novática
CEPIS UPGRADE Revista de la Asociación de Técnicos de Informática

Novática, revista fundada en 1975 y decana de la prensa informática española, es el órgano oficial de expresión y formación continua de **ATI** (Asociación de Técnicos de Informática), organización que edita también la revista **REICIS** (Revista Española de Innovación, Calidad e Ingeniería del Software). ***Novática*** co-edita asimismo **UP**GRADE, revista digital de **CEPIS** (*Council of European Professional Informatics Societies*), en lengua inglesa, y es miembro fundador de **UP**ENET (***UP****GRADE* **E***uropean* **NET***work*).

<http://www.ati.es/novatica/>
<http://www.ati.es/reicis/>
<http://www.cepis.org/upgrade>

ATI es miembro fundador de **CEPIS** (*Council of European Professional Informatics Societies*) y es representante de España en **IFIP** (*International Federation for Information Processing*); tiene un acuerdo de colaboración con **ACM** (*Association for Computing Machinery*), así como acuerdos de vinculación o colaboración con **AdaSpain**, **AI2**, **ASTIC**, **RITSI** e **Hispalinux**, junto a la que participa en **ProInnova**.

Coordinación Editorial, Redacción Central y Redacción ATI Madrid
Padilla 66, 3º, dcha., 28006 Madrid
Tlfn.914029391; fax.913093685 <novatica@ati.es>
Composición, Edición y Redacción ATI Valencia
Av. del Reino de Valencia 23, 46005 Valencia
Tlfn./fax 963330392 <secreval@ati.es>
Administración y Redacción ATI Cataluña
Via Laietana 46, ppal. 1ª. 08003 Barcelona
Tlfn.934125235; fax 934127713 <secregen@ati.es>
Redacción ATI Aragón
Lagasca 9, 3-B. 50006 Zaragoza.
Tlfn./fax 976235181 <secreara@ati.es>
Redacción ATI Andalucía <secreand@ati.es>
Redacción ATI Galicia <secregal@ati.es>
Suscripción y Ventas <http://www.ati.es/novatica/interes.html>, ATI Cataluña, ATI Madrid
Publicidad
Padilla 66, 3º, dcha., 28006 Madrid
Tlnf.914029391; fax.913093685 <novatica@ati.es>
Imprenta: Derra S.A., Juan de Austria 66, 08005 Barcelona.
Depósito legal: B 15.154-1975 -- ISSN: 0211-2124; CODEN NOVAEC
Portada: Resolución en marcha - Concha Arias Pérez / © ATI
Diseño: Fernando Agresta / © ATI 2003

Nº 211, mayo-junio 2011, año XXXVII

sumario

editorial
El papel de las TIC en los movimientos sociales > 02

en resumen
Inteligencia de negocios en clave de presente > 02
Llorenç Pagés Casas

Noticias de IFIP
Reunión del TC-1 (*Foundations of Computer Science*) > 03
Michael Hinchey,Karin Breitman, Joaquim Gabarró
Reunión anual del TC-10 (*Computer Systems Technology*) > 04
Juan Carlos López López

Actividades de ATI
V Edición del Premio *Novática* > 05

monografía
Business Intelligence
(En colaboración con **UP**GRADE)
Editor invitado: Jorge Fernández González
Presentación. *Business Intelligence*: analizando datos para extraer nueva información y tomar mejores decisiones > 06
Jorge Fernández González
***Business Information Visualization:* Representación de la información empresarial** > 08
Josep Lluís Cano Giner
***BI Usability*: evolución y tendencia** > 16
R. Dario Bernabeu, Mariano A. García Mattío
Factores críticos de éxito de un proyecto de *Business Intelligence* > 20
Jorge Fernández González, Enric Mayol Sarroca
Modelos de construcción de *Data Warehouses* > 26
José María Arce Argos
***Data Governance*: ¿qué?, ¿cómo?, ¿por qué?** > 30
Óscar Alonso Llombart
***Business Intelligence* y pensamiento sistémico** > 35
Carlos Luis Gómez
Caso de estudio: Estrategia BI en una ONG > 39
Diego Arenas Contreras

secciones técnicas

Arquitecturas
Extensiones al núcleo de Linux para reducir los efectos del envejecimiento del software > 43
Ariel Sabiguero, Andrés Aguirre, Fabricio González, Daniel Pedraja, Agustín Van Rompaey

Derecho y tecnologías
La protección de datos personales en el desarrollo de software > 50
Edmundo Sáez Peña

Enseñanza Universitaria de la Informática
Reorganización de las prácticas de compiladores para mejorar el aprendizaje de los estudiantes > 56
Jaime Urquiza Fuentes, Francisco J. Almeida Martínez, Antonio Pérez Carrasco

Estándares Web
Especificación y prueba de requisitos de recuperabilidad en transacciones WS-BusinessActivity > 61
Rubén Casado Tejedor, Javier Tuya González, Muhammad Younas
Referencias autorizadas > 70

sociedad de la información

Informática práctica
Criptoanálisis mediante algoritmos genéticos de una comunicación cifrada en la Guerra Civil > 71
Tomás F. Tornadijo Rodríguez

Programar es crear
El problema del decodificador (Competencia UTN-FRC 2010, problema C, enunciado) > 75
Julio Javier Castillo, Diego Javier Serrano
Triangulo de Pascal y la Potencia Binomial (Competencia UTN-FRC 2010, problema E, solución) > 76
Julio Javier Castillo, Diego Javier Serrano, Marina Elizabeth Cardenas

asuntos interiores

Coordinación editorial / Programación de Novática / Socios Institucionales > 77

Tema del próximo número: "*Innovación y emprendimiento en Informática*"

Edmundo Sáez Peña
Junta de Andalucía

<edmundo.saez@juntadeandalucia.es>

La protección de datos personales en el desarrollo de software

(Versión revisada para corregir errores de edición)

Resumen: *La Ley Orgánica de Protección de Datos de Carácter Personal y su Reglamento de desarrollo imponen una serie de restricciones y medidas de seguridad a los sistemas informáticos que traten datos personales de forma que el desarrollo de un sistema de estas características debe necesariamente observar dicha normativa. A lo largo de este artículo se realiza un análisis de las implicaciones que la normativa vigente en materia de protección de datos tiene en el desarrollo de software, así como de las medidas que dicho software debe implantar con objeto de cumplir con las exigencias legales.*

Palabras clave: *desarrollo de software, LOPD, protección de datos personales.*

1. Introducción

Una de las primeras etapas que se llevan a cabo durante el proceso de desarrollo de software es la que se conoce como análisis del sistema de información, donde se realiza, entre otras tareas, la definición detallada de los requisitos del sistema con el objetivo de obtener un catálogo de requisitos que permita definir con precisión el sistema que se pretende desarrollar. La participación de los usuarios en esta etapa es fundamental, pues sus especificaciones sobre lo que esperan que sea el comportamiento del sistema serán las que posteriormente guíen el proceso de desarrollo software.

Si bien los requisitos del sistema son, en muchos desarrollos, fijados únicamente por los usuarios en base a sus necesidades, en los sistemas que tratan datos de carácter personal los requerimientos de éstos tienen que ser considerados conjuntamente con las restricciones e imposiciones que exigen tanto la Ley Orgánica de Protección de Datos (LOPD) [1], como el Real Decreto que la desarrolla (RDLOPD) [2]. Por tanto, la libertad del cliente para decidir sobre la funcionalidad de su nuevo sistema encontrará en este caso ciertos límites.

Más aún, el RDLOPD incorpora una única disposición adicional sobre los productos de software, la cual estipula que deberá incorporarse, en la descripción técnica de los productos software destinados al tratamiento de datos de carácter personal, el nivel de seguridad, básico, medio o alto, descrito en dicha norma, que permitan alcanzar. Esto implica que, no sólo es necesario incorporar al sistema la funcionalidad necesaria para hacer cumplir con las medidas de seguridad del nivel al que vaya dirigido, sino que, además, debe quedar constancia en su descripción técnica de que el sistema permite el tratamiento de datos personales cumpliendo con las medidas de seguridad del nivel exigido impuestas por el RDLOPD. Así, en el caso de una hipotética sanción al responsable del fichero por parte de la Agencia Española de Protección de Datos (AEPD) [3], en la que se demostrara que la infracción cometida ha sido originada por un desarrollo software que no cumple con los preceptos legales en materia de protección de datos, éste podría actuar judicialmente contra quien hubiera desarrollado dicho sistema, dado que la descripción técnica del mismo establece que cumple con los requisitos necesarios para tratar datos personales a determinado nivel de seguridad. Por tanto, es imprescindible tener presente las implicaciones de la normativa vigente en materia de protección de datos personales a la hora de desarrollar un sistema de información.

Este artículo analiza dichas implicaciones y muestra como deben trasladarse al sistema de información. Para ello, realiza en primer lugar una descripción de los distintos niveles de seguridad en que se categorizan los ficheros que contienen datos personales. Seguidamente, analiza las implicaciones que las medidas de seguridad conllevan en el desarrollo de sistemas de información, en función de cada uno de los tres niveles de seguridad existentes. A continuación, se realizan otras consideraciones que deben tenerse en cuenta a la hora de diseñar un sistema de información, no derivadas directamente de las medidas de seguridad pero sí de otros aspectos de la normativa. Finalmente, se ofrecen unas breves conclusiones.

2. Niveles de seguridad

La protección de los datos de carácter personal en los sistemas informáticos viene garantizada a través de las medidas de seguridad impuestas por el RDLOPD. La aplicación de las medidas de seguridad se organiza en base al concepto de nivel de seguridad, de forma que se establecen tres niveles de seguridad: básico, medio y alto. A los ficheros con datos de carácter personal en una organización les corresponderá siempre uno de estos niveles de seguridad. A la hora de desarrollar un sistema de información es necesario tener claro qué tipo de datos van a manejarse y cuál es la finalidad de estos datos, pues en base a esta información al fichero resultante le corresponderá un determinado nivel de seguridad y, por tanto, el sistema software deberá incorporar las medidas de seguridad correspondientes. La **tabla 1** ofrece una relación de los niveles de seguridad que corresponden a cada fichero con datos personales en función de los datos que contiene y la finalidad de los mismos, y constituye una síntesis del artículo 81 del RDLOPD.

Una inspección detenida de la **tabla 1** refleja que, en principio, cualquier fichero con datos de carácter personal recibe la consideración de fichero de nivel básico, y por tanto le corresponde adoptar las medidas de seguridad propias de este nivel. Sin embargo, existen determinados tipos de datos que se consideran más sensibles y que, por tanto, merecen unas medidas de protección más elevadas.

En primer lugar, se encuentran aquellos datos que elevan el nivel de seguridad de un fichero hasta el nivel medio. Como puede verse, son numerosos los ficheros a los que les corresponde este nivel de seguridad, aunque generalmente su descripción en la tabla permite identificarlos con facilidad. Quizás el tipo de ficheros que pueden suscitar algún tipo de duda son aquellos que *"ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos"*. A este respecto, el Informe Jurídico 0590/2008 de la AEPD establece que se encuentran dentro de la categoría de este tipo de ficheros todos aquellos que contengan datos *"a partir de los cuales puedan deducirse los hábitos, preferencias, aficiones, actividades o posición económica de los afectados"*, o bien *"datos curriculares que incluyan información muy detallada sobre el sujeto que permitan deducir un perfil de estudios o de trabajador"*.

Y en segundo lugar, se encuentran aquellos ficheros a los que les corresponde el nivel de seguridad alto. Estos ficheros son aquellos que contienen datos que se denominan especialmente protegidos, recogidos en el artículo

Nivel básico	Nivel medio	Nivel alto
• Cualquier fichero con datos de carácter personal. • Fichero con datos de ideología, afiliación sindical, religión, creencias, salud, origen racial o vida sexual cuando 1. Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros. 2. Se trate de ficheros o tratamientos en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad. • Ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos.	• Ficheros relativos a la comisión de infracciones administrativas o penales. • Ficheros de prestación de servicios de solvencia patrimonial y crédito. • Ficheros de las Administraciones tributarias relacionados con el ejercicio de sus potestades tributarias. • Ficheros de las entidades financieras para las finalidades relacionadas con la prestación de servicios financieros. • Ficheros de las Entidades Gestoras y Servicios Comunes de la Seguridad Social relacionados con el ejercicio de sus competencias. • Ficheros de las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social relacionados con el ejercicio de sus competencias. • Ficheros que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos. • Ficheros de los operadores de comunicaciones electrónicas, respecto de los datos de tráfico y localización.	• Ficheros con datos sobre ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual, cuando no proceda adoptar el nivel básico. • Ficheros con datos recabados para fines policiales sin consentimiento de los afectados. • Ficheros con datos derivados de actos de violencia de género.

Tabla 1. Niveles de seguridad de los ficheros con datos de carácter personal.

7 de la LOPD. Se trata de datos especialmente sensibles, sobre los cuales hay que extremar el control pues su tratamiento no autorizado podría suponer perjuicios importantes a los afectados. Estos datos son los relativos a la ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual. Por tanto, en principio, cualquier fichero que incluyera datos de estas categorías debería considerarse un fichero de nivel alto. Aquí el problema suele aparecer cuando no está claro si un dato determinado se considera o no perteneciente a alguna de las categorías que lo convierten en dato especialmente protegido. En particular, los datos relativos a la salud suelen ofrecer bastante confusión, motivo por el cual el RDLOPD incluye una definición específica de datos de carácter personal relacionados con la salud, configurándolos como *"las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética"*. Aún así, son numerosos los informes jurídicos que la AEPD ha tenido que emitir para aclarar situaciones relacionadas con este tipo de datos, como por ej. el Informe Jurídico 0445/2009, que viene a establecer que los test psicotécnicos suponen el tratamiento de datos psicológicos, los cuales quedan encuadrados dentro de la categoría de datos de salud, o como el Informe Jurídico 0129/2005, que concluye que el mero hecho de ser o no fumador no puede considerarse dato relativo a la salud, pues *"debería considerarse dato directamente vinculado con la salud aquel que reflejase, en relación con las sustancias estupefacientes en general, su mero consumo. Sin embargo, en el caso del consumo de alcohol o tabaco el dato referido al mero consumo, sin especificación de la cantidad consumida, no sería en principio un dato vinculado con la salud, revistiendo tal naturaleza el dato que reflejase la cantidad consumida, en caso de que el mismo significase un consumo abusivo"*.

No son los datos de salud los únicos que presentan esta problemática, aunque sí los que la presentan más frecuentemente. Sin embargo, otros tipos de datos como la profesión pueden convertirse en datos especialmente protegidos en determinadas circunstancias, como la que analiza el Informe Jurídico 0044/2004 de la AEPD en la que un fichero que contiene el dato de profesión es susceptible de revelar, en algún momento, las creencias de una persona, como ocurriría en el caso de que alguien desempeñara la profesión de sacerdote. El citado informe, concluye que *"en caso de que los datos (…) puedan revelar la ideología, afiliación sindical, religión o creencias de los afectados, los mismos tendrán en todo caso la condición de especialmente protegidos (…) Por todo ello, ha de concluirse que será precisa la implantación sobre los ficheros que contengan datos profesionales de los afectados entre los que pueda encontrarse el de sacerdote de las medidas de seguridad de nivel alto"*.

La interpretación del carácter de dato especialmente protegido puede resultar muy controvertida en algunas ocasiones, como la derivada del Informe Jurídico 0524/2009 de la AEPD, en el que se analiza el nivel de seguridad que procede aplicar a los ficheros que almacenan datos relacionados con la actividad de asesoramiento fiscal. Concretamente, establece que la decisión de un contribuyente de efectuar un aporte a la Iglesia Católica en su declaración de IRPF no revela necesariamente sus creencias, dado que *"la contribución puede traer causa de las relaciones personales o familiares del sujeto o de su conocimiento de la obra llevada a cabo por la Iglesia, denotando la marcación de la casilla únicamente la preferencia del contribuyente por una determinada obra social, sin que ello implique necesariamente que aquél profesa unas determinadas creencias"*. Aunque la conclusión más llamativa del informe es la relacionada con el dato que revela el matrimonio entre personas del mismo sexo, afirmando que *"si hasta la Ley 13/2005, de 1 de julio, por la que se modifica el Código Civil en materia de derecho a contraer matrimonio, los hechos relativos al matrimonio inscritos en el Registro Civil no se consideraban especialmente protegidos, la misma conclusión*

debe mantenerse con posterioridad a aquella. En consecuencia el tratamiento de este dato no requiere la adopción de medidas de seguridad de nivel alto".

Además de los datos especialmente protegidos, existen otros tipos de datos que también obligan a elevar el nivel de seguridad a alto para el fichero que los contenga, como son los datos recabados por las Fuerzas y Cuerpos de Seguridad para fines policiales sin consentimiento de los afectados, o aquéllos derivados de actos relacionados con la violencia de género, por el evidente riesgo que para la seguridad de las víctimas supondría su revelación no autorizada.

No obstante, el RDLOPD ha venido a rebajar el nivel de seguridad para los ficheros que contengan ciertos datos en determinadas circunstancias, con objeto de simplificar la gestión de la seguridad en determinados ficheros muy habituales en las organizaciones. Así, los ficheros que contengan datos especialmente protegidos se considerarán de nivel básico en dos circunstancias:
1. Cuando los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros. Éste es el caso de los ficheros de nóminas, en el que el dato de afiliación sindical se emplea, únicamente, para deducir al empleado el importe de la cuota sindical y transferir dicho importe al sindicato del que éste forma parte.

2. Cuando se trate de ficheros o tratamientos en los que, de forma incidental o accesoria, se contengan aquellos datos sin guardar relación con su finalidad. Éste es el caso de los ficheros de control de presencia, pues suelen ser ficheros mixtos que, en su parte automatizada, almacenan datos no especialmente protegidos sobre la ausencia de los trabajadores, pero que sin embargo, en la parte no automatizada, incluyen copias de los justificantes de ausencia que, en ocasiones, son partes de asistencia médica en los que se refleja la patología por la que el trabajador ha sido asistido.

Por otra parte, también se considerarán de nivel básico los ficheros que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos. Para clarificar este precepto, la AEPD ha dictado, entre otros, el Informe Jurídico 0179/2008, que establece que *"serán únicamente exigibles las medidas de seguridad de nivel básico en aquellos ficheros que contengan uno o varios de los siguientes datos:*
1. La mera indicación del grado o porcentaje de minusvalía del afectado o de los miembros de su unidad familiar a los efectos previstos para el cálculo de las retenciones en la legislación reguladora del Impuesto sobre la Renta de las Personas Físicas.
2. La indicación del dato "apto" o "no apto" de un trabajador a los efectos previstos en la Ley de Prevención de Riesgos Laborales.
3. Los datos relacionados con las obligaciones impuestas al empresario por la legislación vigente en materia de seguridad social que se limiten a señalar únicamente la existencia o no de enfermedad común, enfermedad profesional o accidente laboral o no laboral, así como la incapacidad laboral del trabajador".

3. Implicaciones de las medidas de seguridad

Las medidas de seguridad de implantación obligatoria en los sistemas que traten datos de carácter personal pretenden garantizar la confidencialidad, integridad y disponibilidad de éstos. Su aplicación se realiza en función del nivel de seguridad que corresponde al fichero, pero de forma acumulativa. Esto es, a un fichero de nivel básico corresponderá la aplicación de las medidas de seguridad de nivel básico, pero a un fichero de nivel medio corresponderá la aplicación de las medidas de nivel básico y de nivel medio. Finalmente, a los ficheros de nivel alto les corresponde la aplicación de las medidas de nivel básico, medio y alto. Por otra parte, las medidas de seguridad tienen la condición de mínimos exigibles, por lo que nada impide que se adopten medidas más rigurosas, siempre y cuando se garantice la adopción de las medidas exigidas en el RDLOPD.

Para la efectiva implantación de estas medidas es preciso que los sistemas de información que tratan datos de carácter personal hayan sido diseñados incorporando como requisitos, además de los propios de la aplicación, aquellos que permitirán el cumplimiento de las citadas medidas de seguridad. Si bien no todas las medidas de seguridad son susceptibles de ser aplicadas en el momento del desarrollo del sistema de información, algunas de ellas solo alcanzarán toda su efectividad mediante su consideración en esta fase.

A continuación, se relacionan las medidas cuya incorporación al sistema como requisito durante su desarrollo es necesario, o al menos recomendable. Las medidas se presentan organizadas en base al nivel de seguridad que corresponde.

3.1. Nivel básico

Las medidas de seguridad aplicables a los ficheros de nivel básico se relacionan en los artículos 89 a 94 del RDLOPD. En relación al control de acceso, es necesario tener en cuenta las siguientes consideraciones:
1. Los usuarios deberán poder acceder únicamente a los recursos necesarios para el desarrollo de sus funciones. Deberán establecerse mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados. Será preciso establecer perfiles en la aplicación de forma que cada usuario únicamente tenga acceso a aquella información que le vaya a ser necesaria para el desarrollo de sus funciones. Por ejemplo, los operadores del sistema informático de un hospital, que asignan citas médicas a los pacientes, no necesitan tener acceso a la historia clínica de éstos, a diferencia de los facultativos. Por ello, la aplicación debe estar diseñada de forma que a cada usuario le corresponda un perfil determinado, de manera que sea imposible el acceso a aquellos datos de carácter personal que no tengan relación con el perfil del puesto desempeñado.
2. Exclusivamente el personal autorizado podrá conceder, alterar o anular el acceso autorizado sobre los recursos. Deberán existir usuarios con el perfil de administradores que sean los únicos habilitados para modificar los permisos de acceso del resto de los usuarios. Los usuarios de la aplicación que no tengan este perfil no podrán modificar los accesos autorizados de los demás usuarios.
3. Deberá existir una relación actualizada de usuarios y perfiles de cada uno, así como de sus accesos autorizados. Se trata de una imposición de la normativa que, si bien puede ser perfectamente alcanzada al margen del propio sistema informático, facilitaría enormemente su cumplimiento por parte del responsable del fichero que la propia aplicación pudiera generar dicha relación, por lo que su inclusión como requisito es una opción a tener en cuenta.

En lo que respecta a la identificación y autenticación de los usuarios, deben considerarse los siguientes aspectos:
1. Se 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. Las cuentas genéricas están taxativamente prohibidas, dado que posibilitarían el acceso de una multiplicidad de personas al sistema sin que puedan quedar identificadas de forma inequívoca y personalizada. El Informe Jurídico 0021/2009 de la AEPD apunta en este sentido ante la consulta de si es posible la utilización de la misma cuenta por parte de varias personas para el acceso a datos personales en una Administración pública. La plena consecución de esta medida no es responsabilidad exclusiva de la aplicación, puesto que nada impide al administrador de la misma la creación de cuentas cuyas credenciales de acceso sean posteriormente distribuidas a varias personas. Sin embargo, sí es posible realizar un diseño del módulo de gestión de usuarios

que minimice en lo posible estas acciones. Por ejemplo, previo a la creación de un nuevo usuario en el sistema, podría mostrarse un mensaje indicando la prohibición de crear cuentas genéricas. Además, podría incluirse como dato asociado a la cuenta de usuario el nombre y apellidos de la persona que lo utilizará, de forma que fuera requisito indispensable completar esta información para tramitar el alta del nuevo usuario. Mención especial merece la cuenta de administrador del sistema, pues conceptualmente se trata de una cuenta genérica que, además, mantiene los máximos privilegios. Si bien no se tiene constancia de un dictamen jurídico a este respecto, parece evidente que una cuenta con tales características no debería ser permitida, pues a través de la misma se podría acceder a todos los datos del sistema sin que pudiera determinarse qué persona en concreto ha realizado el acceso. Por tanto, y salvo que se pudiera garantizar que en cada instante una y sólo una persona va a contar con las credenciales de administrador, lo recomendable sería no contar con cuentas de administración del sistema, sino con perfiles de administrador que fueran asignados a los usuarios individuales del sistema. De esa forma podrían existir varias cuentas de administrador, garantizando que en cada acceso al sistema el titular de la cuenta queda perfectamente identificado de forma inequívoca.

2. **Las contraseñas deberán ser cambiadas con una periodicidad no superior a un año**. Deberá existir un mecanismo en el sistema que informe al usuario de que su contraseña está próxima a caducar, impidiéndole el acceso una vez que haya transcurrido más de un año sin que la contraseña haya sido cambiada.

3. **Las contraseñas se almacenarán de forma ininteligible** . El procedimiento de almacenamiento de las contraseñas debe garantizar que no sea posible, de ninguna manera, la recuperación de éstas. Para conseguirlo, el procedimiento más sencillo es el cifrado de las mismas con algún algoritmo que no permita reconstruir la contraseña original, como MD5 o SHA-1. De esta forma se consigue que ningún atacante que consiguiera tener acceso a las contraseñas cifradas pudiera descifrarlas para suplantar posteriormente a los usuarios mediante la utilización de sus credenciales.

4. **Existirá un procedimiento de asignación, distribución y almacenamiento de contraseñas que garantice su confidencialidad e integridad**. Se deberá garantizar que sólo el usuario conoce su contraseña de acceso al sistema. Para ello, es recomendable que la aplicación ofrezca al usuario la posibilidad de cambiar su contraseña, sin que sea necesaria la intervención de ningún administrador u operador. Más aún, puesto que la primera contraseña de un usuario en el sistema suele ser fijada por el administrador, sería conveniente dotar al sistema de la posibilidad de forzar al usuario el cambio de contraseña en el primer acceso al sistema.

Finalmente, las medidas de seguridad de nivel básico contemplan actuaciones en materia de copias de respaldo. Sería interesante considerar la siguiente:

1. **Deberá realizarse una copia de respaldo semanal como mínimo, salvo que en dicho periodo no se hubiera producido ninguna actualización de los datos**. Por lo general, para alcanzar esta medida de forma satisfactoria no es necesario plantearla durante el desarrollo del sistema de información. Lo habitual es disponer de una política de copia de seguridad global que se encargue de realizar la salvaguarda de toda la información corporativa. Sin embargo, es conveniente tener en cuenta esta medida para el caso en que se desarrolle un sistema de información para una organización en la que no exista definida una política de copia de seguridad previa. En este caso, podría incorporársele la funcionalidad consistente en la realización de una copia de seguridad semanal de los datos de forma automatizada, liberando así al administrador del sistema de la tarea de realizar la copia de seguridad manualmente cada semana, o de tener que definir y poner en marcha una política de copia de seguridad global para todos los activos de información, lo cual, por otra parte, sería lo recomendable.

3.2. Nivel medio

Las medidas de seguridad aplicables a los ficheros de nivel medio se relacionan en los artículos 95 a 100 del RDLOPD. La única consideración aplicable al desarrollo de sistemas de información que traten datos personales almacenados en ficheros de nivel medio está relacionada con la identificación y autenticación de los usuarios, y es la siguiente:

1. **Se establecerá un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información**. Deberá implementarse un mecanismo que, ante un número prefijado de intentos fallidos de acceso al sistema, bloquee la cuenta de usuario. Para el desbloqueo de la misma, el usuario deberá personarse ante el administrador del sistema, que comprobará su identidad y las causas que originaron el bloqueo.

3.3. Nivel alto

Las medidas de seguridad aplicables a los ficheros de nivel alto se relacionan en los artículos 101 a 104 del RDLOPD. El control de acceso en los sistemas de información que tratan datos personales almacenados en ficheros de nivel alto impone la siguiente consideración:

1. **Existirá un registro de acceso que almacenará, como mínimo, la identificación del usuario, la fecha y hora del acceso, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado. En caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido. El periodo mínimo de conservación de los datos registrados será de dos años**. Se trata de una medida que influye de manera significativa en el desarrollo del sistema de información, pues será preciso crear como estructura en la base de datos el registro de acceso como tal, y diseñar todas las transacciones del sistema que operen sobre datos personales de forma que dejen constancia de la operación realizada en el registro. En el caso de consultas masivas de información, teniendo en cuenta que deben almacenarse los datos que permitan identificar los registros accedidos, habrá que tener en cuenta el posible impacto sobre el rendimiento que pudiera tener esta medida.

En relación a las comunicaciones electrónicas, es preciso tener en cuenta lo siguiente:

1. **La transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos, o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros**. Esta exigencia viene a imponer el uso de protocolos cifrados (como puede ser HTTPS en el caso de aplicaciones web) para las aplicaciones que transmitan datos a través de redes inseguras. La elección del mecanismo de cifrado no es tema baladí, como se desprende del Informe Jurídico 0494/2009 de la AEPD, que establece que *"no sólo es necesario cifrar, sino cifrar de forma que la información no sea inteligible ni manipulada por terceros. Sin esta última condición, no se cumplirá lo estipulado en el citado artículo 104. Esto implica (...) que el sistema de cifrado a emplear no esté comprometido, es decir, que no se conozca forma de romperlo. (...) tanto el cifrado que ofrecen los productos que generan archivos PDF o el realizado por WinZip tienen vulnerabilidades conocidas y se disponen de herramientas de libre distribución que aprovechan dichas vulnerabilidades. Más concretamente, no sólo se pueden obtener en Internet fácilmente utilidades que rompen las protecciones de los archivos PDF o ZIP, sino que el propio algoritmo en el que descansa la cifra de documentos PDF, el algoritmo RC4, es manifiestamente vulnerable. Aunque para el uso particular pudieran considerarse adecuadas, no así para el intercambio de información con las garantías que se precisan en el Reglamento"*.

Finalmente, en relación con la gestión y distribución de soportes, es conveniente considerar las siguientes medidas:

1. La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte. Si el sistema de información ofrece la posibilidad de exportar datos para su almacenamiento en soportes, sería conveniente dotarlo de una opción que permita realizar la exportación de datos de forma cifrada, evitando así tener que efectuar un posterior procesamiento para el cifrado de dichos datos. En el proceso de cifrado deberá tenerse en cuenta lo anteriormente indicado por el Informe Jurídico 0494/2009 de la AEPD respecto a la seguridad del algoritmo de cifrado escogido. Es más, otorgando a la aplicación la funcionalidad de exportación cifrada de datos se elimina la posibilidad de que el responsable del fichero utilice mecanismos de cifrado inseguros.

2. Se cifrarán los datos que contengan los dispositivos portátiles cuando éstos se encuentren fuera de las instalaciones que están bajo control del responsable del fichero. Si se prevé que la aplicación y los datos personales que maneja pudieran ser instalados en un dispositivo portátil, sería una opción a tener en cuenta la creación de una versión de la misma que fuera capaz de trabajar con la base de datos cifrada, de forma que en caso de robo o pérdida del dispositivo no pudiera accederse a los datos. Al igual que el punto anterior, esta medida puede conseguirse fácilmente a posteriori, sin necesidad de incorporarla en el propio sistema de información. No obstante, es recomendable considerar su inclusión para evitar, nuevamente, que el responsable del fichero utilice mecanismos de cifrado inseguros del dispositivo portátil.

4. Otras consideraciones

Si bien las medidas de seguridad condicionan sensiblemente el desarrollo de un sistema de información, hay otros aspectos de la normativa que también tienen una influencia decisiva sobre el proceso de desarrollo. A continuación se analizan los más importantes.

4.1. Recogida de datos mediante formularios web

La LOPD exige, por norma general, el consentimiento inequívoco del afectado para el tratamiento de sus datos de carácter personal, salvo en una serie de excepciones que se encuentran reguladas en el artículo 6.2 de la norma. El consentimiento deberá ser libre (obtenido sin intervención de vicio alguno del consentimiento), específico (referido a una determinada operación de tratamiento y para una finalidad determinada, explícita y legítima del responsable del fichero), informado (el usuario debe conocer, antes de su tratamiento, la existencia y las finalidades para las que se recogen los datos) e inequívoco (debe existir expresamente una acción u omisión que implique la existencia del consentimiento; no se admite el consentimiento presunto). El artículo 5 de la LOPD es el que establece la información que ha de facilitarse al afectado para que el consentimiento se pueda considerar informado y, por tanto, válido.

Cuando el propio afectado facilita sus datos personales a una aplicación web a través de un formulario deben tenerse en cuenta las consideraciones del Informe Jurídico 0093/2008 de la AEPD, que establece lo siguiente: *"En cuanto al consentimiento informado, éste habrá de recabarse de tal forma que resulte imposible la introducción de dato alguno sin que previamente el afectado haya conocido la advertencia que contenga las menciones a las que nos hemos referido, pudiendo servir como prueba del consentimiento la acreditación de que el programa impide introducir los datos sin antes haber aceptado el aviso legal al que hemos hecho referencia. Todo ello tiene por objeto asegurar que el consentimiento de los afectados sea efectivamente específico e inequívoco tal y como exige la Ley"*. Esto es, no será suficiente con mostrar una cláusula al pie del formulario informando al usuario de los preceptos que establece el artículo 5 de la LOPD y solicitando el consentimiento para el tratamiento de sus datos, sino que deberá articularse un mecanismo que impida al usuario la introducción de datos en el formulario hasta que éste haya aceptado expresamente que es consciente de que se van a recoger sus datos, a qué finalidad se van a destinar, los derechos que le amparan, y que consiente en el tratamiento.

4.2. Cancelación de datos

Es práctica habitual por parte de las organizaciones la conservación indefinida de los datos a modo de histórico o para la realización de estudios estadísticos o de mercado. Sin embargo, cuando estos datos son de carácter personal, esta política debe ser revisada, pues el mantenimiento de los mismos se encuentra regulado por la normativa de protección de datos. En particular, el artículo 4.5 de la LOPD establece que *"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"*. El concepto de cancelación se clarifica en el artículo 16.3 de la LOPD, que determina que *"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"*.

Por tanto, una vez que los datos hayan dejado de ser necesarios para la finalidad que originó su recogida, el sistema debe ofrecer la posibilidad de cancelarlos, lo que implica su bloqueo. El Informe Jurídico 0127/2006 de la AEPD viene a aclarar el significado del término bloqueo, de la siguiente forma: *"en cuanto al modo de llevar a cabo el bloqueo, deberá efectuarse de forma tal que no sea posible el acceso a los datos por parte del personal que tuviera habitualmente tal acceso, por ejemplo, el personal que preste sus servicios en el centro consultante, limitándose el acceso a una persona con la máxima responsabilidad y en virtud de la existencia de un requerimiento judicial o administrativo a tal efecto. De este modo, pese a permanecer el tratamiento de los datos, el acceso a los mismos quedaría enteramente restringido a las personas a las que se ha hecho referencia"*.

Es decir, el sistema debe estar dotado con una funcionalidad que permita la cancelación de datos mediante su bloqueo. De esta forma, únicamente aquellos usuarios que tengan asignado un perfil de máxima responsabilidad deberían poder acceder a los mismos, no siendo posible el acceso para el resto de usuarios que, hasta el momento de la cancelación, podían acceder a los datos sin más restricciones que las impuestas por las medidas de seguridad.

Asimismo, el sistema debe permitir la supresión definitiva de los datos una vez que el plazo de prescripción de las responsabilidades nacidas del tratamiento se haya cumplido. La determinación del citado plazo de prescripción es una cuestión puramente normativa, que queda fuera del ámbito de este trabajo. No obstante, y a modo de ejemplo, el citado Informe Jurídico 0127/2006 cita algunos de estos plazos: *"podría considerarse que el bloqueo habrá de efectuarse durante los plazos de prescripción de las acciones derivadas de la relación jurídica que funda el tratamiento, en los términos previstos por la legislación civil o mercantil que resulte de aplicación, así como el plazo de cuatro años de prescripción de las deudas tributarias, en cuanto los datos puedan revestir trascendencia desde el punto de vista tributario (habida cuenta de la obligación de conservación que impone el artículo 111 de la Ley General Tributaria y el plazo legal de prescripción de cuatro años previsto en el artículo 24 de la Ley de Derechos y Garantías de los Contribuyentes) (…) o el plazo de prescripción de tres años, previsto en el artículo 47.1 de la propia Ley Orgánica 15/1999 en relación con las conductas constitutivas de infracción muy grave"*.

En caso de que la organización desee conservar los datos una vez que hayan dejado de ser necesarios para la finalidad que motivó su recogida, y transcurrido el plazo de prescripción de las responsabilidades nacidas del tratamiento, sólo podrá conservarlos previa disociación de los mismos, salvo la excepción prevista en el artículo 9 del RDLOPD, consis-

tiendo el procedimiento de disociación en *"todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable"*.

4.3. Pruebas con datos reales

Una etapa de vital importancia en el desarrollo de software es la que corresponde a la realización de pruebas para verificar el correcto funcionamiento del sistema desarrollado. Los sistemas que gestionan datos de carácter personal no son distintos al resto de los sistemas, por lo que para garantizar la corrección de dichos sistemas antes de su puesta en producción es necesario realizar las pruebas pertinentes.

Sin embargo, la realización de pruebas en estos sistemas se encuentra limitada por el artículo 94.4 del RDLOPD, que establece que *"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 tratamiento realizado (…). Si está previsto realizar pruebas con datos reales deberá haberse realizado una copia de seguridad"*. Es decir, que en la realización de pruebas deberán emplearse datos ficticios preferentemente. Si las características del sistema desarrollado exigen la realización de pruebas con datos reales, la normativa impone, por una parte, que se asegure el nivel de seguridad correspondiente (acceso a los datos por parte del personal autorizado únicamente, transferencia cifrada de información en redes públicas, etc.), y, por otra parte, la realización de una copia de seguridad previa a la ejecución de las pruebas.

5. Conclusiones

La normativa de protección de datos de carácter personal ha venido a introducir una serie de consideraciones en el desarrollo de sistemas software, en forma de requisitos funcionales impuestos al sistema, o bien en forma de limitaciones a los requerimientos solicitados por los usuarios. En este artículo se ha efectuado una revisión de los distintos niveles de seguridad definidos en la norma, así como las implicaciones que sobre el desarrollo de sistemas de información que gestionan datos de carácter personal tienen las medidas de seguridad impuestas por dicha norma.

Si bien, la categorización del nivel de seguridad que corresponde a cada fichero está en principio bien definida en el RDLOPD, es necesario poner en común los preceptos de tal disposición con las aclaraciones e interpretaciones que la AEPD realiza, contribuyendo así a aclarar algunas dudas que pueden surgir fácilmente cuando se pretende poner en marcha un sistema para la gestión de datos personales.

Por otra parte, ha quedado establecido que para el cumplimiento de las medidas de seguridad impuestas por la normativa es necesario incorporar a los sistemas de información, desde su desarrollo, la funcionalidad que les permita alcanzar el nivel de seguridad al que están obligados. En función del nivel de seguridad, las medidas de seguridad a implantar supondrán un impacto mayor o menor para el sistema. En concreto, las medidas impuestas por el nivel de seguridad básico, consistentes principalmente en medidas para el control de acceso, identificación y autenticación de los usuarios, son, en buena parte, medidas que vienen aplicándose habitualmente en el desarrollo de nuevos sistemas de información, y que suponen un bajo impacto en el rendimiento del sistema. Sin embargo, las medidas impuestas por el nivel de seguridad alto, tales como el registro de accesos o el cifrado de la información en la transferencia a través de redes inseguras, pueden suponer un impacto mayor en el rendimiento, por lo que deben estudiarse con mayor detenimiento.

Finalmente, no sólo es necesario tener en cuenta las medidas de seguridad impuestas por el RDLOPD en el desarrollo de sistemas de información. La propia LOPD contiene preceptos que, para ser alcanzados, deben incorporarse a los sistemas durante su desarrollo, como los relativos a la obtención de datos personales desde formularios web o los que afectan a la cancelación de datos.

Sin duda, el conocimiento de la normativa en materia de protección de datos personales es un deber que todo aquel que asuma la responsabilidad sobre el desarrollo de un sistema de información para el tratamiento de datos personales debe tener presente, de cara a conseguir sistemas cuyo funcionamiento se adecue a las exigencias legales que afectan a este tipo de software.

Referencias

[1] BOE. *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Persona*, <http://www.boe.es/boe/dias/1999/12/14/pdfs/A43088-43099.pdf>.

[2] BOE. *Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal*, <http://www.boe.es/boe/dias/2008/01/19/pdfs/A04103-04136.pdf>.

[3] AEPD. Agencia Española de Protección de Datos, <http://www.agpd.es>.