la publicación de normas ha hecho ver que los datos personales forman parte del derecho a la intimidad y que no es una información que se puede utilizar de forma libre, sino que se deberán

respetarse las “normas de juego” establecidas y, principalmente, respetar la decisión de las personas en cuanto a la forma de gestionar sus datos personales. Esto ha sido recogido por los entes que gestionan datos personales que cada vez tienen más prudencia a la hora llevarlo a cabo. Pero todavía no es suficiente (lo hemos visto cuando hemos hecho mención a las sanciones de la Agencia de Protección de Datos). Se ha podido observar que todavía existen infracciones de la normativa sobre protección de datos, hecho que debe ser evitado a través de diferentes medios. Debe existir una mayor concienciación de que los datos personales son un bien (informático por lo general) que debe protegerse y, por ello, deben establecerse todo tipo de procedimientos, normas y medidas para conseguir tal fin.

8

La Seguridad en Sistemas Microsoft

El derecho de los usuarios de sistemas de información a comunicarse de una forma segura es una prioridad para la industria de IT. Para Microsoft éste es uno de los retos de la informática de este siglo.

La seguridad se ha convertido durante los últimos años en uno de los pilares sobre los que se asienta la estrategia presente y futura de Microsoft. El derecho de los usuarios de sistemas de información a comunicarse y desarrollar su actividad de forma segura es un objetivo fundamental de la corporación.

Sin embargo, no es sencillo. Sólo cuando la informática inspire la confianza relativa que ofrecen hoy servicios tan aceptados como la electricidad o el abastecimiento de agua, la gente se sentirá confiada y familiarizada con la idea de disponer de un microprocesador en un número creciente de dispositivos. Y hablamos de confianza relativa porque la realidad nos hace ver que las centrales eléctricas pueden fallar, las tuberías de conducción de agua se rompen, se producen catástrofes aéreas pero, sin embargo, nuestro nivel de confianza en estos servicios es muy elevado. No dedicamos demasiado tiempo a preguntarnos si cuando abro un grifo de agua, el agua fluirá como yo espero que lo haga. Simplemente ocurre. Es un servicio que en base a nuestra experiencia cotidiana ha ganado nuestra confianza. Por eso, el concepto de confianza apropiada resulta más acertado. Los sistemas de computación e información sólo serán confiables a ese mismo nivel cuando podamos utilizarlos sin pensar demasiado sobre si funcionarán correctamente. Ése es el nivel de confianza que sería necesario.

En las dos ultimas décadas, los sistemas de información han cambiado de un modelo centralizado con acceso limitado a un modelo distribuido en términos de

cómo se recoge la información, cómo se comparte y cómo se hace accesible. Con ello, las necesidades de seguridad han aumentado de forma exponencial.

Microsoft tiene una importante responsabilidad para cumplir con el compromiso de proporcionar una interacción segura con el ordenador para cualquiera de lo usos que de él se hagan: trabajo, comunicación, transacciones, etc.

8.1 TrustWorthy Computing. La estrategia de Microsoft

Microsoft trabaja activamente para proporcionar sistemas seguros. Para ello se ha centrado en tres líneas que se han denominado como "Secure by Design", "Secure by Default" y Secure by Deployment".

Una tecnología sólida es clave para construir un entorno de computación seguro, pero la tecnología por si sola no pude responder totalmente a las amenazas existentes. Productos bien diseñados, procesos establecidos y efectivos y equipos de operaciones bien formados y eficaces, son elementos necesarios para proporcionar un elevado nivel de seguridad y funcionalidad.

8.2 Construyendo la plataforma segura

En enero de 2002 Bill Gates movilizó a los 50.000 empleados de Microsoft para construir el entorno de "Trustworthy computing" para los clientes de Microsoft. Tres son los pilares sobre los que esta estrategia se asienta:

- Fiabilidad: significa que un sistema es de confianza, accesible cuando se le necesita y que responde como se espera de él a los niveles apropiados.
- Seguridad: significa que un sistema es resistente a un ataque, y que la confidencialidad, integridad y accesibilidad , tanto del sistema como de los datos, están protegidos.
- Privacidad: significa que los individuos tienen la capacidad de controlar los datos recogidos sobre ellos y que el uso de esos datos se destinará exclusivamente para el fin con el que se recogieron.

El marco de trabajo creado para la consecución de este objetivo tiene tres aspectos fundamentales: seguridad en el diseño; seguridad por defecto y seguridad en el despliegue.

8.2.1 Seguridad en el diseño

El objetivo de esta iniciativa es considerar la seguridad como parte fundamental de todo elemento creado por Microsoft en la propia fase de diseño.

A lo largo de la más reciente historia hemos visto como elementos e incluso protocolos no fueron concebidos con la seguridad como fase crítica del diseño. El mismo TCP/IP, globalmente utilizado hoy en día, fue concebido con criterios más próximos a maximizar la interoperabilidad que a la propia seguridad (por eso debemos hablar posteriormente de IPSec, etc.). Por tanto, uno de los objetivos de esta fase es minimizar la aparición de vulnerabilidades de seguridad antes de que el producto vea la luz y añadir características que aumenten su seguridad.

Por ello, algunas iniciativas en marcha a este respecto son:

Windows Secure Initiative

Reingeniería de los procesos utilizados por los grupos de desarrollo en la producción de los productos Microsoft. Esta iniciativa afecta tanto a las personas como a los procedimientos y herramientas utilizadas.

Evaluación externa de productos

Iniciativa dirigida a certificar y llevar a examen la seguridad de nuestros productos a fuentes externas. En esta iniciativa cabe destacar las certificaciones:

FIPS 140-1 del NIST del CSP (Cryptographic Service Provider) Remitidos a FIPS 140-2:

Componentes evaluados:

- The two Microsoft default Cryptographic Services Providers (CSPs)
- The Windows Kernel Mode Cryptographic Module
- The Exchange Cryptographic Services Provider (CSP)

Productos que incorporan dichos componentes:

- Windows 98 (default CSPs); Windows NT Versión 4.0 (default CSPs)
- Windows 2000 (default CSPs y Kernel Mode Cryptographic Module)
- Windows XP (default CSPs y Kernel Mode Cryptographic Module)
- Internet Explorer cuando se ejecuta como un componente de Windows 98
- Windows NT Versión 4.0, Windows 2000, o Windows XP
- Internet Information Server Versiones 4 y 5

- Microsoft Outlook utiliza Exchange Cryptographic Services Provider cuando se ejecuta con Windows 98, Windows NT Versión 4.0, Windows 2000, o Windows XP; Windows 2000 Public Key Certificate Server

Protocolos que aprovechan los componentes certificados:

- El protocolo SSL; La familia de protocolos IPSEC; El protocolo de cifrado de email S/MIME; El protocolo SQL TDS (Tabular Data Stream).

Common Criteria Certification para Windows 2000 de nivel EAL4+

"Creo que Windows es más seguro que Linux…", "Ni hablar, Linux es más seguro que Windows pero menos que Solaris, etc." ¿Cuántas veces hemos participado o asistido a conversaciones de este estilo? Y realmente es una conversación que nunca o casi nunca lleva a conclusiones porque suele estar enormemente cargada de subjetividad. Pero no podría ser de otra manera. Siempre suele transcurrir en torno a la experiencia personal y profesional de cada uno, así como a los conocimientos adquiridos sobre cualquiera de ellas.

Se hizo necesaria la existencia de un organismo de estandarización independiente que arrojara cierta objetividad sobre este tipo de disquisiciones en torno a la seguridad de los productos. Este organismo, no sin enormes dificultades en su constitución, existe y se llama Common Criteria (ISO-IEC 15408). Desde el 29 de octubre de 2002 podemos responder objetivamente a la pregunta: ¿Cómo de segura es la plataforma Windows 2000? Pues la respuesta es EAL4+ (la máxima certificación Common Criteria de seguridad para un sistema operativo comercial), en el más amplio espectro de evaluación remitido hasta la fecha a Common Criteria. Por descontado que cada profesional de IT opinará de una u otra manera según su propia experiencia, pero no cabe duda que resultará muy útil introducir en este tipo de observaciones el único factor objetivo reconocido internacionalmente en materia de seguridad en productos IT, y ese se llama Common Criteria.

Un poco de historia

Common Criteria es el resultado final de importantes esfuerzos en el desarrollo de criterios de evaluación unificados para la seguridad de los productos IT y ampliamente aceptado por la comunidad internacional.

A principios de los años 80 se desarrollaron en Estados Unidos los criterios de seguridad recogidos bajo el nombre de TCSEC (Trusted Computer System Evaluation Criteria) y editados en el famoso "libro naranja". En las décadas posteriores, varios países tomaron como base el TCSEC americano y evolucionaron las especificaciones para hacerlas mas flexibles y adaptables a la constante evolución de los sistemas de IT.

De ahí la comisión europea, en el año 1991 publicó el ITSEC (Information Technology Security Evaluation Criteria) desarrollado conjuntamente por Francia, Alemania, Holanda y el Reino Unido. En Canadá, igualmente se desarrollaron en 1993 los criterios CTCPEC (Canadian Trusted Computer Product Evaluation) uniendo los criterios americanos y europeos. En ese mismo año el gobierno americano publicó los Federal Criteria como una aproximación a unificar los criterios europeos y americanos.

El escenario comienza a aclararse con la decisión de estandarizar internacionalmente estos criterios para uso general. En esa labor, ISO comienza a trabajar a principios de los años 90 dando como resultado la certificación Common Criteria (o ISO-IEC 15408)

Es el resultado de una laboriosa e intensa negociación entre países para obtener un acuerdo de reconocimiento mutuo de las certificaciones de seguridad de productos IT realizadas entre un grupo de 14 países entre los que figura España como firmante del acuerdo a través del Ministerio de Administraciones Públicas (*www.map.es/csi/pg3432.htm*).

¿Cuáles son los beneficios de Common Criteria?

Estos 14 países signatarios de los acuerdos de Common Criteria, llegaron a este arreglo porque permitiría establecer un único criterio con el que evaluar la seguridad de los productos de IT, contribuyendo a aumentar la confianza de los usuarios en los mismos. Este hecho es beneficioso porque habilita a los usuarios la posibilidad de tomar decisiones con información y criterio, por encima de otras consideraciones:

- Los usuarios pueden comparar sus requerimientos específicos frente a los estándares de Common Criteria para determinar el nivel de seguridad que necesitan.
- Los usuarios pueden determinar más fácilmente cuándo un producto cumple una serie de requisitos. Igualmente, Common Criteria exige a los fabricantes de los productos certificados publicar una documentación exhaustiva sobre la seguridad de los productos evaluados.
- Los usuarios pueden tener plena confianza en las evaluaciones de Common Criteria por no ser realizadas por el vendedor, sino por laboratorios independientes. La evaluación de Common Criteria es cada vez más utilizada como condición necesaria para concurrir a concursos públicos. Por ejemplo, el Departamento de Defensa Americano ha anunciado planes para utilizar exclusivamente productos certificados por Common Criteria.

- Debido a que Common Criteria es un estándar internacional, proporciona un conjunto común de estándares que los usuarios con operaciones internacionales pueden utilizar para escoger productos que se ajusten localmente a las necesidades de seguridad.

En definitiva, proporcionando un conjunto de estándares en seguridad como los recogidos por Common Criteria, se crea un lenguaje común entre los fabricantes y los usuarios que ambos pueden entender. Los fabricantes utilizarán este lenguaje para contar a sus clientes potenciales las características de sus productos evaluadas según Common Criteria e, igualmente, habilita a los usuarios a identificar y comunicar adecuadamente sus necesidades de seguridad.

En definitiva, se proporcionan unos medios y mecanismos objetivos que nos permitirán tomar decisiones en base algo más sólido que las meras percepciones.

Certificación EAL4+ de Windows 2000

Microsoft remitió en el año 2000 Microsoft Windows 2000 Proffesional, Server y Advanced Server, a certificación de Common Criteria. Tras dos años sometiendo cientos de componentes a exhaustivos análisis y test, según los estrictos requerimientos de Common Criteria, el nivel obtenido se denomina “EAL4+Flaw Remediation”.

¿Qué significa esto?

A grandes rasgos y simplificando mucho, pues no es objeto de este apartado una exhaustiva revisión de Common Criteria, en una de las fases del proceso se especifica un objetivo de evaluación (TOE), es decir, se define qué es lo que se va a examinar concretamente y, por otro lado, a qué tipo de examen se le va a someter. Pues bien, el TOE al que se sometió la plataforma Windows 2000 fue el más amplio al que hasta la fecha se ha sometido un sistema operativo y, por otro lado, el nivel al que se somete a examen es el EAL4, que es el nivel máximo para un sistema operativo comercial.

Para conocer mejor el alcance de lo que significa este resultado, debemos saber que existen hasta 7 niveles, EA7, aunque los requerimientos de los niveles EAL5-7 se orientan a productos construidos exclusivamente con técnicas y objetivos especializados, por lo que no es generalmente aplicable a ningún producto distribuido comercialmente. EAL4 es por tanto el nivel más elevado para un producto no construido específicamente para cumplir los niveles EAL5-7. El añadido “+ Flaw Remediation” significa que, además, se ha obtenido EAL4 también en la categoría Flaw Remediation, donde se evalúa el procedimiento establecido por el fabricante en el seguimiento y correción de defectos, en este caso, el funcionamiento del Microsft Security Response Team.

En consecuencia, el nivel “EAL4+Flaw Remediation” obtenido por la plataforma Windows 2000 es la mas elevada obtenida por ningún sistema operativo comercial.

Existe gran cantidad de información de detalle sobre el alcance y detalle de los componentes evaluados. En la siguiente URL se puede encontrar esa información: *www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/secureev.asp*.

A grandes rasgos, el objeto de evaluación ha estado compuesto por los requisitos derivados del Controlled Access Protection Profile (CAPP) que incluye control de accesos, identificación y autenticación, auditoría, separación de dominios de seguridad, gestión de la seguridad, etc.

Además se incluyeron las evaluaciones correspondientes a los apartados:

- Sensitive Data Protection: evaluaciones del sistema de encriptación de ficheros en disco o EFS.
- Multi-Master Directory Services: Directorio Activo.
- Virual Private Network: generación de redes privadas virtuales con el IPSEc, L2TP y PPTP de Windows 2000.
- Single Sign On: aunque no está descrito en un Protection Profile específico, la capacidad de establecer SSO está formada por componentes evaluados.
- Flaw Remediation: Microsoft Security Response Center.
- Software Signature creation Device: Certificaciones del NIST: FIPS 140-1 del CSP; FIPS 186-2 para implementaciones de los algoritmos de firma de RSA y DSA.
- Network Management: Windows Management Instrumentation, Active Directory Group Policy, Network Management tools.
- Desktop management: Group Policy.

Los sistemas operativos MS Windows XP y MS Windows Server 2003 están en la "pipeline" para comenzar idéntico proceso que el seguido por Windows 2000. No olvidemos que el proceso es exhaustivo y requiere tiempo.

Y siendo usuario de la plataforma MS Windows 2000 ¿cómo puedo beneficiarme ya de esta evaluación ?

Ya hemos apuntado que uno de los beneficios de la Certificación Common Criteria es que proporciona a los usuarios guías que simplifican el despliegue y la operación de Windows 2000 en un entorno de red seguro.

Con este objetivo, Microsoft ha trabajado para asegurarse que el esfuerzo hecho para Common Criteria sea presentado para proporcionar una utilidad inmediata para los usuarios. De esta forma hemos generado estas guías con sus correspondientes plantillas y checklists para faciltar la puesta en marcha de las configuraciones certificadas:

- Windows 2000 Common Criteria Evaluated Configuration User's Guide: *www.microsoft.com/technet/security/issues/W2kCCUG/default.asp*
- Windows 2000 Common Criteria Evaluated Configuration Administrator's Guide: *www.microsoft.com/technet/security/issues/W2kCCAdm/default.asp*
- Windows 2000 Common Criteria Security Configuration Guide: *www.microsoft.com/technet/security/issues/W2kCCSCG/default.asp*

Conclusiones

Actualmente Common Criteria representa uno de los principales organismos que nos permiten conocer las necesidades de seguridad de los usuarios y responder en consecuencia.

Es decir, establecer un lenguaje común de entendimiento en el que seamos capaces de identificar objetivamente las necesidades de seguridad que como usuarios requerimos así como identificar los productos que reúnen tales características, por encima de percepciones e ideas preconcebidas. Tomar las decisiones oportunas con la propiedad que otorga la información y el conocimiento siempre será la mejor opción.

Shared Source Initiative

Código fuente licenciado a grandes clientes, integradores, universidades, laboratorios y organismos gubernamentales a través de este modelo de licencia (*www.microsoft.com/licensing/sharedsource/default.asp*) y su versión personalizada para grandes empresas (*www.microsoft.com/licensing/sharedsource/enterprise.asp*)

Especificaciones WS-Security (GXA)

Iniciativa para describir como adjuntar cabeceras de firma y encriptación a los mensajes SOAP en la fase de diseño. También, describe cómo adjuntar tokens de seguridad, incluyendo tokens binarios como certificados X.509 o tickets Kerberos a los mensajes.

Palladium

Palladium es una nueva arquitectura de hardware y software. Esta arquitectura incluirá un nuevo "chip de seguridad", cambios en los diseños de las CPUs, chipsets y periféricos como teclados o impresoras. Proporcionará un entorno

en el que las aplicaciones y sus componentes se ejecuten en áreas protegidas de la memoria, altamente resistentes a cualquier tipo de interferencia, proporcionando a los individuos y grupos de usuarios mayores niveles de seguridad, privacidad e integridad de su sistema. ¿De qué forma?

Integridad del sistema

Palladium reducirá enormemente el riesgo de ataques de software (troyanos, virus y demás códigos maliciosos) proporcionando a los usuarios la integridad de un sistema protegido end-to-end a través de la red.

Proporcionará un entorno seguro de proceso donde el código "Trusted" se ejecutará en un área de memoria físicamente aislada, protegida e inaccesible al resto del sistema, haciéndolo inherentemente impermeable a virus, espionaje u otros ataques.

Tanto el software como el hardware podrán ser criptográficamente validados ante los usuarios y ante otros ordenadores, programas y servicios, es decir, el sistema podrá verificar que otros computadores y procesos son de confianza antes de utilizarlos o compartir información con ellos. Nadie podrá hacerse pasar por el usuario desde un ordenador diferente.

El código fuente del "Trusted Operating Root", la pieza clave del sistema, será publicado a través de la Shared Source Inititive de forma que pueda ser evaluado por terceras partes.

Queremos generar confianza con respecto al funcionamiento del sistema entre los integradores y los usuarios, del mismo modo que en su momento la publicación de los algoritmos de RSA tuvieron ese efecto. Como comenta John Manferdelli, General Manager de Microsoft "Palladium" Business Unit : «la belleza de publicar el código fuente del Trusted Operating Root es que corresponde a un tipo de tecnología que, incluso siendo conocida, permanecerá irrompible. En efecto, conocer lo que está ocurriendo va a ser muy importante para ganar confianza».

La interacción con el ordenador será mucho más segura porque una nueva arquitectura de hardware opcional proporcionará vías o caminos protegidos desde el teclado hasta la pantalla del monitor de forma que los pulsos del teclado no podrán ser husmeados o suplantados, ni siquiera por drivers maliciosos, y sólo se presentarán en la pantalla salidas gráficas de confianza, es decir, una interface segura que no podrá ser suplantada o interceptada.

Privacidad Personal

Palladium previene las suplantaciones de identidad y los accesos no autorizados a datos personales tanto en Internet como en otras redes. No une intrínsecamente la identidad personal al ordenador.

Es muy importante destacar que en todo momento el usuario controlará que información se revela dado que podrá operar en diferentes entornos en una misma máquina, como un conjunto de cámaras aisladas cada una con sus propios identificadores, políticas y categoría de datos.

Las transacciones y procesos son verificables y fiables (a través de la arquitectura hardware y software "comprobada"), y no pueden ser suplantados puesto que los secretos del sistema están encadenados firmemente al ordenador y sólo se pueden revelar en los términos que el usuario permite. Igualmente, la interface segura de usuario previene el espionaje y la suplantación.

El usuario escogerá cuándo utilizar Palladium o no. De hecho, los ordenadores saldrán con las características de Palladium desactivadas por defecto.

Los otros programas Windows y funciones que operen independientemente de Palladium no podrán acceder nunca a las características de Palladium ni a sus secretos

Seguridad mejorada

Las características de seguridad robusta hacen del PC el mejor sitio para guardar de forma segura cualquier dato o contenido, ya sea comercial o privado.

La seguridad es mantenida a través del sistema de forma que el código en el que se confía no puede ser observado ni modificado mientras se ejecuta en ese entorno de confianza. De la misma forma, los ficheros son encriptados con parámetros secretos específicos de la máquina, haciéndolos inaccesibles si son sustraídos o copiados sin permiso dado que los secretos específicos de la máquina se protegen física y criptográficamente.

Esta nueva arquitectura evitará la suplantación, el engaño y la interceptación de datos.

Los ataques BORE (Break Once, Run Anywhere), se hacen impracticables por varios motivos: los secretos del sistema se almacenan en hardware donde ningún ataque por software puede revelarlos, incluso expuesto a sofisticados ataques de hardware; los secretos del sistema sólo serán aplicables a los datos en el sistema y no pueden usarse para desarrollar ataques generalizados.

En conclusión, Palladium ofrecerá una respuesta adecuada a la creciente necesidad de seguridad derivada de los nuevos usos que hacemos de la informática, abriendo nuevas posibilidades y capacidades.

Es importante tener en cuenta que Palladium no está diseñado para reemplazar nada de lo que transcurre y se ejecuta hoy en día en Windows, sino

que introducirá un nuevo nivel de funcionalidad opcional que, de ser utilizada, proporcionará nuevos horizontes de seguridad aprovechables tanto por sistemas empresariales, como por sistemas de DRM, comercio electrónico, etc.

8.2.2 Seguridad por defecto

La idea principal de esta iniciativa es deshabilitar servicios que no son requeridos en muchos escenarios. Esto reduce la "superficie de ataque" accesible.

Es una realidad que muchos sistemas Microsoft se ponen en producción con configuraciones por defecto, lo que no es en absoluto recomendable ni para un producto Microsoft ni para cualquier sistema. El conocimiento de la plataforma es fundametal para la seguridad de la misma.

En cualquier caso, este tipo de configuraciones son una realidad por lo que contemplando ese escenario surge esta iniciativa en la que la instalación por defecto dará más peso a la seguridad, en detrimento de la funcionalidad por defecto.

De esta forma, y a modo de ejemplo, las siguientes versiones de Windows .Net Server 2003 dispondrá de: un servidor de web (IIS6) a habilitar si se requiere su uso pero, por defecto, no será la opción habilitada; Firewall de conexión a Internet habilitado por defecto en Windows XP, etc.

8.2.3 Seguridad en el despliegue

Seguridad en el diseño y seguridad por defecto son muy importantes pero sólo se aplican en el momento de la creación de los productos. Seguridad en el despliegue es más crítico porque la operación de los sistemas es una actividad continua.

A través del programa STPP y otras iniciativas, Microsoft proporciona herramientas, servicios y materiales de formación para que los usuarios puedan inmediatamente beneficiarse de ellos y elevar el nivel de seguridad de sus sistemas. Microsoft se centra en tres elementos:

Personas

Educar a los administradores en prácticas de seguridad y en determinar cómo políticas de seguridad consistentes es absolutamente crítico. Microsoft ha desarrollado nuevos trainings centrados en la seguridad (*www.microsoft.com/traincert/solutions/security.asp*) impartidos por Microsoft Certified Technical Education Centers (CTECs) y Authorized Academic Training Partners (AATP). Estos trainings enseñan a los administradores cómo configurar

y manejar las características de seguridad de sus sistemas, incluyendo temas como la protección de servidores contra ataques utilizando las características propias del sistema, protección antivirus y cómo desarrollar aplicaciones web seguras.

Procesos

Diseñar la seguridad en los procesos de negocio desde el principio y validar esos components de seguridad es fundamental. Microsoft ofrece el Microsoft Security Toolkit gratuito, que incluye guias de buen uso, información sobre la securización de Windows NT 4.0 y sistemas Windows 2000, así como service packs y parches que eliminan vulnerabilidades especialmente peligrosas. Resultan asimismo muy interesantes las guías de operaciones de seguridad de Windows 2000 (*www.microsoft.com/spain/technet/seguridad/2000server/*)

Tecnología

Las herramientas de seguridad y actualizaciones de productos son las piezas clave en los esfuerzos de Microsoft en seguridad. Estos incluyen:

- Software Update Service (SUS). (*www.microsoft.com/windows2000/windowsupdate/sus/*), proporciona a los administradores más flexibilidad y control sobre cómo y cuándo se instalan los updates críticos de seguridad. Para ello, se utiliza la tecnología de Windows Update, es decir, el servidor (o servidores) de Windows Update al que se conectarán los servidores internos no serán los de Microsoft, sino los servidores internos de Windows Update corporativos, que utilizando la misma tecnología que emplea Microsoft, podrán distribuir dichas actualizaciones internamente y, lo que es más importante, de forma controlada y administrada.

  Mediante el correcto funcionamiento de esta tecnología, se podrán mantener actualizados los sistemas en términos de seguridad de forma más eficiente.

  En cualquier caso, la forma más adecuada para este tipo de distribuciones sigue siendo SMS con el ValuePack que permite la distribución controlada de updates de seguridad.

- Microsoft Baseline Security Analyzer (MBSA). (*www.microsoft.com/technet/security/tools/Tools/MBSAhome.asp*), permite a los administradores escanear automáticamente sistemas para detectar problemas como passwords en blanco o débiles, nivel de parcheo o errores comunes. La herramienta de informe permite identificar muy fácilmente qué problemas necesitan ser corregidos y en qué máquina. Otras herramientas incluyen el IIS Lockdown (*www.microsoft.com/technet/security/tools/tools/locktool.asp*) y el URLScan (*www.microsoft.com/technet/security/tools/tools/urlscan.asp*) para IIS.

- Firewall Internet Security and Acceleration (ISA) Server 2000 (*www.microsoft.com/firewall/*) y Systems Management Server (SMS) (*www.microsoft.com/smserver/*) con SMS Value Pack para gestión de updates y parches a gran escala.

9

La Aplicación del Reglamento de Seguridad en los Sistemas Microsoft

La siguiente guía pretende dar respuestas básicas a los problemas que para el cumplimiento de la norma puede encontrarse el responsable de seguridad en el entorno de los sistemas operativos Microsoft Windows 2000 y Microsoft Windows XP. La integración de los productos Microsoft produce que la mayoría de las medidas de seguridad sean establecidas desde el sistema operativo. Ello no quiere decir que existan medidas adicionales o especializadas para determinados productos, como por ejemplo Microsoft SQL Server 2000 o Microsoft Exchange Server 2000, sino que las características básicas de seguridad las tendremos que contemplar primero y de forma general desde el sistema operativo para luego ir ampliándolas a las especialidades del resto de productos.

Las aplicaciones que generen ficheros susceptibles de contener datos objeto de la norma en cuestión, incluyendo las aplicaciones de productividad Microsoft del tipo Microsoft Office XP, sustentarán la mayoría de las características de seguridad en el sistema operativo, de ahí la importancia de conocer en primer lugar las características de seguridad que éste nos ofrece.

Pero también las bases de datos relacionales han supuesto para la mayoría de las empresas la capacidad de almacenar una gran cantidad de datos fácilmente disponibles y ofreciendo una gran ventaja para su análisis y la toma de decisiones. Sin duda, la mayor parte de los datos que una empresa contiene son guardados en sistemas relacionales de bases de datos y, sin duda, muchos de los datos contemplados en la norma serán almacenados en un gestor de base de datos Microsoft SQL Server 2000 por lo que haremos una breve semblanza de las características que el producto nos ofrece para adecuarnos a la seguridad que la norma exige.

Igualmente, el intercambio de información de forma ininterrumpida ha convertido a los sistemas de mensajería en la aplicación fundamental para las compañías de hoy día y ha logrado que la tarea de crear y mantener una infraestructura de mensajería fiable se convierta en uno de los trabajos más importantes de los profesionales de las tecnologías de la información. El intercambio de información da pie a que se puedan transmitir datos de carácter personal y, por ello, es necesario dotar de medidas de seguridad a esos intercambios. Asimismo, la realidad nos indica que gran cantidad de información de todo tipo es almacenada en servidores de Microsoft Exchange Server 2000.

Así, esta guía irá proponiendo aproximaciones para el cumplimiento de la norma artículo por artículo y fijándonos en las características que para cumplirla nos ofrecen estos productos.

9.1 Tecnología de seguridad en Microsoft Windows

La seguridad en los sistemas operativos Microsoft Windows 2000 y Microsoft Windows XP la gestionaremos de forma básica desde las aplicaciones *Directiva de seguridad local* para un ordenador aislado y *Directiva de seguridad de dominio* para un sistema de ordenadores integrados en un dominio. Estas aplicaciones serán la base de actuación y nos facilitarán y asegurarán el establecimiento de medidas de seguridad en un ordenador o en un grupo de ordenadores.

En un entorno de redes, la utilización del Directorio Activo de Microsoft Windows 2000 producirá un mayor control de la seguridad de todos los ordenadores integrantes con un menor coste administrativo gracias a la utilización de *Directiva de seguridad de dominio* y ofrecerá sistemas de seguridad no existentes en ordenadores aislados por lo que resulta altamente recomendable su utilización cuando el sistema de información contenedor de los datos se encuentre distribuido en una serie de ordenadores tal y como sucede normalmente en la actualidad.

Junto a la tecnología la definición de los procedimientos operativos es algo primordial. No es objeto de esta guía la definición de estos procedimientos pero un buen comienzo para su definición puede ser la Guía de Operaciones de Seguridad de Microsoft Windows 2000 la cual puede ser consultada en el siguiente enlace: *www.microsoft.com/technet/treeview/default.asp?url=/TechNet/security/prodtech/windows/windows2000/staysecure/DEFAULT.asp*.

Igualmente esta guía no pretende ofrecer una visión exhaustiva de cada una de las medidas posibles para el cumplimiento de la norma, simplemente dotar de una aproximación que tendrá que completarse con la ayuda, los manuales del producto y la información que Microsoft pone a disposición de todos los usuarios, la cual puede ser consultada en *www.microsoft.com/security*.

La norma divide las medidas de seguridad en tres tipos dependiendo de la información contenida, de tal forma que los ficheros que contengan esta información cumplan las medidas correspondientes al tipo de información que guardan, y estas medidas han de cumplirse tanto en lo que respecta al almacenamiento y explotación de los ficheros en local, esto es, en un mismo ordenador, como en lo que respecta a su utilización en red, esto es, en varios ordenadores que se comunican entre ellos. Asimismo la norma requiere que los ficheros temporales generados por la explotación de un fichero con datos de carácter personal cumplan las mismas medidas que el fichero originante.

9.2 Tecnología aplicable a las medidas de nivel básico

Como anteriormente hemos señalado, la seguridad de Microsoft Windows 2000 y Microsoft Windows XP se basa en la atribución de derechos de acceso y utilización de privilegios otorgados a los principales, usuarios o aplicaciones, sobre objetos y recursos existentes en el sistema; básicamente ficheros, impresoras y dispositivos. Las características de seguridad en ambos productos han sido centralizadas mediante una serie de herramientas denominadas *Security Configuration Tool Set* que son simplemente unos gestores de plantillas y políticas que nos permiten definir la *Directiva de seguridad local* (*Local Security Policy*). Todos los ordenadores Microsoft Windows 2000 o Microsoft Windows XP, excepto los controladores de dominio de un Directorio Activo que comparten una entre todos denominada *Directiva de seguridad de los controladores de dominio*, poseen una *Directiva de seguridad local* que se aplica cada vez que un ordenador se inicia. Esta política local se crea en la instalación y se modifica bien manualmente, bien mediante la utilización de plantillas de seguridad, bien mediante la aplicación de Objetos de Políticas de Grupo (*Group Policy Object*) cuando el ordenador está integrado en un Directorio Activo, en este último caso con una comprobación cada cierto tiempo de la adecuación de los valores locales con los establecidos por el objeto de la política de grupo.

En la figura 9.1 podemos ver la política de seguridad local de Microsoft Windows 2000 y de Microsoft Windows XP.

No es misión de esta guía detallar uno a uno el significado de cada parámetro de dichas políticas, para lo que remitimos a la ayuda de cada producto, simplemente señalar la importancia de su conocimiento y utilización para la realización de las acciones posteriormente descritas.

El acceso a la *Directiva de seguridad local* se realiza desde el botón Inicio, Panel de Control, Herramientas administrativas en ambos productos tal y como puede verse en la figura 9.2.

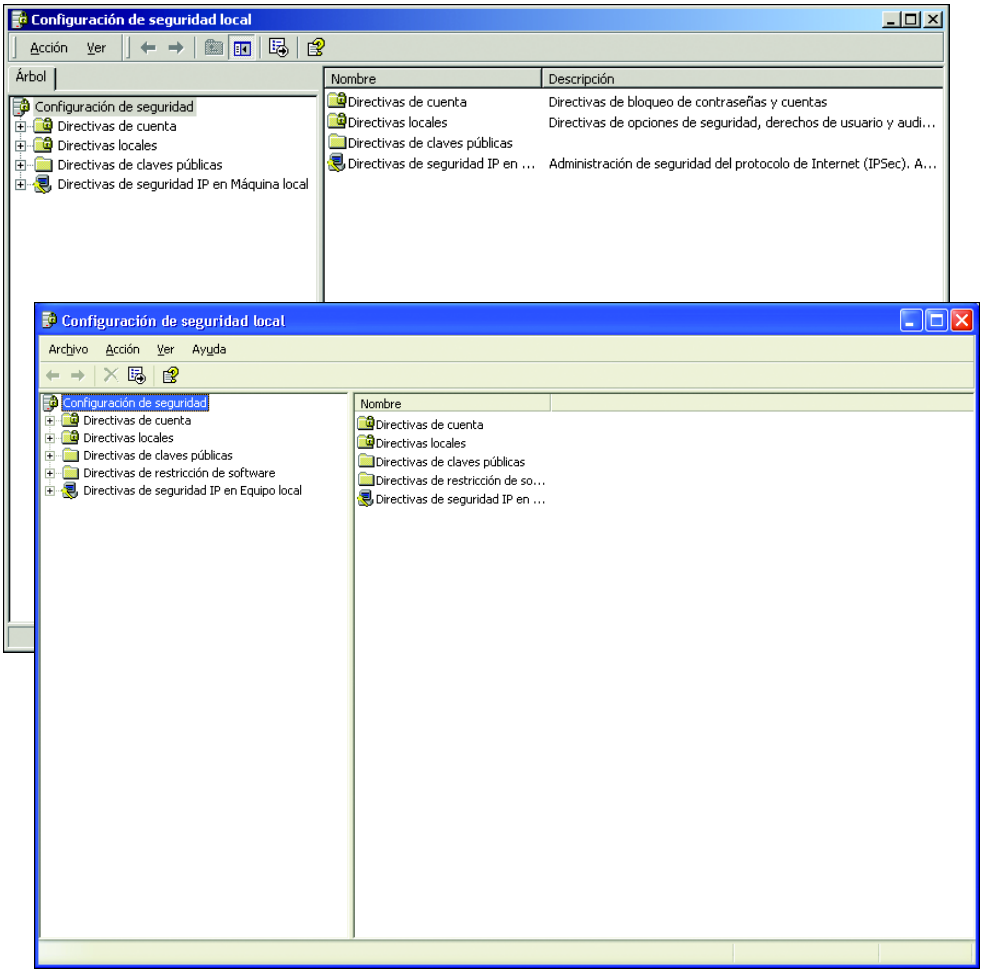


Figura 9.1. *Políticas de seguridad locales en Windows 2000 y Windows XP.*

La inclusión de los clientes Microsoft Windows 2000 y Microsoft Windows XP en un Directorio Activo posibilita la centralización de estas características de seguridad, la simplificación de la administración y la autentificación única posibilitando las funcionalidades de *single sign on* que provocan una mejor gestión del control de acceso. Además, el Directorio Activo nos ofrece características de seguridad mucho más avanzadas no disponibles en máquinas aisladas como son la posibilidad de la utilización de tarjetas inteligentes para el inicio de sesión, el uso del protocolo *Kerberos* para la autentificación en la red y la posibilidad de implementación de sistemas de infraestructuras de clave pública (*Public Key Infrastructure* o PKI) absolutamente integrados en el Directorio.

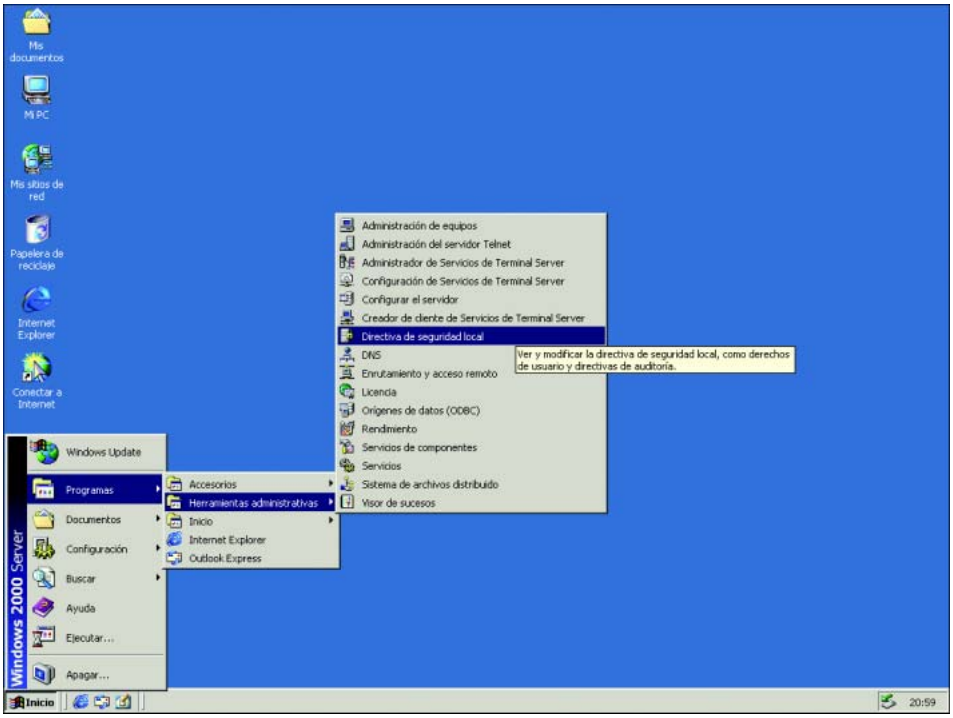


Figura 9.2. *Acceso a la Directiva de seguridad local*

9.2.1 Ficheros temporales en Microsoft Windows 2000 y Microsoft Windows XP

Las aplicaciones Microsoft que generan ficheros temporales, bien con motivo de copia de respaldo o con motivo de ejecutarse en un entorno multiusuario, borran éstos una vez finalizada su utilización.

En la figura 9.3 podemos ver la generación de ficheros temporales de copias de seguridad y entorno de red ante la apertura de un fichero Microsoft Office XP.

Una vez terminada la edición, los archivos temporales desaparecen, quedando únicamente los archivos que hemos creado voluntariamente, de esta manera estamos a salvo de olvidar los datos que la aplicación utiliza como copia de seguridad (ver figura 9.4.).

Además de lo anterior, debido a las propias características del sistema operativo, los ficheros temporales se generan siempre con los permisos que heredan del objeto que los crea. Esto es, si el usuario que tiene permiso a un fichero es único y abre el fichero, los ficheros temporales que se creen tendrán los

mismos permisos que el fichero origen por lo que ningún otro usuario podrá leerlos aun cuando se quedaran sin borrar debido a un error de la aplicación o a un apagado accidental del sistema operativo.

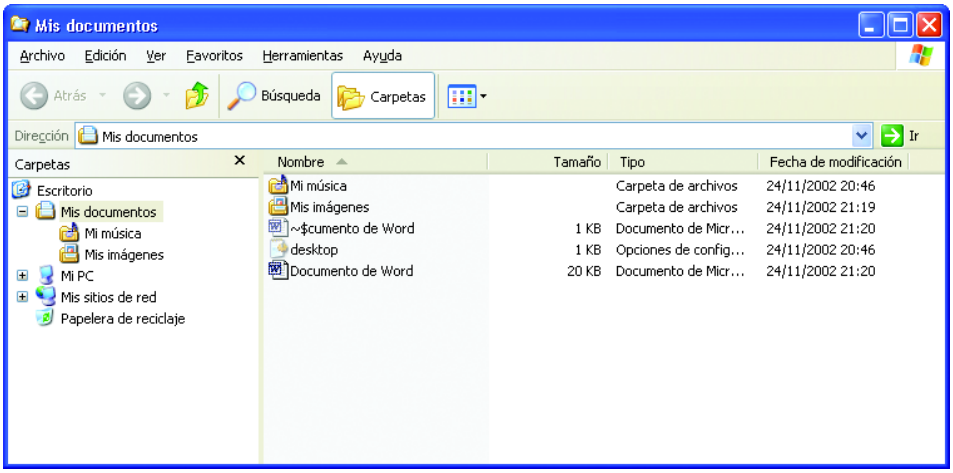


Figura 9.3. *Generación de ficheros temporales*

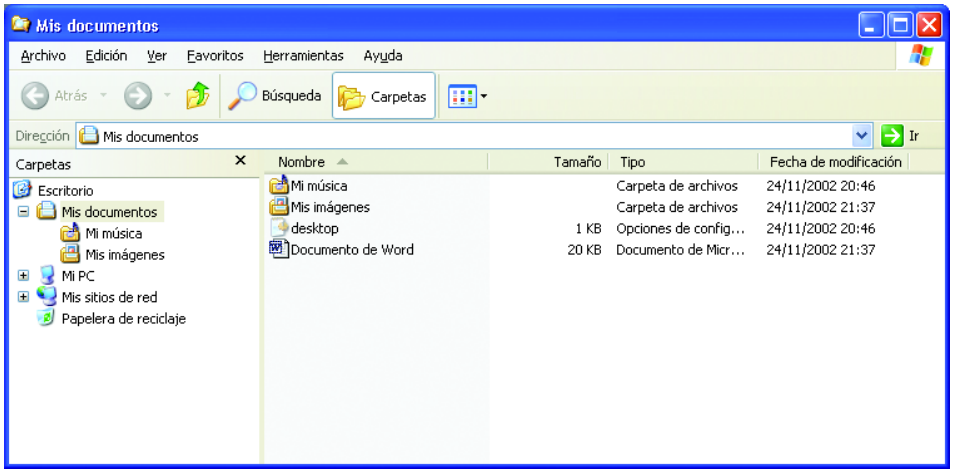


Figura 9.4. *Sin ficheros temporales*

No obstante lo anterior, el administrador o usuario debe realizar una limpieza de mantenimiento respecto de los ficheros temporales que accidentalmente puedan quedar en el sistema, lo que puede hacer con la utilidad *Liberador de espacio en disco* la cual nos eliminará tanto estos archivos temporales como otros tipos de archivos que ya no se pretenden utilizar, tales como:

- Páginas de caché y programas obtenidos de Internet
- Archivos en la papelera

En la figura 9.5 podemos observar la pantalla de opciones de la utilidad a la cual podemos invocar desde el comando Accesorios del menú Inicio.

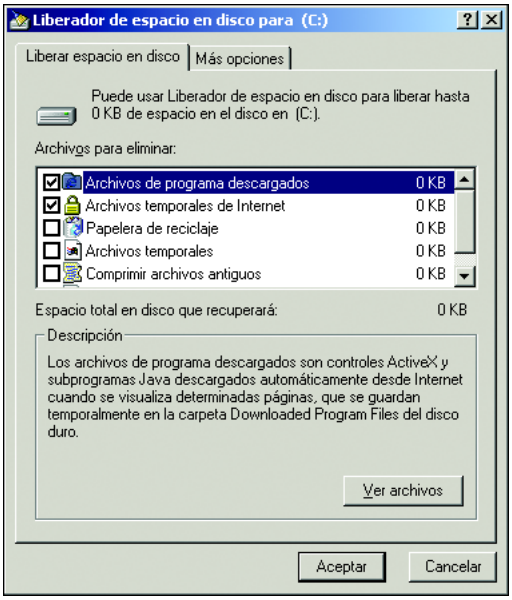


Figura 9.5. *Acceso al Liberador de espacio en disco*

Igualmente, Microsoft Windows 2000 y superior utilizan parte del disco como extensión de la memoria física. A esto lo llamamos memoria virtual y almacena datos de la memoria volátil en disco mientras no son requeridos para liberar memoria y realizar otros procesos de cálculo. Para asegurarnos que este fichero no contenga ningún tipo de datos podemos forzar al sistema para que lo borre cada vez que se apague, de tal forma que ningún dato de la memoria se almacenará en disco una vez apagado el sistema. Para ello bien en la directiva local o de dominio habilitaremos la opción Borrar el archivo de páginas de la memoria virtual al apagar el sistema, como podemos ver en la figura 9.6.

En un entorno multiusuario (a través *Servicios de terminal*), se encuentra definido por defecto que se eliminen los archivos temporales generados por las aplicaciones. No obstante, existe la posibilidad de deshabilitar esta opción, hecho que no aconsejamos ya que pudieran no eliminarse archivos temporales que contuvieran datos de carácter personal.

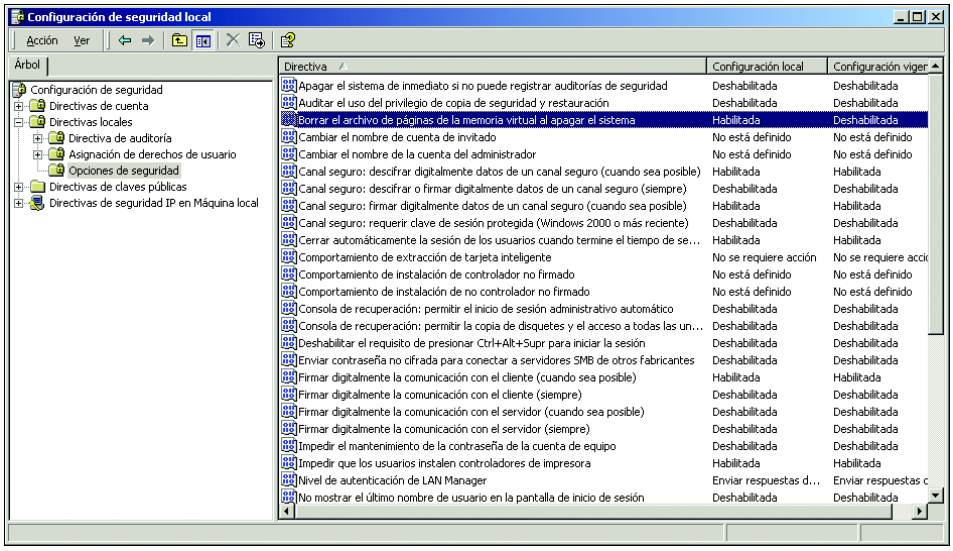


Figura 9.6. *Activación del Borrar el archivo de páginas de la memoria virtual.*

Señaladas estas características básicas veamos como aplicarlas en cada caso concreto.

9.2.2 Artículo 9.2 (Conocimiento de los procedimientos)

> *"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."*

Tanto en el sistema operativo Microsoft Windows 2000 como en el sistema operativo Microsoft Windows XP podemos introducir un aviso legal que se presente cada vez que el usuario accede al sistema de forma interactiva y que asegure que el usuario validado conoce las normas de seguridad al remitirles a ellas.

Para introducir esto en la Directiva de seguridad local o Directiva de seguridad de dominio en la carpeta Opciones de Seguridad haremos doble clic sobre la opción Texto de mensaje para los usuarios que intentan conectarse introduciendo el mensaje apropiado como vemos en las figuras 9.7a y 9.7b.

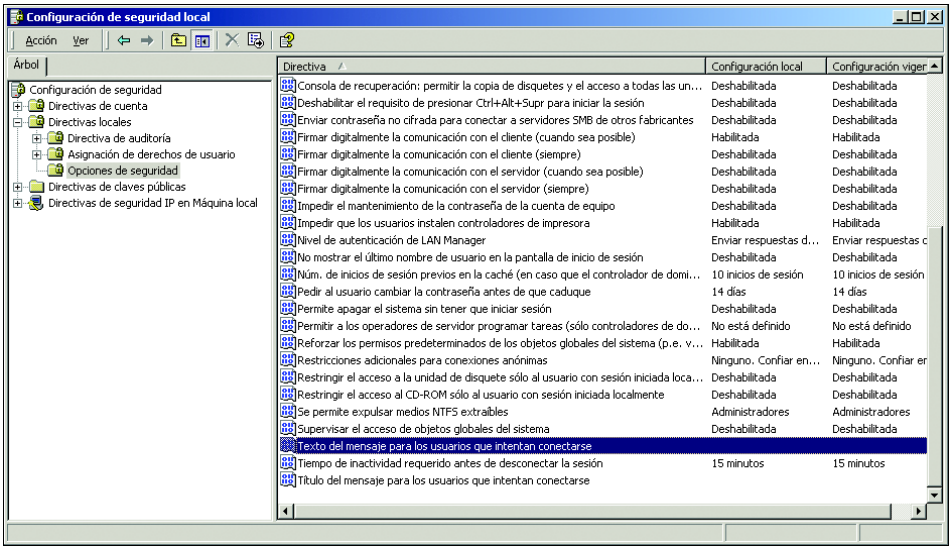


Figura 9.7a. *Opción "Texto del mensaje para los usuarios que intentan conectarse"*

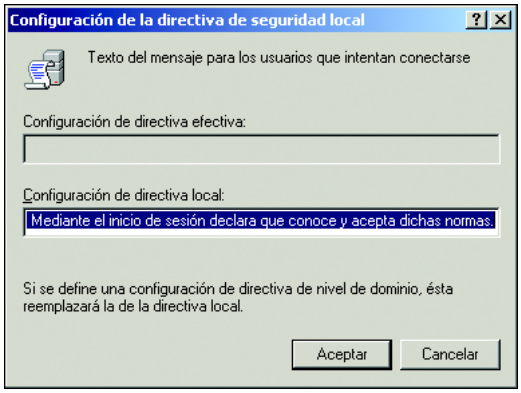


Figura 9.7b. *Configuración del mensaje de advertencia para usuarios que intenten acceder.*

Cada vez que un usuario intente iniciar una sesión interactiva en el sistema este mensaje le aparecerá de forma previa como podemos comprobarlo en la figura 9.8.

Lo que nos asegura el conocimiento y aceptación de las políticas de acceso establecidas por el responsable de seguridad.

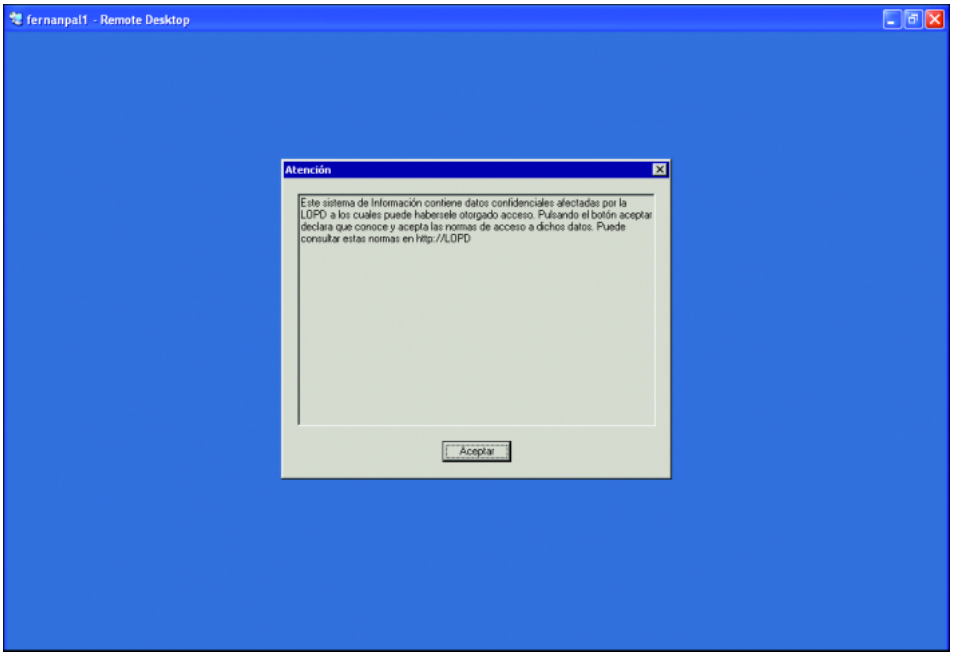


Figura 9.8. *Mensaje de alerta: "Acceso a información sensible afectada por la legislación vigente de LOPD".*

9.2.3 Artículo 10. Registro de incidencias. (Auditoría)

> *"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."*

Es importante señalar que el sistema de registro de acciones de Microsoft Windows 2000 y Microsoft Windows XP no garantiza pleno cumplimiento de esta medida ya que debería implantarse un registro de incidencias para las "no informáticas".

El sistema de registro de acciones de Microsoft Windows 2000 y Microsoft Windows XP es muy potente y permite la obtención de un registro detallado de acciones realizadas en el sistema configurables por el administrador que, junto con el servicio de alertas que veremos posteriormente, puede ser utilizado para la creación del sistema de registro y notificación señalado por la norma.

Estas acciones registradas, respecto a la perspectiva de seguridad, se referirán tanto al uso de privilegios como al control de acceso a objetos asegurados.

Microsoft Windows 2000 y Microsoft Windows XP poseen varias categorías de auditoría referidas a eventos de seguridad y, cuando diseñamos la estrategia de auditoría, debemos definir como auditamos los eventos de auditorías referidos a:

- Eventos de inicio de sesión interactivo.
- Eventos de inicio de sesión en el dominio.
- Gestión de cuentas.
- Acceso a objetos.
- Acceso al Directorio Activo si existe.
- Utilización de privilegios.
- Seguimiento de procesos.
- Eventos de sistema.
- Cambios de política de seguridad.

La norma no señala en este nivel que eventos en concreto debemos registrar, si en niveles más restrictivos se nos indican algunos, así que realizaremos una visión general y posteriormente un somero repaso a los posibles eventos para poder realizar una definición estratégica posterior aplicada a cada caso concreto.

La configuración de la captura de eventos y registro a través de la política local se realiza a través de la carpeta Directiva de auditoría, contenida en la carpeta Directivas locales (ver figura 9.9).

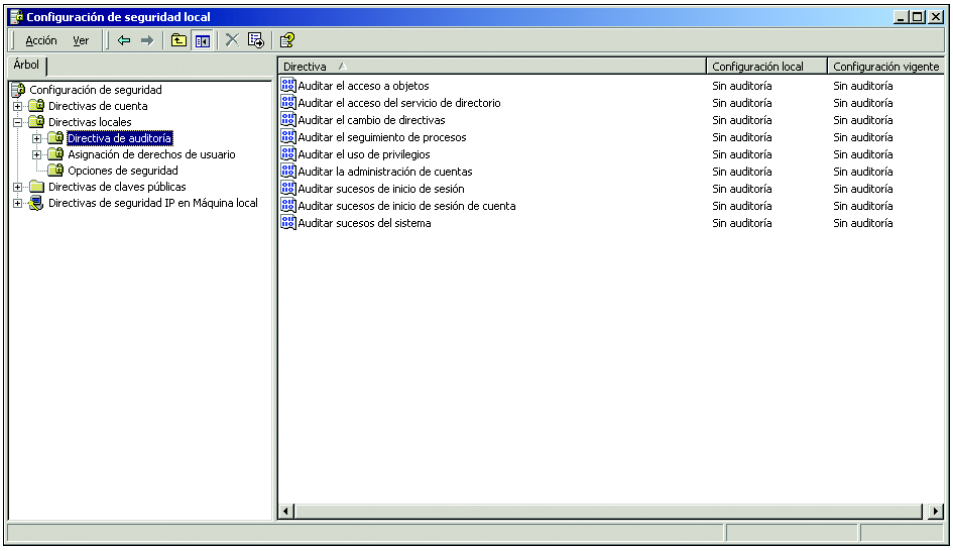


Figura 9.9. *Acceso a las configuraciones de auditoria.*

Podemos auditar cualquiera de las nueve categorías contempladas anteriormente tanto en su vertiente de éxito como fallo en su realización, aunque evidentemente lo que deseemos capturar dependerá del rol que el sistema tiene dentro de la red y de las necesidades de cumplimiento de la norma. Vamos a detallar las posibilidades de auditoría que nos ofrecen cada una de estas categorías.

Eventos de Inicio de sesión

Cada vez que un usuario inicia la sesión o termina la sesión en un sistema, ya sea de forma interactiva o en un sistema remoto con una cuenta local, es generado un evento en el registro de seguridad del ordenador donde se ha producido el inicio de sesión. Igualmente se registran los inicios de sesión de máquina cuando la conexión se realiza desde un ordenador Microsoft Windows NT o superior.

Este registro permitirá saber quién y cuándo intenta iniciar una sesión interactiva, si lo logra o no y los intentos de acceso realizados desde un ordenador predeterminado de la red. Igualmente los accesos vía *Terminal Services*.

Cada evento tiene asociado un ID que señala una acción única como antes hemos visto, en esta categoría los eventos destacables serán los señalados en la tabla 9.1

ID	Descripción
528	Inicio de sesión en un ordenador
529	Intento de inicio de sesión con cuenta o contraseña errónea
530	Intento de inicio válido fuera de las horas permitidas
531	Intento de inicio utilizando una cuenta deshabilitada
532	Intento de inicio utilizando una cuenta caducada
533	Intento de inicio en un ordenador donde no está permitido
534	Intento de inicio no permitido a la cuenta
535	Contraseña caducada
536	El Servicio *Net Logon* no está activo
537	Inicio falló por otras causas

538	La cuenta cerró sesión
539	La cuenta se bloqueó
540	Inicio de sesión de red
682	Reconexión a *Terminal Service*
683	Desconexión a *Terminal Service*

Tabla 9.1. *Tabla de principales eventos.*

Estos eventos me permitirán diagnosticar los siguientes sucesos:

- Fallos locales de inicio de sesión. Cualquiera de los eventos 529 a 534 y el 537 pueden indicar ataques de diccionario que deben ser investigados si se producen repetidamente y según las circunstancias.

- Mal uso de la cuenta. Los eventos 530 a 533 pueden indicar un mal uso de la cuenta o que la restricción aplicada debe ser modificada.

- Bloqueo de cuenta. El evento 539 indica que una cuenta ha sido bloqueada por superar el número de intentos de inicio de sesión, lo que puede suponer un ataque de diccionario.

- Ataques a los servicios de terminal. El evento 683 indica cuándo un usuario desconecta la sesión en un Terminal Service sin cerrarla y el 682 cuándo se reconecta a esa sesión.

Eventos de Inicio de sesión en el dominio

Cuando un usuario inicia una sesión en el dominio se registra un evento en el Controlador de dominio donde se le han verificado los credenciales. Esto nos señalará cuando un usuario intenta iniciar una sesión que le permita la utilización de los recursos del dominio. No obstante, deberemos, para tener una visión global, consolidar todos los sucesos de todos los controladores de dominio para tener una visión general.

Una herramienta para esta consolidación y una monitorización activa es Microsoft Operations Manager 2000 del que se puede obtener más información en *www.microsoft.com/mom.*

Eventos de esta categoría se recogen en la tabla 9.2.

ID	Descripción
672	Un ticket de Servicio de Autentificación (AS) ha sido exitosamente emitido y validado
673	Un ticket de acceso a servicio (TGS) ha sido emitido
674	Un principal renovó su ticket AS o TGS
675	Fallo de pre-autentificación
676	Fallo en la petición de ticket
677	Un TGS no fue emitido
678	Una cuenta fue satisfactoriamente mapeada a una cuenta de dominio
680	Inicio de sesión válido y paquete de autentificación utilizado
681	Un inicio de sesión de una cuenta de dominio fue intentada
682	Un usuario reconectó una sesión de *Terminal Service* desconectada
683	Un usuario desconectó una sesión de *Terminal Service* sin cerrar la sesión

Tabla 9.2. *Eventos de inicio de sesión en dominio*

De la misma forma estos eventos nos permitirán diagnosticar:

- Fallos de inicio de sesión en el dominio. Los eventos 675 y 677 que habrá que investigar si son repetidos
- Problemas de sincronización de tiempo. Si aparece repetidamente un evento 675 puede producirse un error en el servicio de tiempo el cual es necesario para el sistema *Kerberos*.
- Ataques de Servicios de Terminal de la misma forma que en el caso anterior.

Gestión de cuentas

La auditoría de la gestión de cuentas es utilizada para determinar cuándo los usuarios o grupos son creados, modificados o borrados y quién realiza esa tarea, lo que puede resultar útil para la confección y mantenimiento de los listados exigidos por la norma.

Eventos de esta categoría se recogen en la tabla 9.3.

ID	Descripción
624	Una cuenta de usuario ha sido creada
625	Una cuenta de usuario ha cambiado de tipo
626	Una cuenta de usuario ha sido habilitada
627	Se intentó un cambio de contraseña
628	Se estableció una contraseña de usuario
629	Se deshabilitó una cuenta
630	Se borró una cuenta
631	Se creó un grupo global
632	Se añadió un miembro a un grupo global
633	Se quitó un miembro a un grupo global
634	Se borró un grupo global
635	Se deshabilitó un grupo local creado
636	Se añadió un miembro a un grupo local
637	Se borró un miembro de un grupo local
638	Se borró un grupo local
639	Se modificó un grupo local
641	Se modificó un grupo global
642	Se modificó una cuenta
643	Se modificó una política de dominio
644	Se bloqueó una cuenta

Tabla 9.3. *Eventos correspondientes a la gestión de cuentas*

De la misma forma estos eventos nos permitirán diagnosticar:

- Creaciones de cuentas
- Cambios de la contraseña
- Cambio de estado de una cuenta

- Modificación de los grupos de seguridad
- Bloqueos de cuenta

Acceso a objetos

La auditoría de acceso a objetos se utiliza para saber quién, cuándo y cómo un principal ha accedido a un objeto o recurso del sistema y puede realizarse siempre que el objeto tenga habilitada la Lista de control de accesos de sistema o SACL que detallaremos posteriormente, esto es, que se encuentre en un medio formateado mediante NTFS.

La SACL es una lista que contiene el mismo objeto donde se registra:

- El principal que va a ser auditado
- El tipo específico de acceso que va a ser auditado
- Si lo que vamos a auditar dado el principal y el tipo es la generación de un evento de error o de fallo

Previamente a que los eventos aparezcan en el visor de sucesos de seguridad resulta necesario habilitar esta auditoría mediante la definición de la característica "*Auditar el acceso a objetos*" como podemos observar en las figuras 9.10 y 9.11.

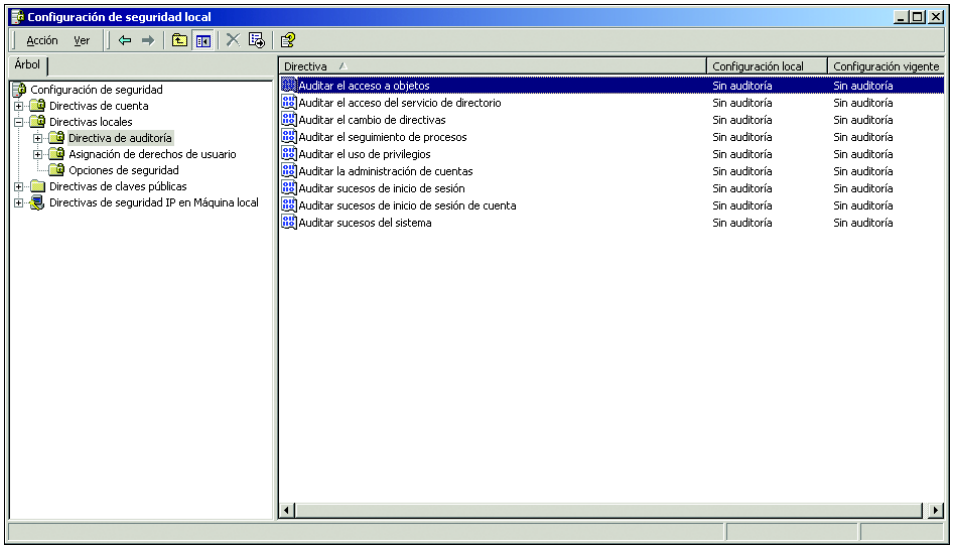


Figura 9.10. *Activación de la auditoría de acceso a objetos.*

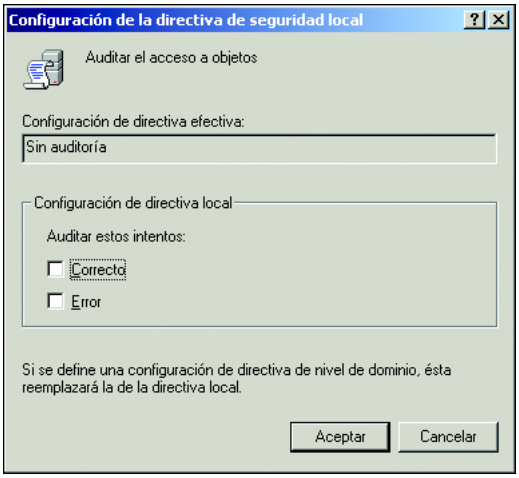


Figura 9.11. *Activación de la auditoría de acceso a objetos.*

Realizado lo anterior debemos acudir al objeto y señalar la auditoría que queremos establecer sobre cada objeto. En la figura 9.12 podemos observar un ejemplo de configuración de la SACL.

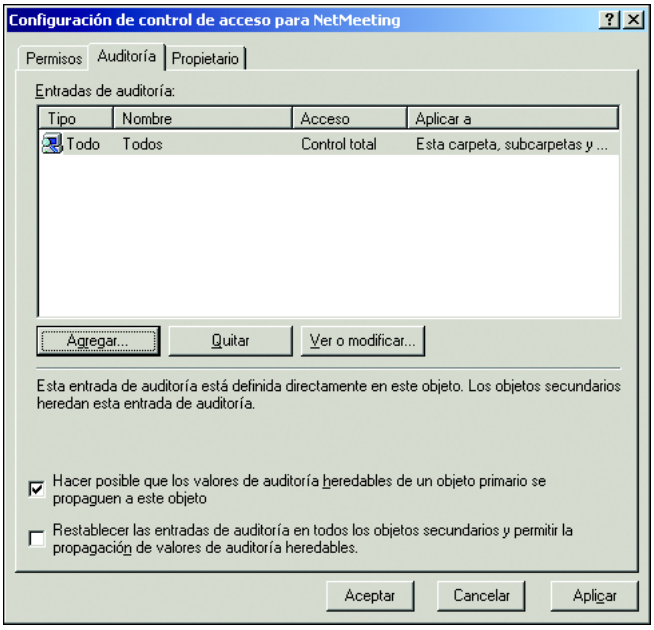


Figura 9.12. *Configuración de la SACL.*

Establecer una buena estrategia de auditoría de este tipo de eventos es vital debido a la importancia que puede tener sobre el rendimiento del servidor y en la carga administrativa, no obstante lo anterior en un sistema basado en Directorio Activo podemos minimizar esta carga administrativa mediante el empleo de políticas de grupo.

Eventos de esta categoría se recogen en la tabla 9.4.

ID	Descripción
560	Se permitió el acceso a un objeto
562	Se cerró el acceso a un objeto
563	Se realizó un intento de borrado
564	Un objeto fue borrado
565	Se permitió un tipo de acceso a un objeto

Tabla 9.4. *Eventos asociados al acceso a objetos.*

Acceso al servicio de Directorio

Los objetos del Directorio Activo también tienen una SACL asociada y que puede ser configurada para auditar. Previamente ya vimos cierta auditoría del Directorio Activo mediante la auditoría de la gestión de cuentas, sin embargo existen otros objetos no asociados al contexto de nombres que puede desearse ser auditados, como los contextos de nombres de configuración y esquema.

La configuración de la SACL de los objetos del Directorio Activo se realiza con la herramienta de consola ADSIEDIT incluida en las herramientas de soporte existentes en el CD de instalación, a través del diálogo "*Advanced Security Settings*" que podemos observar en la figura 9.13 y 9.14.

La auditoría del Directorio Activo es compleja debido a la gran cantidad de eventos que pueden generarse, la mayoría de los cuales serán inocuos, de ahí que la práctica habitual sea sólo auditar aquellos eventos que producen un fallo de acceso lo que ayuda a identificar intentos de acceso no autorizado. Estos eventos se muestran con el ID 565 en el visor de sucesos de seguridad y sólo mirando los detalles podemos determinar a qué objeto corresponden.

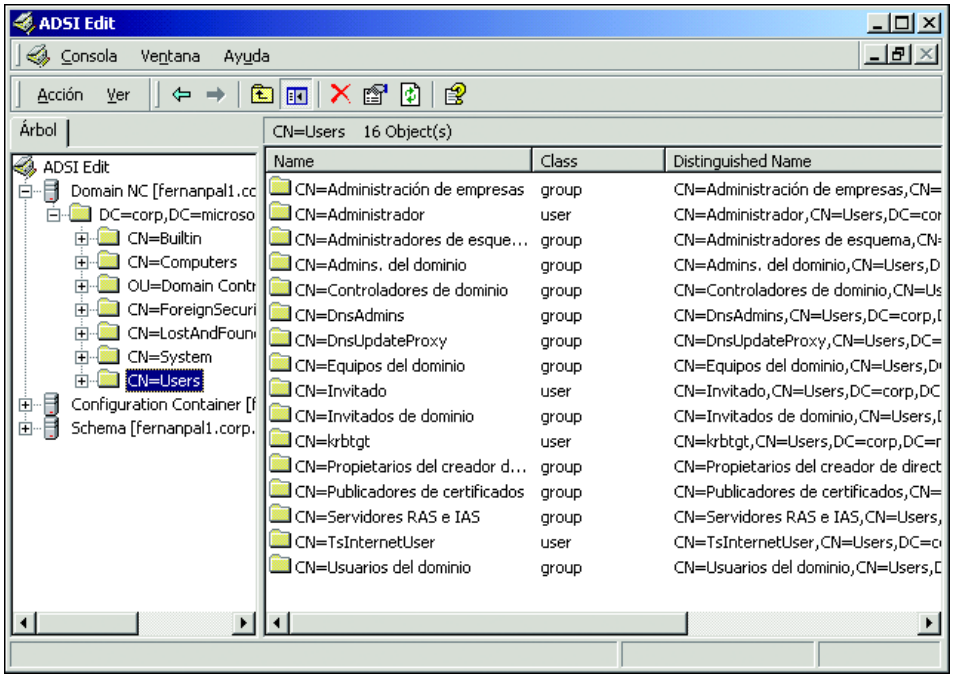


Figura 9.13. *Acceso a Advanced Security Settings.*

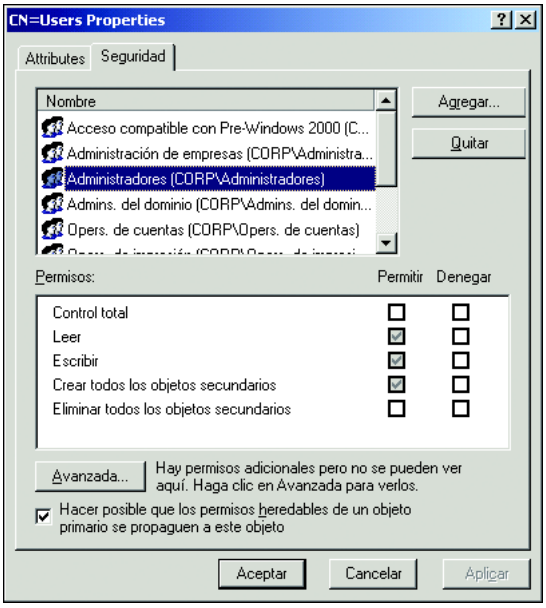


Figura 9.14. *Definición de Permisos.*

Utilización de privilegios

Cada usuario que se encuentre trabajando en un sistema de información tendrá una serie de privilegios, los cuales veremos posteriormente, que pueden ir desde el tipo de sesión que pueden realizar hasta las posibilidades de realizar tareas administrativas como puede ser la realización de una copia de respaldo. En la figura 9.15 podemos observar en la consola local de seguridad los privilegios asociados a los distintos usuarios y grupos de un controlador de dominio por defecto.

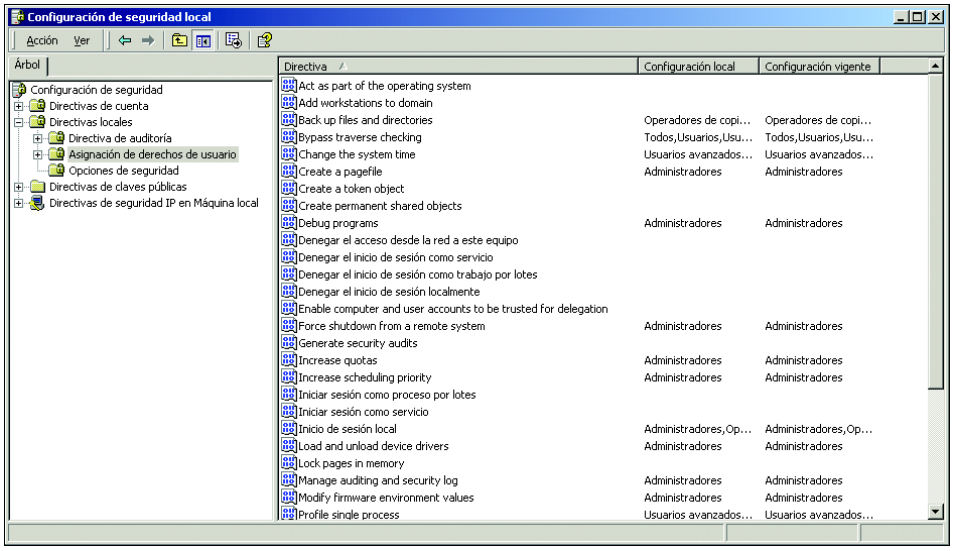


Figura 9.15. *Privilegios asociados s distintos usuarios y grupos.*

Este tipo de auditoría monitoriza la utilización de estos privilegios, lo que en algún caso será un requerimiento de la norma para niveles de protección superiores.

Los eventos que genera este tipo de auditoría se recogen en la tabla 9.5.

ID	Descripción
576	El privilegio especificado se agregó a un *token* de un usuario (Este evento se genera cuando un usuario con determinado privilegio inicia sesión)
577	Un usuario intentó realizar una operación de privilegio
578	Un privilegio fue utilizado sobre un objeto

Tabla 9.5. *Eventos asociados a los privilegios.*

Estos eventos nos permitirán diagnosticar:

- Un intento de elevación de privilegio. Cuando un usuario produce eventos 577 y 578 sobre el privilegio *SeTcbPrivilege* puede indicarnos un intento de elevación de privilegios, el ataque conocido como *GetAdmin* produce este tipo de eventos. El único usuario que debería utilizar este privilegio debería ser la cuenta de Sistema y las cuentas de aquellos servicios a los que se ha asignado el privilegio "*Act as part of the operating system*".

- Un intento de cambio de hora del sistema. Eventos 577 y 578 sobre el privilegio *SeSystemtimePrivilege* indica el intento de un cambio de hora en el sistema, lo que podría servir para enmascarar una acción no autorizada.

- Apagado del sistema. Eventos 577 y 578 con el privilegio *SeRemoteShutdownPrivilege* indican el usuario que ha intentado apagar el sistema de forma remota. Si el intento de apagado es local sólo se generará un evento 577 sobre el privilegio *SeShutdownPrivilege.*

- Carga y descarga de controladores de dispositivo. Los eventos 577 y 578 con el privilegio *SeLoadDriverPrivilege* pueden indicar un intento de cargar un virus troyano en el sistema

- Gestión de eventos y de registros de seguridad. Los eventos 577 y 578 con el privilegio *SeSecurityPrivilege* indican la modificación de estos registros lo que puede suponer un intento de borrar pruebas de un acceso no autorizado.

- Toma de la propiedad de un objeto. Un evento 577 o 578 con el privilegio *SeTakeOwnershipPrivilege* indica el intento de un usuario por obtener el derecho de saltarse la seguridad de acceso a un objeto mediante la adquisición de su propiedad. Veremos esta acción posteriormente en los párrafos dedicados al control de acceso a los ficheros.

Seguimiento de procesos

El seguimiento de procesos se utiliza sobretodo por los desarrolladores para comprobar cómo se generan y finalizan los procesos que una aplicación realiza. Su activación no resulta recomendable por el alto número de eventos que plantea si no es para el propósito antes señalado. Los eventos que genera se recogen en la tabla 9.6.

ID	Descripción
592	Un nuevo proceso se ha creado
593	Un proceso ha finalizado
594	Un *handle* a un objeto fue duplicado
595	Un acceso indirecto a un objeto fue obtenido

Tabla 9.6. *Eventos asociados al seguimiento de procesos.*

Eventos de sistema

Los eventos de sistema se generan cuando un usuario o proceso altera aspectos del entorno del ordenador.

Estos eventos se recogen en la tabla 9.7.

ID	Descripción
512	El sistema se inició
513	El sistema se apagó
514	Un paquete de autentificación fue cargado por la LSA. Posteriormente veremos el significado de esto en detalle.
515	Un proceso de confianza fue registrado por la LSA.
516	No existen recursos para almacenar más registros de auditoria de seguridad
517	El registro de seguridad fue limpiado
518	Un paquete de notificación fue cargado por la SAM

Tabla 9.7. *Eventos del sistema.*

Especial importancia en este tipo de eventos cobrarán el 516 y el 517 para medidas de protección más altas que veremos posteriormente.

Cambios en la política de seguridad

Como estamos observando la política de seguridad se configura como un elemento básico de gestión y protección de los activos contenidos en el sistema y del propio sistema en si. Por tanto, es básico establecer la auditoría del intento de realizar modificaciones en la política para cumplir los requisitos de la norma de comunicación de incidencias.

Los eventos que genera esta categoría se recogen en la tabla 9.8.

ID	Descripción
608	Se asignó un derecho a un usuario
609	Se quitó un derecho a un usuario
610	Se estableció una relación de confianza con otro dominio
611	Se eliminó una relación de confianza con otro dominio
612	Se modificó la política de auditoría
768	Se produjo una colisión de espacio de nombres entre dos bosques

Tabla 9.8. *Eventos de la política de seguridad.*

Los eventos más importantes a destacar en este aspecto son los numerados como 608 ó 609 y su importancia vendrá dada por el privilegio otorgado o eliminado.

Protección de los registros

Hasta el momento hemos señalado qué auditar pero, para la comprobación de incidencias, resulta básica también la salvaguarda de los registros, por ello deberemos asegurarnos que cumplen su función y que mantienen su integridad. Esto lo realizamos mediante el establecimiento de una política de operaciones de auditoría que defina quién tiene acceso a los archivos de registro y a sus parámetros de mantenimiento, qué tamaño alcanzarán los archivos de registro, el tiempo que se mantendrán, las acciones a tomar cuando un archivo se llene. Todas estas características se realizan mediante el Visor de sucesos en las propiedades de cada tipo de eventos como podemos ver en la figura 9.16.

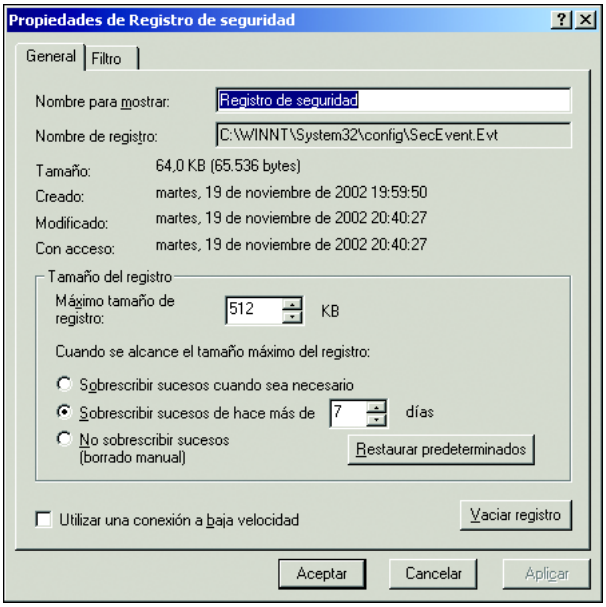


Figura 9.16. *Características del visor de sucesos sobre cada tipo de evento.*

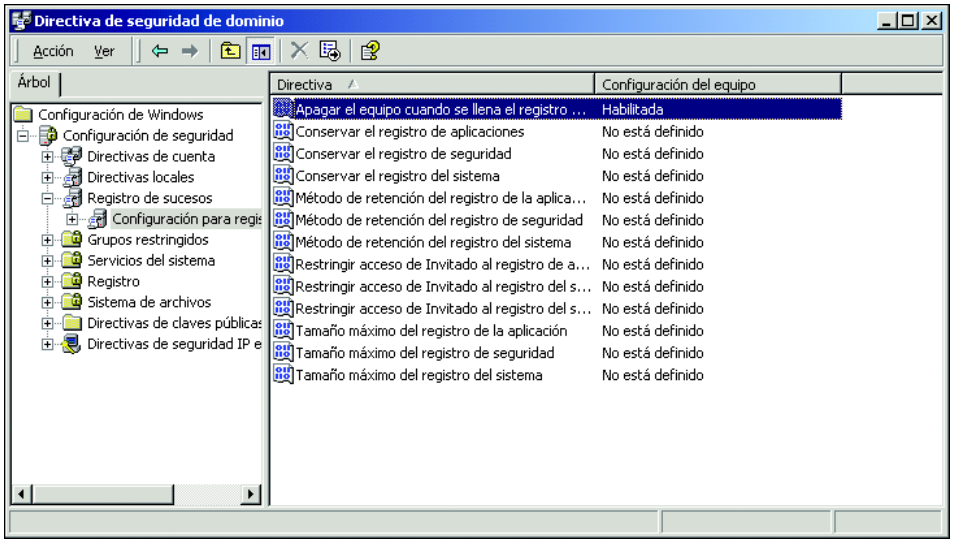


Figura 9.17. *Configuraciones sobre el registro de sucesos.*

En sistemas integrados en un Directorio Activo podremos gestionar toda esta configuración en la política de grupo abriendo la carpeta *Registro de sucesos* y seleccionando la subcarpeta *Configuración para registro de sucesos* donde por defecto podremos señalar tanto los tamaños máximos que ocuparán en el disco los

distintos registros de sucesos, la restricción de acceso a determinadas cuentas, el tiempo y el método de retención de los registros e incluso obligar a parar la máquina ante cualquier incidencia en el registro de seguridad. Ver figura 9.17.

Auditoría en Microsoft SQL Server 2000

Ninguna utilidad exclusivamente informática, y por ello tampoco SQL Server 2000, posee un herramienta tal que sea capaz de realizar una auditoría de seguridad según lo dispuesto en el Reglamento de Seguridad, dado el alcance administrativo que conlleva esta medida.

No obstante, lo que si que existe son determinadas herramientas capaces de facilitar determinados aspectos de la labor auditora sobre la adecuación a las normas de protección de datos.

Estas herramientas son varias y relacionadas con la administración de cambios, configuración y versiones, la administración de la seguridad, la administración de los sistemas y la administración de los problemas e incidencias.

Además, hemos de señalar que las entidades que trabajen con SQL Server 2000 deberán elegir, configurar e implementar alguna o todas de estas herramientas en función de sus necesidades concretas en relación con las labores auditoras que deban realizar (o deban ser realizadas por terceros).

Para cumplir esta función podríamos utilizar el servicio *SQL profiler*. Mediante este servicio podemos cumplir parte de los requisitos marcados por la norma y alcanzar incluso los niveles señalados por la normativa de seguridad C2 definida por el gobierno de los Estados Unidos.

No pretendemos señalar todas y cada una de estas herramientas y nos remitiremos a lo señalado en los diferentes manuales sobre SQL Server 2000 que Microsoft posee.

Auditoría en Microsoft Exchange Server 2000

En el registro de sucesos de Microsoft Windows 2000 se informa de los buzones a los que obtiene acceso cualquier persona que no sea el propietario principal del mismo. Siempre que sea posible, debe asegurarse de que se le notifica siempre que se active un descriptor de seguridad de un buzón. Si mantiene también una lista de los usuarios que pueden tener acceso a cada buzón, podrá contrastar en la lista cualquier cambio efectuado. Como mínimo, debe recopilar información del registro de sucesos que pueda consultar en caso de que surja un problema de seguridad.

Para mantener la seguridad en los equipos con Exchange Server, examine cuidadosamente la pertenencia a grupos. Uno de los grupos críticos que debe supervisar es el de servidores de dominio de Exchange. Cualquier cuenta de usuario o de equipo que pertenezca a la cuenta de servidores de dominio de Exchange tiene pleno control de la organización de Exchange, por lo que es de extrema importancia controlar la pertenencia a este grupo. También debe comprobar el bloqueo de la pertenencia al grupo de administradores integrados de los equipos con Exchange Server. A los miembros de este grupo se les otorgan automáticamente permisos para enviar como en todos los buzones del servidor. La manera más eficaz de controlar la pertenencia a estos grupos es a través de la directiva de grupo.

Asimismo, es recomendable auditar los cambios de configuración aplicados a Exchange. Un sistema adecuado de administración de la configuración y cambios garantiza que no se efectúen cambios que no se han autorizado en el sistema. Por ello, la comprobación sistemática del registro de sucesos (o cualquier otro sistema de supervisión que haya elegido) le permite ver si se han realizado cambios no autorizados.

9.2.4 Artículo 11.1 (Autentificación)

> *"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."*

Microsoft Windows 2000 y Microsoft Windows XP ofrecen un sistema de relación de usuarios con acceso al sistema y diversos procedimientos de autentificación tanto mediante acceso interactivo como mediante acceso desde la red.

En los sistemas Microsoft Windows 2000 y Microsoft Windows XP todo proceso se realiza en el entorno de una cuenta sin que existan procesos anónimos. Esto lo podemos observar en la figura 9.18 donde aparecen los procesos y la cuenta en cuyo contexto se están realizando los procesos.

El sistema de identidad para un entorno de red se basa en el Directorio Activo de Microsoft Windows 2000 y para un sistema local en el archivo local de cuentas (*Security Account Manager* o SAM). Aunque podemos mantener un entorno de red sin utilizar el Directorio Activo la administración se complica y perderemos algunas de las características de seguridad y operaciones que este nos ofrece como antes hemos señalado.

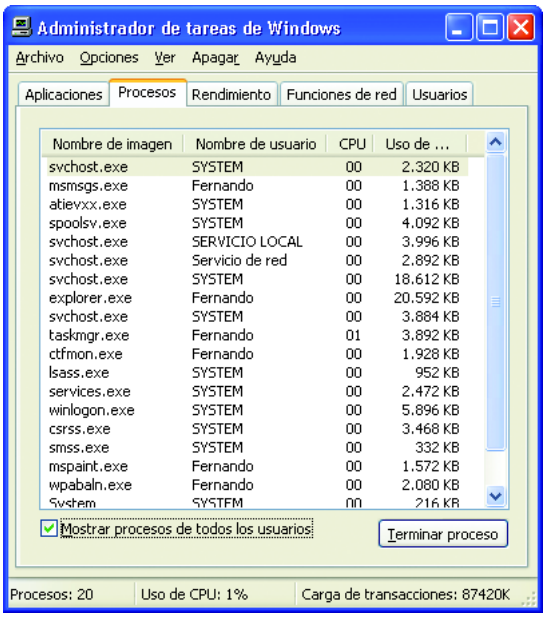


Figura 9.18. *Vista de los procesos en ejecución y cuenta de contexto asociada.*

La gestión de usuarios en ambos casos es muy similar aunque las posibilidades de atributos que identifiquen al usuario son absolutamente flexibles en al ámbito del Directorio Activo mientras que son contadas en la SAM local.

Esta inflexibilidad de la SAM local no quiere decir que la identificación del usuario no pueda realizarse de forma unívoca ya que tanto en la SAM local como el Directorio Activo toda cuenta es identificada de forma única por un identificador de seguridad (*Security Identifiers* o SID). Este SID lleva asociados unos atributos que el Administrador de cuentas puede utilizar para identificar inequívocamente al usuario que pertenece la cuenta. Estos atributos para la SAM local son:

- Nombre de la cuenta que será la palabra que identificará al usuario en el sistema.
- Nombre completo, en el que el Administrador de cuentas puede poner el nombre completo del usuario al que se le ofrece la cuenta.
- Descripción, un campo de texto en que el Administrador de cuentas puede señalar cualquier otra información que considere necesaria para la identificación correcta del usuario.
- Contraseña, palabra clave sólo conocida por el usuario que junto con el nombre de la cuenta le da acceso al sistema y le autentifica.

En el Directorio Activo estos atributos pueden ser configurados para cumplir cualquier tipo de necesidad de identificación mediante la extensión del esquema. A diferencia de la SAM, podemos establecer control de acceso a estos atributos, por ejemplo, para que sólo determinados usuarios puedan ver uno determinado de una cuenta.

Los siguientes atributos son los que por defecto contiene el Directorio Activo visibles en la ventana de propiedades:

- Nombre
- Segundo nombre
- Apellidos
- Nombre completo
- Descripción
- Oficina
- Número de teléfono
- Dirección de correo electrónico
- Página web
- Dirección completa
- Apartado de correos
- Ciudad
- Provincia
- Código Postal
- País
- Teléfono privado
- Buscapersonas
- Teléfono móvil
- Fax
- Teléfono IP
- Notas
- Cargo
- Departamento
- Compañía
- Responsable
- Subordinados

Respecto al procedimiento de autentificación de Microsoft Windows 2000 y Microsoft Windows XP, éste siempre es realizado a nivel local por el componente de autoridad de la seguridad local (*Local Security Authority* o LSA) el cual recogerá los credenciales introducidos y comprobará su veracidad contra una base de datos de autentificación, la SAM local, o el Directorio Activo, a través de un componente de autentificación (*Authentication Package)* que será el encargado de contactar con la base de datos donde existen almacenadas las características de la cuenta. Estos credenciales pueden ser desde una cuenta y contraseña hasta un certificado de cliente o un ticket de sesión *Kerberos*. Comprobada la validez de éste, creará un testigo con el que acompañará todos los identificativos del usuario para el uso de los permisos y privilegios, que veremos posteriormente, y para el acceso a los recursos, que también veremos.

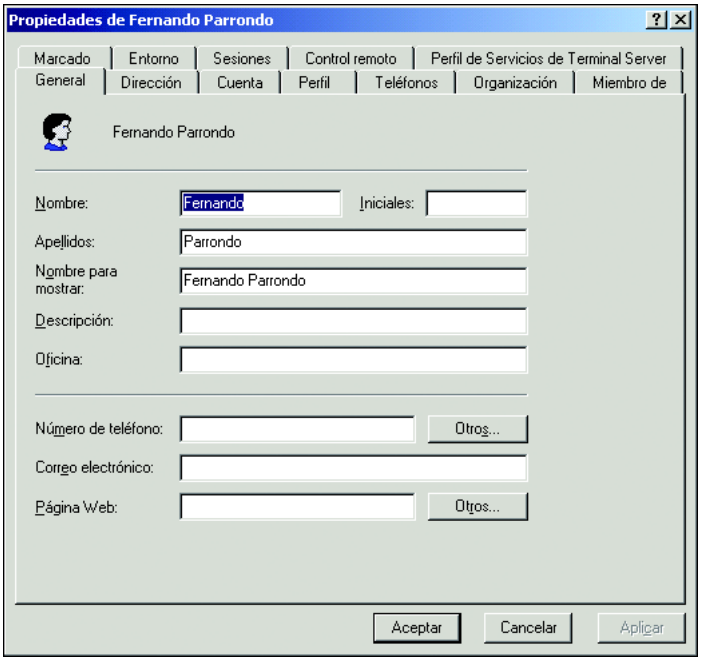
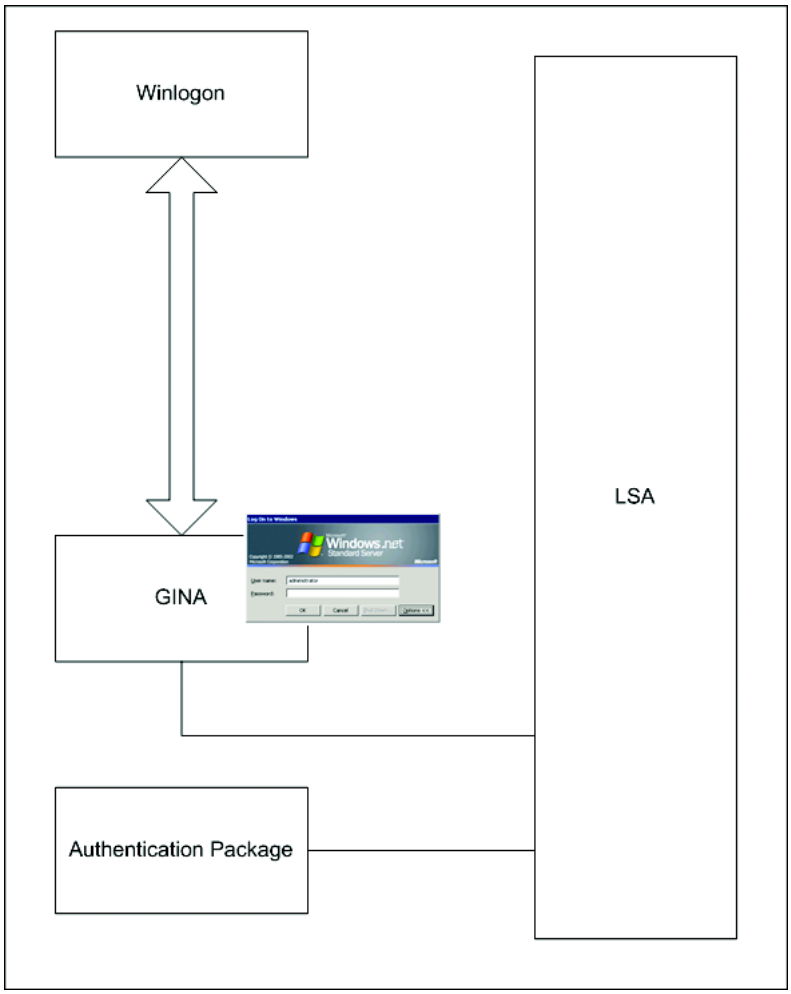


Figura 9.19. *Atributos de identificación.*

Pero para llegar a la LSA existen una serie de procesos previos que en detalle son distintos según la autentificación se intente realizar de una u otra de estas maneras:

- Accedemos de forma interactiva a una máquina con una cuenta local
- Accedemos de forma interactiva a una máquina con una cuenta de dominio
- Accedemos mediante red con una cuenta local de la máquina remota
- Accedemos mediante red con una cuenta de dominio

En el primero de los casos la cuenta que intenta validarse debe existir en la SAM de la máquina en la que intentamos autentificarnos. La SAM local se encuentra almacenada de manera protegida en el registro de la máquina. Cuando un usuario quiere iniciar una sesión, lo primero que realiza es invocar el proceso *Winlogon* a través de una secuencia de atención segura (SAS o *Secure Attention Sequence*), por defecto la combinación de teclas Control-Alt-Delete. Con esto, *Winlogon* envía la notificación al componente denominado GINA (*Graphical Identification aNd Authentication*). La GINA admitirá una combinación de cuenta/contraseña por defecto, aunque es modificable para que admita distintos tipos de credenciales, y pasará esta combinación a la LSA la cual comprobará que existen en la SAM local y que la contraseña es válida a través del paquete de autentificación MSV1_0.



Esquema 1. *Esquema de autenticación.*

La contraseña se pasa a este paquete de autentificación en forma de una clave secreta no reversible generada mediante una función *hash*. Una función *hash* es una fórmula matemática a través de la cual, dada una cadena de caracteres, obtengo un resultado único. La modificación de un solo carácter altera el resultado y, obtenido el resultado con éste, no puedo calcular la cadena de caracteres que lo genera. La SAM, al recibir el paquete de autentificación comprobando la existencia del usuario, realiza la misma función *hash* sobre la contraseña que tiene almacenada y compara ambos resultados, si concuerdan devuelve a la LSA vía el paquete de autentificación el SID del usuario y todos los SID de los grupos a los que el usuario pertenece, junto con otra información que tiene como los privilegios de los SIDs enviados. La LSA con esos datos crea un

testigo de seguridad (*Access token*) el cual es devuelto a *Winlogon*. *Winlogon*, creado el *token*, puede ya abrir el escritorio del usuario en base a los permisos y privilegios que el propio usuario tiene (ver Esquema 1).

Cuando accedemos a una máquina de forma interactiva con una cuenta de dominio, el proceso cambia debido a que el usuario y la contraseña ya no se quedan almacenados en la SAM local sino que se debe autentificar previamente en el dominio para acceder a los recursos locales. Además, igualmente en este caso, la GINA por defecto admite nuevas formas de autentificación que aseguran aun más la identidad del usuario, como puede ser el inicio de sesión con tarjeta inteligente o medidas biométricas, las cuales suponen mayor seguridad al requerir un medio físico además de la combinación de cuenta y contraseña.

Abstrayéndonos de lo anterior, en este caso la LSA utilizará por defecto el paquete de autentificación *Kerberos* versión 5 al que igualmente pasará la combinación de cuenta y *hash* de la contraseña para que éste último, conectándose con cualquier controlador del dominio, requiera del servicio KDC un ticket de sesión que le permita autentificarse en la máquina local. Esto se realiza enviándole al KDC la identidad del cliente e información de pre-autentificación, típicamente la hora del dominio encriptada con el *hash* de la contraseña. Si el KDC puede desencriptar esa información con el propio *hash* de la contraseña que tiene almacenada en el directorio y validarla le enviará al cliente una clave de sesión encriptada con la clave del cliente y un ticket de autentificación o TGT encriptado con la clave del KDC. El TGT actúa como un *token* y permite al cliente requerir otros tickets para servicios existentes en el dominio como el acceso a los recursos del ordenador local de forma que la petición se hace enseñando este ticket. La LSA cogerá este ticket y, validando su información, creará el *token* de seguridad con los SID asociados.

Si no se encuentra un KDC, esto es, no existe un Directorio Activo o el controlador de dominio no es contactado, el paquete de autentificación a utilizar será MSV1_0 que intentará hacer una autentificación *pass-through* de la misma forma que se realiza en Microsoft Windows NT 4.0 y anteriores. Si tampoco puede hacer esta autentificación MSV1_0 intentará realizarla con los credenciales existentes en caché de forma protegida.

Si queremos limitar la utilización de esta caché y exigir que siempre se produzca la autentificación en el dominio, deberemos establecerlo en la Directiva de seguridad mediante la habilitación de esta opción, según se indica en la figura 9.20.

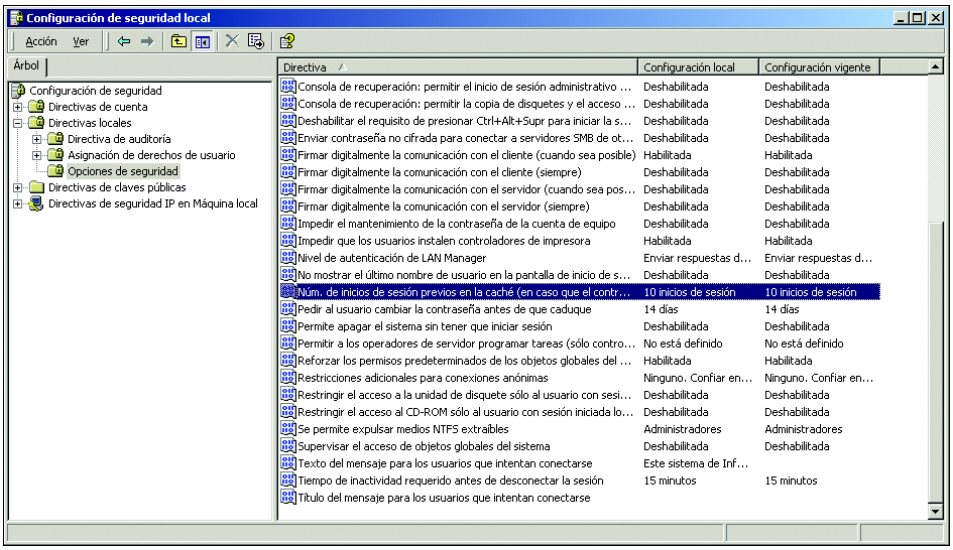
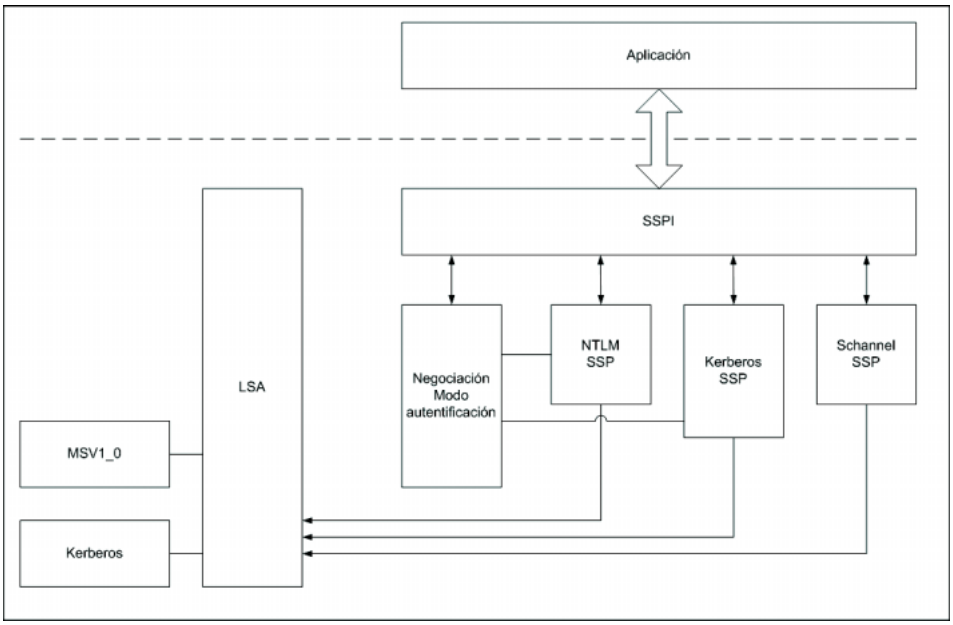


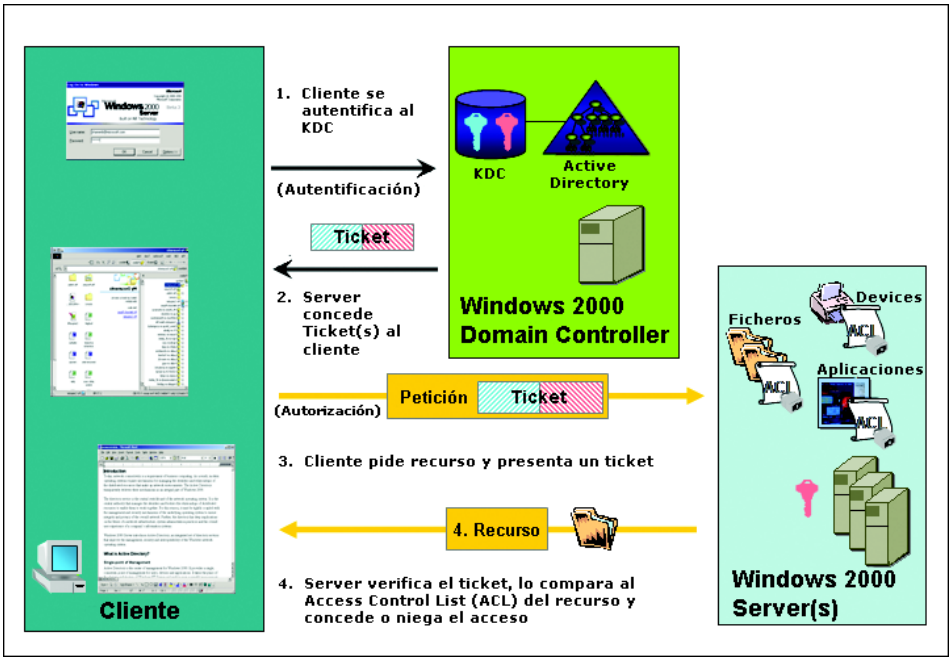
Figura 9.20. *Activación de la opción "Número de inicios de sesión previos en la cache".*

Cuando el proceso de autentificación se realiza contra un recurso de la red, y no sobre la máquina local, los componentes *Winlogon* y GINA no son utilizados sino que, por el contrario, se utiliza el componente *Security Support Provider* (SSP) cuya misión es facilitar paquetes de autentificación a las aplicaciones de red que pueden interactuar con la LSA para autentificarse. Los paquetes que por defecto proporcionan Microsoft Windows 2000 y Microsoft Windows XP son *Kerberos*, NTLM y SSL. Mediante estos paquetes la aplicación pasa de forma segura los credenciales necesarios para autentificarse a la máquina la cual utilizará estos credenciales para remitirlos a la LSA que finalizará la autentificación apoyándose en los paquetes de autentificación *Kerberos* y MSV1_0 de la misma forma que anteriormente hemos visto. Si el acceso a través de red se realiza con una cuenta de dominio, el protocolo por defecto será *Kerberos*, si se realiza con una cuenta local únicamente podremos utilizar la interfaz NTLM la cual podrá utilizar como protocolos LM, NTLM y NTLMv2. En los cuales profundizaremos más adelante.

Como ejemplo, cuando intento acceder a los recursos de un ordenador de un dominio previamente me habré autentificado en el dominio desde la máquina en la que me encuentro y habré conseguido un TGT. Contactaré con el KDC de nuevo para pedir un ticket de sesión contra la máquina que quiero autentificarme y lo presentaré al SSP de esta máquina. Esta máquina utilizará el paquete *Kerberos* para obtener el ticket que le he enviado y mandará la información de sesión existente en el ticket a la LSA local la cual contactará con el KDC para verificar la validez del ticket de sesión. Establecida esta validez la LSA creará el *token* asociado a los SID necesarios para acceder a los recursos (ver Esquema 9.3).



Esquema 9.2. *Flujo de autenticación.*



Esquema 9.3. *Autenticación Kerberos.*

Autentificación en Microsoft SQL Server 2000

Microsoft SQL Server 2000 soporta dos tipos de autentificación: la primera propia, a la que denominamos *mixta* y la segunda totalmente integrada con el sistema operativo Microsoft Windows 2000.

Indudablemente resulta aconsejable establecer el tipo de autentificación de nuestro sistema con la autentificación integrada lo que nos permitirá gestionar en un único punto el registro de usuarios y supondrá una menor carga administrativa además de ofrecernos formas de autentificación diversas y flexibles para la realización del cumplimiento de la norma.

No obstante, si por cualquier razón establecemos el tipo de autentificación como *mixta* también podremos asegurar:

- Identificación única de los principales mediante cuenta y contraseña.
- Establecimiento de contraseñas complejas.
- Encriptación de la contraseña.

Otra ventaja de la autenticación de Windows es que los usuarios no necesitan volver a escribir sus contraseñas para conectarse a una instancia de SQL Server. Cuando el usuario inicia sesión en un dominio de Windows 2000, se crea un identificador para él. Este identificador el SID y los SID de grupo relacionados. El SID de grupo indica los grupos de Windows a los que pertenece el usuario de red. Cuando el usuario inicia sesión en SQL Server 2000 con la autenticación de Windows, se solicita el identificador y, a continuación, se pasa a SQL Server mediante la Interfaz de proveedor de soporte de seguridad (SSP). Todos los SID devueltos se comprueban con la tabla *sysxlogins* de la base de datos principal. Primero se comprueba si hubo alguna denegación. Si se ha denegado acceso a SQL Server a un usuario o a un grupo de Windows al que pertenece el usuario, no se otorgará el acceso. Si no hay denegación, el proceso pasa a comprobar si existe un SID válido o inválido que coincida con la cuenta en Windows del usuario. Si coinciden, se otorga acceso al usuario. De lo contrario, el proceso continúa buscando en *sysxlogins* un SID que coincida con cualquiera de los grupos de Windows a los que pertenece el usuario. Si se encuentra en la tabla *sysxlogins*, se concederá acceso al usuario; de lo contrario, se le denegará.

No obstante, la autenticación de Windows tiene alguna desventaja. Si no hay un controlador de dominio disponible por alguna razón, el usuario no podrá iniciar sesión en el dominio ni conectarse a SQL Server. Si el usuario cambia de grupo tras iniciar sesión satisfactoriamente en Windows 2000 y en SQL Server, dichos cambios tendrán lugar sólo cuando el usuario cierre sesión en la red y

vuelva a iniciarla. Para realizar cambios en grupos o en permisos a grupos en dominios, es necesario que el administrador le haya asignado los permisos de administración necesarios, o bien el administrador tendrá que pedir a otra persona que tenga dichos permisos administrativos que lleve a cabo los cambios.

En este punto debemos incidir en materia de contraseñas. Hay que tener en cuenta dos áreas: contraseñas de funciones de aplicación y restablecimiento de contraseñas.

- Contraseñas de funciones de aplicación: las funciones de aplicación permiten a los administradores de SQL Server restringir el acceso a la base de datos a una aplicación concreta. Los usuarios que activen la función de aplicación pierden sus permisos actuales para la sesión y obtienen los permisos concedidos a la función de aplicación. La función de aplicación se activa con sp_setapprole. Cuando se activa una función de aplicación, la contraseña puede protegerse de varias maneras. Puede colocarse de manera segura en el registro de manera que sólo la aplicación pueda recuperarla. De manera alternativa, la contraseña puede cifrarse en el momento en que se active la función de aplicación con la función de cifrado OLE-DB (Base de datos de vinculación e incrustación de objetos) u ODBC (Conectividad abierta de bases de datos). La contraseña también puede cifrarse como parte del proceso de comunicación entre el servidor y el cliente con SSL/TLS (Nivel de sockets seguros/Seguridad de nivel de transporte) o con el cifrado de protocolos.
- Restablecer contraseñas: las contraseñas pueden modificarse de una o dos maneras, dependiendo del tipo de cuenta de inicio de sesión. Para las cuentas de usuario de Windows, cualquier usuario de red o cualquier administrador puede cambiar la contraseña con el privilegio apropiado para restablecer contraseñas. No es necesario realizar ningún cambio en SQL Server 2000 para reflejar esto ya que Windows 2000 valida al usuario. Para las cuentas de inicio de sesión de SQL Server, los miembros de las funciones fijas de servidor sysadmin y securityadmin o el usuario, si ejecuta sp_password, pueden cambiar la contraseña de un usuario. Los miembros de las funciones sysadmin, db_owner y db_securityadmin pueden cambiar las contraseñas de aplicación almacenadas en la tabla de sistema sysusers de la base de datos.

Autentificación en Microsoft Exchange Server 2000

Microsoft Exchange Server 2000 está totalmente integrado con el modelo de seguridad de Microsoft Windows 2000. Al utilizar el Directorio Activo, puede otorgar a los usuarios y administradores de Microsoft Exchange Server 2000 permisos para llevar a cabo tareas específicas y acceder a recursos específicos.

Así, vemos que las medidas de seguridad descritas para Microsoft Windows 2000 son aplicables para Microsoft Exchange Server 2000, por lo que en este punto nos remitimos a lo señalado en él.

Autentificación en Microsoft Office XP

Una de las grandes novedades de Office XP es la posibilidad de firmar digitalmente ciertos documentos. Una de las características principales de la firma electrónica es que permite la identificación del autor de dicha firma. La firma electrónica se basa en la Infraestructura de Clave Pública (PKI) y en los Certificados Digitales.

La firma digital utiliza las claves de un certificado digital para proteger datos contra falsificaciones y asegurar la autentificación del remitente. Para ello, el software de firma genera una "huella digital" única que representa un bloque de datos (por ejemplo, un documento o un paquete de red). Esta huella (también denominada *suma de comprobación* o valor *hash*) se cifra con la clave privada de quien firma, de modo que todo aquel que disponga de su clave pública pueda descifrarla. El valor *hash* es un número generado mediante un algoritmo de cifrado (como MD5 o SHA1) a partir de los datos que se deseen firmar. La característica principal del algoritmo de *hash* es que resulta prácticamente imposible cambiar los datos sin cambiar el valor de *hash* asociado. Si se cifra el valor de la suma de comprobación o *hash* en lugar de los datos, la firma digital garantiza al usuario final que éstos no han sido modificados.

Para comprobar una firma, el destinatario comprueba en primer lugar el certificado del remitente con el fin de asegurarse de que no ha caducado y de que sus firmas son válidas. A continuación, el software descifra la suma de comprobación cifrada con la clave pública del remitente, que obtiene a partir del certificado del cliente. El software del destinatario calcula de forma independiente la suma de comprobación de los datos del archivo. Si la suma de comprobación calculada coincide con la descifrada, el destinatario puede estar seguro de que alguien con acceso a la clave privada ha cifrado los datos y que éstos no han sido manipulados.

Office XP utiliza tecnología de firma digital para firmar archivos, documentos, presentaciones, libros de trabajo y macros. Si se firma todo el archivo, la firma asegura que el archivo no ha sido modificado desde que se firmó. Del mismo modo, si el archivo contiene macros firmadas, el certificado utilizado para firmarlas garantiza que no han sido manipuladas desde el momento de su firma. Hay que advertir que la firma de macros y la firma de archivos son dos procesos independientes.

La firma de código y las firmas digitales parecen muy similares. En este apartado, el término "firmas digitales" se refiere al proceso de firmar documentos, mientras que "firma de código" hace referencia al uso de firmas en código ejecutable (incluidas las macros). La firma de código se aplica a los controles ActiveX con Microsoft Authenticode para comprobar que el código no ha sido modificado desde el momento en que se firmó. Un control o macro firmados supone un alto grado de garantía de que el objeto ha sido en efecto creado por quien lo firma y que no ha sufrido cambios. La firma no garantiza la confiabilidad, la competencia ni la bondad de las intenciones del firmante, sólo asegura que el objeto proviene de él.

9.2.5 Artículo 11.2 (Autentificación)

> *"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."*

Tanto la SAM local como el Directorio Activo permiten garantizar la integridad de la contraseña y su conocimiento exclusivo por el usuario de la cuenta.

Al crearse la cuenta, el Administrador puede indicar que el usuario deberá cambiar la contraseña en el primer inicio de sesión que realice de tal forma que el Administrador, que en un primer momento le había asignado contraseña, ya no la conocerá. Para realizar esto ver figura 9.21.

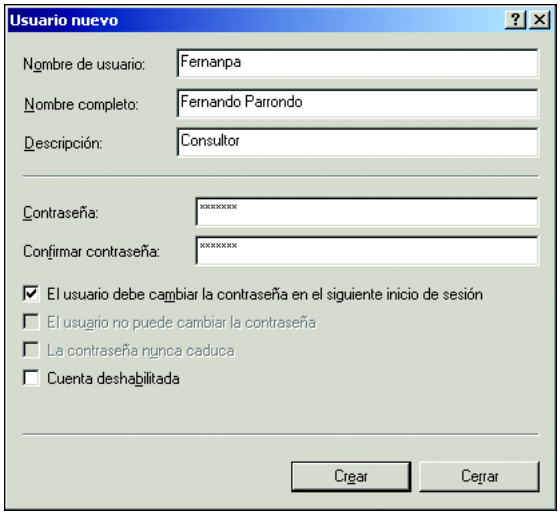


Figura 9.21. *Cambio de contraseña en primer inicio de sesión.*

Igualmente, por defecto las contraseñas se almacenan encriptadas mediante el algoritmo RC4 utilizando las técnicas de *Syskey* que permiten almacenar la clave de encriptación fuera del sistema de ficheros para mayor seguridad, y su utilización se realiza mediante la comparación de una función *hash* MD5 encriptada no almacenándose la contraseña por defecto en texto claro.

Como anteriormente hemos visto siempre que utilicemos el protocolo *Kerberos* la información que viaja por la red para requerir servicios nunca contiene la contraseña de manera que la integridad de ésta es absoluta. Si no utilizamos *Kerberos* por no disponer de un Directorio Activo, la autentificación para acceder a los recursos de red será NTLM, en este caso tampoco viaja la contraseña sino un *hash* de ésta no reversible. Para mantener compatibilidad con el sistema *LAN Manager*, el paquete de autentificación NTLM permite autentificarse con los protocolos LM, NTLM y NTLMv2. La mayor seguridad en la autentificación nos la ofrece este último por lo que será conveniente en la medida de lo posible evitar el uso de los dos primeros. En la tabla 9.9 vemos una estrategia de limitación de los protocolos de autentificación que utiliza el paquete NTLM:

Sistema operativo cliente	**Protocolo utilizado por defecto**	**Posibilidad de utilizar NTLMv2**
Microsoft Windows 95	LM	Sí, contra un dominio de Directorio Activo instalando DSClient en las máquinas.
Microsoft Windows 98	LM	
Microsoft Windows NT 4.0	NTLM	Sí, instalando el Service Pack 4 o superior

Tabla 9.9. *Utilización de NTLM.*

Para limitar los protocolos que el paquete de autentificación NTLM puede emplear, estableceremos en la Directiva de seguridad local o de dominio en el parámetro *LAN Manager authentication level* contenido en la subcarpeta Opciones de seguridad de la carpeta Directivas locales, la opción Enviar sólo respuesta NTLMv2\ rechazar LM como podemos ver en las figuras 9.22 y 9.23.

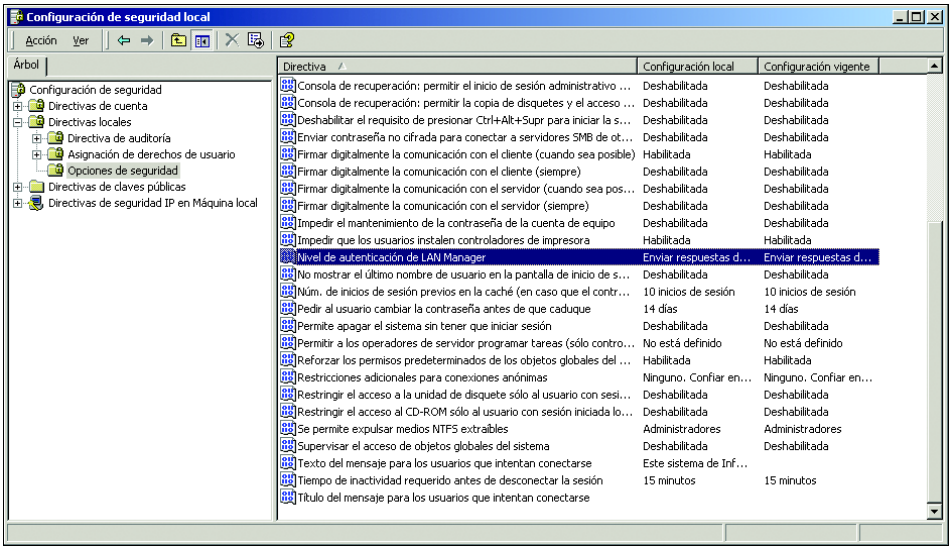


Figura 9.22. *Nivel de autenticación de LAN Manager.*

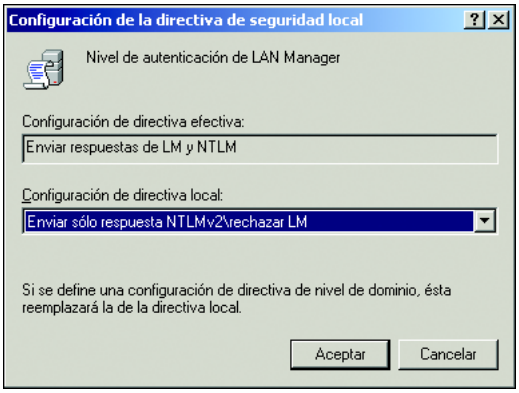


Figura 9.23. *Limitar uso de NTLM.*

9.2.6 Artículo 11.3 (Autentificación)

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

Establecer una política adecuada de contraseñas en Microsoft Windows 2000 o Microsoft Windows XP resulta muy sencillo a través de la Directiva de seguridad local o de dominio. En la subcarpeta Directiva de contraseñas contenida

en la carpeta Directivas de cuenta, podemos establecer no sólo el tiempo máximo de validez de la contraseña sino también el tiempo mínimo, su longitud mínima, su complejidad y evitar la repetición de contraseñas (ver figura 9.24).

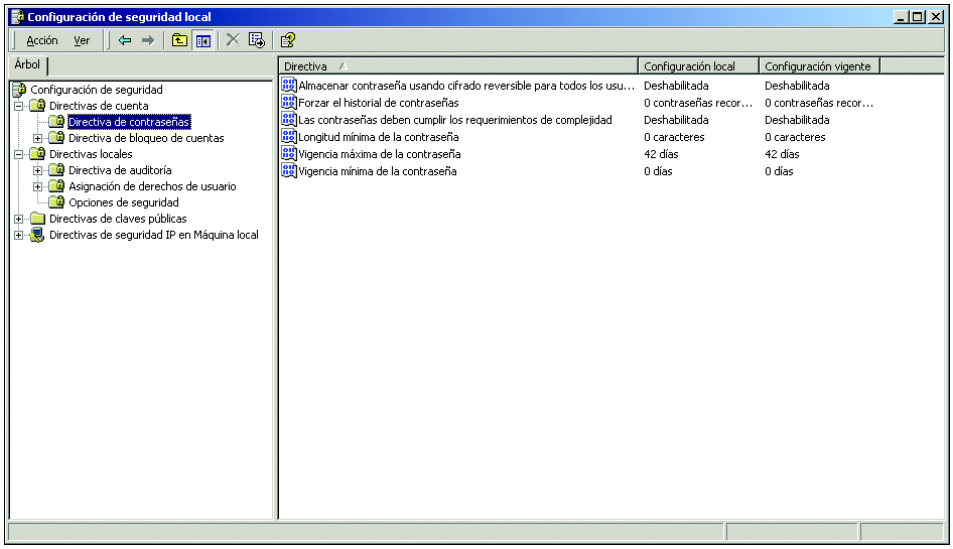


Figura 9.24. *Directivas de contraseñas.*

Como antes señalamos, las contraseñas se almacenan encriptadas tanto en la SAM como en el Directorio Activo. Microsoft Windows 2000 y Microsoft Windows XP utilizan la tecnología *Syskey* para asegurar la integridad de las contraseñas. La tecnología *Syskey* utiliza una clave (*startup key*) para encriptar toda la información importante que puede contener una máquina. Entre otras cosas:

- Las claves maestras (*Master keys*) utilizadas para proteger las claves secretas de los certificados que posee cada usuario en local.
- Las claves de protección de los *hash* de la contraseña de usuario en el Directorio Activo.
- Las claves de protección de los *hash* de la contraseña de usuario en la SAM local.
- Las claves de protección del módulo *LSA secrets*.
- La clave de protección de la contraseña del administrador que es utilizada para iniciar un sistema en modo de recuperación.

Esta clave por defecto se almacena en la misma máquina mediante un complejo algoritmo de ocultación que la coloca en algún lugar del registro.

Evidentemente, si la clave se encuentra físicamente en la misma máquina puede terminar siendo encontrada, por lo que *Syskey* permite, en sistemas que requieran mayor seguridad, la posibilidad de almacenar esta clave fuera de la máquina, bien mediante un dispositivo físico, bien mediante el uso como clave de una generada mediante la contraseña introducida por un administrador previamente a que inicie el sistema.

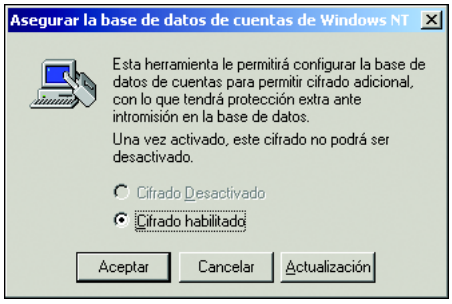


Figura 9.25. *Habilitación del cifrado de contraseñas mediante* Syskey.

Para seleccionar el modo de actuar de *Syskey* simplemente ejecutaremos el comando syskey y nos aparecerá la pantalla de la figura 9.25 señalándonos el estado de habilitación de esta funcionalidad.

Si queremos establecer un estado distinto al actual pulsaremos el botón Actualización y nos aparecerá la pantalla de la figura 9.26 donde definiremos la opción que estimemos conveniente.

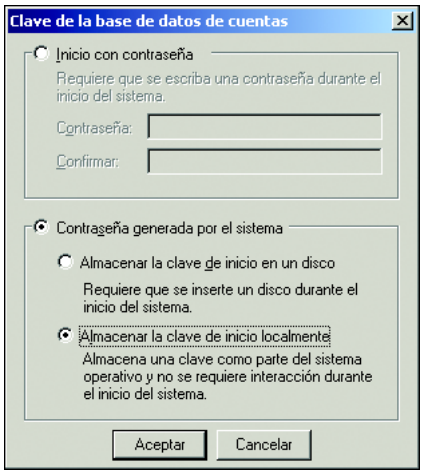


Figura 9.26. *Opciones de almacenamiento de clave.*

Además del almacenamiento descrito anteriormente que hace ininteligible la contraseña, tanto la SAM local como el Directorio Activo permiten la gestión de cuentas de manera avanzada, esto es: el cambio periódico de contraseña mediante políticas y otras funciones de la contraseña como longitud, complejidad, evitación de repetición de contraseñas, expiración de cuentas, etc.

9.2.7 Artículo 12.2 (Autorización)

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

El mecanismo de autorización de Microsoft Windows 2000 y Microsoft Windows XP se basa en las listas de control de acceso. Para su utilización lo primero que requerimos es que al instalar la máquina el sistema de ficheros establecido sea NTFS. Esto lo observamos en la figura 9.27.

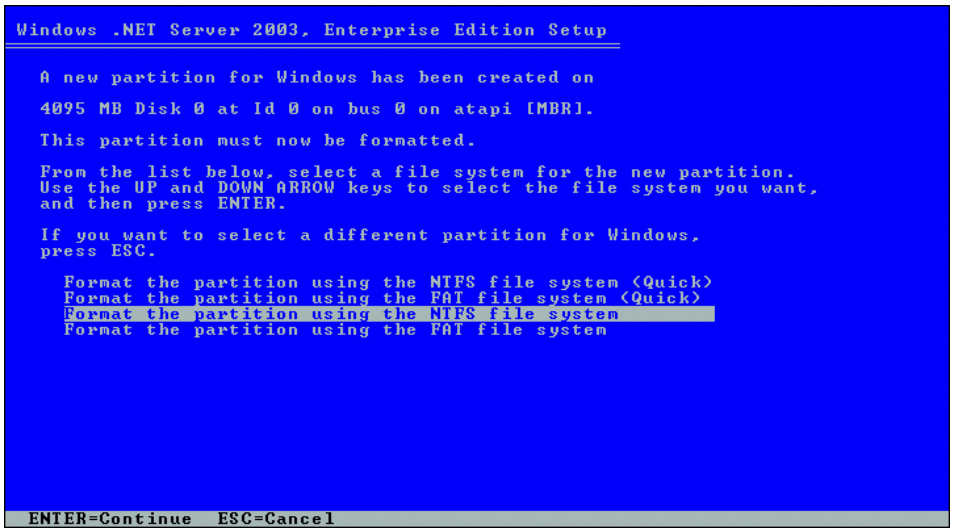


Figura 9.27. *Selección de la opción NTFS durante el proceso de instalación de Windows 2000.*

Si instalamos un disco con otro sistema de ficheros distinto a NTFS, podemos convertirlo a éste en cualquier momento utilizando el comando *convert.exe*. Por el contrario, nunca podemos convertir un sistema de ficheros NTFS a otro sistema como FAT o FAT 32 sin realizar un formato previo del disco (ver figura 9.28).

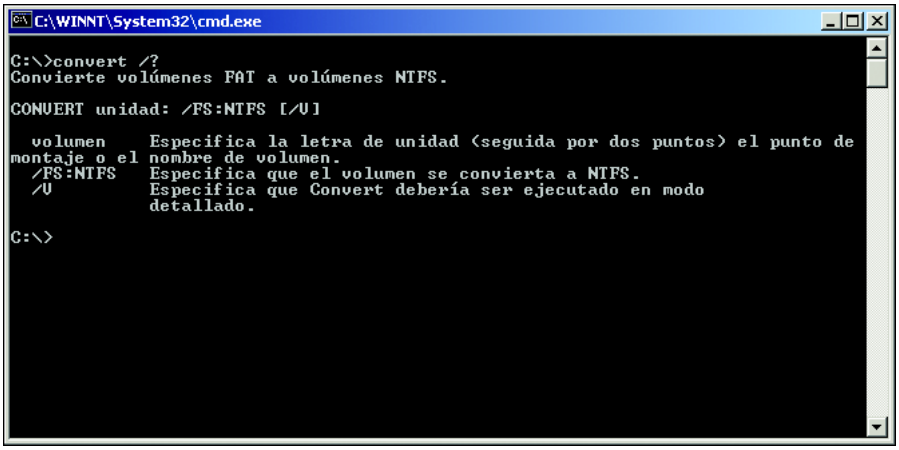


Figura 9.28. *Utilización del comando Convert para convertir volúmenes de disco a NTFS.*

Establecido el sistema NTFS nos aseguramos que el acceso a los recursos únicamente se produce por los usuarios que se describen y en la forma en que se describen en el fichero (ver figura 9.29).

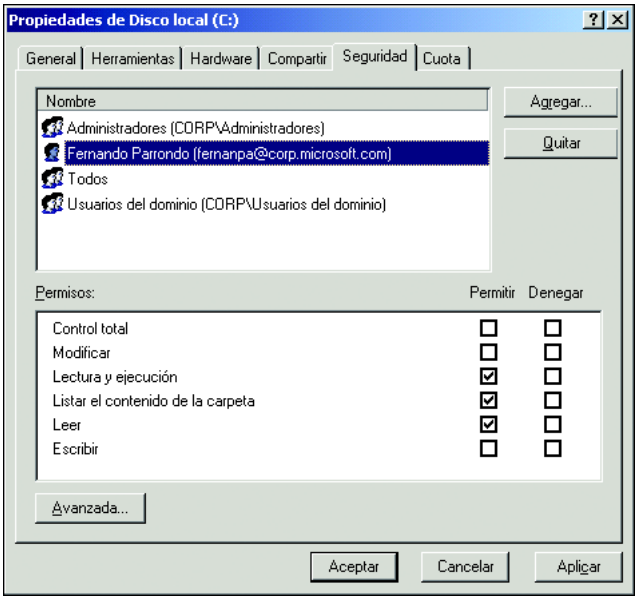


Figura 9.29. *Configuración de acceso a recursos.*

El sistema de autorización y control de acceso de Microsoft Windows 2000 y Microsoft Windows XP se basa en asegurar la utilización de los objetos por los sujetos y, para una mejor comprensión, necesitamos conocer el funcionamiento específico del sistema que lo hace distinto de otros por lo que vamos a explicarlo brevemente.

Aunque los usuarios son los que deciden leer, borrar o modificar un archivo o un atributo de una cuenta del Directorio Activo, en realidad estas acciones son programas. Más específicamente, secuencias dentro de estos programas que actúan dentro de un proceso. Estas secuencias se denominan hilos (*Threads*) y suponen la gran diferencia del funcionamiento existente entre los sistemas basados en Microsoft Windows NT y otros sistemas como UNIX. Debido a que estos 'hilos' tienen sus propios registros, *kernel*, bloques de entorno y pila de usuario en el espacio direccionado por un proceso, diferentes hilos de un mismo proceso pueden ejecutarse concurrentemente. Aunque sólo los 'hilos' pueden actuar como objetos de sistema, éstos no llevan una información de seguridad propia, sino que asumen los derechos y privilegios del principal, el sujeto, que los ha iniciado. Como anteriormente vimos, cuando un usuario inicia sesión, ya sea de forma interactiva o a través de la red, el sistema operativo crea un *Access token* para ese usuario. Este *Access token* contiene el identificador del usuario y los identificadores de todos los grupos a los que pertenece, además de los privilegios tanto del usuario como de esos grupos.

Cuando el usuario inicia una aplicación cada 'hilo' que ejecuta obtiene una copia de ese *Access token*. El 'hilo' por tanto actúa como agente del usuario presentando el *access token* al sistema operativo cada vez que éste le requiere algún nivel de acceso a un objeto asegurado. El sistema operativo, con el *token* recibido, lo compara con la información de seguridad que el propio objeto asegurado contiene, verificando con esto que el principal que requiere una acción sobre un objeto está autorizado a realizarla. La información de seguridad de cada objeto se define en el propio objeto en lo que denominamos descriptor de seguridad (*Security descriptor*), que además de contener el SID del propietario del objeto contiene una lista de entradas que especifican los derechos de accesos permitidos y/o denegados a los usuarios y grupos.

Para cada objeto el descriptor incluye una lista de control de acceso discrecional (*Discretionary Access Control List* o DACL) que se crea por la unión de las distintas entradas de control de acceso (*Access Control Entries* o ACE).

Una ACE contiene una serie de mapas de bits en una máscara de acceso y el SID del principal que identifica a quien se le permite dicho acceso. El sistema operativo intenta confrontar el SID obtenido del *Access token* con alguno de los SID que señalan el tipo de acceso pretendido para ver si concuerdan y, en caso positivo, realizar la operación.

Junto al DACL, el descriptor contiene también la lista de control de acceso de sistema (*System Access Control List* o SACL) que es utilizada por el sistema de seguridad para realizar las tareas de auditoría de accesos al objeto.

Evidentemente, el sistema no sabe a quién ofrecer finalmente esos accesos y tendrán que ser los administradores del sistema los que los definan dando el acceso y el tipo de acceso a los usuarios adecuados. Para facilitar esta labor en entornos con muchos usuarios, Microsoft Windows 2000 y Microsoft Windows XP ofrecen grupos administrativos, lo que nos permite facilitar esta tarea al centrarnos sobre el grupo en vez de sobre cientos, tal vez miles, de usuarios. Imaginemos que tenemos un fichero con datos de carácter personal al que pueden acceder 25 usuarios los cuales, en algunos casos, podrán acceder como lectores nada más y, en otros casos, como editores. En este caso el planteamiento sería crearnos un grupo por cada tipo de acceso al fichero y en cada grupo añadir los usuarios correctos. Los permisos del fichero quedarán de la forma representada en la figura 9.30.

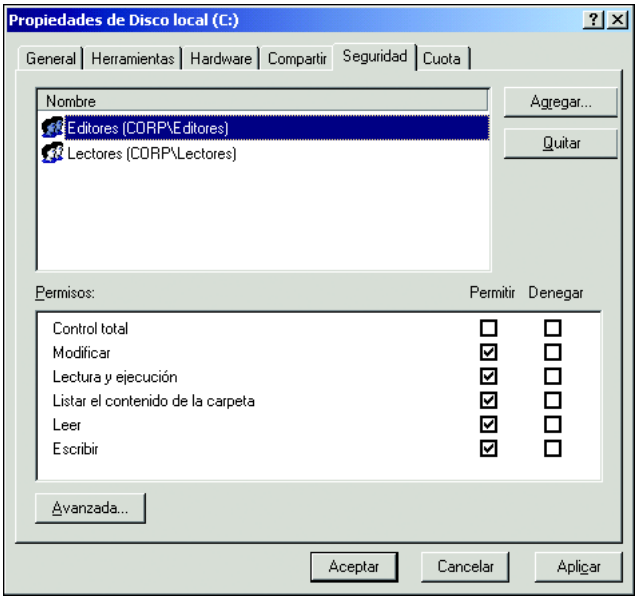


Figura 9.30. *Permisos sobre ficheros.*

Los usuarios pertenecientes al grupo serían más fácilmente manejables. Permitiéndonos extender estos grupos a multitud de ficheros. Esto también nos permite realizar excepciones sin sacar a un usuario de un grupo denegándole un tipo de acceso de forma explícita, o sacándole del grupo si en algún momento le tenemos que quitar el acceso sin bloquearle la cuenta.

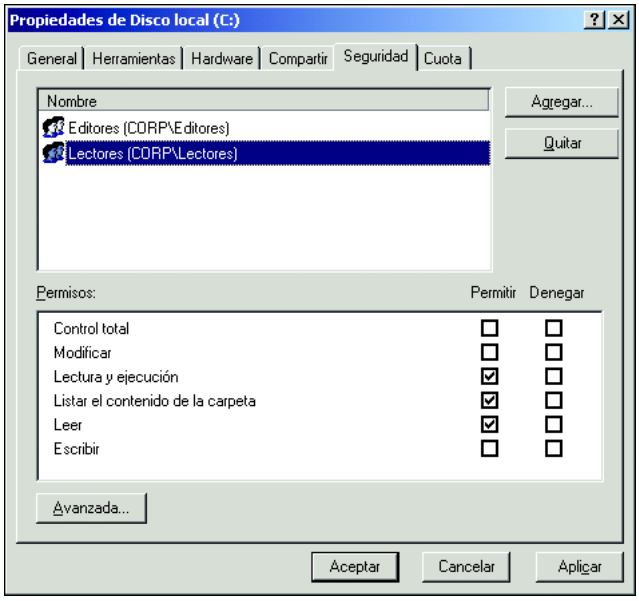


Figura 9.31. *Permisos sobre ficheros.*

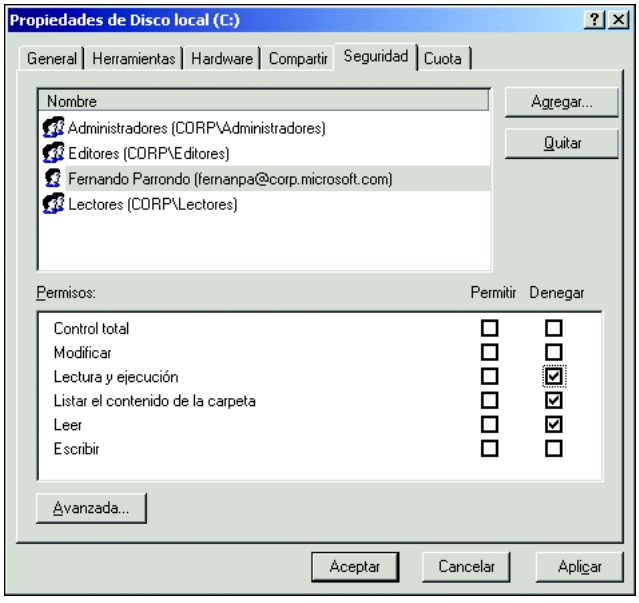


Figura 9.32. *Denegación de permisos.*

Un tema a considerar será la toma de posesión que es una facultad que tiene por defecto el grupo administradores locales para sobrescribir valores de permisos en un determinado fichero, aun no teniendo ningún tipo de permiso, y sobrescribir el descriptor de seguridad de un objeto con su propio SID como propietario. Si queremos evitar esto o asignarlo a otro grupo simplemente otorgaremos este privilegio al responsable de seguridad en las máquinas en que existan ficheros en los que queremos garantizar que no se produzca (ver figura 9.33).

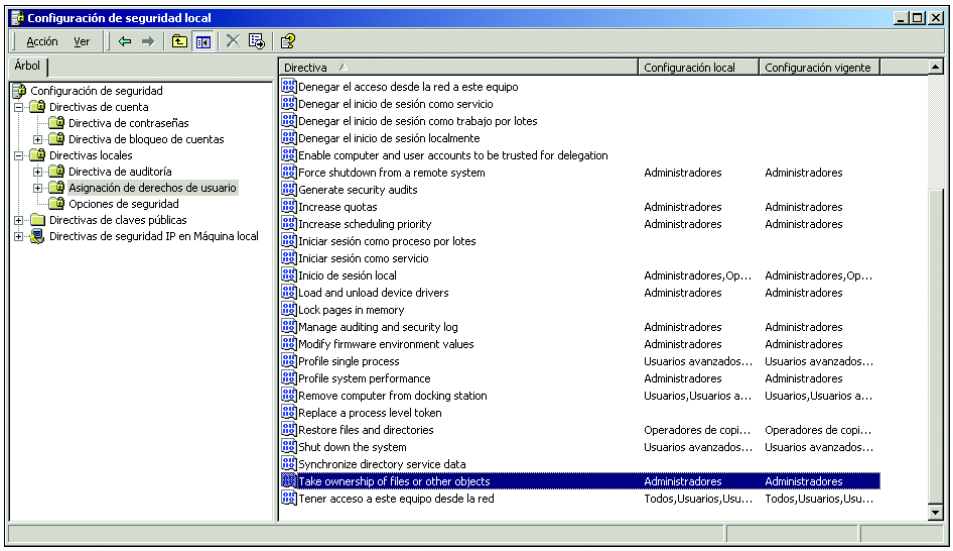


Figura 9.33. *Toma de propiedad de permisos.*

Control de acceso en Microsoft SQL Server 2000

El control de accesos se ejerce en Microsoft SQL Server 2000 a través de permisos. Éstos pueden concederse en un número seleccionado de columnas de una tabla. La seguridad de las filas puede implementarse únicamente mediante una vista, un procedimiento almacenado o una función. Puesto que la administración de los permisos de las columnas puede ser compleja, se recomienda que la seguridad de filas y columnas se administre creando vistas o, de manera alternativa, procedimientos almacenados o funciones. Estos objetos especificarán las columnas y filas a las que se tendrá acceso. Los permisos deben concederse en el objeto en lugar de en la tabla subyacente.

Si la organización está desarrollando software personalizado, se debe impedir que los usuarios obtengan cualquier forma de acceso directo a las tablas. En su lugar, cree vistas de cada tabla y conceda permisos únicamente a aquellas vistas mediante funciones de aplicación.

Hay que tener en cuenta estas tres áreas: los tipos de permisos, conceder/revocar/denegar permisos y los permisos efectivos.

Tipos de permisos

Existen varios tipos de permisos en SQL Server 2000 incluidos los permisos del objeto, los permisos de la instrucción, los permisos predefinidos y los permisos implícitos o derivados. A excepción de los procedimientos almacenados en el sistema, los permisos no pueden concederse en varias bases de datos. Debe crearse una cuenta de usuario en cada una de las bases de datos a la que tendrá acceso la cuenta de inicio de sesión.

- Los permisos del objeto se otorgan a un usuario en un objeto de base de datos existente, como una tabla, una vista, un procedimiento almacenado o una función. Estos permisos incluyen SELECT, INSERT, UPDATE, DELETE, REFERENCES y EXECUTE (ver figura 9.34).

- Los permisos de la instrucción permiten a un usuario crear objetos en la base de datos. Estos permisos incluyen CREATE DATABASE, CREATE DEFAULT, CREATE FUNCTION, CREATE INDEX, CREATE PROCEDURE, CREATE RULE, CREATE SCHEMA, CREATE TABLE, CREATE TRIGGER, CREATE VIEW, BACKUP DATABASE y BACKUP LOG.

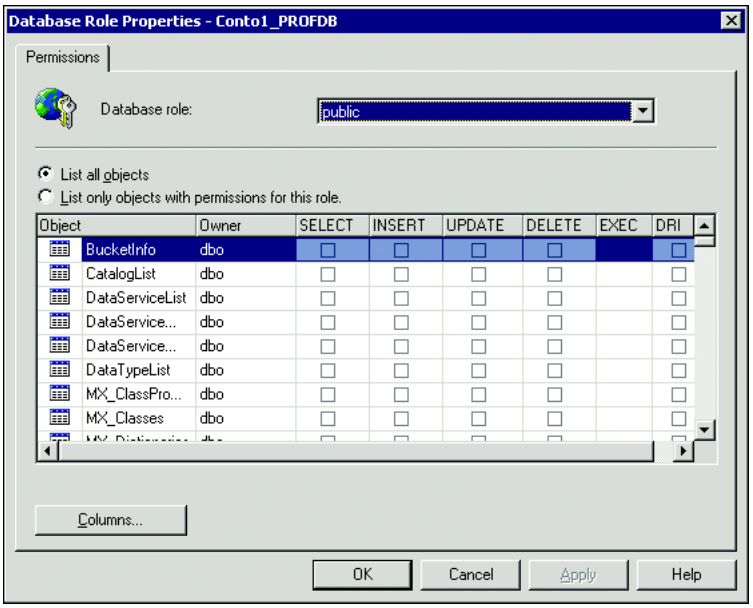


Figura 9.34. *Permisos de objetos en SQL Server.*

- Los permisos predefinidos se dan con la pertenencia a grupos en funciones fijas de servidor o de base de datos. Estos permisos forman parte de la definición de funciones y no pueden modificarse.

- Los permisos implícitos o derivados se dan cuando el usuario es el propietario del objeto. Por ejemplo, el propietario de una tabla puede crear un desencadenador, conceder permisos o modificar una tabla que pertenece al usuario.

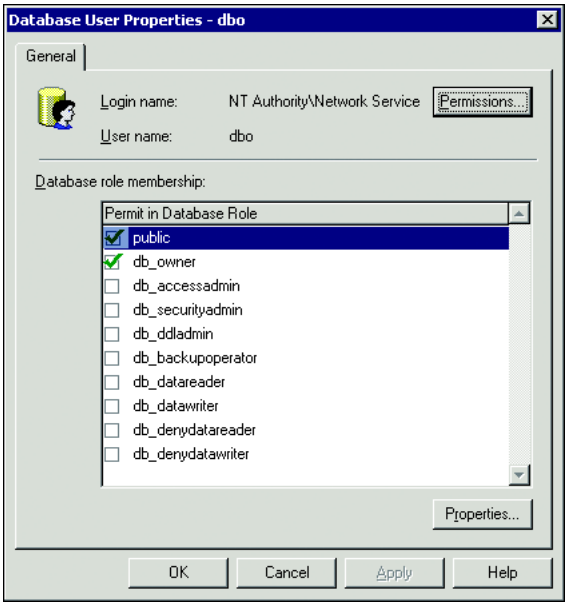


Figura 9.35. *Roles de usuario en la base de datos.*

Los permisos deben concederse con secuencias T-SQL de tal manera que puedan realizarse auditorías. Por ejemplo, un administrador recibe una solicitud del responsable del fichero para que permita que un nuevo empleado tenga acceso a una base de datos con datos de carácter personal. Todas las operaciones, desde la creación de la cuenta de inicio de sesión hasta la concesión de permisos, deben documentarse en tablas de auditoría que registran quién agregó una determinada cuenta de inicio de sesión o de usuario, en qué momento, dónde y la razón por la que se creó cada inicio de sesión. Las secuencias T-SQL para todas las operaciones deben guardarse en una ubicación segura. Es imprescindible que ésta y otras operaciones administrativas se estandaricen.

Conceder/revocar/denegar permisos

Los permisos pueden concederse, revocarse o denegarse con el Administrador corporativo o con los comandos Grant/Revoke/Deny de T-SQL. Como se mencionó anteriormente, los permisos deben concederse a funciones con secuencias siempre que sea posible, en lugar de otorgarlos directa e individualmente a las cuentas de usuario de la base de datos.

La información relativa a los permisos se encuentra en la tabla *syspermissions* de cada base de datos. Los administadores pueden realizar más fácilmente un seguimiento de la información adicional sobre permisos si realizan solicitudes a la pseudotabla *sysprotects*, creada dinámicamente. Un permiso GRANT muestra en la columna *protecttype* de *sysprotects* la entrada positiva 204 para *grant_w_grant* (permite a los usuarios con permisos conceder el permiso otorgado; requiere el uso del comando grant de T-SQL) ó 205 para una concesión estándar. Un permiso DENY muestra la entrada negativa 206. Un permiso REVOKE elimina un permiso concedido o deniega el permiso y no aparece ninguna entrada en *sysprotects*. Esto significa que el usuario o el grupo al que se revocó el permiso ya no tiene acceso. De nuevo, la excepción serían los permisos concedidos mediante la pertenencia a grupos de funciones.

Los permisos son acumulativos, de manera que los permisos eficaces de un usuario de la base de datos son más permisivos que los concedidos a la cuenta de usuario de la base de datos o a cualquier función dentro de la base de datos a la que pertenece el usuario. Esto no incluye las funciones de las aplicaciones ya que no contienen ni usuarios ni funciones.

Un permiso denegado a nivel de usuario o de función tiene prioridad sobre el resto de los permisos concedidos. Por ejemplo, Felipe es un miembro de la Función_Nóminas de la base de datos Trabajadores. A Felipe se le han otorgado permisos para realizar selecciones en la tabla tblConfeccionNominas. A la Función_Nominas también se le han otorgado permisos para realizar selecciones en la misma tabla. Si se revocan los permisos individuales de Felipe, le seguirá quedando el permiso gracias a su pertenencia a la función. Por otra parte, si sólo se ha revocado el permiso a la Función_Nominas, Felipe seguirá teniendo su propio acceso a la tabla tbl_ConfeccionNominas. El resto de los usuarios de la función perderán los permisos concedidos mediante la Función_Nominas. Los usuarios de esta función pueden seguir realizando selecciones en la tabla tbl_ConfeccionNominas ya que se les ha concedido explícitamente el permiso o pertenecen a otro grupo con dicho permiso y no se les ha denegado el acceso a este nivel.

Sin embargo, si los permisos de Felipe son denegados, no tendrá acceso, independientemente de los permisos para las funciones a las que pertenece. Los usuarios de la Función_Nominas seguirán teniendo acceso. Si se deniega el

permiso de Función_Nominas, Felipe y cualquier miembro de la función ya no tendrán acceso independientemente de cualquier otro permiso de función para realizar selecciones en tbl_ConfeccionNominas.

Permisos efectivos

Son permisos otorgados a los usuarios y a las funciones y son específicos de una base de datos. Todos los permisos son acumulativos a excepción de DENY. Un permiso *denegado* a nivel de usuario o de función anula el mismo permiso *concedido* a través de otra pertenencia a funciones a excepción de la función fija de servidor *sysadmin*. (Una función sysadmin retiene todos los permisos, incluso si la función a la que pertenece tiene un permiso DENY.) Si se aplica un permiso DENY a una función, se denegarán todos los miembros de dicha función. En general, debe utilizarse el permiso REVOKE de un permiso concedido en lugar de DENY para eliminar permisos. Un permiso REVOKE elimina un permiso GRANT o DENY. Un permiso DENY puede causar problemas de permisos difíciles de descubrir. Tenga cuidado especialmente al aplicar un permiso DENY a un único usuario. Si utiliza permisos REVOKE y funciones, la administración de permisos y la documentación serán más sencillas.

Control de Acceso en Microsoft Exchange 2000

Microsoft Exchange Server 2000 basa sus características de seguridad en las establecidas por Microsoft Windows 2000 y posee características específicas que vamos a detallar someramente.

Para obtener acceso a la cuenta de correo electrónico de otro usuario es necesario iniciar sesión del mismo modo que dicha persona o conseguir acceso administrativo al servicio de Directorio Activo, lo que le permite otorgar los permisos para enviar y recibir como en el buzón (concretamente se requiere el acceso Operador de cuentas o superior para el objeto usuario y los permisos administrativos de Microsoft Exchange Server 2000 en el buzón para efectuar los cambios).

Control de acceso a Archivos Microsoft Office XP

En Office, al margen de los mecanismos que proporciona el sistema operativo, se permite establecer contraseñas para acceder a los documentos y, así, establecer una funcionalidad adicional a esta medida de Nivel Básico. Lo cual, en cierto modo, garantiza el acceso a los datos únicamente por parte de aquellos usuarios que conozcan las contraseñas. Tanto en modo lectura como en modo escritura. Este nivel de autenticación y control de acceso se ve complementado en gran medida en Office XP con la capacidad de firma electrónica que, además de estas capacidades, garantiza implícitamente la integridad de la información firmada.

La información que se guarda en formato web no permite ser protegida por contraseña.

Incidiendo un poco más en esta cuestión, dentro de Office XP y más concretamente en Word, Excel y PowerPoint, se habilita una serie de medidas de protección, relacionadas con el control de acceso. En concreto:

- Protección de la apertura de archivos: requiere que el usuario especifique una contraseña para abrir el archivo. El documento se cifra (con el algoritmo que especifique) de modo que no se pueda leer sin conocer la contraseña.
- Protección de la modificación de archivos: permite a los usuarios abrir el documento sin la contraseña pero, en caso de no especificarla, no podrán realizar cambios ni guardarlos en el documento.
- Protección de recomendación de sólo lectura: se solicita al usuario que abra el archivo en modo de sólo lectura pero se le permite que lo abra para lectura y escritura sin contraseña.

En Microsoft Word XP para evitar cierto tipo de cambios en un documento, en el menú Herramientas, haga clic en Opciones y, a continuación, en la ficha Seguridad haga clic en Proteger documento. Los códigos de campo pueden verse en un procesador de texto como el Bloc de notas y las celdas ocultas de una hoja de cálculo de Excel se pueden ver si un usuario copia un rango de celdas que las incluya, lo pega en una nueva hoja de cálculo y aplica el comando Mostrar. Los controles del cuadro de diálogo permiten proteger el documento de las formas siguientes mostradas en la figura 9.36.

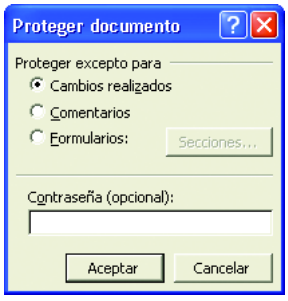


Figura 9.36. *Puede proteger elementos individuales de metadatos en los documentos del Word.*

- Cambios realizados: cuando se selecciona, esta opción permite a los revisores efectuar cambios en el documento, pero los resalta para que el autor pueda controlarlos y decidir si los acepta o los rechaza. Cuando un documento se protege ante los cambios realizados, el usuario no puede desactivar este control, ni aceptar o rechazar los cambios.
- Comentarios: cuando se selecciona, esta opción permite a un revisor especificar comentarios, pero no cambiar el contenido del documento.
- Formularios: cuando se selecciona, protege el documento frente a cambios, excepto en campos de formularios o secciones sin proteger.
- Secciones: cuando se selecciona, permite activar la protección de una sección específica. Una sección es una parte de un documento con opciones de formato diferentes del resto. Al combinar las opciones Formularios y Secciones puede crear un documento con múltiples secciones que contenga formularios e instrucciones, y permitir realizar cambios en algunas zonas al tiempo que protege otras.

Microsoft Excel XP permite proteger elementos adicionales dentro de una misma hoja de cálculo o libro. El menú Herramientas | Protección cuenta con cuatro comandos. Ver figura 9.37.

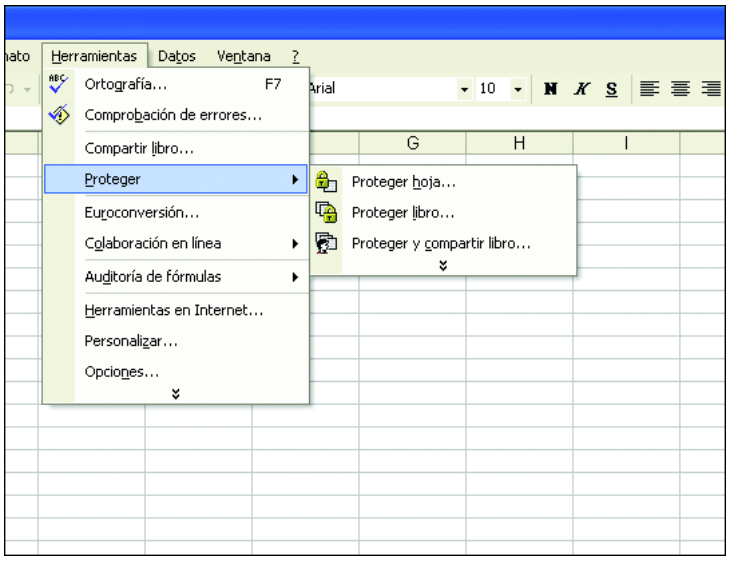


Figura 9.37. *Opciones de protecćon de Excel.*

El comando Proteger hoja permite proteger celdas seleccionadas de la hoja de cálculo e impide modificar tanto las celdas bloqueadas como las que no lo están. El usuario puede bloquear celdas con el comando Formato de celdas. La protección de hojas también permite otorgar acceso a operaciones específicas dentro de cada hoja, como el formato de celdas, filas y columnas, la inserción y eliminación de columnas y filas, la modificación o inserción de hipervínculos, y la modificación de objetos de diversos tipos.

El comando Permitir que los usuarios modifiquen rangos permite conceder permisos a grupos, usuarios o equipos específicos para que tengan acceso y puedan modificar celdas y rangos específicos de la hoja de cálculo protegida.

El comando Proteger libro permite especificar los elementos de un libro que se desea proteger, así como una contraseña para impedir a los usuarios no autorizados retirar la protección.

El comando Proteger y compartir libro permite compartir un libro y activa el control de cambios. De este modo otros usuarios pueden hacer cambios que deben controlarse, aunque también puede especificar una contraseña para desactivar el control de cambios. Cuando se comparte un libro, es posible activar la protección para compartir y controlar los cambios, pero no se puede asignar una contraseña hasta haber dejado de compartirlo.

En Microsof Access XP también existen una serie de medidas relacionadas con el Control de Acceso. En concreto:

- Mostrar u ocultar objetos en la ventana Base de Datos.
- Protección mediante contraseña.
- Seguridad para el usuario.
- Impedir que los usuarios repliquen una Base de Datos, establezcan contraseñas o configuren opciones de inicio.
- Zonas de seguridad
- Cifrado y descifrado de Bases de Datos de Access

Microsoft Access XP incluye diversos métodos para controlar el nivel de acceso que los usuarios tienen a una base de datos de Access y a sus objetos. Estos métodos son los siguientes:

Mostrar u ocultar objetos en la ventana Base de datos

El más sencillo de los métodos de protección permite ocultar los objetos de la base de datos en la ventana Base de datos para protegerlos de otros usuarios. Es el menos seguro, porque resulta relativamente sencillo mostrar cualquier objeto oculto.

Cifrado y descifrado de bases de datos de Access

El cifrado de una base de datos de Access comprime el archivo de base de datos y lo hace ilegible para programas de utilidades, procesadores de texto y aplicaciones similares. El descifrado de la base de datos invierte el cifrado. Sin embargo, cifrar una base de datos que no esté protegida de otro modo supone un nivel de seguridad relativamente reducido, ya que cualquier usuario que conozca la contraseña tendrá un acceso completo a todos los objetos. Aun así, el cifrado puede ser útil: por ejemplo, puede cifrar la base de datos al enviarla por correo electrónico o al almacenarla en un disco, cinta o CD.

Con el fin de cifrar o descifrar una base de datos de Microsoft Access, debe ser su propietario o bien, si la base de datos está protegida, miembro del grupo Administradores del archivo de información de grupos de trabajo que contenga las cuentas utilizadas para proteger la base de datos. Igualmente, debe disponer de los permisos Abrir o ejecutar y Abrir en modo exclusivo para poder abrir la base de datos en modo exclusivo.

Protección mediante contraseña

Otro método de mejorar la seguridad consiste en establecer una contraseña para el acceso a la base de datos de Access. Una vez establecida una contraseña, aparece un cuadro de diálogo que la solicita siempre que se intenta el acceso a la base de datos. Este método es fácil de aplicar y es relativamente seguro porque Access cifra la contraseña de modo que no es posible observarla mediante la lectura directa del archivo de base de datos. La protección mediante contraseña sólo se aplica al abrir la base de datos. Una vez abierta, el usuario puede disponer de todos los objetos, salvo que se definan otros mecanismos de seguridad. Este método puede aplicarse cuando un grupo reducido de usuarios compartan una base de datos en un solo equipo.

Nota

No utilice una contraseña para la base de datos si la va a replicar. Las bases de datos replicadas no se pueden sincronizar cuando se utilizan contraseñas en la base de datos.

Seguridad para el usuario.

El mejor modo de proteger una base de datos es aplicar la seguridad para el usuario, lo que permite establecer distintos niveles de acceso a los datos y objetos reservados. Para facilitar esta labor puede usar el Asistente para seguridad por

usuarios mostrado en la Seguridad para el usuario. Para utilizar una base de datos protegida para los usuarios, éstos deben especificar una contraseña al iniciar Access. Access lee un archivo de información de grupos de trabajo en el que se identifica a cada usuario con un código único. El nivel de acceso y los objetos a los que un usuario tiene acceso pueden establecerse en función de este código de identificación y de una contraseña.

Este asistente permite proteger una base de datos de Access en un solo paso. Además, al implementar esquemas de seguridad comunes, el asistente reduce lo máximo posible, y puede incluso eliminar, la necesidad de utilizar el comando Seguridad del menú Herramientas.

Una vez ejecutado el Asistente para seguridad por usuarios, puede crear sus propios grupos de usuarios y asignarles o retirarles permisos para una base de datos y sus tablas, consultas, formularios, informes o macros. Igualmente, puede establecer los permisos predeterminados que Microsoft Access debe asignar a las nuevas tablas, consultas, formularios, informes y macros creados en una base de datos.

Impedir que los usuarios repliquen una base de datos, establezcan contraseñas o configuren opciones de inicio. En un entorno multiusuario hay numerosas situaciones en las que es deseable evitar que los usuarios puedan copiar la base de datos. Al copiar una base de datos, un usuario puede copiar la base de datos compartida e incluso agregarle campos y hacer cambios como establecer una contraseña, retirar la protección mediante contraseña o cambiar las propiedades de inicio. Al dejar que los usuarios realicen este tipo de cambios, se les está permitiendo impedir el acceso adecuado de otros usuarios o que la base de datos funcione del modo para el que fue diseñada.

Si una base de datos compartida no tiene definida la seguridad para los usuarios, no es posible evitar que un usuario efectúe estos cambios. Cuando se define la seguridad para los usuarios, un usuario o grupo debe disponer del permiso Administrar para replicar la base de datos, establecer una contraseña o cambiar las propiedades de inicio. Sólo los miembros del grupo Administradores del grupo de trabajo tiene el permiso Administrar.

Si un usuario o grupo dispone de ese permiso para una base de datos, al retirárselo se le impide llevar a cabo los cambios descritos. Si se requiere que un usuario o grupo pueda realizar alguna de estas tareas puede asignársele el permiso Administrar. No puede controlar el acceso a cada una de estas tres tareas independientemente.

Zonas de seguridad

Access ha agregado las características necesarias para aplicar zonas de seguridad en el acceso a bases de datos a través del web. Access utiliza las

opciones de seguridad de Internet Explorer (disponibles en Internet Explorer 4.0 y posteriores) para determinar si una base de datos remota se encuentra en una zona de seguridad de confianza. Internet Explorer divide Internet en zonas, de forma que es posible asignar cada sitio web a la zona con el nivel de seguridad que le corresponda.

Siempre que se intenta abrir o descargar una base de datos desde el web, Access utiliza el Administrador de seguridad de Internet Explorer para comprobar en qué zona de seguridad se encuentra el sitio web correspondiente. Hay cuatro zonas distintas:

- Zona Internet: de forma predeterminada, esta zona contiene todo lo que no se encuentre en su propio equipo o en una intranet, y que no esté asignado a otra zona. El nivel de seguridad predeterminado para la zona Internet es Medio.

- Zona Intranet local: normalmente, esta zona contiene las direcciones que no requieren un servidor proxy, definidas por el Administrador del sistema. Entre ellas se encuentran los sitios especificados en la ficha Conexiones, las rutas de red (como \\servidor\recurso) y los sitios de la intranet local (normalmente, direcciones que no contienen puntos, como http://interno). Si lo desea, puede asignar sitios a esta zona. El nivel de seguridad predeterminado para la zona Intranet local es Medio-bajo.

- Zona Sitios de confianza: contiene los sitios de confianza, es decir, aquellos desde los que cree poder descargar o ejecutar archivos sin preocuparse de que puedan causar daños en el equipo o en los datos. Si lo desea, puede asignar sitios a esta zona. El nivel de seguridad predeterminado para la zona Sitios de confianza es Bajo.

- Zona Sitios restringidos: contiene sitios que no son de confianza, es decir, sitios de los que duda si puede descargar o ejecutar archivos sin dañar el equipo o los datos. Si lo desea, puede asignar sitios a esta zona. El nivel de seguridad predeterminado para la zona Sitios restringidos es Alto.

Además, se supone que los archivos que ya se encuentran en el equipo son muy seguros, de modo que se les asigna una configuración de seguridad mínima. No es posible asignar una carpeta o unidad del equipo a una zona de seguridad.

Access sólo abre archivos que se encuentren en las zonas Intranet local o Sitios de confianza. No abrirá ningún archivo de las zonas Internet o Sitios restringidos. Access no se ve afectado por el cambio del nivel de seguridad de una zona.

Como conclusión Microsoft Office XP permite administrar la seguridad de las aplicaciones y documentos a través de diversos métodos de control de acceso

relacionados. Conocer la forma de establecer los controles de acceso de seguridad siguientes le ayudará a crear un entorno seguro para las aplicaciones y los datos de los usuarios.

9.2.8 Artículo 12.3 (Autorización)

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

Tanto Microsoft Windows 2000 como Microsoft Windows XP poseen la ventana de seguridad en cada objeto almacenado que nos permite ver a nivel de archivo o carpeta la seguridad aplicada.

Microsoft Windows XP, además, posee la opción de obtener una relación de derechos para determinado grupo de usuarios respecto de un objeto determinado.

Además, existen utilidades que nos permiten saber los permisos que sobre determinadas carpetas y ficheros tiene un usuario. Por ejemplo, la utilidad gratuita DumpSec (aka DumpACL) de *Somarsoft, www.somarsoft.com,* nos vuelca todos los permisos respecto de ficheros, claves de registro o carpetas concretas de forma fácil y rápida.

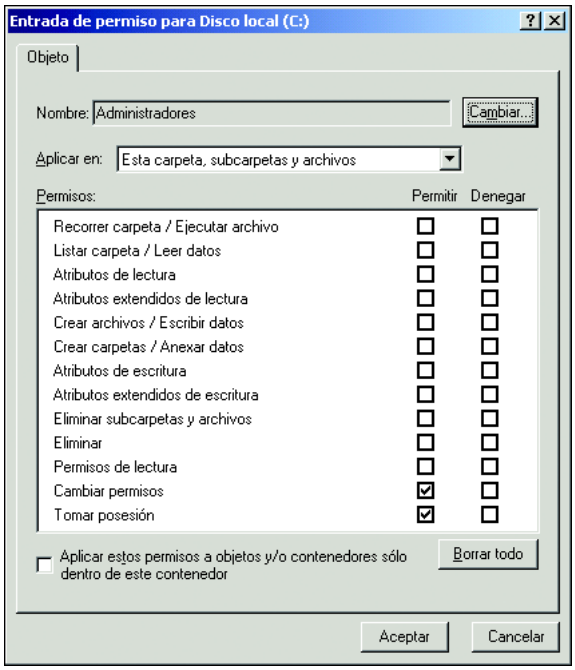


Figura 9.38. *Cambio de permisos y toma de control.*

Estas utilidades permitirán obtener la información necesaria para el posterior cumplimiento de la norma (el reglamento de seguridad exige que los usuarios han de estar claramente identificados y autorizados para acceder a los datos).

9.2.9 Artículo 12.4 (Autorización)

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

La labor de administración de permisos también se realiza a través de ACLs, como anteriormente hemos visto, ya que para el sistema operativo es otro tipo de acceso más. Esta labor se realiza específicamente con los permisos *Cambiar permisos* y *Tomar posesión* los cuales son igualmente aplicables como podemos observar en la figura 9.38.

9.2.10 Artículo 13.1. Gestión de soportes

> "*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.*"

Microsoft Windows 2000 y Microsoft Windows XP no sólo poseen la capacidad de etiquetado de discos y medios. También ofrecen un servicio con capacidades de inventario y gestión de archivos denominado *Removable Storage.*

Este servicio facilita la gestión de los medios desmontables y el manejo de los dispositivos que los utilizan: CD-R, Iomega Zip o Jaz, dispositivos de Backup, etc.; *Removable Storage* cataloga, etiqueta y contabiliza los datos escritos en el medio, además de controlar los dispositivos. Funciona siempre asociado a una aplicación de gestión de datos y es capaz de compartir el medio con datos de diversas aplicaciones requiriendo el montaje y desmontaje de dispositivos según va necesitando acceder a ellos para escribir o recuperar datos.

Junto con el anterior, Microsoft Windows 2000 Server ofrece el servicio *Remote Storage* que complementa al anterior ofreciendo capacidades de gestión de volúmenes y ficheros.

9.2.11 Artículo 14.2. Copias de respaldo

"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."

Microsoft Windows 2000 y Microsoft Windows XP poseen una herramienta para la realización de copias de seguridad y para la restauración de las mismas. Esta herramienta permite realizar una copia (o restaurar en su caso) uno o varios archivos concretos o uno o varios directorios. La copia de seguridad se puede guardar en un disquete, en el disco duro de un ordenador o en otro tipo de medios en los que se puedan guardar este tipo de copias (por ejemplo cintas).

El proceso para la realización de la copia de seguridad es relativamente sencillo:

- Se seleccionan los archivos o los directorios de los que se quiera realizar la copia de seguridad.
- Se selecciona el medio donde se quiera guardar la copia de seguridad que se va a realizar.
- Se selecciona el tipo de copia de seguridad deseada.
- Se inicia el procedimiento de copia de seguridad.

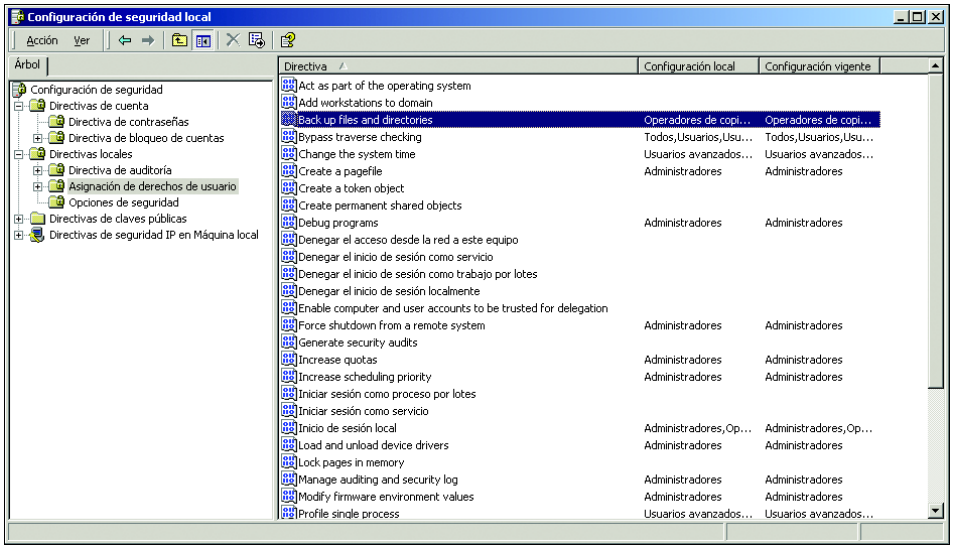


Figura 9.39. *Control de los privilegios para back-up de ficheros y directorios.*

Por lo que respecta al procedimiento de restauración de las copias de seguridad realizadas, el procedimiento es, igualmente, sencillo y similar al anterior:

- Se selecciona la copia de seguridad que se desee restaurar.
- Se selecciona el destino donde se quiera restaurar esa copia de seguridad.
- Se inicia el procedimiento de restauración de copias de seguridad.

Es importante señalar que, tanto el procedimiento de copias de seguridad como la restauración de las mismas, deben ser realizadas por una persona debidamente autorizada ya que, como reflejamos en la parte legal del presente libro, en determinadas ocasiones existen una serie de requisitos legales para iniciar ambos procedimientos.

Microsoft Windows 2000 y Microsoft Windows XP tratan como un privilegio restringido las acciones de realizar copias de seguridad y restaurarlas que, por defecto, únicamente se da a los grupos locales Operadores de copia, Operadores de Servidor y Administradores.

A continuación reflejamos en la figura 9.40 la herramienta de copia de seguridad y de restauración

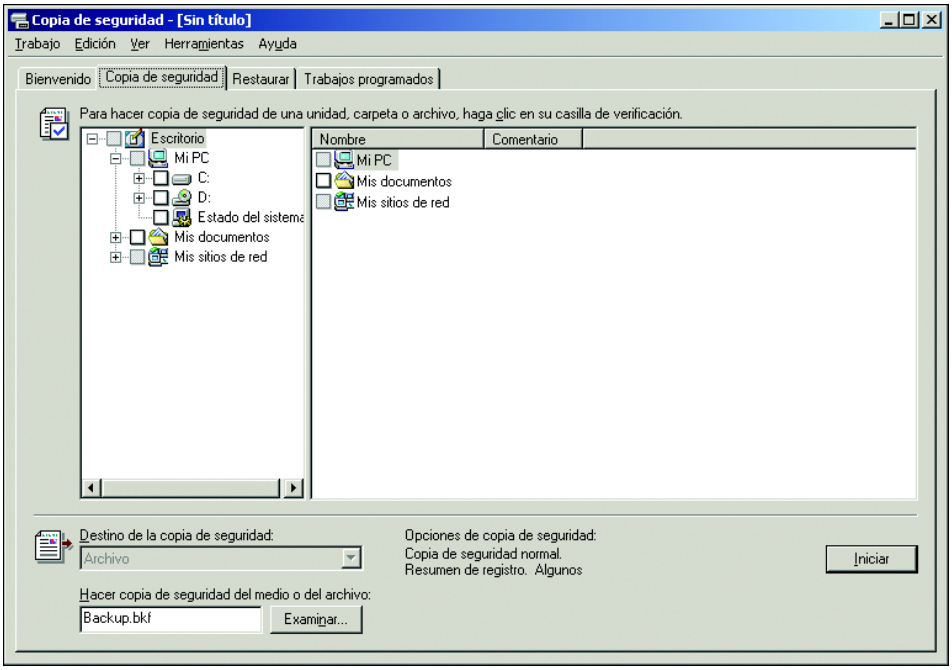


Figura 9.40. *Herramienta de copia de seguridad y de restauración.*

Copias de respaldo en Microsoft SQL Server 2000

Microsoft SQL Server 2000 proporciona las herramientas necesarias para hacer copias de seguridad y restaurar tanto las bases de datos del sistema como las definidas por el usuario. Entre estas herramientas se incluye el Administrador corporativo, los Asistentes para planes de mantenimiento de bases de datos y los comandos Backup y Restore de Transact-SQL.

Para evitar errores accidentales o agregar un nivel de seguridad adicional que impida el acceso de personas no autorizadas, el administrador de bases de datos puede utilizar una contraseña para el conjunto de copias de seguridad o para el conjunto de medios. Con la primera se evita que se realicen restauraciones no autorizadas del conjunto de copias de seguridad y, con la segunda, se impide el mismo proceso pero en los conjuntos de copias de seguridad contenido en los medios. El uso de contraseñas también evita que se hagan copias de seguridad no autorizadas de los propios medios. Agregar una contraseña para el conjunto de medios evita que las copias de seguridad de otros productos, como las de Microsoft Windows 2000, se anexen a los medios.

En cuanto a la recuperación de las bases de datos, existen diversas maneras de revertir una base de datos a un momento determinado para reconstruir los datos en el estado en que se encontraban en el caso en que se produzca, por un error de la aplicación o del usuario, una pérdida o destrucción de los mismos. Cuando se trabaja con copias de seguridad del registro de transacciones, la base de datos se puede restaurar al estado en que se encontraba en un momento determinado o cuando se produjo una transacción marcada.

Hay varios tipos de copias de seguridad disponibles: completa, diferencial, del registro de transacciones y de archivo o grupo de archivos. Además, hay varios modelos de recuperación disponibles: simple, de registro masivo y completa.

Copias de seguridad completas

Son las predeterminadas y el punto de partida de los demás tipos. Con ellas se captura toda la base de datos, incluidas todas las entradas del registro de transacciones, aunque se excluyen las extensiones sin asignar de los archivos. Las páginas se pueden leer directamente del disco para incrementar la velocidad de la operación. Este tipo de copia de seguridad se debe realizar de forma periódica en bases de datos del sistema y en las definidas por el usuario. Se debe realizar copia de seguridad de las bases de datos *master* y *msdb* siempre que se produzca algún cambio que las afecte. Habrá que realizar una copia de seguridad de la base de datos *master* cuando cree o altere bases de datos, inicios de sesión, servidores vinculados, cambios de configuración, etc. Se deberá realizar una copia de seguridad de la base de datos *msdb* cuando cree o altere trabajos, alertas, operadores, programaciones, etc. También debe hacer copia de seguridad de la base de datos *distribution* si el servidor

está realizando la función de distribución. De la base de datos *model* también se debe hacer copia de seguridad si en ella se han efectuado cambios significativos. Las copias de seguridad completas de las bases de datos definidas por el usuario se deben realizar después de crearlas para proporcionar un punto de partida al proceso de recuperación. Asimismo, se debe realizar de forma periódica una copia de seguridad completa. La programación dependerá de las circunstancias. Una copia de seguridad completa no borra el registro de transacciones. Es necesario iniciar un proceso para borrar el registro periódicamente con el fin de evitar que se llene. No obstante, cualquier transacción que estuviera en proceso durante la realización de la copia de seguridad se incluirá en la misma.

Copias de seguridad diferenciales

Capturan todos los datos que hayan cambiado desde la última copia de seguridad completa. Al realizarlas, se incrementa la velocidad de las operaciones de copia de seguridad y restauración. Debido a que sólo se capturan las extensiones recién asignadas o que hayan cambiado (seguimiento de mapas de bits), las copias de seguridad diferenciales son más rápidas y menores que las completas. Además, en un proceso de recuperación, la última copia de seguridad diferencial se puede restaurar sin aplicar cada una de la serie de copias de seguridad del registro de transacciones ni diferenciales que se realizan entre la última copia completa y la última copia diferencial (todos los datos modificados se capturan en la última copia diferencial). Las copias de seguridad diferenciales no permiten recuperar el registro hasta una marca ni hasta un momento concreto.

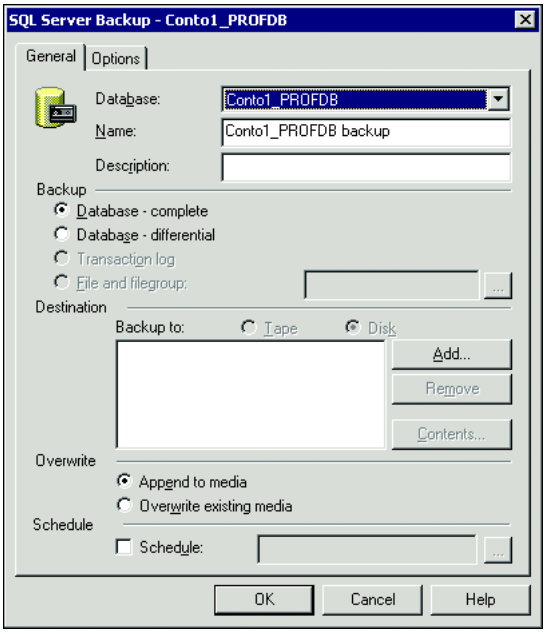


Figura 9.41. *Copia de seguridad en SQL Server.*

Copias de seguridad del registro de transacciones

Capturan las modificaciones de la base de datos. El registro de transacciones graba estas modificaciones en serie. Este tipo de copias proporciona un historial de las transacciones que han tenido lugar en la base de datos. Las copias de seguridad del registro se utilizan entonces en el proceso de recuperación para restaurar la base de datos completamente, en un momento determinado (STOPAT) o en una marca del registro (STOPATMARK o STOPBEFOREMARK), y se aplican para recuperar una base de datos al completar (rehacer) los cambios confirmados que no se reflejan en la base de datos y revertir (deshacer) las transacciones sin confirmar. Además, estas copias de seguridad son más pequeñas y se realizan con más frecuencia que las completas y las diferenciales.

En cuanto a la recuperación de las bases de datos, existen diversas maneras de revertir una base de datos a un momento determinado para reconstruir los datos en el estado en que se encontraban en el caso en que se produzca, por un error de la aplicación o del usuario, una pérdida o destrucción de los mismos. La copia de seguridad de la base de datos, ya sea diferencial o del registro de transacciones, se puede restaurar con la opción WITH RECOVERY y revertir así la base de datos al estado en que se encontraba en el momento de realizar la copia de seguridad. Cuando se trabaja con copias de seguridad del registro de transacciones, la base de datos se puede restaurar al estado en que se encontraba en un momento determinado o cuando se produjo una transacción marcada.

Recuperación hasta un momento determinado

Este tipo de recuperación sólo funciona con copias de seguridad del registro de transacciones. El administrador de la base de datos utilizará el argumento STOPAT de la instrucción RESTORE para especificar una fecha y una hora que determine el momento hasta el que recuperar la base de datos. Debido a la gran cantidad de bases de datos de producción que funcionan ahora con muchas zonas horarias internacionales diferentes, es imprescindible que el administrador calcule la fecha y la hora correctas del usuario que ha informado del error. La opción STOPAT no se puede combinar con NO_RECOVERY para probar los datos incorrectos, por tanto, se requiere la hora correcta. Las transacciones que no se hayan confirmado antes de la fecha y la hora especificadas en el comando RESTORE se revertirán, con lo que se pierde el trabajo.

Las transacciones marcadas dan al administrador de la base de datos mayor control a la hora de determinar el momento en que se produjo una transacción incorrecta y, de este modo, el proceso de recuperación resulta mucho más fácil. A la transacción se le asigna un nombre mediante la instrucción BEGIN TRAN y el nombre se almacena en el registro con el argumento WITH MARK. Si el administrador de la base de datos necesita recuperar la instrucción incorrecta,

podrá especificar STOPBEFOREMARK o STOPAFTERMARK para controlar si la instrucción se aplica o no a la base de datos. El argumento STOPBEFOREMARK no incluye la transacción marcada en la restauración a diferencia del argumento STOPAFTERMARK, que sí la incluye. Todas las transacciones que no se hayan confirmado "antes de" o "a continuación de" la marca (según la opción elegida), no se reflejarán en la base de datos. Cuando los nombres de la marca sean iguales en el registro de transacciones, utilice el argumento AFTER *datetime* para diferenciarlos. El espacio de registro se debe establecer de modo que crezca automáticamente y la cantidad de espacio del registro se debe supervisar constantemente ya sea mediante secuencias de comandos y tablas de auditoría, o a través de una alerta de la condición de rendimiento en Objeto – *SQL Server: Bases de datos* Contador: *Porcentaje utilizado del registro.* Si el registro de transacciones se llena, la actividad en la base de datos se detiene hasta que se borre o se aumente su tamaño. Si el registro se llena, intente borrarlo con la instrucción BACKUP LOG o intente aumentar su tamaño (o agregue un registro adicional) con el comando ALTER DATABASE; el archivo se puede reducir más adelante si fuera necesario. El registro de transacciones debe colocarse en un conjunto de unidades con tolerancia a errores que esté separado de los datos reales. De este modo, el rendimiento se incrementa porque las escrituras en los archivos de registro se escriben secuencialmente y las escrituras en los archivos de datos se suelen escribir de forma aleatoria a través de sus páginas. Además, al separar el archivo o archivos de registro del archivo o archivos de datos también se reduce la pérdida de datos porque el registro huérfano se puede seguir capturando en el caso de que resulte dañado. Si se hacen copias de seguridad del registro de transacciones con frecuencia, se puede reducir la pérdida de datos. También se deben implementar en este escenario copias de seguridad diferenciales para disminuir el tiempo de recuperación y la pérdida de datos. Si se intenta realizar copias de seguridad del registro de transacciones cuando la base de datos está en modo de recuperación simple o está habilitada la opción Truncate log on checkpoint (truncar registro en punto de comprobación), la opción del registro de transacciones del Administrador corporativo estará atenuada y el Analizador de objetos devolverá el mensaje de error 4208. Estas opciones no deben establecerse para realizar copias de seguridad del registro de transacciones.

Modelo de recuperación de registro masivo

Este modelo es similar al de recuperación completa en que se registran todas las operaciones, incluidas las masivas. La diferencia entre ellos radica en que en la recuperación de registro masivo se registran y mantienen sólo las asignaciones de página de ciertas operaciones y no las filas individuales. Entre estas operaciones se incluyen las de texto e imágenes: CREATE INDEX, SELECT INTO, BCP.EXE o BULK INSERT. El resultado de este proceso es que se registran menos entradas y el archivo de registro es menor. Si el archivo de datos se pierde mientras se está ejecutando la recuperación de registro masivo, todas las

transacciones del registro actual no se pueden recuperar porque el registro sólo contiene punteros a las páginas de datos que contienen los datos, no a los datos reales. De este modo, en este modelo no se puede realizar la recuperación hasta un momento determinado.

Se deben cumplir varias condiciones para que se lleve a cabo un registro mínimo con operaciones de copia masiva en el modelo de recuperación de registro masivo. La tabla de destino debe cumplir los siguientes requisitos:

- No ser parte de una publicación.
- No tener desencadenadores habilitados.
- No tener índices.
- Utilizar sugerencias de optimizador TABLOCK.

En los casos en los que se inserten masivamente enormes cantidades de datos en la tabla de destino con índices, es posible que sea más eficaz eliminar los índices antes de llevar a cabo el proceso de inserción. Los índices se pueden volver a crear después de cargar los datos. De este modo, las inserciones en los índices no se tienen que registrar en el momento de la carga de datos.

Modelo de recuperación simple

En este modelo se utilizan copias de seguridad completas de base de datos y, opcionalmente, copias de seguridad diferenciales; las copias de seguridad de registro de transacciones no están disponibles. Por tanto, no se puede realizar la recuperación hasta un momento determinado ni hasta una marca en el registro. Las bases de datos sólo se pueden recuperar hasta el momento de la última copia de seguridad completa o diferencial: la que esté disponible. No obstante, el modelo de recuperación simple es el más fácil de administrar y mejora el rendimiento de ciertas operaciones masivas, y de otras operaciones, al reducir la cantidad de registros y reutilizar automáticamente el espacio del registro. Este modelo es absolutamente adecuado para probar entornos en los que se está examinando la funcionalidad de una aplicación y los datos que se están utilizando carecen de importancia.

Hay diversas formas de comprobar la confiabilidad del proceso de copia de seguridad y sus datos. Por lo general, se suele utilizar un servidor de reserva. Las copias de seguridad se pueden realizar en el servidor de producción y luego aplicarlas al servidor de reserva. El servidor de reserva (en modo de espera) admite comandos DBCC, como DBCC CHECKDB, para ejecutarlos con los datos. De este modo, el administrador de bases de datos se asegurará de que la operación de copia de seguridad se ha realizado correctamente y que la copia de seguridad y sus datos no se han dañado.

Si se daña la base de datos original tras el proceso de copia de seguridad completa de base de datos y restauración, las copias de seguridad del registro no detectarán el daño en el servidor de producción porque el registro no contiene las páginas de datos reales.

Los administradores pueden ejecutar la instrucción RESTORE VERIFYONLY para comprobar la copia de seguridad. Esta instrucción examina el dispositivo o dispositivos de copia de seguridad para asegurarse de que están todos los archivos y que se pueden leer. Esta instrucción no comprueba si los datos están dañados (ver figura 9.42).

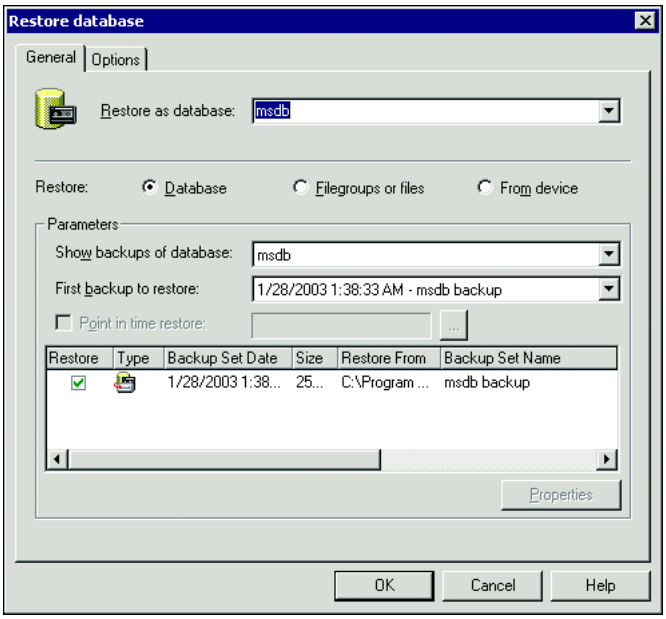


Figura 9.42. *Restauración de las bases de datos.*

9.2.12 Artículo 14.3. Copias de respaldo

> *"Deberán realizarse copias de respaldo al menos semanalmente, salvo que en dicho periodo no se hubiera producido ninguna actualización de los datos."*

Si utilizamos la aplicación de copia de seguridad anteriormente señalada podremos establecer el calendario de realización de copias en la pestaña Tareas Programadas como podemos observar en la figura 9.43.

Otras aplicaciones de copia de seguridad que no tengan su propio sistema de lanzamiento automático pueden ser invocadas desde la aplicación *Tareas*

Programadas de Microsoft Windows 2000 o Microsoft Windows XP. Esta aplicación, a la que se accede a través del Panel de control nos permite establecer cuándo, en qué entorno de usuario y con qué parámetros serán ejecutadas las distintas aplicaciones que deseemos mediante la cumplimentación de un sencillo asistente.

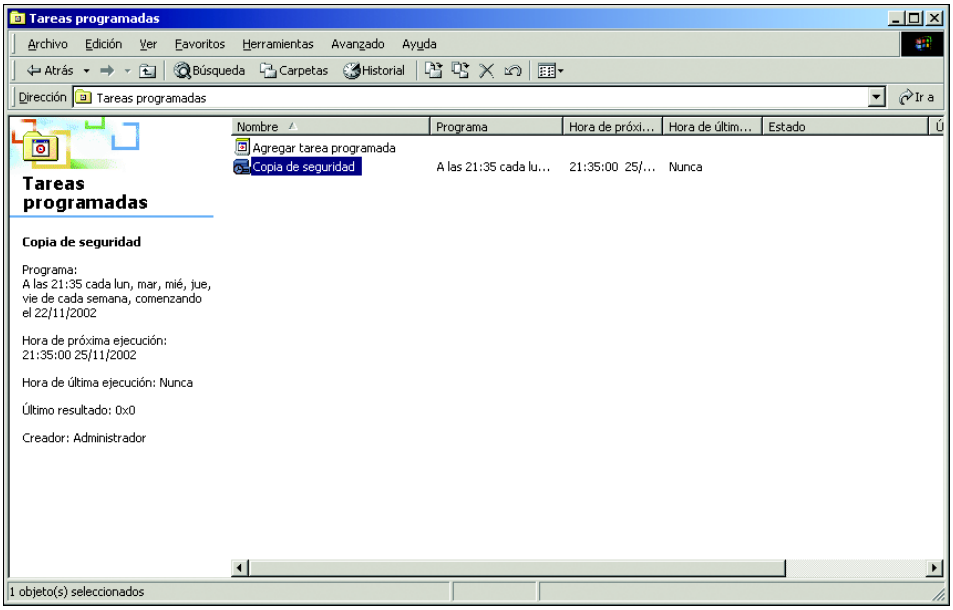


Figura 9.43. *Programación de tareas.*

9.3 Tecnología aplicable a medidas de nivel medio

Cuando existan datos de nivel medio, además de las medidas de nivel básico, tendremos que aplicar medidas más restrictivas en los siguientes aspectos que a continuación detallamos.

9.3.1 Artículo 18.1. Identificación y autenticación

> *"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."*

Se nos recalca en este artículo la necesidad de autentificación para el usuario, la cual entendemos se cumple mediante la utilización de cuenta y contraseña debidamente gestionada en el tiempo tal y como señalamos anteriormente.

En este capítulo se nos recalca la necesidad de la cuenta única por usuario de tal manera que una cuenta no pueda ser utilizada por más de dos personas, evitando así las llamadas "cuentas genéricas".

La gestión de la cuenta en el tiempo incluye aquellos métodos que permitan asegurarnos que el usuario es el único conocedor de la contraseña, esto lo logramos mediante el cambio de la contraseña, la evitación de repeticiones, etc. tal y como comentamos anteriormente.

Para la verificabilidad tendremos que activar la auditoría de seguridad que nos indicará el buen o mal uso por parte de los usuarios de los privilegios y accesos que tienen. Esto también lo vimos anteriormente en lo referente a auditoría y registro de sucesos del sistema.

Microsoft Windows 2000 y Microsoft Windows XP, al requerir que cada proceso se realice en el entorno de una cuenta, crean por defecto una serie de cuentas con derechos restringidos para realizar tareas internas de proceso requeridas por el sistema operativo. Estas cuentas no son utilizadas para el acceso a datos ni son identificadas con respecto a un usuario, por lo que las excluiremos de los derechos de acceso a estos archivos para que, aun en el hipotético caso de su uso fraudulento por un usuario el acceso, les sea denegado. Estas cuentas denominadas *Built-in Security Principals* son en Microsoft Windows 2000 la cuenta *System* o *Local System Account*, y en Microsoft Windows XP, además de la anterior, las cuentas *NetworkService* y *LocalService*.

Igualmente, distintas aplicaciones pueden crear otras cuentas de las que también deberemos verificar el acceso que tienen a los archivos a proteger sin olvidarnos de su adscripción a distintos grupos con acceso o privilegios.

Como regla general, a los archivos que señala la norma sólo concederemos acceso a cuentas identificadas y grupos que únicamente contengan estas cuentas autentificadas.

Respecto a las cuentas por defecto creadas por Microsoft Windows 2000 y Microsoft Windows XP, *Administrador* e *Invitado*, nos aseguraremos que se tiene una contraseña más fuerte aún que la política, que la contraseña de *Administrador* sólo es conocida por el responsable de seguridad y se encuentra almacenada en un lugar seguro y que la cuenta de *Invitado* se encuentra deshabilitada. Ninguna de estas dos cuentas deberá tener tampoco acceso a los archivos a proteger. Señalando explícitamente una denegación de acceso como podemos ver en la figura 9.44.

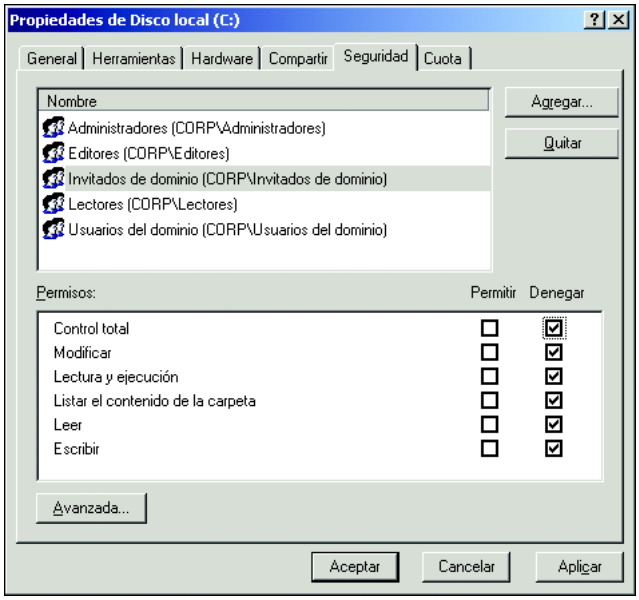


Figura 9.44. *Denegación de acceso.*

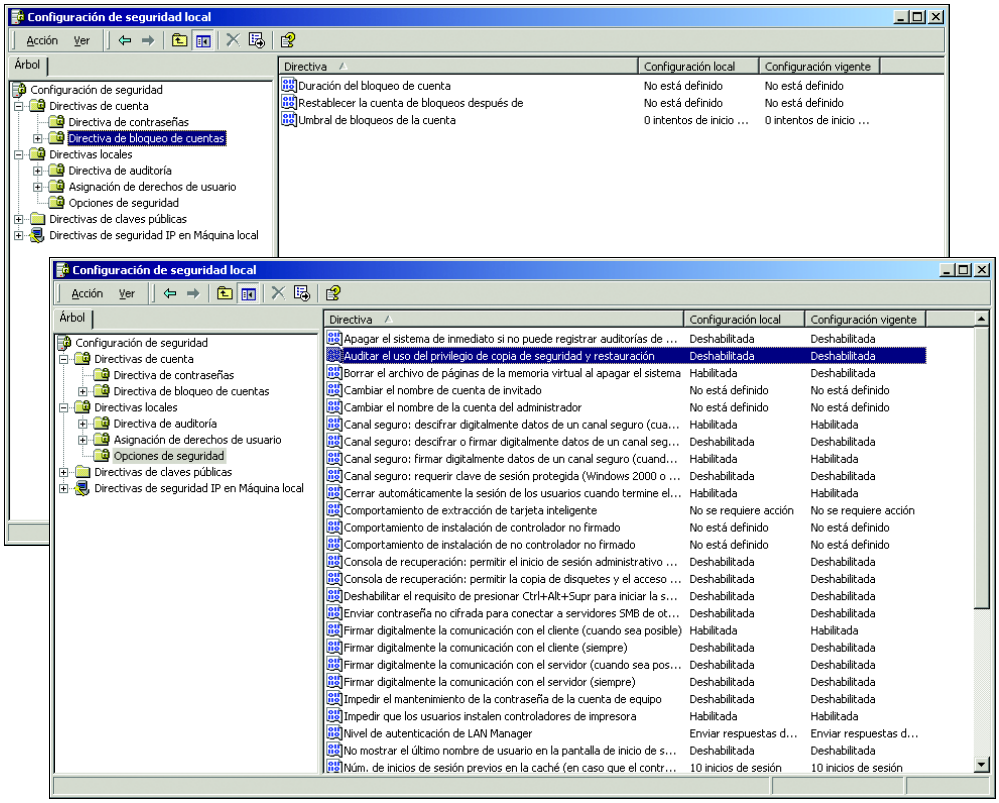


Figura 9.45. *Bloqueos de cuenta.*

9.3.2 Artículo 18.2 (Autentificación)

> "*Se limitará la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.*

El cumplimiento de este control se realiza mediante el bloqueo de cuentas al sistema. Por defecto podremos bloquear las cuentas cuando transcurridos varios intentos, en un tiempo determinado, no se haya introducido una contraseña correcta. En este caso, la cuenta quedará bloqueada durante un determinado tiempo o hasta que un administrador la desbloquee. La cuenta bloqueada supone la denegación de acceso al sistema aun cuando la contraseña sea correcta.

Para establecer esto en la política local o en la política de grupo tenemos la subcarpeta Directiva de bloqueo de cuentas en la subcarpeta Directivas de cuenta donde podemos definir el número de intentos de acceso permitidos, el intervalo de tiempo en el que se contabilizará ese número y la duración del bloqueo de la cuenta una vez realizados los intentos señalados (ver figura 9.45).

9.3.3 Artículo 20.4. Gestión de soportes (Encrypted File System)

> "*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.*"

Los sistemas de seguridad basados en la autentificación protegen los recursos a nivel de acceso, bien interactivo, bien a través de la red, controlando el acceso y evitando el acceso no autorizado mediante componentes de bajo nivel del sistema operativo. Ahora bien, si un usuario tiene acceso físico al depósito de datos, la máquina o un dispositivo de medios, y es capaz de acceder a los datos sin utilizar el sistema operativo original puede saltarse las funcionalidades de seguridad que este ofrece y por consiguiente tener acceso a datos sensibles.

Cifrar estos archivos con datos sensibles es entonces la única opción que tenemos para evitar este acceso. Los sistemas operativos Microsoft Windows 2000 y Microsoft Windows XP disponen de un sistema de cifrado de ficheros que mediante la utilización de criptografía avanzada, permiten asegurar los datos aún cuando se haya accedido al almacenamiento de éstos saltándose la seguridad que ofrece el sistema operativo. A este sistema le denominamos Sistema de ficheros cifrados (*Encrypted File System* o EFS).

EFS se encuentra integrado directamente con el sistema de ficheros NTFS, por tanto, se encuentra a más bajo nivel que el módulo de seguridad del sistema operativo. Esta integración tan baja permite asegurar el cifrado del sistema de almacenamiento de forma totalmente transparente al usuario y con una mínima carga de proceso respecto del sistema operativo, de tal forma que un atacante aun apropiándose del sistema de almacenamiento y cargándolo en otro sistema sólo accedería a datos ininteligibles.

Su integración también provoca que para el usuario que quiere el cifrado sobre ciertos documentos o discos sea tan simple como marcar una casilla en las propiedades de la carpeta o fichero. EFS descifra los datos cuando los lee del disco y los cifra cuando los escribe en el disco sin que el usuario reciba ninguna percepción de esto.

El funcionamiento de EFS es el siguiente:

EFS utiliza una clave única por fichero para cifrarlo y descifrarlo. Esta clave, denominada clave de cifrado de fichero (*File Encryption Key* o FEK), se genera cuando se cifra un fichero y se almacena en el mismo fichero.

Para que cualquiera que tenga acceso físico al fichero no pueda utilizar el FEK para descifrarlo, lo que sucede es que este FEK a su vez es cifrado con la clave pública del usuario antes de almacenarlo.

Para conseguir descifrar el fichero, el usuario utilizará su clave privada para acceder al FEK cifrado, descifrarlo y, una vez realizado, descifrar el fichero con ese FEK.

El sistema de cifrdo utilizado en Microsoft Windows 2000 es DESX, mientras que en Microsoft Windows XP puede elegirse entre DESX y 3DES.

Microsoft Windows XP también ofrece algunas características no ofrecidas por Microsoft Windows 2000 como son:

- Usuarios adicionales pueden ser autorizados a acceder a los ficheros cifrados.
- Los ficheros *Offline* pueden ser cifrados.
- Los agentes de recuperación son recomendables pero no obligatorios.
- Los ficheros cifrados pueden almacenarse en *Webfolders*.

Aunque EFS puede ser utilizado desde el primer momento, su estrategia de uso diferirá si nos referimos a un dominio o a un ordenador aislado debido a temas de manejabilidad de los agentes de recuperación, potencia de la guarda, gestión de perdidas de claves de los usuarios y a la emisión de certificados en vez de por el propio usuario en local desde una PKI.

Normalmente, en un dominio el certificado que el usuario utiliza para EFS debería obtenerse de la PKI corporativa, al igual que el de los agentes de recuperación, con lo que la pérdida de la clave secreta del usuario me permitiría el descifrado del archivo por el/los agentes de recuperación de dominio.

En un ordenador aislado resulta conveniente establecer una copia de seguridad de las claves al menos del agente de recuperación ante el borrado accidental de las claves del usuario.

Por defecto en cada máquina local el agente de recuperación es el administrador de la máquina y, en un Directorio Activo, el administrador del primer dominio creado, aunque esto se puede modificar mediante políticas. La función del agente de recuperación es la de poder desencriptar el FEK con su propia clave privada de tal manera que no haya perdida de datos. El agente de recuperación lo que nunca podrá hacer será obtener la clave privada del usuario de manera que otros datos de los que él no sea agente de recuperación le resultarán vedados.

Otros temas importantes respecto a EFS son:

- EFS no afecta a otros atributos del fichero como los permisos inherentes al fichero.
- Sólo funciona la encriptación si el sistema de ficheros es NTFS de Microsoft Windows 2000 o Microsoft Windows XP.
- Se puede encriptar y desencriptar ficheros en remoto pero el fichero en su viaje a través de la red no va encriptado.
- No pueden encriptarse archivos o carpetas de sistema.
- No pueden encriptarse archivos o carpetas comprimidos.
- La encriptación de una carpeta nos asegura que cualquier fichero que se cree o copie desde el mismo sistema en esa carpeta se encripta de forma automática. Por el contrario un fichero que se mueva desde el mismo sistema a una carpeta encriptada conservará el grado de encriptación que tuviera antes, si viene encriptado lo estará pero si no lo está no se encriptará.

- Si queremos asegurarnos que los ficheros temporales generados por una aplicación también se encriptan, la mejor opción es señalar la encriptación a nivel de carpetas.
- Mover o copiar un fichero encriptado a otro sistema elimina la encriptación
- Hacer una copia de respaldo de un fichero encriptado supone el mantenerlo encriptado si el programa de encriptación está certificado para Microsoft Windows 2000.
- Encriptar una carpeta no supone su encriptación sino automatizar la encriptación de los ficheros que contiene.

Por lo que respecta a medios removibles, EFS será capaz de encriptar el contenido sin que en el medio permanezca clave alguna del usuario o del agente de recuperación, con lo que la seguridad será muy alta. Esto se realiza de forma automática en los medios en los que se puede utilizar NTFS.

9.3.4 Artículo 21.1 Registro de incidencias. (Auditoría de copias de seguridad)

> "*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.*"

Para ayudar al responsable de seguridad en esta tarea podremos establecer que se auditen las acciones de copia de respaldo y recuperación en el sistema y apoyarnos en los registros de las aplicaciones de copia de respaldo para conocer que ha sido lo respaldado o restaurado. Para señalar al sistema que debe auditar la realización de la copia de respaldo o la realización de la restauración en la subcarpeta Opciones de Seguridad de la carpeta Directivas locales correspondientes a la Directiva de seguridad local o de dominio, habilitaremos la opción Auditar el uso del privilegio de copia de seguridad y restauración.

9.4 Tecnología aplicable a medidas de nivel alto

9.4.1 Artículo 23. Distribución de soportes

> "*La distribución de los soportes que contengan datos de carácter personal se realizará cifrando los datos o bien utilizando cualquier otro mecanismo que garantice que dicha información, no sea inteligible ni manipulada durante su transporte.*"

Como antes comentamos, EFS nos facilita esta labor al posibilitarnos el cifrado completo de un dispositivo que soporte NTFS. En dispositivos que no soporten el sistema de ficheros NTFS podemos utilizar EFS realizando una copia de respaldo de ficheros cifrados y almacenándola en dicho dispositivo.

En estos casos resulta importante establecer una correcta gestión de claves y certificados y, para una correcta gestión de certificados, nada mejor que la utilización de la característica de PKI que ofrece Microsoft Windows 2000 Server.

Una infraestructura de PKI se encarga de emitir los certificados, esto es, de firmar las claves públicas, de los componentes subordinados y verificar la autenticidad y vigencia de los certificados por ella emitidos cuando se le solicita por una aplicación. Su uso junto al Directorio Activo de Microsoft Windows 2000 produce una integración total, lo que facilita la gestión y seguridad de uso de la criptografía necesaria para tareas como EFS.

En un entorno sin directorio, cada usuario generará en cada máquina que utilice EFS un par de claves distintas con las dificultades de gestión que eso conlleva: gestionar las claves mediante su exportación a otras máquinas para la utilización de la misma clave resulta tedioso, complicado e inseguro.

Utilizar un único par de claves contenidas en el Directorio Activo supone transparencia al usuario y mayor seguridad de los propios datos al no encontrarse la clave secreta en la máquina en la que éstos se encuentran.

La emisión de los certificados desde la PKI a través del Directorio Activo también es bastante eficaz y se centraliza el tipo de certificados emitidos y las políticas de emisión y comprobación de estos.

La utilización de la PKI también permite emitir otros certificados para añadir más seguridad a la autentificación mediante la utilización de tarjetas inteligentes y la emisión de certificados para la firma y encriptación del correo electrónico, además de certificados para la simple autentificación de usuarios y máquinas pertenecientes al dominio.

Encriptación en Microsoft Office XP

Además de la posibilidad de firma digital que vimos anteriormente los archivos individuales de Word, PowerPoint y Excel pueden firmarse digitalmente, cifrarse o ambas cosas a través de la ficha Seguridad del cuadro de diálogo Opciones (la figura 9.46 muestra la ficha Seguridad de Word, pero las de las demás aplicaciones son similares).

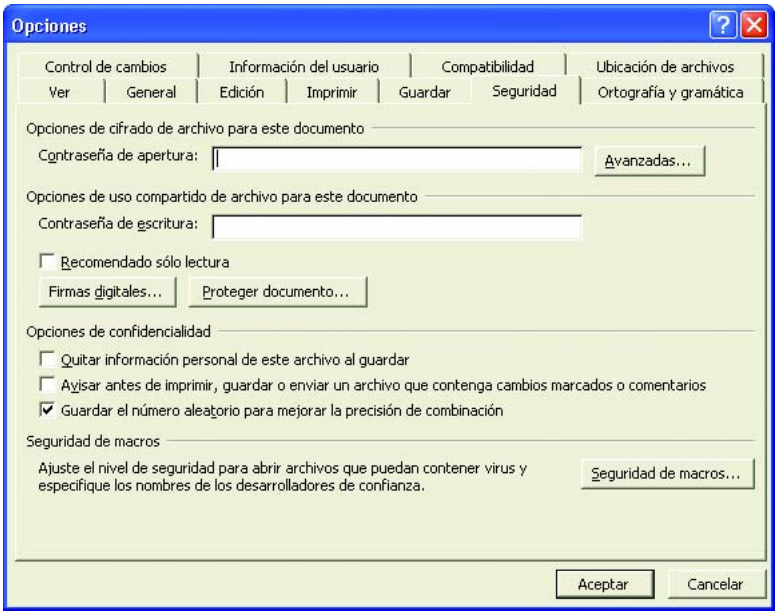


Figura 9.46. *Ficha de seguridad de Word.*

El botón Avanzada de la ficha Seguridad le permite elegir el proveedor de cifrado que desea utilizar para cifrar un documento en particular. Office puede utilizar cualquier proveedor CryptoAPI instalado en el sistema. Igualmente están disponibles los proveedores "Cifrado mínimo (OEX)" y "Compatible con Office 97/ 2000". También puede especificar la longitud de la clave en los tipos de proveedor que utilizan longitudes de clave variables (sin embargo, recuerde que las longitudes de clave disponibles varían en función del nivel de cifrado del sistema operativo subyacente). Los documentos cifrados con CryptoApi no pueden abrirse con versiones anteriores de Office.

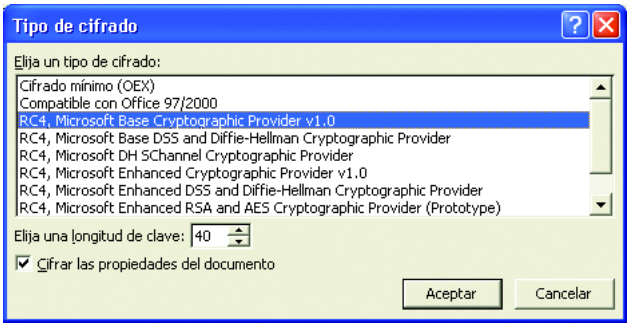


Figura 9.47. *Tipos de encriptación.*

Nota

Los archivos cifrados no se pueden indizar con Búsqueda rápida ni con la característica de búsqueda de SharePoint Team Services.

9.4.2 Artículo 24.1 Registro de accesos

"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."

Como vimos anteriormente la auditoría que ofrece Microsoft Windows 2000 y Microsoft Windows XP nos permite el registro detallado de eventos ocurridos en el sistema. Cumplir por tanto con lo exigido por la norma en este caso para archivos sensibles resulta sencillo en su aspecto mas operacional.

En primer lugar, en la política de grupo o local activamos la auditoría de objetos, tanto para los accesos autorizados como para los denegados. Esto lo realizamos en la subcarpeta Directiva de auditoría contenida en la carpeta Directivas locales como vemos en la figura 9.48.

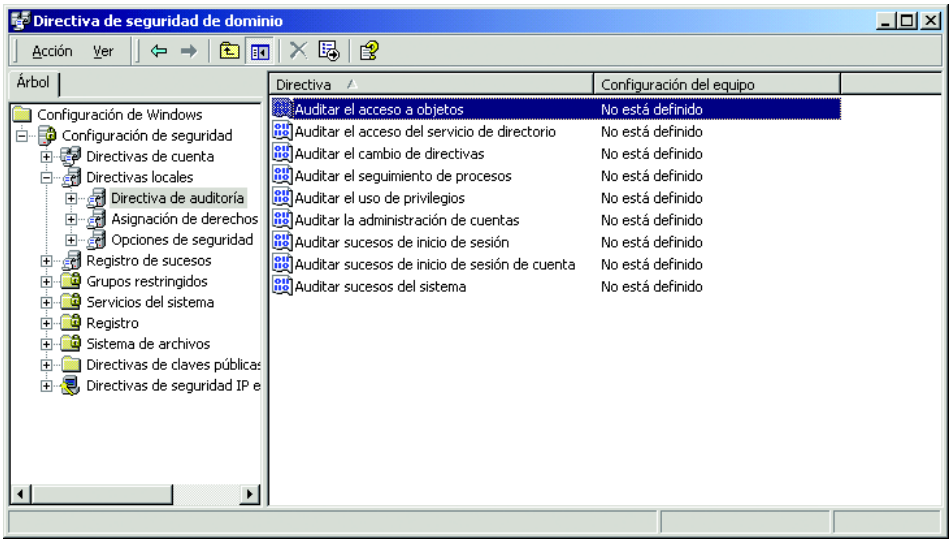


Figura 9.48. *Auditoría del acceso a objetos.*

Y haciendo doble clic se nos abrirá la ventana de la figura 9.49 donde señalaremos que vamos a auditar tanto los accesos autorizados como denegados activando las casillas Correcto y Error como podemos observar seguidamente.

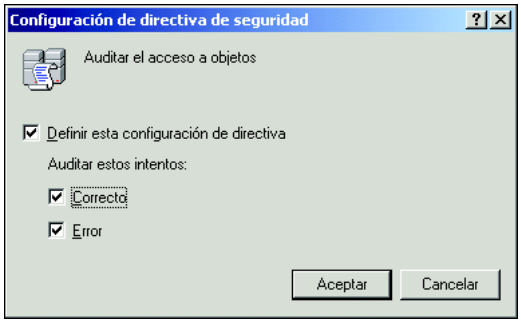


Figura 9.49. *Selección de los intentos a auditar.*

Realizado lo anterior nos desplazaremos con el explorador hacia la carpeta o fichero que por su nivel de protección debamos auditar y marcándolo con el botón derecho del ratón ejecutaremos el comando Propiedades y seleccionaremos la pestaña Seguridad (ver figura 9.50).

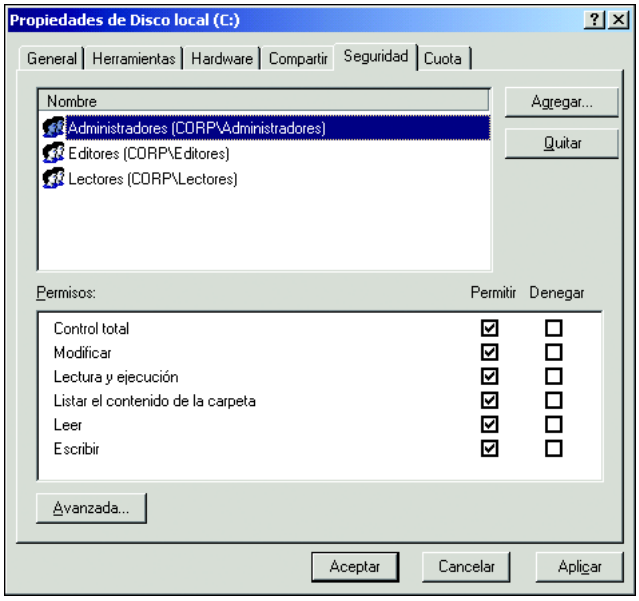


Figura 9.50. *Características de seguridad.*

En esta ventana pulsaremos el botón Avanzadas y en la ventana que nos aparece seleccionamos la pestaña Auditoría (ver figura 9.51).

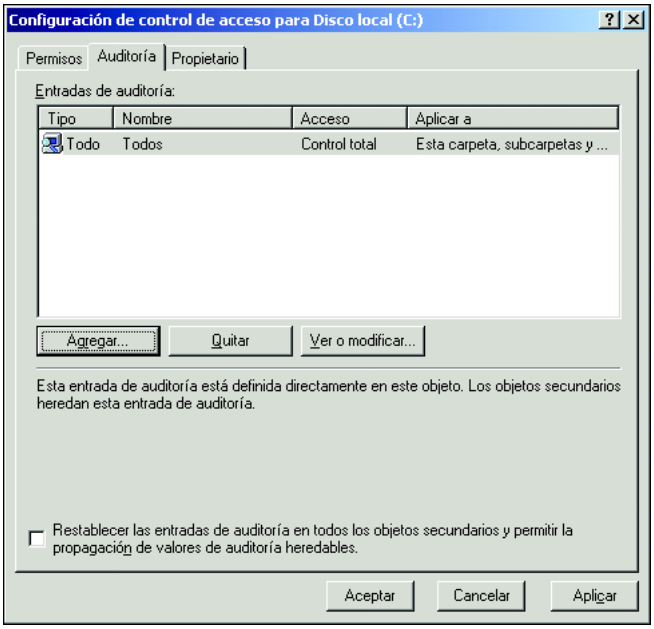


Figura 9.51. *Configuración de auditoría.*

En esta nueva ventana pulsaremos el botón Añadir y, en la nueva ventana, dado que debemos auditar cualquier tipo de acceso, introduciremos al grupo Todos y pulsaremos el botón Aceptar con lo que nos aparecerá la siguiente pantalla:

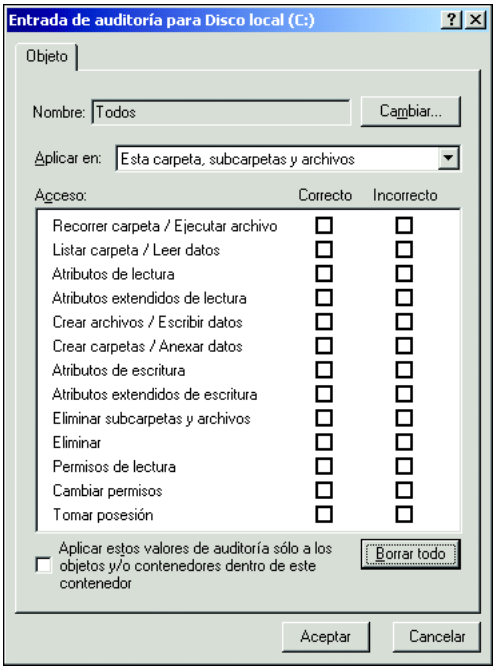


Figura 9.52. *Entrada de auditoría para datos.*

Como igualmente deberemos auditar cualquier tipo de acceso en la opción Control Total habilitaremos tanto la casilla de Éxito como la de Fallo y pulsaremos el botón Aceptar.

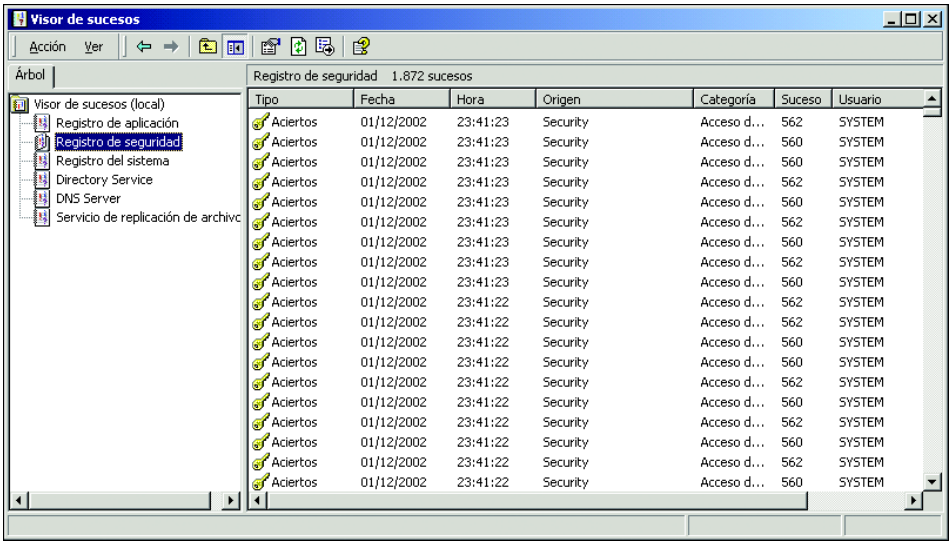


Figura 9.53. *Registro del visor de sucesos de seguridad.*

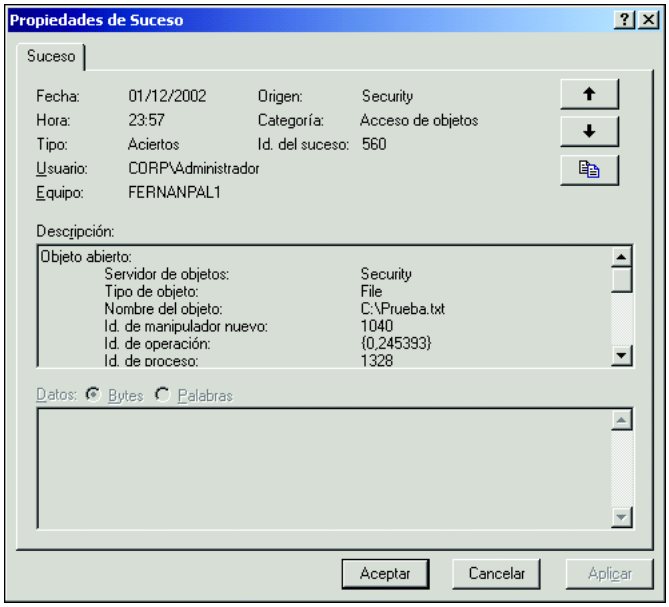


Figura 9.54. *Propiedades del suceso registrado.*

A partir de este momento cualquier tipo de acceso al objeto por parte de cualquier principal queda registrado en el Visor de sucesos de seguridad con los parámetros exigidos por la norma como podemos comprobar en la figura 9.53.

9.4.3 Artículo 24.2. Registro de accesos

> "*En caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.*"

Este artículo se enfoca hacia sistemas de bases de datos y no hacia ficheros planos. En este aspecto Microsoft SQL Server 2000 permite la auditoría de accesos mediante el servicio *SQL Profiler* que veremos más adelante.

9.4.4 Artículo 24.3. Responsable de los registros

> "*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.*"

Como vimos anteriormente, resulta recomendable proteger los archivos que almacenan los registros. En el caso de datos de nivel alto esta recomendación se eleva a la categoría de necesidad por lo que los derechos de acceso de esos archivos deberán estar limitados a los administradores de estos sucesos y al propio sistema con el privilegio mínimo para introducirlos. Para esto comprobaremos que el archivo de registro de seguridad, el cual se encuentra en %system%\system32\config\secevent.evt, limita el acceso únicamente a los responsables de seguridad y al sistema para la escritura de los eventos tal y como podemos comprobar en la figura 9.55.

Junto a lo anterior, para evitar la desactivación de los mismos, podemos señalar al sistema que se apague cuando el registro se encuentre lleno, como vimos anteriormente, o cuando por cualquier motivo el sistema no pueda grabar algún evento de seguridad. Para esto último en la subcarpeta *Opciones de Seguridad* de la carpeta Directivas locales habilitaremos la opción Apagar el sistema de inmediato si no se puede registrar auditorías de seguridad como vemos en la figura 9.56.

9.4.5 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.*"

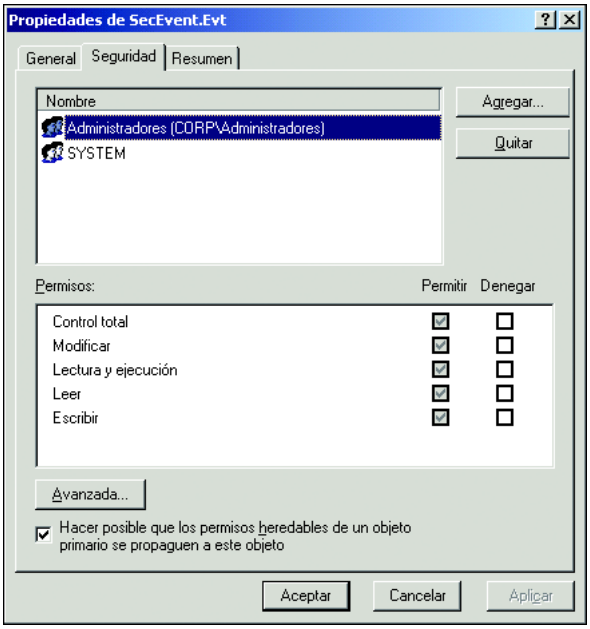


Figura 9.55. *Acceso al registro.*

Como ya vimos anteriormente, los sistemas de copia de respaldo compatibles con Microsoft Windows 2000 y Microsoft Windows XP, incluyendo la propia herramienta de realización de copias de respaldo que acompaña al sistema operativo, permite la realización de copias de respaldo de archivos cifrados mediante EFS manteniendo el cifrado.

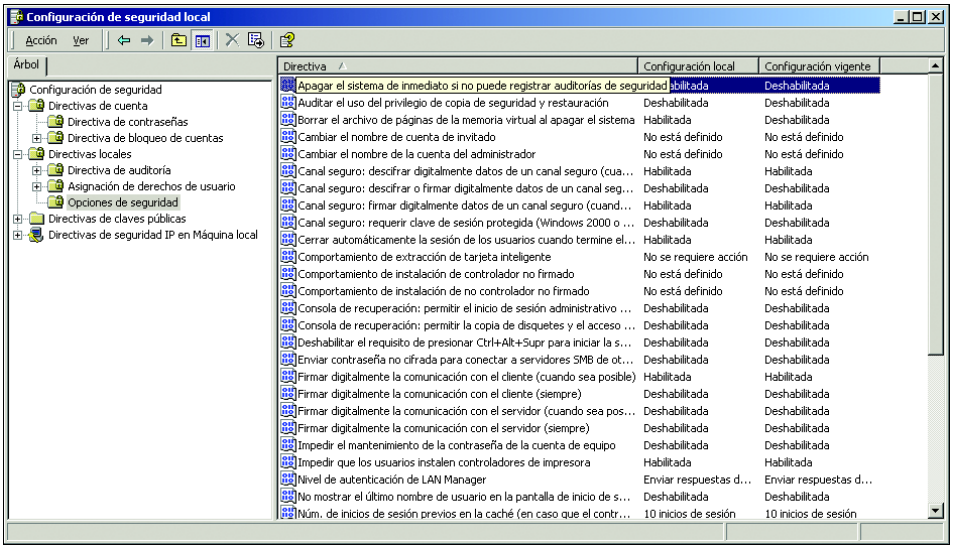


Figura 9.56. *Opción de desactivación del sistema si el registro no está activado.*

9.4.6 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.*"

Con los sistemas operativos Microsoft Windows 2000 y Microsoft Windows XP podemos responder a la exigencia de la norma no sólo en el ámbito de las telecomunicaciones sino más allá en al ámbito de la comunicación local.

Para comunicaciones a través de Internet realizadas mediante correo electrónico podemos utilizar certificados generados por la propia PKI de Microsoft Windows 2000 o de terceros que cumplan la especificación S/MIME tanto utilizando Microsoft Outlook XP como Microsoft Outlook Express que acompaña al explorador Microsoft Internet Explorer.

Para comunicaciones punto a punto podemos utilizar el protocolo SSL para autentificarnos ante el servidor que contiene los ficheros y establecer un canal encriptado de transferencia.

Igualmente, podemos utilizar el estándar *IPSec* para el acceso a servicios de red, como Microsoft SQL Server 2000, que contengan datos sensibles. *IPSec* permite establecer sobre un adaptador de red políticas que autentifiquen y garanticen la integridad y verificabilidad de cualquier comunicación entre varios servidores, utilizando como método de autentificación tanto certificados como *Kerberos*, como método de encriptación del paquete algoritmos de la potencia de DES y 3DES y como método de integridad los algoritmos SHA1 o MD5.

La política *IPSec* puede ser gestionada a nivel centralizado como una política más de dominio mediante las políticas de grupo y también su despliegue se beneficia de la gestión integrada de certificados que ofrece la PKI de Microsoft Windows 2000 (ver figura 9.57).

IPSec también lo podemos utilizar directamente con ordenadores conectados a Internet tanto para el establecimiento de conexiones punto a punto como para el establecimiento de conexiones que creen un túnel que pueda conectarnos dos redes propias a través de Internet con la seguridad que nos ofrecen las tecnologías de encriptación e integridad señaladas.

Para el usuario que accede remotamente a las instalaciones Microsoft Windows 2000 y Microsoft Windows XP ofrecen además de PPTP, el protocolo estándar L2TP sobre *IPSec* que, además de las ventajas que nos ofrece *IPSec*,

nos permite el establecimiento de accesos a la red y la autentificación del usuario incluso mediante el uso de certificados y tarjetas inteligentes (ver figura 9.58).

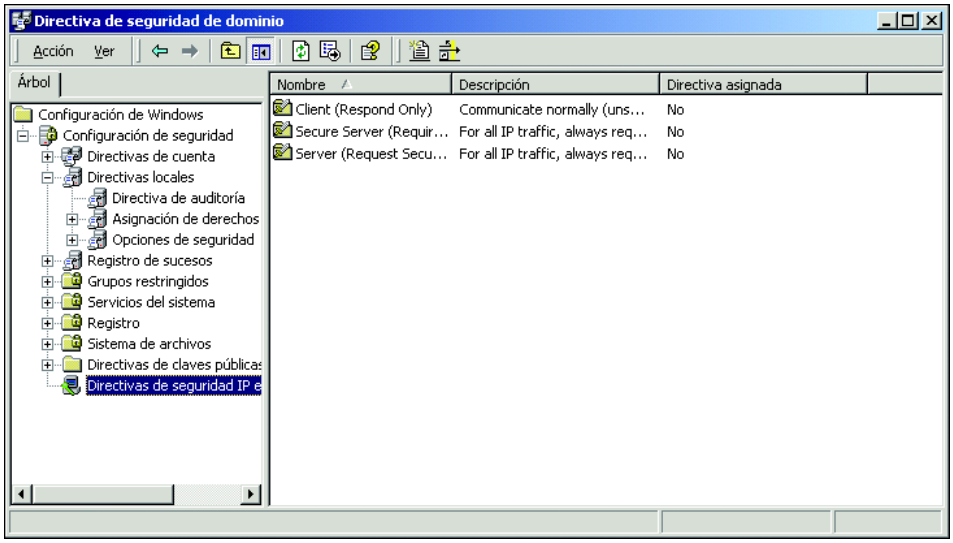


Figura 9.57. *Gestión integrada de la seguridad con Directorio Activo.*

Respecto a las cada vez más importantes comunicaciones inalámbricas, Microsoft Windows XP ofrece soporte total del protocolo estándar IEEE 802.1x con autentificación EAP/TLS que permite el control de acceso a la red y la comunicación cifrada con gestión dinámica de claves.

Figura 9.58. *Utilización de certificados personales.*

Telecomunicaciones en Microsoft SQL Server 2000

Además del uso de las capacidades anteriormente descritas, Microsoft SQL Server 2000 también permite la encriptación de las telecomunicaciones entre servidor y cliente mediante la opción comunicación Multiprotocolo. Para ello en la utilidad de red de cliente simplemente tendremos que marcar la casilla Force protocol encryption y, a partir de este momento, todas las comunicaciones entre el cliente y el servidor utilizarán para comunicarse el protocolo SSL.

Microsoft Outlook XP y correo electrónico

El cada vez mayor uso del correo electrónico, y la transferencia de datos sensibles en él, requieren también una respuesta de encriptación. Microsoft Outlook asegura este nivel mediante:

- La encriptación de la conexión MAPI desde Outlook 2002 al servidor de Exchange.
- La firma y encriptación de mensajes mediante S/MIME.

Microsoft Exchange 2000 dispone de una característica de seguridad integrada que permite el cifrado de 128 bits de la comunicación RPC. Las conexiones MAPI se realizan a través de RPC por lo que puede aprovechar esta característica para aumentar la seguridad de la conexión desde el cliente de Microsoft Outlook XP al servidor de Microsoft Exchange. El cifrado RPC sólo cifra los datos del cliente MAPI al servidor de Exchange, no cifra los mensajes en si.

Microsoft Outlook 2002 permite firmar y encriptar mensajes para entregarlos a destinatarios internos o externos. Para este cifrado necesita un certificado. Si desea enviar correo electrónico cifrado o firmado a destinatarios de Internet, necesita utilizar un certificado reconocido (conocido como id. digital) de un tercero.

Cuando tenga el certificado instalado en el cliente, puede comenzar a enviar mensajes firmados y cifrados mediante S/MIME. Sólo se puede enviar correo cifrado a otros usuarios si tiene acceso a su clave pública. Para ello, haga que el otro usuario le envíe un mensaje firmado y, después, agregue ese usuario a su lista de contactos. Ahora ya dispone de su clave pública.

Si desea que los usuarios de su organización de Exchange se envíen mensajes firmados y cifrados de forma habitual, considere la posibilidad de utilizar el servicio de administración de claves incluido en Microsoft Exchange 2000. Este servicio utiliza los servicios de PKI de Microsoft Windows 2000 y proporciona acceso a las claves públicas y acceso seguro y centralizado a las claves

privadas. De esta manera, el cliente tiene acceso sin problemas a los mensajes firmados y cifrados y puede enviar estos mensajes a cualquier otro destinatario de la lista global de direcciones que tenga la seguridad habilitada.

10

Política de Seguridad

La necesidad de definir una política de seguridad es algo absolutamente indiscutible. Las actuaciones voluntaristas de un departamento IT en materia de seguridad siempre estarán lejos de conseguir muchos de los objetivos que nos marcamos en esa visión multidimensional del problema. Ni la tecnología es el único problema, ni evidentemente es la única solución.

El cumplimiento de la LOPD representa un indiscutible impulsor del sector de la seguridad en España. Aprovechar la necesidad legal de su cumplimiento para extender el alcance de las iniciativas tomadas hacia una política de seguridad general mas allá del estricto dato personal, es una decisión tomada por numerosas empresas.

Resultará interesante hablar de qué pasos podemos dar para conseguir una correcta política de seguridad.

Existen numerosos procedimientos que determinan la calidad de un sistema en este aspecto, BS 19977, ISO, recientes normas AENOR, etc. Cuyos aspectos están fuera del alcance de este capítulo. Sin embargo, todos aquellos responsables de poner en marcha una política de seguridad saben de la dificultad innata a la tarea de ajustar una iniciativa como ésta a la idiosincrasia de la empresa.

Desde el momento en el que una política de seguridad afecta a toda la compañía, a todos y cada uno de sus departamentos, ya sabemos que nos enfrentamos a una tarea compleja cuyo éxito depende en gran medida del compromiso de los implicados en su definición fundamentalmente, pero de toda la compañía en general.

Sin pretender dar un recetario, exponemos unos puntos de reflexión extraídos de experiencias de profesionales de la seguridad, y que recogen algunas de las dificultades y métodos para la definición inicial de una política de seguridad y acercarnos a ese compromiso deseado de la compañía. Son puntos muy prácticos que arrojan algo de luz sobre los pasos previos necesarios a dar en su definición.

Establecemos cinco fases fundamentales con objetivos muy definidos, aunque sólo comentaremos las tres primeras por ser las más orientadas a dar esos primeros pasos organizativos iniciales.

- Fase 1.- Organización y Análisis.
- Fase 2.- Desarrollo de un estudio sobre las necesidades de privacidad.
- Fase 3.- Evaluar las necesidades tecnológicas para la protección de la privacidad
- Fase 4.- Desarrollo de la política y planes.
- Fase 5.- Implementación del plan.

Fase 1: Organización y Análisis

Esta fase supone la puesta en marcha de la iniciativa y requiere una toma de datos básica así como estructurar un grupo de trabajo capaz de ponerla en marcha. Podemos definir nueve puntos a tener en cuenta en esta fase:

Desarrollo de una filosofía general de privacidad

Es decir, establecer un equilibrio de consenso entre las perspectivas de bajo y alto riesgo. Es decir, entre una perspectiva de bajo riesgo en la que una política de seguridad está en marcha, la diseminación de información está fuertemente controlada, las políticas se establecen por tipo de dato, todas las salidas de información fuera de la empresa necesitan ser previamente aprobadas, etc.; o una perspectiva de alto riesgo en la que políticas no severas están en marcha, la información se controla débilmente, existen políticas globales poco específicas y se permite a las unidades de negocio y departamentos el tomar sus propias decisiones sobre el uso de la información. Ambos extremos delimitan una filosofía de privacidad llena de grises. Definir a priori la filosofía más cercana a nuestras necesidades es muy conveniente y complicado pues, dentro de la misma compañía, existirán departamentos más decididos por una política de bajo riesgo, mientras otros abogarán por una de alto riesgo.

Responsable de Privacidad

Los más elevados niveles de la dirección deben apoyar los planes de privacidad ante toda la compañía. Es un indicador de la importancia que este

asunto tiene para la compañía. Aunque el apoyo es fundamental, no es lo más recomendable que este nivel esté involucrado en el día a día del desarrollo del plan de seguridad. Simplemente por no ser lo más efectivo. Un director de nivel medio es más adecuado para coordinar la tarea. La persona encargada deberá dedicar gran parte de su tiempo a esta tarea que, en ocasiones, requerirá una dedicación total. Debe mantener una buena relación con todos los departamentos de la empresa y con los recursos externos.

Creación del Grupo de Trabajo de Privacidad (Privacity Task Force)

Es necesario crear un Grupo de Trabajo interdepartamental liderado por el responsable de privacidad y con representación de todos los departamentos de la compañía (dos por departamento, uno principal y otro suplente). El mejor posible roll del CEO sería asegurarse que la Task Force de seguridad obtiene los recursos, participación y cooperación necesaria para este desempeño. La función del CEO en este sentido es la de dejar constancia de la importancia del grupo en todos sus reportes directos, así como dar el apoyo necesario para situar la importancia de la tarea asignada al grupo creado.

Organización a nivel departamental

Cada departamento deberá tener su propio equipo de privacidad que desarrolle los trabajos de investigación, evaluación o implementación, liderados por su representante en la Task Force. Debería contituirse con niveles de supervisión y técnicos.

Evaluación de la capacidad del Grupo de Trabajo

Es necesario evaluar las capacidades y conocimientos del grupo de trabajo, formación, experiencia en asuntos relacionados con la privacidad, etc. Igualmente, es una tarea a desarrollar por cada miembro del grupo de trabajo en su grupo departamental. Identificar correctamente esto permitirá identificar necesidades de formación y/o contratación de ayuda externa (legal, consultoría, etc.). El objetivo es cubrir las carencias detectadas en el apartado anterior.

Establecer el calendario de trabajo

Será imprescindible desarrollar una agenda de reuniones periódicas desde el primer momento, con objetivos concretos. Una reunión de frecuencia fija será necesaria, además de las que el proceder vaya marcando. Serán necesarias para formar subcomités, identificar responsabilidades, asignar tareas interdepartamentales, etc. Los grupos departamentales, deberán reunirse con la frecuencia necesaria para respetar las agendas y compromisos de la Task Force global.

Campaña de concienciación

La iniciativa necesita ser apoyada y conocida por toda la compañía. Los distintos grupos de trabajo tendrán escaso éxito sin el apoyo y conocimiento de todos los empleados. Se deben utilizar todos los medios de comunicación interna: newsletters, intranets, reuniones, marketing interno, etc.; así como plantear planes de formación al respecto para las nuevas incorporaciones y para los empleados.

Establecer el escenario para el inicio del estudio de necesidades de privacidad

Notificar a los empleados el tipo de información que será necesaria recoger en el inicio del estudio (a acometer en la siguiente fase).

Fase 2: Desarrollo de un estudio sobre necesidades de privacidad

La compañía debe comenzar a conocer los diferentes tipos de datos e información que almacena y utiliza. Esta fase ayuda a la compañía a identificar esos datos, determinar su origen, establecer cómo deben ser utilizados, identificar de qué forma y cómo se diseminan. Además, este proceso ha de identificar aquellas leyes y regulaciones gubernamentales y requerimientos internos que pueden gobernar la forma en la que se recogen y difunden esos datos.

Establecer un sistema de inventario de datos

Apoyarse en una base de datos es una herramienta útil para almacenar la información recogida. Probablemente, los campos indicados constituyan una buena base de partida para la construcción de dicha base. El inventario ha de ser lo más profundo posible. Ninguna compañía debería tener una falsa percepción de seguridad como fruto de un inventario de datos incompleto. Es muy común leer en el periódico un caso concreto sobre problemas de privacidad de un determinado tipo de datos y prematuramente concluir con que no somos vulnerables. Los campos de esta base de datos bien podrían ser: descripción del dato, departamento responsable, fuente, sistema donde reside, donde residen copias en papel, cómo y dónde se utilizan internamente, cómo y dónde se distribuyen, política existente sobre el uso de datos, leyes al respecto del uso de esos datos, incidentes previos respecto a su uso, notas del grupo de seguridad sobre esos datos, etc.

Puesta en marca del proceso de inventario

Son muchas las fuentes de datos que hay que considerar. Cada departamento debe determinar que tipo de datos recoge, crea o utiliza. El grupo departamental debe proporcionar esta información al grupo de seguridad. Las compañías no deben presuponer que el departamento de IT conoce todos los datos utilizados por

los demás departamentos o unidades de negocio. Los almacenes de datos surgen "como setas" en las compañías. Por ejemplo, ficheros de los usuarios, ficheros de los proveedores, del canal de partners, registros desde el web site, registros de empleados, ficheros de I+D, ficheros de suscripción para newsletter corporativas, etc. En cualquier caso, las compañías deben ser muy realistas en este aspecto ya que todos los departamentos y unidades de negocio se sienten como propietarios absolutos de esos datos. Hay una barrera cultural al cambio. Existe una tendencia observada en el tiempo a no cooperar totalmente con las iniciativas de ámbito global. La mejor herramienta para conseguir esa profundidad en el análisis de los datos puede que no sea enviar un formulario enorme a cada supervisor para que sea completado, sino una aproximación más de concienciación en la que tanto supervisores clave como expertos técnicos son encuestados sobre cómo son manejados los datos.

Tres puntos de la estrategia global puesta en marcha pueden ayudar a vencer resistencias:

1. Campaña de información interna sobre la importancia de la privacidad, realizada en la fase anterior, proporcionando al empleado una forma de dar feedback sobre vulnerabilidades potenciales de la privacidad.

2. Comenzar el proceso formal de inventario de datos.

3. Crear y distribuir una encuesta a los empleados clave para recoger sus inputs sobre la vulneración de la privacidad.

La compañía puede triangular estas tres fuentes de información y obtener valiosa información mientras construye el inventario de datos.

Existencia de políticas previas

¿Existe ya alguna política previa asociada a determinado tipo de dato? ¿Incluso cuando no se haya identificado como política? Si existe, es el momento de recogerla, ya esté escrita o no, para su posterior análisis por el grupo de seguridad. Este proceso debe examinar si las políticas existentes no contradicen las nuevas. No se deben cambiar las existentes si se adaptan bien a las nuevas.

Leyes actuales. LOPD

¿Existe una normativa especial que gobierne el manejo de los datos que manejamos? La asesoría legal es un aspecto muy importante para evitar posibles malas interpretaciones o acciones incorrectas en lo que respecta a la normativa existente.

Asesoría y cobertura de seguros

Se deben estudiar las ofertas de compañías de seguros en materia de coberturas por interrupción de actividad y/o violación de privacidad. Las grandes compañías suelen tener un departamento de análisis de riesgos, bajo cuyo paraguas caería la responsabilidad de evaluar los riesgos y las coberturas de los seguros asociados.

Identificar problemas de privacidad pasados y presentes

Desafortunadamente, muchas compañías no comienzan a tomarse en serio la seguridad hasta que existe algún incidente. El grupo de trabajo debe ser informado sobre cómo se actuó en este sentido. El mayor obstáculo se presenta cuando se recurre a la "memoria institucional" y vemos que los implicados en el problema ya no están en la compañía o que la memoria tiende a ser muy selectiva.

Revisar políticas de seguridad y problemas de los partners de negocio

¿ Podríamos ser vulnerables por las prácticas de nuestros proveedores, canal, etc.? Estos partners de negocio deben ser informados de la puesta en marcha del plan. El mayor obstáculo es conseguir su cooperación, la que dependerá en gran medida del número de partners y la capacidad de influencia en sus procesos.

Chequear reputación entre organismos jurídicos especializados

Las compañías deberían contactar directamente con organizaciones jurídicas o no jurídicas pero con algún interés existente en indagar en la privacidad con la que tratamos nuestros datos, y chequear si han encontrado algún problema. De paso aprovechar para informar sobre el desarrollo de un nuevo plan de privacidad.

Consolidación de resultados y clasificación de datos

Una vez recogida toda la información, es la hora de consolidar en informes todo lo correspondiente a esta fase, con especial atención a la clasificación de los datos recogidos en base a criterios de sensibilidad e importancia de su privacidad. A partir de esto, puede comenzarse a adelantar un borrador sobre la política de seguridad y procedimiento en el manejo de ese tipo de datos.

Como resultado de esta fase, deberíamos tener muy claro el inventariado de datos y su clasificación según su sensibilidad e importancia, así como toda la normativa legal que les afecta.

En este apartado, un subcomité del grupo de seguridad debería iniciar la siguiente fase, en estrecha colaboración con el departamento de IT o un consultor externo de tecnologías de la información, para llevar a cabo una evaluación de la tecnología que puede ayudar a mantener el nivel de privacidad deseado.

Fase 3: Evaluar las necesidades tecnológicas para la protección de la privacidad

Es necesario evaluar las capacidades existentes en la empresa para operar e implantar la tecnología necesaria para asegurar la privacidad de la información corporativa. Esta evaluación requiere un detenido análisis de tecnologías, personal de seguridad, fondos para seguridad y planes de seguridad. Este estudio debería ser llevado a cabo por un subcomité de la Task Force, en trabajo conjunto con el departamento IT y, si fuera necesario, contar con una consultoría externa.

Las funciones de este subcomité irían orientadas a:

- Asesorar a la Task Force sobre aspectos tecnológicos.
- Preparar reuniones sobre problemas tecnológicos específicos.
- Educar a la Task Force sobre el potencial y limitaciones de la tecnología.
- Examinar las capacidades en materia de seguridad en las tecnologías de la información.
- Revisar problemas tecnológicos derivados de las necesidades de privacidad detectadas en la fase anterior.
- Revisar los procedimientos y planes de seguridad de la información existentes.
- Testear la seguridad de la tecnología de la información.
- Ayudar en las pruebas sobre las debilidades existentes en los procedimientos en torno a la privacidad.

Las tecnologías sobre las que tenemos que reflexionar en cada uno de los aspectos necesarios se pueden perfectamente clasificar en:

1. Tecnologías para la protección de la información almacenada en sistemas.
2. Tecnología para la protección de los datos en tránsito.
3. Tecnología para la protección de las comunicaciones de voz.
4. Tecnologías para la proteccion física de las copias de información.
5. Tecnología para el cumplimiento de las especificaciones de “Puerto Seguro” (Safe Harbor)

En este punto resulta fundamental conocer lo que la tecnología nos ofrece y seleccionar los elementos que nos permitan afrontar cada uno de estos aspectos.

Microsoft es el fabricante de software que más soluciones de seguridad aporta a sus productos. El objetivo es la "democratización" del acceso a la seguridad, que la seguridad no se convierta en algo inalcanzable . En el gráfico de la figura 10.1 mostramos algunas de las tecnologías que los productos de Microsoft incorporan y de que forma resuelven muchos de los aspectos contemplados.

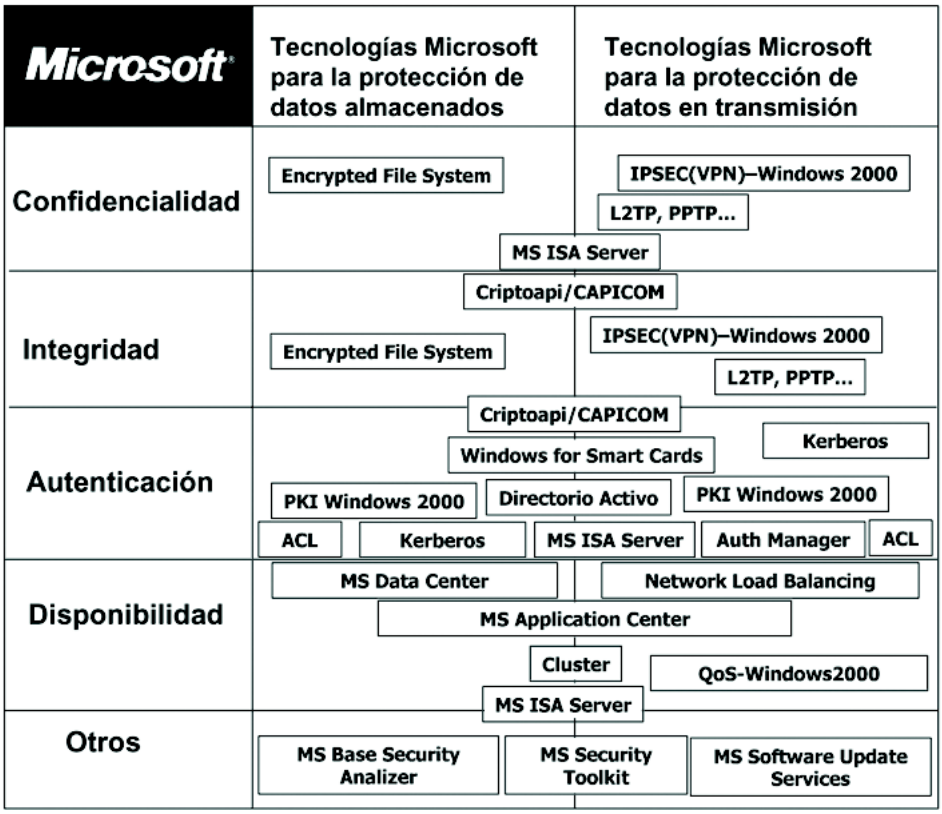


Figura 10.1. *Algunas de las tecnologías de seguridad integradas en la plataforma Microsoft.*

En cualquier caso, es IMPRESCINDIBLE que el subcomité tecnológico de la Task Force revise las capacidades, conocimientos y certificaciones de todo el staff responsable de la gestión de la red y control de los productos de software, y recomendar formación adicional si fuera necesario. En términos tecnológicos, los sistemas se constituyen tan seguros como los conocimientos de las personas que los operan. No caigamos en el repetido error de dar la operación de determinados sistemas a personas inexpertas o sin la debida formación. Todos los sistemas requieren ser operados por personal cualificado y certificado. No descuidemos este aspecto que la experiencia nos enseña ya que puede ser fuente de posteriores problemas o vulnerabilidades en la integridad del sistema.

Anexos

ANEXO I: Plan de Adaptación al Reglamento de Medidas de Seguridad de los Ficheros Automatizados que Contengan Datos de Carácter Personal de IPS Certification Authority S.L. (ipsCA)

Introducción al PAR

El Plan de Adaptación al Reglamento (PAR) facilita la adaptación de las bases de datos de las empresas al Reglamento de medidas de seguridad en vigor desde el día 26 de Junio de 1999, en el que se indica que todos los ficheros automatizados que contengan datos de carácter personal deben tener determinadas medidas que garanticen la seguridad de los mismos.

El objetivo del PAR es poder realizar la adaptación al Reglamento de forma sencilla y ágil, para ello, el PAR se compone de cinco fases: análisis, elaboración, implementación, formación y auditoría.

Fase I: Análisis de seguridad

En la fase de análisis de seguridad se procede a analizar los ficheros que contienen datos de carácter personal protegidos por el Reglamento y se establece el grado de cumplimiento del Reglamento por parte de la Organización.

En el Análisis de Seguridad del PAR se comprueba si se cumplen las exigencias del Reglamento para cada fichero automatizado y se realizan los siguientes puntos:

- Determinación de los ficheros que deben estar protegidos según el Reglamento.
- Comprobación de que los ficheros se encuentran registrados en la Agencia de Protección de Datos.
- Definición de los niveles de seguridad requeridos para cada fichero según el Reglamento.
- Comprobación de la seguridad de cada uno de los ficheros automatizados en los accesos a través de las redes de comunicación.
- Comprobación de la seguridad de los datos fuera del lugar de ubicación física del fichero.
- Comprobación la seguridad de los ficheros en el lugar de la ubicación física.

- Comprobación del establecimiento de un responsable de los ficheros automatizados con datos de carácter personal.
- Comprobación de la existencia de un registro de incidencias.
- Comprobación de la existencia de un listado actualizado de usuarios con acceso a la información restringida.
- Comprobación de la existencia de mecanismos de identificación y autenticación.
- Comprobación de la existencia de listados de usuarios, claves y renovación.
- Comprobación de la existencia de métodos de inventariado y clasificación de los soportes informáticos, en donde se almacenan los datos con acceso restringido.
- Comprobación de 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.
- Comprobación de la existencia de un calendario de realización de copias de seguridad.

Además, para el nivel de seguridad medio y el nivel de seguridad alto, se realizará lo siguiente:

- Comprobación de la existencia de un calendario de controles periódicos para verificar el cumplimiento de la propia normativa y medidas a adoptar en caso de desechar o reutilizar un soporte.
- Comprobación de la existencia de auditorías de seguridad cada dos años como mínimo.
- Comprobación de la existencia de mecanismos que identifiquen a cualquier usuario que acceda a datos restringidos y que comprueben su autorización para ello.
- Comprobación de la existencia de mecanismos que limiten los accesos reiterados y no autorizados a los datos restringidos.
- Comprobación de la existencia de un control de acceso físico a los locales donde se encuentren los datos a proteger.
- Comprobación de que los mecanismos de gestión de entrada y salida de soportes informáticos cumplen los requisitos del presente Reglamento.
- Comprobación de que los procedimientos de recuperación de datos son autorizados por la persona responsable del fichero y se encuentran documentados.

Y además para el nivel de seguridad alto, se realizará:

- Comprobación de que son cifrados los datos antes de la distribución y transporte de los soportes que los contengan.
- Comprobación de la existencia de un registro de accesos a la información, donde conste al menos la identificación del usuario, fecha y hora, fichero accedido y si ha sido denegado o aceptado, con un "log" de al menos 2 años.
- Comprobación de la realización de un informe de este registro al menos una vez al mes.
- Comprobación de que la conservación de las copias de seguridad se realiza en lugares diferentes al de los equipos informáticos.
- Comprobación de que la transmisión de datos se realiza mediante cifrado de dichos datos o por cualquier otro mecanismo que garantice la integridad de los mismos.

Al finalizar el análisis de seguridad se realizará un informe en el que se deberán detallar todos los puntos analizados y el grado de cumplimiento del reglamento.

Fase II: Elaboración de la normativa de seguridad

En la segunda fase del PAR se elabora un documento de obligado cumplimiento para el personal con acceso a los ficheros automatizados de carácter personal y a los sistemas de información.

El documento resultante contendrá como mínimo los siguientes aspectos:

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

- Planificación de los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento.
- Definición de las medidas que son necesarias adoptar cuando un soporte vaya a ser desechado o reutilizado.
- Definición de las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y a los sistemas de información.

Fase III: Implementación de la normativa de seguridad

En la tercera fase del PAR, se procede, con la colaboración de los responsables de seguridad y de ficheros, a implementar la normativa de seguridad de la organización, elaborada en la fase anterior:

- Configuración de las aplicaciones para que cumplan los requisitos especificados en el presente Reglamento.
- Implementación de las modificaciones técnicas y organizativas que fueran necesarias para cumplir la normativa de seguridad.

Fase IV: Formación a los responsables de seguridad y de los ficheros

En la cuarta fase del PAR, se procede a realizar la formación de los responsables de los ficheros automatizados y de los responsables de seguridad.

La formación a realizar consta de los siguientes puntos:

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

Fase V: Auditoría de seguridad

La última fase del PAR (auditoría de seguridad) sólo es de obligado cumplimiento, según el Reglamento, para el nivel medio y el nivel alto de seguridad.

Estas auditorías son obligatorias cada dos años.

En la auditoría de seguridad se hace una evaluación del cumplimiento de la LOPD y del Reglamento, según los siguientes puntos:

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

ANEXO II: Ley Orgánica de Protección de Datos

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 las Fuerzas 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.

5. 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 MARÍAAZNAR LÓPEZ

ANEXO III: 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 de 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.

CAPITULO 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 incidencias.

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

Articulo 9. Funciones y obligaciones del persona.
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 en 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 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 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 del fichero se encargará de verificar la definición y correcta aplicación de los procedimientos de realización de copias de respaldo y de recuperación de 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, slavo que en dicho periodo no se hubiera producido ninguna actualización de los datos.

CAPITULO III

Medidas de seguridad de nivel medio

Artículo 15. Documento de seguridad.
El documento de seguridad deberá contener, además de lo dispuesto en el articulo 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.

Articulo 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 de fichero de acuerdo con este Reglamento.

Articulo 17. Auditoría.
1. Los sistemas de información e instalaciones de tratamiento de datos se someterán a una auditoria 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 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.

Articulo 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.

Articulo 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.

CAPITULO 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 los 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 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 periodo 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.

CAPITULO 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 511992:

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.

ANEXO IV: Recursos, fuentes y documentación sobre Seguridad

Direcciones de Interés

Para más información sobre los temas que se tratan en este libro, les sugerimos que visiten las siguientes direcciones:

- www.microsoft.com/spain/seguridad
- www.agenciaprotecciondatos.org.
- www.delitosinformaticos.com
- www.ips.es
- www.ipsca.com
- www.madrid.org/cmadrid/apdcm
- www.microsoft.com/spain
- www.microsoft.com/spain/technet
- www.microsoft.com/technet
- www.microsoft.com/security
- www.microsoft.com/spain/mspress

Fuentes

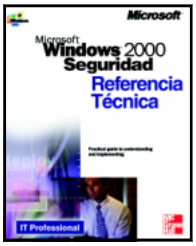
Para la realización de este libro se han consultado las siguientes fuentes:

- "Memoria 2001". Agencia de Protección de Datos. Madrid, 2002.
- "Memoria 2000". Agencia de Protección de Datos. Madrid, 2001.
- "Premio Protección de Datos Personales IV Edición: Regulación Jurídica de los tratamientos de datos personales realizados por el sector privado en Internet". María de los Reyes Corripio Gil-Delgado y Agencia de Protección de Datos. Madrid, 2000.
- "LORTAD. Reglamento de Seguridad". Emilio del Peso Navarro y Miguel Ángel Ramos González. Ed. Díaz de Santos, S.A. Madrid,1999.

- "Jornadas sobre el derecho español de la protección de datos personales". Agencia de Protección de Datos. Madrid, 1996.
- Net Privacy: A Guide to Developing & Implementing an Ironclad ebusiness Privacy Plan by Michael Erbschloe, John R. Vacca

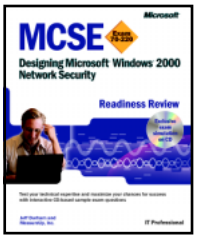
Documentación sobre seguridad

Microsoft Press publica una amplia gama de títulos sobre tecnologías Microsoft. En este apartado encontrará la documentación disponible sobre seguridad tanto en castellano como en inglés.



Título: Microsoft Windows 2000 Seguridad. Referencia Técnica
ISBN: 84-481-3023-5
Autor: Internet Security Systems, Inc.
648 págs.

Este título explora el tipo de decisiones que hay que tomar al encontrarnos ante el dilema de proporcionar una seguridad a toda prueba y el máximo de eficiencia en el lugar de trabajo. Le ayudará a decidir el nivel de seguridad que necesita y también a utilizar Windows 2000 para configurar y mantener esa seguridad.



Título: MCSE Designing Microsoft Windows 2000 Network Security Readiness Review; Exam 70-220
ISBN: 0-7356-1365-6
Autor: Jeff Durham and MeasureUp, Inc.
320 págs.
Incluye 1 CD-ROM

Pruebe si ya está listo para el examen MCP 70-220 al responder a preguntas de práctica generadas al azar en la herramienta de simulación de examen basada en CD. El texto que lo acompaña ofrece explicaciones útiles para todas las preguntas y respuestas además de sugerencias adicionales para preparar el examen.

Título: MCSE Training Kit: Designing Microsoft Windows 2000 Network Security
ISBN: 0-7356-1134-3
Autor: Microsoft Corporation
864 págs.
Incluye 2 CD-ROM

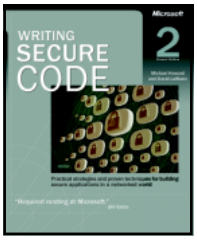
Este kit reúne toda la información acerca de cómo diseñar soluciones de seguridad en la red en Windows 2000. Incluye conceptos y aplicaciones prácticas como tutoriales, casos prácticos y herramientas, que le ayudarán a preparar el examen 70-220.

Título: MCSE Training Kit: Microsoft Internet Security and Acceleration Server 2000; Exam 70-227
ISBN: 0-7356-1347-8
Autor: Microsoft Corporation
656 págs.
Incluye 1 CD-ROM

Con este manual, los profesionales IT aprenderán cómo configurar y dar soporte con Microsoft Internet Security and Acceleration (ISA) para optimizar la seguridad y el rendimiento de la red. Los temas están preparados a la medida de los objetivos del examen 70-227, incluyendo la instalación, configuración y resolución de problemas.

Título: Seguridad de Microsoft Windows XP y Windows 2000 Running +
ISBN: 84-481-3807-4
Autor: Ed Bott; Carl Siechert
800 págs.
Incluye 1 CD-ROM
Disponible: Febrero 2003

¡Lleve su experiencia en seguridad de Windows al siguiente nivel! Esta referencia sumamente bien organizada incluye cientos de soluciones que ahorran tiempo, sugerencias para localizar fallas, además de soluciones útiles en un formato conciso de respuestas rápidas. El CD incluye herramientas, demos, un eBook, y mucho más.

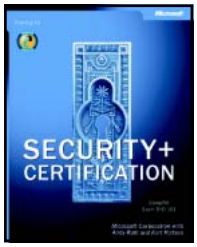


Título: Writing Secure Code, Second Edition
ISBN: 0-7356-1722-8
Autor: Michael Howard y David LeBlanc
800 págs.

Mantenga a los hackers a raya con las sugerencias y técnicas que ofrece este libro, entretenido a la vez de revelador. Los desarrolladores aprenderán a poner candados a sus aplicaciones a lo largo de todo el proceso de desarrollo, desde diseñar aplicaciones seguras hasta escribir código robusto que puede resistir los ataques, e incluso probar las aplicaciones en busca de cualquier fallo de seguridad.

Título: Building Secure Microsoft ASP.NET Applications
ISBN: 0-7356-1890-9
Autor: Microsoft Corporation
624 págs.
Disponible: Febrero 2003

Esta guía ofrece un práctico escenario de aproximación para diseñar y construir aplicaciones seguras con ASP.NET, centrándose en la autentificación, Autorización y comunicación segura entre los niveles de distribución de las aplicaciones Microsoft .NET.

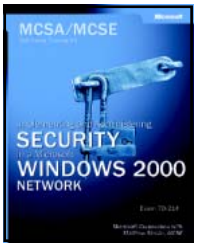


Título: Security+ Certification Training Kit
ISBN: 0-7356-1822-4
Autor: Microsoft Corporation; Andy Ruth; Kurt Hudson
512 págs.
Incluye 1 CD-ROM
Disponible: Febrero 2003

Este completo manual ofrece la información tanto para preparar el nuevo examen de certificación de Security+, con sus metas y objetivos, como soluciones fundamentales de seguridad que pueden surgir en el trabajo; contiene lecciones y ejercicios prácticos incluidos en el CD-ROM, además de una versión electrónica del manual.

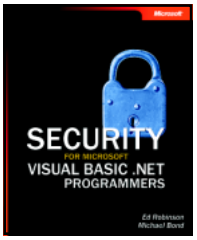
Título: Secure Messaging with Microsoft Exchange Server 2000
ISBN: 0-73561876-3
Autor: Paul Robichaux
432 págs.
Disponible: Febrero 2003

Los virus informáticos y los mensajes no solicitados generan un gasto enorme a las empresas todos los años. Este manual ofrece la información crítica que los administradores, arquitectos de seguridad y diseñadores de correo que trabajan con Microsoft Exchange necesitan para combatir estos mensajes infectados y correos basura.



Título: MCSA/MCSE Self-Paced Training Kit: Implementing and Administering Security in a Microsoft Windows 2000 Network, Exam 70-214
ISBN: 0-7356-1878-X
Autor: Microsoft Corporation y Matthew Strebe
704 págs.
Incluye 2 CD-ROM
Disponible: Febrero 2003

Aprenda como manejar y organizar la seguridad para una infraestructura del sistema Windows 2000 y poder preparar y superar el examen 70-214, examen opcional de la certificación MCSA/MCSE.

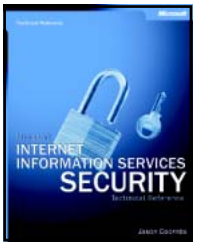


Security for Microsoft Visual Basic .NET Programmers
ISBN: 0-7356-1919-0
Autor: Ed Robinson and Michael Bond
400 págs.
Disponible: Abril 2003

Este manual simplifica el aprendizaje al incluir explicaciones concisas de los términos clave en seguridad, problemas y jerga de los desarrolladores que trabajan con Visual Basic. Podrán aprender como configurar herramientas de seguridad, características de seguridad añadidas, etc.

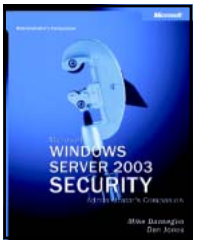
Kit de Recursos de seguridad
ISBN: 84-481-3808-2
Autor: Ben Smith y Elliot Lewis
1.100 págs.
Incluye 1 CD-ROM
Disponible: Julio 2003

El manual de seguridad fundamental que los administradores de sistema Windows necesitan para implantar la seguridad de sistemas operativos Microsoft Windows, servidores, clientes, servicios de intranet y servicios de internet; incluye la mejor información facilitada por el equipo de seguridad de Microsoft.



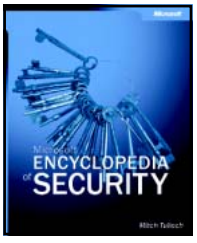
Microsoft Internet Information Services Security Technical Reference
ISBN: 0-7356-1572-1
Autor: Jason Coombs
400 págs.
Disponible: Abril 2003

Este libro enseña a los desarrolladores y administradores como evitar errores de seguridad y conocer tanto las vulnerabilidades de seguridad de Internet Information Services (IIS) como las mejores técnicas de seguridad IIS en el mundo real.



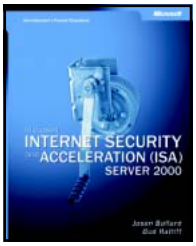
Microsoft Windows Server 2003 Security Administrator's Companion
ISBN: 0-7356-1574-8
Autor: Mike Danseglio and Don Jones
500 págs.
Incluye CD-ROM
Disponible: Abril 2003, Castellano Diciembre 2003

Con este libro los profesionales IT aprenderán como usar las poderosas características de seguridad en los últimos sistemas operativos para servidores web, incluyendo las mejores prácticas y detalles técnicos para alcanzar la máxima seguridad con Windows Server 2003.



Microsoft Encyclopedia of Security
ISBN: 0-7356-1877-1
Autor: Mitch Tulloch
800 págs.
Disponible: Junio 2003

Más de 2000 entradas con temas y problemas al detalle de la seguridad hoy en día, de la A a la Z. Esta es la referencia definitiva que cubre tanto la plataforma Microsoft Windows como otras plataformas, tecnologías y productos más vendidos incluyendo Sun y Cisco.



Microsoft Internet Security and Acceleration (ISA) Server 2000
Administrator's Pocket Consultant
ISBN: 0-7356-1442-3
Autor: Jason Ballard y Bud Ratliff
400 págs.
Disponible: Junio 2003

Ésta es una guía totalmente práctica, de bolsillo, dirigida a los profesionales IT que necesitan distribuir conectividad segura en Internet, facilitándoles detalles esenciales para usar la nueva generación de Microsoft Internet Security and Acceleration (ISA) Server.

Distribuye y comercializa:
McGraw-Hill Interamericana de España.
profesional@mcgraw-hill.com