Seguridad y protección de datos en las AA.PP.

La seguridad y protección de datos es una cuestión vital para el desarrollo de la Sociedad de la Información y para la consecución plena de la Administración electrónica. Organismos como los Ministerios de Administraciones Públicas o el de Trabajo y Asuntos Sociales son muy conscientes de ello. Mientras, las Agencias de Protección de Datos (estatal, madrileña, catalana y vasca), y las agencias de certificación, juegan un papel de primer orden. ***Por Javier Labiano.***


Francisco López Crespo.


Joseba García Celada.


José Luis Piñar.

LA seguridad de la información y de los sistemas que la manejan ocupa, cada vez con mayor prioridad, a responsables públicos y profesionales, de forma pareja a la trascendencia que la seguridad de las TIC tiene para que las organizaciones puedan cumplir su propia misión. A juicio del Jefe de Área de Sistemas Telemáticos del Ministerio de Administraciones Públicas, Francisco López Crespo, las actuaciones en este ámbito están teniendo reflejo en la regulación, en la creación de productos y servicios de utilidad común, y en políticas y acuerdos internacionales.

En nuestro país, se ha producido una serie de hitos importantes en relación con la seguridad de los sistemas de información y la protección de los datos. En concreto, a partir de 1992, con la Ley 30/1992 (de 26 de noviembre), de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, comenzó el impulso de la utilización por parte de las administraciones públicas de técnicas y medios electrónicos, informáticos y telemáticos en la actividad administrativa.

Ese mismo año, se reguló el tratamiento automatizado de los datos de carácter personal, a través de la Ley Orgánica 5/1992, derogada posteriormente por la ley de Protección de Datos de Carácter Personal (RD 994/1999).

El Consejo Superior de Informática ha impulsado la realización sistemática de análisis y gestión de riesgos de los sistemas de información.

En 1995, se creó el comité técnico del Consejo Superior de Informática de Seguridad de los Sistemas de Información y Protección de Datos Personalizados Automatizados (SSITAD), con el fin de preparar, elaborar, desarrollar y aplicar la política de seguridad de los sistemas de información y de seguridad de los datos en la Administración Pública. El SSITAD produce recomendaciones y promueve y desarrolla proyectos de interés general. Entre otros asuntos, produce la metodología de análisis y gestión de riesgos MAGERIT y elabora los Criterios de Seguridad, Normalización y Conservación, previstos por el Real Decreto 263/1996, de 16 de febrero, de utilización de los medios electrónicos, informáticos y telemáticos por la AGE. Asimismo, la Ley 66/1997, de 30 de diciembre, de Medidas fiscales, administrativas y del orden social, en su artículo 81, habilita a la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda para la prestación de los servicios técnicos y administrativos necesarios para garantizar la seguridad, validez y eficacia de las comunicaciones de las administraciones públicas y de los organismos públicos, a través de técnicas y medios electrónicos, informáticos y telemáticos. A raíz de esta disposición, se desarrolló el Proyecto de Certificación Electrónica Española (CERES).

Iniciativas

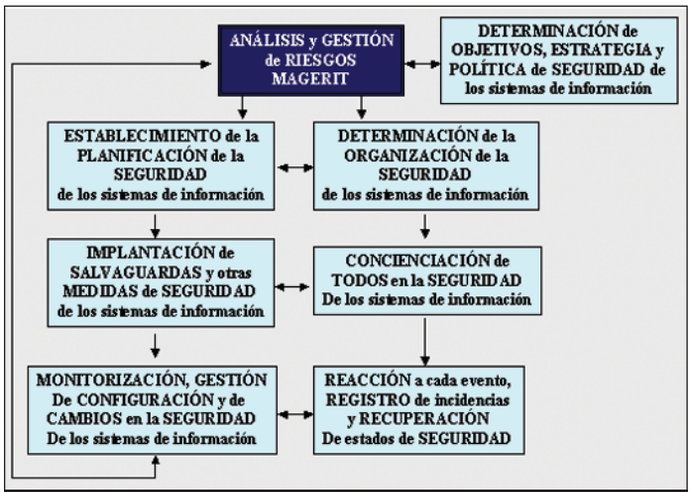
Como recuerda Francisco López Crespo, el Consejo Superior ☞

de Informática acordó llevar a cabo una serie de iniciativas en materia de seguridad. Entre otras, destaca la implantación de la Intranet Administrativa de la Administración General del Estado, la potenciación de la realización sistemática de análisis y gestión de riesgos de los sistemas de información, y la suscripción del Arreglo sobre el Reconocimiento de los Certificados de Criterios Comunes, en el campo de la Seguridad de la Tecnología de la Información. Esta suscripción se realizó el 23 de mayo de 2000 y, "desde esa fecha, España, representada por el MAP y por el Centro Criptológico Nacional, es un miembro muy activo del Arreglo".

En 2003, un real decreto reguló los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos. "En su disposición final primera, dispone que se establecerán (en el marco de los criterios de seguridad, normalización y conservación) los requisitos de autenticidad, integridad, disponibilidad y confidencialidad de los dispositivos y aplicaciones de registro y notificación, así como los protocolos y criterios técnicos a los que deben sujetarse".

Más recientemente, en septiembre de 2004, se anunció el Plan Conecta, "un plan estratégico de modernización que contempla la seguridad, tanto en su marco director como en los proyectos de que se compone". Finalmente, en 2005, se asignan los recursos para el despliegue paulatino del e-DNI.

A juicio de López Crespo, toda actuación en materia de seguridad, técnica u organizativa, debe ir precedida de un riguroso análisis de riesgos para garantizar que se tienen en cuenta todas las amenazas y vulnerabilidades, y que las salvaguardas que se decidan aplicar están justificadas económicamente, en función del impacto. Afirma que esto es particularmente importante en la Administración electrónica y para cualquier clase o tipo de tecnología, como centros de back-up y planes de contingencia, seguridad de las aplicaciones web y nuevos riesgos de la movilidad (PDAs, Wi-Fi, etc).



Análisis y gestión de riesgos Magerit.

Actuaciones del MAP

El jefe del Área de Sistemas Telemáticos del Ministerio de Administraciones Públicas explica algunas actuaciones que ha llevado a cabo el MAP en el ámbito de la seguridad y protección de datos.

Toda actuación en materia de seguridad, técnica u organizativa, debe ir precedida de un riguroso análisis de riesgos.

En primer lugar, se refiere a la Metodología de Análisis y Gestión de Riesgos para la seguridad de los sistemas de información (MAGERIT). Este modelo propone un modo ordenado de analizar y administrar el estado de la seguridad de los sistemas de información, "imprescindible para que las organizaciones puedan cumplir su misión".

Los procesos y técnicas de los que consta proporcionan una evaluación del riesgo para, a continuación, gestionarlo. "Esto es, reducirlo mediante salvaguardas, hasta alcanzar un nivel que se esté en condiciones de asumir" (http://www.csi.map.es/csi/pg5m20.htm).

En segundo lugar, explica, los Criterios de Seguridad, Normalización y Conservación de las aplicaciones utilizadas para el ejercicio de potestades. "Se trata de una serie de criterios (obligatorios) o recomendaciones para la adopción de un conjunto de medidas organizativas y técnicas, necesarias para garantizar la validez y eficacia de los procedimientos administrativos en los que se utilicen medios electrónicos, informáticos y telemáticos, y para asegurar la protección de la información de los ciudadanos en sus relaciones con la Administración.

Estos Criterios son de seguridad para la implantación de las medidas de seguridad en las aplicaciones utilizadas; Criterios de normalización, orientados a facilitar la compatibilidad técnica y la interoperabilidad de las aplicaciones; y Criterios de conservación de la información en soporte electrónico, durante todo el ciclo de vida de la tramitación electrónica administrativa, desde su creación hasta su archivo o destrucción.

La tercera actuación comprende el Generador de declaraciones sobre políticas de protección de datos de carácter personal. "Es una herramienta didáctica, cuyo objeto es ofrecer orientación sobre cómo realizar una revisión interna de las prácticas existentes sobre datos de carácter personal, y cómo elaborar una correcta declaración sobre políticas de protección de estos datos, adaptada a la legislación española".

López Crespo indica que se pretende que el uso del Generador ayude a una serie de cuestiones: "fomentar el conocimiento de los temas relativos a la protección de datos de carácter personal, entre los propietarios de páginas web; aumentar el conocimiento, entre los visitantes, sobre las prácticas de protección de datos de carácter personal en las páginas web que visiten; conocer y divulgar la normativa española vigente en cuestiones de protección de datos de carácter personal; y animar a usuarios y consumidores a confiar en las redes mundiales y el comercio electrónico".

Pero las actuaciones del MAP, para las que se está utilizando "la tecnología propia de apoyo de toma de decisiones y las encuadradas en 'web services'", no terminan aquí. Entre los retos de futuro que se ha planteado, se encuentra desarrollar de forma coordinada con las otras Administraciones Públicas (españolas y europeas) y otros actores (por ejemplo, del sector privado) ciertas actuaciones de infraestructura tecnológica (como las relacionadas con la certificación de la seguridad de la tecnología de la información o de verificación del cumplimiento de los requisitos de las infraestructuras de clave pública). Además, contempla el desarrollo del soporte organizativo, para la promoción e implantación de la 'cultura de la seguridad' y para la ordenación de la seguridad de la información y de las tecnologías que la manejan.

Ministerio de Trabajo

El Ministerio de Trabajo y Asuntos Sociales también mantiene una especial sensibilidad sobre la seguridad y protección de datos. El Subdirector General ☞

Web www.agpd.es.

de Proceso de Datos de este ministerio, Joseba García Celada, califica de medio-alto el nivel de aplicación de las TIC en este ámbito por parte del conjunto de las administraciones públicas españolas. Este responsable afirma que el ritmo con el que se ha avanzado en esta materia en los últimos años ha sido creciente, "aumentando la sensibilidad por el tema muy rápidamente en los últimos dos años".

García Celada explica que en el MTAS "se gestionan datos personales, incluso con protección alta, para los cuales se establecen protecciones en base a autenticación con X509, cifrado de ese tipo de datos, redundancia de los sistemas y auditoría de los accesos". Además, apunta que se dispone de extranet, "incluso con dispositivos móviles, que acceden vía VPN".

En cuanto a actuaciones concretas que ha llevado a cabo el ministerio en este campo, Celada señala que, además de cumplir con las obligaciones de la LOPD, se ha adjudicado recientemente el rediseño y reforzamiento de la seguridad perimetral. "El futuro concurso de comunicaciones metropolitanas, provinciales e interprovinciales contemplará importantes requerimientos de seguridad, a partir de la experiencia de estos años".

La tecnología que se utiliza en los desarrollos se centra en certificados X509v3, IPSEC, SSL, doble firewall, detección de vulnerabilidades, auditoría centralizada, cifrado hardware, etc. Para su implementación, cuentan con la colaboración de diversas empresas tecnológicas, como Da Vinci, Telefónica España, SIA, Unisys y SUN.

AEPD

El Director de la Agencia Española de Protección de Datos, José Luis Piñar Mañas, pone de manifiesto que "con el esfuerzo de todos, la cultura de la protección de datos va arraigándose en los responsables de los tratamientos de datos personales en las Administraciones Públicas, que son conscientes de la importancia de la protección de las informaciones relativas, tanto a los ciudadanos, como a los propios funcionarios".

Según su experiencia, los tratamientos de la Administración General del Estado, las administraciones autonómicas, y los entes locales importantes, se adaptan, de un modo más que aceptable, a la legislación sobre protección de datos. Sin embargo, señala que "en los pequeños ayuntamientos, se percibe cierta dificultad para lograrlo, debido en parte a sus especiales características, si bien existen notables diferencias de unas provincias a otras".

Piñar resalta también el hecho de que la creación de algunas Agencias Autonómicas de Protección de Datos (en este momento, Madrid, Cataluña y País Vasco), con específicas competencias en los ficheros creados por las comunidades autónomas, y por la administración local de su ámbito territorial, "supone una gran contribución al conocimiento y cumplimiento de la normativa de protección de datos en el ámbito de la administración pública".

"Todo ello, advierte, no debe hacernos bajar la guardia, ya que es precisa una continua revisión de los procedimientos, ante los nuevos riesgos y retos que plantea el uso de las nuevas tecnologías, al objeto de conseguir el respeto necesario al derecho fundamental a la protección de datos".

Durante los últimos años, el avance ha sido importante. Las cifras de inscripción de ficheros de titularidad pública en el Registro General de Protección de Datos reflejan una subida muy acentuada, sobre todo desde 2002, llegando a finales de enero de 2005 a los 48.272 ficheros inscritos. "Es claro el efecto que en ello ha tenido tanto la Ley Orgánica 15/1999 de Protección de Datos, que establecía un periodo transitorio para adaptar a sus nuevas previsiones las disposiciones de regulación de los ficheros que deben publicarse en los boletines oficiales, como el Reglamento de Medidas de Seguridad, aprobado por el Real Decreto 994/1999, que obliga a los responsables de fichero a poner en marcha medidas técnicas y organizativas, entre las que se encuentra la elaboración del Documento de Seguridad y, en los ficheros con tipos de datos más sensibles, a la realización de auditorías periódicas".

El Reglamento de Medidas de Seguridad prevé la obligación de definir y aplicar procedimientos de realización de copias de respaldo y de recuperación de datos, por lo que siempre que estemos hablando de sistemas de información que traten datos personales, existe la obligación de ponerlos en marcha. "Sin embargo, esta medida, como todas las contenidas en el Reglamento, tiene la condición de mínimo exigible, y en este caso concreto, es posible que muchos de los sistemas de las Administraciones Públicas requieran procedimientos de obtención de copias de seguridad más sofisticados".

En cuanto a la aparición de nuevos dispositivos y tecnologías (algunas no tan nuevas como las aplicaciones web), Piñar subraya que la LOPD, el Reglamento de Medidas de Seguridad, y las demás normas relativas a la protección de datos personales, han de ser respetadas, con las adaptaciones precisas. "Nuevamente, es preciso citar la importancia de la concienciación, ya que generalmente los dispositivos móviles y las redes inalámbricas están dotadas de suficientes mecanismos de seguridad, que muchas veces no son utilizadas por desconocimiento".

La Administración central quiere desarrollar con otras Administraciones Públicas y el sector privado infraestructuras tecnológicas, como las relacionadas con la certificación de la seguridad de las TI.

La Agencia Española de Protección de Datos, como ente público independiente encargado de velar por el cumplimiento de la legislación sobre protección de datos, tiene como uno de sus principales objetivos conseguir la máxima difusión posible de la normativa afectada, por lo que participa en multitud de eventos, jornadas y foros. También, dispone de una página web (www.agpd.es), que renueva constantemente, para conseguir que está información llegue, tanto a los responsables de los ficheros, como a los ciudadanos.

En el ámbito de la Administración Pública, la AEPD participa en los cursos selectivos de diferentes cuerpos, ya sean o no especializados en TIC, y en cursos de formación destinados a funcionarios públicos.

SOCINFO **Sociedad de la Información** ADMINISTRACIONES PÚBLICAS

Evento TIC

Deloitte. SIEMENS T-Systems

Seminario
Planes de Seguridad y protección de datos

Madrid, 15 marzo de 2005
Instituto de la Ingeniería.
General Arrando, 38.
28010 Madrid.

En preparación

5 de Abril
Educación y Nuevas Tecnologías
26 de Abril
Gobierno electrónico en el área de Sanidad
24 de Mayo
Ciudades Digitales
14 de Junio
Gestión de Recursos Humanos en las AA.PP.
5 de Julio
Organismos informáticos del sector público

09:30 Bienvenida
D. José García Méndez. Director de la revista "Sociedad de la Información".

09:40 Políticas y herramientas de seguridad en la Administración General del Estado
D. Domingo Laborda. Director General de Modernización Administrativa. MAP.

10:10 El Plan Director de Seguridad del Gobierno de Navarra
D. Angel Sanz. Director General para la Sociedad de la Información. Gobierno de Navarra.

10:40 La Protección de Datos en la Justicia
D. Pedro Alberto González. Consejo General del Poder Judicial.

11:10 La seguridad de las aplicaciones web
D. Juan Miguel Ramos. Socio. Deloitte.

11:20 Puntos clave a la hora de abordar un plan de continuidad de negocio
Dª Carolina de Oro. Responsable Área de Seguridad. Siemens.

11:30 Turno de preguntas. **11:40 Pausa café**

12:00 Los nuevos riesgos de seguridad introducidos por la movilidad
D. Juan José Gilsanz. Director Mobile Solutions. T-Systems.

12:10 El Plan de Seguridad en la Diputación Foral de Guipúzcoa
D. Javier Gómez. Director General. Sociedad Foral de Servicios Informáticos (IZFE) de Guipúzcoa.

12:40 Hacia un sistema de gestión de la seguridad de la información: La experiencia de la Universitat Jaume I
D. Vicent Andreu.Técnico Superior de Organización. Universidad Jaime I.

13:10 Certificación de Sistemas de Gestión de la Seguridad de la Información
D. Carlos Fernández. Responsable de Seguridad de Sistemas de Información. AENOR.

13:40 Turno de preguntas. 13:50 Clausura.

Cuota de inscripción
- ❑ Funcionarios Sector público: Gratis.
- ❑ Sector privado*. 250 euros (+ 16% IVA).
- ❑ Suscriptores*: 225 euros (+ 16% IVA).

(*) Sujeto a aceptación por patrocinadores.

Forma de pago
❑ Transferencia, mencionando nombre del inscrito, a favor de: Socinfo SL. Cajamadrid. 2038.2490.06.6000.209153.
❑ Cheque nominativo a la entrada.
❑ Tarjeta de crédito Visa o Master Card.
Nº _ _ _ _ . _ _ _ _ . _ _ _ _ . _ _ _ _.
Fecha caducidad _ _ / _ _.

Información inscripciones
Tel./fax: 916-319-696.
comercial@socinfo.info www.socinfo.info

Inscripción Evento TIC: "Seguridad y Protección de Datos"
Deseo que me inscriban como asistente a este evento:
D: . . . . . .
Cargo: . . . . . .
Empresa: . . . . . Ciudad: . . . . . .
CIF/DNI: . . . . . C.P.: . . . . . .
Domicilio: . . . . . .
Teléfono: . . . . . Firma
e-mail: . . . . . .

(*) Enviar e-mail (socinfo@socinfo.info) o fax (916-319-696) para recibir confirmación.

De conformidad con la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, Ud. queda informado de que sus datos de carácter personal van a formar parte de un fichero automatizado del que es responsable SOCINFO. Asimismo, al facilitar los datos solicitados, Ud. presta su consentimiento para poder llevar a cabo el tratamiento de los datos personales para las siguientes finalidades: a) Envío de publicidad de actividades promovidas por SOCINFO y de las empresas patrocinadoras. b) Asistencia al evento para el que se envían los datos y otros futuros que puedan organizarse. Del mismo modo, le informamos que otorga su consentimiento para la cesión de sus datos a las personas que intervengan en los actos organizados por SOCINFO, y a sus patrocinadores, pudiendo ejercitar sus derechos de acceso, rectificación o cancelación, así como revocar su consentimiento enviando una comunicación a la dirección arriba indicada.

Otra de las actividades realizadas por la Agencia son los Planes Sectoriales de Oficio, que tienen como resultado la posterior formulación de unas recomendaciones, en función de los resultados del Plan. En lo que se refiere a Administraciones Públicas, destaca los realizados al Instituto Nacional de Administración Pública (2004), a petición del propio Instituto, o al Instituto Nacional de Estadística, respecto a los Censos de población y vivienda (2003).

La Agencia también tiene la función de informar, con carácter preceptivo, de los proyectos de disposiciones generales que desarrolla la LOPD y, además, con el objetivo de atender en las cuestiones relativas al derecho de protección de datos, emite informes jurídicos relativos a las consultas planteadas. Junto a todo lo anterior, ejerce la potestad sancionadora, por lo que también instruye y resuelve estos procedimientos.

Como responsable de tratamiento de datos de carácter personal, la Agencia Española tiene implantadas las medidas de seguridad correspondientes. "No obstante, siempre se ha pretendido mantener una 'neutralidad' con respecto a las tecnologías a utilizar por los responsables de los ficheros. El Reglamento de Medidas de Seguridad establece cuáles son necesarias, pero no indica, ni debe hacerlo, cuál es la tecnología concreta que ha de emplearse ya que existen diferentes que se adecúan perfectamente a los requisitos establecidos y, además, evolucionan constantemente".

Aunque, la agencia cuenta con la colaboración de diversas empresas tecnológicas para el desarrollo de sus proyectos, en lo que respecta a las obligaciones que la LOPD y el Reglamento de Medidas de Seguridad imponen a los responsables de ficheros de titularidad pública, "generalmente, se puede optar por su desarrollo dentro de la propia entidad o por la colaboración con empresas externas". Un ejemplo es la auditoría a la que deben someterse cada dos años los sistemas con tratamiento de datos personales de nivel medio y alto, en la que el Reglamento indica textualmente que puede ser "interna o externa". "Tampoco hay que olvidar que, cuando el responsable del fichero se apoye en empresas externas para la prestación de servicios que requieran el acceso de éstas a los datos personales, la realización del tratamiento deberá estar regulada en un contrato con las condiciones que recoge el artículo 12 de la LOPD".

Antonio Troncoso, director de la Agencia de Protección de Datos de Madrid, y Francisco López, subdirector general.

Trabajo gestiona datos con alta protección, autenticación con X509, cifrado, redundancia de sistemas y auditoría de accesos.

Piñar indica que, en lo relativo a TIC, a la Agencia Española de Protección de Datos le han sido atribuidas nuevas competencias. Entre ellas, se encuentra tutelar los derechos reconocidos a los usuarios de servicios de comunicaciones electrónicas, recogida en la Ley 32/2003 General de Telecomunicaciones (LGT), y las incluidas en la modificación de la Ley 34/2002, de Servicios de la Sociedad de la Información y del Comercio Electrónico (LSSI), que cambia el régimen jurídico aplicable a las comunicaciones publicitarias o promocionales, por correo electrónico u otro medio de comunicación electrónica equivalente, así como a los dispositivos de almacenamiento y recuperación de la información en equipos terminales, correspondiendo a la Agencia Española de Protección de Datos la competencia para aplicar las garantías sobre ambos aspectos."

Agencia de Madrid

Según Francisco José López Carmona, subdirector general de Registro de Ficheros y Consultoría de la Agencia de Protección de Datos de la Comunidad de Madrid, la aplicación de las TIC en la protección y la seguridad de datos en las administraciones públicas españolas se encuentra en una situación relativamente más avanzada que la organización de la seguridad. "Es decir, la tecnología aplicada a la seguridad va por delante de las medidas organizativas y del cambio cultural en la gestión de información". Aunque, añade, requiere de "un aumento sustancial en su alcance".

López Carmona explica que, durante los últimos años, el avance que se ha hecho en este ámbito ha sido importante. "Especial significación ha tenido la apertura de servicios interactivos, o de tramitación electrónica, que afectan a componentes sustanciales de los sistemas de información de las administraciones públicas y que, por tanto, han producido una reflexión sobre la seguridad desde los puntos de vistas técnico, operativo y jurídico".

El subdirector señala que tecnologías como centros de back-up y planes de contingencia, seguridad de las aplicaciones web y nuevos riesgos de la movilidad (PDAs, Wi-Fi, etc), plantean, en materia de protección de datos personales, desafíos emergentes de seguridad y requieren de una actualización de la normativa vigente y, muy en particular, del 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 Personales.

López Carmona se hace eco de las principales actuaciones de la Agencia de Protección de Datos de la Comunidad de Madrid en el ámbito de las nuevas tecnologías, como la elaboración y puesta a disposición pública y gratuita de modelos de documentos de seguridad, disponibles en el sitio web de la Agencia www.apdcm.es, y la promoción de la designación de responsables de seguridad y de la realización de auditorías de seguridad en su ámbito de competencia.

Por otra parte, destaca que la agencia organizó en 2004 un total de siete jornadas informativas sobre protección de datos, con más de 1.500 asistentes, así como más de 300 sesiones informativas y cursos, que alcanzaron a un número superior a 3.000 empleados públicos.

Igualmente, la agencia ha lanzado en los últimos meses "publicaciones prácticas, destinadas a apoyar los esfuerzos en protección de datos de distintas instituciones públicas, incluyendo en particular las Guías de Protección de Datos Personales para colegios profesionales, universidades públicas, servicios sociales públicos, ayuntamientos y servicios sanita-

Plan Director de Seguridad Informática

Por Juan Miguel Ramos. Socio. Deloitte.

El mundo de la seguridad informática está tomando desde hace algunos años una importancia cada vez mayor. La omnipresencia de Internet es su primer impulsor pero en España también hay que reconocer el papel que la Ley Orgánica de Protección de Datos de carácter personal (LOPD) ha representado como el otro gran acicate para el desarrollo de la seguridad informática.

Sin embargo, muchas veces el enfoque con el que se aborda el robustecimiento de la seguridad informática de una organización es a través de una cierta improvisación, adquiriendo (apilando dicen algunos) tecnología de seguridad sin una finalidad clara, sin unos planteamientos alineados con la actividad de la organización y enfocados a obtener dicha seguridad de un modo coherente. Ello puede producir dos efectos indeseables:

1. Por una parte, una falsa sensación de seguridad tras haber adquirido herramientas tecnológicas, más o menos disjuntas, con dificultades de relacionarse entre sí, con funcionalidades de seguridad parcialmente solapadas y con ritmos de introducción de mejoras diferentes. No hay que olvidar que las soluciones tecnológicas de seguridad informática están en constante evolución debido a los cambios de la tecnología subyacente y a las características inherentes de las amenazas a la seguridad.

2. Por otra parte, el riesgo de que no se protejan correctamente y con un nivel de seguridad acorde a su valor, los distintos activos de información. Y aquí se puede actuar por defecto o por exceso. En el primer caso, no se habrá alcanzado el objetivo: proteger adecuadamente la información; y, en el segundo, se estarán dilapidando los siempre escasos recursos.

De lo anterior, se pueden deducir fácilmente las ventajas de realizar una adecuada planificación a la hora de encarar la mejora en la seguridad de los sistemas informáticos de una organización y reflejarlo en un Plan Director de Seguridad Informática. El objetivo debe ser identificar un conjunto de acciones a realizar en un plazo de tiempo razonable (se suele considerar de uno a tres años).

En su realización, hay que huir de un error muy común que es considerar la seguridad informática como una cuestión exclusivamente tecnológica y que, por lo tanto, debe ser resuelta por medidas de índole tecnológica exclusivamente. Ello no es así. La tecnología -específica de seguridad, que es de la que estamos hablando- ayuda, y es hasta aceptable que pueda ser el factor más importante de la solución, pero desde luego no es el único. Como todo problema delicado en las organizaciones de hoy en día, tiene una solución basada en el adecuado equilibrio de una combinación de personas, procesos y tecnología. Una vez identificados los componentes de la solución en estos tres ámbitos, se agrupan en proyectos homogéneos cuya ejecución se plasma en una secuencia temporal que conforma el Plan Director de Seguridad.

"Muchas veces se aborda la seguridad informática 'apilando' tecnología sin una finalidad, ni planteamientos claros".

Protección de datos personales

Puede ser uno de los proyectos estrella de un Plan Director de Seguridad Informática aunque, obviamente, puede tener vida por sí solo. De todos es conocido el requerimiento de la LOPD: "El responsable del fichero... deberá adoptar las medidas de índole técnica y organizativa necesarias que garanticen la seguridad de los datos de carácter personal...". En el ámbito que nos ocupa, dichas medidas están enfocadas a proteger adecuadamente los ficheros informáticos que contienen datos de carácter personal. Cumpliendo el requisito legal, se avanza en el robustecimiento de la seguridad de los sistemas informáticos de una organización. La inversa también es cierta pero hay que prestar atención para que el Plan Director de Seguridad Informática contemple todo el abanico de medidas para adaptarse a la LOPD ya que, estrictamente hablando, no todas las acciones necesarias para cumplir con dicha legislación están relacionadas con la seguridad informática. Existen otras actuaciones de índole jurídica y organizativa que, asimismo, es necesario poner en marcha para realizar una adaptación correcta a la normativa de protección de datos. Un Plan Director adecuadamente enfocado debe contemplar todas ellas.

Vigilancia permanente

Y un comentario final. De todos es sabido que las tecnologías de la información son el ejemplo perfecto de un sector en el que el cambio es consustancial al mismo. Y la seguridad no es ninguna excepción: la propia tecnología de seguridad informática está en rápida evolución y consolidación, todos los días aparecen nuevas vulnerabilidades en los sistemas informáticos que los dejan más desprotegidos, los parches no siempre son la solución y los piratas informáticos no cesan en su actividad investigadora. Todo ello obliga a mantener a lo largo del tiempo la atención y el foco y dedicar a la seguridad informática recursos adecuados y correctamente formados y equipados.

La seguridad no es un estado que uno alcanza si no que hay que luchar para mantenerlo. ☒

Juan Miguel Ramos. Tel. 915-145-000. juramos@deloitte.es. www.deloitte.es.

rios públicos; un 'Cuaderno de protección de datos personales para empleados públicos', y el 'Manual de Protección de Datos Personales para las Administraciones Públicas', todas ellas disponibles en el canal *Publicaciones* de la web institucional www.apdcm.es".

En esta web, "se ha producido un incremento significativo en el número de páginas vistas, tanto en el sitio web institucional (con una media superior a las 30.000 páginas mensuales), como en la revista digital www.datospersonales.org (media superior a las 50.000 páginas mensuales), cuya audiencia ha crecido un 130% respecto al segundo semestre de 2003.

Web www.datospersonales.org.

Agencia Catalana

La Agencia Catalana de Protección de Datos fue creada por la ley 5/2002 (de 19 de abril) del Parlamento de Cataluña, mientras que el estatuto de la Agencia fue aprobado el 20 de febrero de 2003. Para el nacimiento de esta autoridad de control, fue necesario constituir el Consejo Asesor de Protección de Datos de Cataluña.

Según su director, Josep Xavier Hernández i Moreno, el objeto de la agencia es velar por el respeto de los derechos fundamentales y de las libertades públicas de los ciudadanos, en todo lo concerniente a las operaciones hechas mediante procesos automatizados o manuales de datos personales.

Según Hérnandez, el gran desarrollo de las tecnologías de la información y de la comunicación, la utilización masiva y habitual de la informática para gestionar múltiples ámbitos de la vida moderna, y la progresiva implantación de estas tecnologías en las administraciones públicas, ha situado en un punto crítico el respeto a la privacidad, "ya que el individuo, la persona concreta, puede perder el control de la información que hace referencia a sí misma".

A su juicio, ha sido fundamental el desarrollo de "una nueva administración, la Administración Electrónica, que presenta grandes expectativas para permitir un mejor y mayor servicio público a los ciudadanos y, a la vez, grandes retos". "No tiene porqué existir, apunta, ninguna contradicción entre el desarrollo de la administración electrónica y la preservación del derecho a la protección de los datos personales. Precisamente, la solución a este aparente dilema la aporta la propia tecnología. Y, por otra parte, la administración electrónica no debe plantearse como una opción entre todo o nada, sino que debe hallar soluciones complementarias. Así, dejando aparte aquellos supuestos en que un interés público superior lo justifique, habrá que recabar el consentimiento de los ciudadanos para la cesión de datos. Y ello porque el edificio de la protección de los datos personales descansa sobre el consentimiento o la habilitación legal".

Este nuevo escenario "ha planteado la cuestión de si la legislación tradicional podía afrontar estos nuevos fenómenos que, por un lado, comportan un avance notable en las posibilidades de comunicación, oferta y prestación de servicios; pero que, por otro lado, posibilitan el uso abusivo, o ilegítimo, de los datos personales de cada uno".

Según Hernández, en el ámbito internacional, se ha configurado el reconocimiento de un nuevo derecho de la personalidad: el derecho a la protección de los datos personales, que viene a sumarse a los ya consolidados derechos a la intimidad, la privacidad y la dignidad. "Ha sido en el contexto europeo donde la regulación de la protección de los datos personales ha comenzado a limitar el papel preponderante que tenían las tecnologías y el mercado".

Según la AEPD, es precisa una continua revisión de los procedimientos, ante los nuevos riesgos y retos que plantea el uso de las nuevas tecnologías.

Para este experto, tres han sido los mecanismos principales que se han considerado imprescindibles para velar por la efectividad del respeto al derecho a la protección de los datos personales. "El primero es la aprobación de una legislación comunitaria, traspuesta a la normativa estatal, reconocedora y preservadora de este derecho fundamental. En segundo lugar, la información a los ciudadanos y ciudadanas de la existencia de tal derecho y su exigibilidad. Y, el tercero, la creación de autoridades de control independientes, con medios y competencias suficientes para procurar el cumplimiento de las leyes y exigir su respeto mediante las agencias de protección de datos (también llamadas comisionados o garantes de la protección de datos)".

Así, en el marco de la Directiva 95/46/CE y de la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal, se ha creado la Agencia Catalana de Protección de Datos "como un instrumento fundamental para velar por el buen funcionamiento de la recopilación y tratamiento de los datos personales y del respeto de los derechos fundamentales de los ciudadanos de Cataluña en el ámbito que establece la Ley".

Según Hernández, la Agencia Catalana se caracteriza, en primer lugar, por ser una autoridad de control, con facultades de registro, control, inspección, sanción y resolución, así como de adopción de propuestas e instrucciones. En segundo lugar, es una institución de derecho público, con personalidad jurídica propia y plena capacidad de obrar para el cumplimiento de sus fines. Por último, actúa con objetividad y plena independencia de las administraciones públicas en el ejercicio de sus funciones.

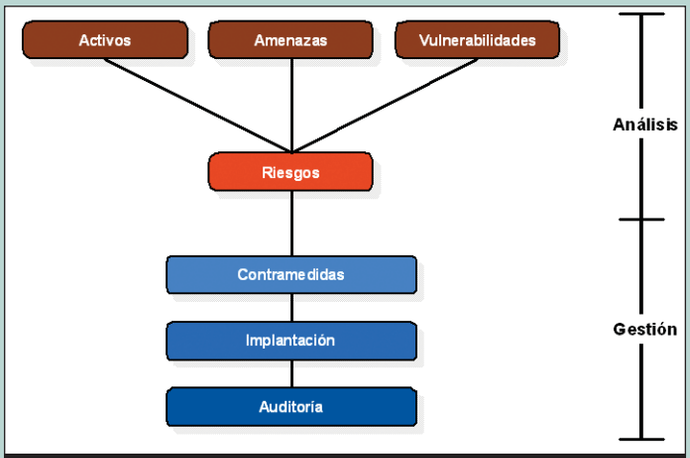
El ámbito de actuación de la Agencia Catalana de Protección de Datos comprende los tratamientos de datos y los ficheros. En concreto, los tratamientos de datos personales realizados por la Generalitat de Cataluña, por los entes locales y entes que integran la Administración Local, por sus organismos y entidades autónomas, por los consorcios de los que formen parte, y por las universidades en el ámbito territorial de Cataluña.

Avances en la Gestión de la Seguridad de la Información

UNA información segura y unas comunicaciones corporativas confidenciales son dos pilares básicos para conseguir el éxito de una organización. Por ello, es cada vez más necesario establecer un Sistema de Gestión de la Seguridad de la Información, SGSI.

Siemens Comunicaciones integra una unidad de negocio especializada en seguridad que ayuda a las organizaciones a identificar y gestionar el riesgo que afecta a sus infraestructuras TI y a su negocio, desde el desarrollo de la política, la estrategia o la concienciación de usuarios hasta el suministro de soluciones completas.

Para la realización de estos análisis, hemos elegido CRAMM, la metodología y herramienta de análisis y gestión de riesgos más completa, premiada y utilizada en el mundo.



Funcionamiento del CRAMM.

Gestión de la Seguridad

El conjunto de normas UNE-ISO/IEC 17799 y UNE 71502 constituyen una referencia sólida para que las organizaciones mejoren la eficacia de sus procesos de seguridad de la información.

La norma UNE-ISO/IEC 17799 recoge, en 127 controles, buenas prácticas para garantizar la seguridad de la información, prácticas que no son sólo tecnológicas, sino también organizativas, físicas o jurídicas.

Por otra parte, la norma certificable UNE 71502 (similar a la también certificable norma británica BS7799-2) define una serie de requisitos para establecer un Sistema de Gestión de la Seguridad de la Información, SGSI.

Entre las actividades básicas para obtener la certificación del SGSI, es necesario realizar un Análisis de Riesgos y una Gestión de Riesgos. Estas dos actividades, en conjunto, se suelen también denominar Valoración de Riesgos.

El Análisis nos va a responder a la pregunta sobre qué amenazas afectan al sistema y el grado de vulnerabilidad del mismo, y establecerá cuál es el nivel de riesgo de cada sistema frente a las distintas amenazas

Por otra parte, la Gestión de Riesgos seleccionará las contramedidas o salvaguardas adecuadas a las amenazas analizadas y los riesgos identificados.

Pero no sólo en la norma certificable 71502 se habla de Valorar los riesgos. En numerosos puntos de la 17799, se indica la conveniencia de realizar este ejercicio para determinar los niveles de contramedidas apropiados.

Sin embargo, nos encontramos con que es extremadamente compleja la realización práctica de una Valoración de Riesgos sin el apoyo de una metodología sólida y una herramienta de apoyo que sirva como repositorio de información y motor de cálculo de contramedidas.

Metodología CRAMM

Después de una selección exhaustiva de las diferentes metodologías existentes, Siemens se decantó por CRAMM.

CRAMM, con más de 20 años de historia, es una metodología de origen británico (al igual que las normas BS7799 o las librerías ITIL). Por esa razón, está perfectamente alineada con los requisitos para obtener la certificación BS7799-2 y, por extensión, también la UNE 71502.

"Con más de 500 copias en 23 países del mundo y en 20 sectores de negocio, CRAMM es una metodología sobradamente conocida".

Con más de 500 copias en 23 países y en 20 sectores de negocio, CRAMM es una metodología sobradamente probada. Un gran número de autoridades nacionales de seguridad la respaldan como Mejor Práctica en Gestión de la Seguridad de la Información.

Entre las características de CRAMM, cabe destacar:

- Más de 400 tipos de activos.
- Más de 25 tipos diferentes de impacto.
- Más de 12 formas de valorar los impactos.
- 38 tipos de amenaza.
- Más de 150 combinaciones posibles de impacto, amenaza y vulnerabilidad.
- 7 niveles de riesgo.
- Más de 3.000 contramedidas.

En el gráfico adjunto se resume el funcionamiento de CRAMM:

En primer lugar, se determinan qué activos componen el sistema de información de la organización y qué valor tienen éstos en términos de disponibilidad, integridad y confidencialidad.

A continuación, de entre las amenazas posibles, se decide cuáles deben ser investigadas y contra qué activos. Se mide su nivel, así como el de la vulnerabilidad de los activos frente a ellas.

En base a una matriz de riesgos, se establece, en una escala del 1 al 7, los niveles de riesgo de la organización.

Finalmente, y partiendo de la base de datos de 3.000 contramedidas, CRAMM selecciona aquellas apropiadas para combatir los riesgos. Esta selección se realiza en base a 3 criterios:

- Nivel de riesgo.
- Tipo de amenaza.
- Tipo de activo.

CRAMM y la Certificación

Entre otras funciones, CRAMM genera automáticamente el Documento de Selección de Controles (*Statement of Applicability*, en la norma inglesa). Este es uno de los documentos requeridos para la certificación, y uno de los más complejos de obtener. Esto es posible gracias a que todas las contramedidas de CRAMM están indexadas a alguno de los 127 controles de la 17799. ☒

Por César Peñacoba. Consultor Senior de Seguridad. Div. Comunicaciones. Siemens.

César Peñacoba. cesar.penacoba@siemens.com. Tel. 900-100-566. www.siemens.com.

Asimismo, los ficheros creados por la Generalidad de Cataluña o por los entes locales que sean gestionados por entidades públicas o privadas en la prestación de servicios públicos; y las asociaciones, fundaciones, sociedades civiles o mercantiles, en las que la Generalitat, o los entes locales, tengan la participación mayoritaria del capital, cuando lleven a cabo actividades por cuenta de una administración pública.

Una de las primeras actuaciones llevadas a cabo por la Agencia Catalana fue solicitar a la Agencia Española de Protección de Datos toda la información respecto a los ficheros inscritos en el Registro General que eran titularidad de las entidades que integran su ámbito de competencia. En total, había unos 528 ficheros declarados de la Generalidad de Cataluña, 3.221 de la Administración local y 43 relativos a Universidades. Durante 2004, se inscribieron en el Registro de Protección de Datos de Cataluña un total de 840 ficheros: 241 de la Generalidad de Cataluña, 571 de la Administración Local y 28 de Universidades.

Por otra parte, la agencia está llevando a cabo una actuación informativa y formativa dirigida a las administraciones públicas, mediante el portal de Internet www.apdcat.net, así como mediante la organización de cursos de formación y la organización y participación en jornadas y seminarios que promueven el conocimiento y las soluciones a la problemática de la protección de datos personales. Durante el pasado año, el portal de internet de la Agencia Catalana recibió más de 12.000 visitantes que han accedido en unas 68.000 ocasiones.

Josep Xavier Hernández afirma que la consolidación de la cultura de la protección de los datos personales exige tanto la sensibilización y actuaciones decididas por parte de las administraciones públicas, en el establecimiento de políticas de seguridad y de respeto a la protección de los datos personales, como una mayor información de los ciudadanos.

En este sentido, aparte del lugar destacado que se reserva a la información sobre derechos de los ciudadanos, a los que se ofrecen formularios para el ejercicio de los

Josep Xavier Hernández, director de la Agencia Catalana de Protección de Datos, y web.

derechos de acceso, rectificación, cancelación y oposición, así como para denuncias y reclamaciones en caso de incumplimiento, se han editado dípticos de información ciudadana, que se distribuyen a través de las propias administraciones públicas y universidades.

También se ha establecido un servicio de atención permanente, mediante el número telefónico 902-011-710 y el email consultes.apdcat@gencat.net. Durante 2004, se realizó un total de 1.147 consultas (976 telefónicas y 171 por correo electrónico), aparte de las consultas formales que han remitido a la agencia las entidades públicas y universidades (27 consultas que giran en torno al ejercicio de los derechos y cesión de datos y, en menor volumen, a las medidas de seguridad).

La puesta en marcha de la agencia y la ubicación en la nueva sede, el año pasado, han determinado la implantación de sistemas de información que se han construido sobre tres ejes: la ofimática y gestión de proyectos, y la actividad productiva propia de la Agencia; el ejercicio de competencias de registro, control, inspección, sanción y adopción de propuestas e instrucciones; y el archivo y repositorio "documedia" Servicios de extranet, como sistemas orientados a facilitar el acceso a la aplicación y sistemas de información internos, desde fuera de la red de área local.

Como criterio general, "se ha establecido siempre un nivel de seguridad por encima de la media que correspondería a una organización de las dimensiones tecnológicas de la Agencia". Además, se ha prestado una especial atención a la seguridad de los sistemas de información y plataformas tecnológicas utilizadas.

"Esta especial sensibilidad se ha puesto de manifiesto en la fase de diseño de los sistemas de información y las plataformas, así como en el día a día y en la verificación de los controles de seguridad, mediante auditorías de sistemas y aplicaciones".

El director apunta que se han ejecutado tests de intrusión en los sistemas de información públicos de la agencia, se han utilizado certificados digitales (CatCert) en los servidores de Internet y se han establecido cortafuegos en las infraestructuras, y antivirus y antiprogramario no deseado, en las estaciones de trabajo. Finalmente, se ha cifrado la información, para preservar la confidencialidad "allí donde se ha considerado necesario".

En cuanto al modelo tecnológico utilizado en la construcción del sistema de información, se ha basado íntegramente en el programario de código abierto, tanto por lo que respecta al sistema operativo, gestor de bases de datos, y servidores de aplicacio-

Para la Agencia Catalana de Protección de Datos no tiene porqué existir ninguna contradicción entre administración electrónica y preservación del derecho a la protección de los datos personales.

nes, como a los lenguajes de programación.

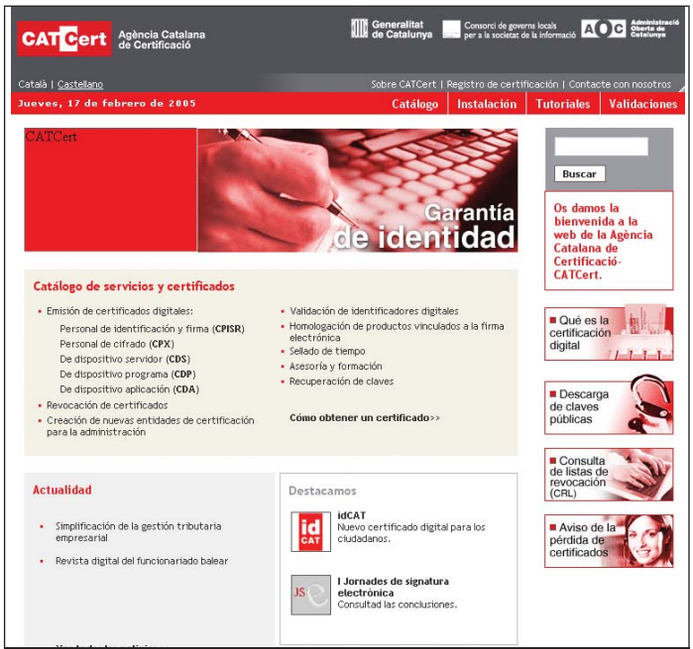
Agencia de Certificación

Según Jordi Masias i Muntada, director general de la Agencia Catalana de Certificació (CATCert), "desde mi punto de vista y orientado a la seguridad, y en concreto al uso de la certificación digital, debo decir que, aunque su uso aún es muy pequeño, sí es cierto que el ámbito de las administraciones públicas españolas es donde se utiliza más. En el sector privado, su uso es mucho menor".

Pero añade que "también es cierto que, en los últimos meses, al menos en Catalunya, este uso se ha visto incrementado de forma muy importante. Son ya varias las administraciones catalanas que lo están requiriendo en sus trámites: Generalitat de Catalunya, diputaciones, ayuntamientos (Barcelona, Sabadell, Santa Coloma, Castellà del Vallés, etc) y empresas públicas (Agència Catalana de l'Aigua, GISA, etc), y otras muchas las que tienen proyectos donde requerirán de su uso".

Masias opina que, en los últimos dos años, el crecimiento en este ámbito ha sido espectacular, con respecto a los años anteriores. "Estamos hablando de una tecnología que está disponible desde hace más de ocho años, pero que realmente se está empezando a aplicar en los últimos ejercicios. En Cataluña, este uso es muy reciente. El año 2004 fue en el que participamos en más proyectos con las administraciones públicas, más de 80, con uso de identidad digital y firma electrónica".

Para el director general de la Agencia Catalana de Certificación, la protección de datos y los planes de seguridad son aspectos básicos. "Ser entidad de certificación nos obliga a cumplir unos niveles de seguridad muy importantes. De hecho, disponemos de un centro de alta seguridad que cumple distintas normas de seguridad, con planes de contingencia, etc. Intentamos que las administraciones públicas también sean sensibles a estos aspectos y detectamos cada día una mayor receptividad".



Web www.catcert.net.

La Agencia Catalana de Certificación ha llevado a cabo, básicamente, seis actuaciones para potenciar la aplicación de las nuevas tecnologías en la seguridad y protección de datos.

En primer lugar, la emisión de certificados digitales para los empleados públicos. "Entendemos que la seguridad debe partir de las administraciones públicas y, por lo tanto, los trabajadores públicos, sean funcionarios o laborales, deben disponer de identidad digital y de firma electrónica. Hoy en día, en Catalunya, tanto la Generalitat, como todas las diputaciones y todos los consejos comarcales, así como más del 70% de los ayuntamientos, disponen ya de firma electrónica".

En segundo lugar, la emisión de certificados digitales para los ciudadanos. "La identidad del ciudadano es básica en la puesta en marcha de nuevos trámites. Esta identidad es proporcionada desde las administraciones públicas catalanas". En tercer lugar, el Servicio de Validación de identidades digitales. "No sólo las administraciones catalanas aceptan certificados de la Agéncia Catalana de Certificació, sino que la relación con ellas está habilitada para certificados digitales de otras entidades de certificación, previamente clasificadas por CATCert. Para validar dichos certificados, utilizan el servicio de validación de CATCert".

Otras actuaciones son el Servicio de *Time Stamping*, así como el asesoramiento y formación; "básico para generar confianza y dar a las administraciones catalanas el conocimiento necesario para que puedan habilitar nuevos trámites a través de la red".

Una sexta actuación la constituye el *Archivo seguro*. "Estamos trabajando en un sistema de archivo de documentos firmados, garantizando la validez tecnológica y legal de estos documentos públicos".

Un gran número de empresas colabora con la agencia. Masias destaca a Safelayer, para el servicio de *Time Stamping* y los certificados digitales de los empleados públicos; Da Vinci, para el certificado digital del ciudadano; Netfocus y T-Systems, para el Validador; GyD, para las tarjetas xip; Telefónica, para el hosting; Cap Gemini para Call Center; e InetSecur y S21sec, para auditoria informática y tests de intrusión. Las instalaciones están ubicadas en Telefónica.

Puesta en marcha del Sidir

El pasado mes noviembre, la Agencia Española de Protección de Datos y las agencias autonómicas firmaron un protocolo de colaboración para la puesta en marcha del Sistema de Información de Intercambio Registral (SIDIR), rubricado por el director de la AEPD, José Luis Piñar, y los directores de las agencias autonómicas creadas hasta la fecha, Antonio Troncoso (Madrid), Xavier Hernández (Cataluña) e Iñaki Vicuña (País Vasco).

Este protocolo, que podrá ser suscrito por las Agencias Autonómicas de Protección de Datos que se creen en un futuro, tiene por objeto establecer un sistema que facilite la comunicación de la información de las inscripciones de los tratamientos de datos personales, entre los registros de ficheros creados al amparo del artículo 41.2 por las Agencias Autonómicas y el Registro General de Protección de Datos, de una forma automatizada, ágil y segura, en la que se garantice el principio de neutralidad tecnológica.

Una vez constituido el grupo de trabajo del SIDIR, los participantes manifestaron su decidido apoyo al proyecto y realizaron una distribución de las tareas a desarrollar, además de definir un calendario de actuaciones. ☒

La AGPD y las agencias de Madrid, Cataluña y País Vasco han firmado un protocolo de colaboración, para la puesta en marcha del Sistema de Información de Intercambio Registral.

COVER

Ministerio de Administraciones Públicas.

Servicio de notificaciones telemáticas seguras

El Servicio de Notificaciones Telemáticas Seguras es un servicio que ofrece el Ministerio de Administraciones Públicas, en colaboración con Correos, para la gestión de notificaciones telemáticas entre las administraciones públicas y los ciudadanos. Posibilita el cumplimiento de la práctica de notificación fehaciente de los actos administrativos hacia los ciudadanos y empresas, a través de medios telemáticos y manteniendo pleno valor jurídico.

Como explica Alfonso Berral López, Jefe de Servicio de Desarrollo del MAP, la puesta a disposición de los interesados de las notificaciones se produce en un único buzón electrónico, identificado a través de la Dirección Electrónica Única del ciudadano, cualesquiera que sean los emisores de las mismas. El servicio se encuentra operativo desde octubre de 2003 y es accesible a través del Portal del Ciudadano, siendo la Sociedad Estatal Correos y Telégrafos la responsable de desarrollo y explotación.

Se descompone en dos subsistemas claramente definidos. Por un lado, se dispone del Sistema de Gestión de Direcciones Electrónicas Únicas y los procedimientos suscritos por los ciudadanos. Este servicio se designa Dirección Electrónica Única (DEU). Mientras que, por otro lado, se encuentra el buzón electrónico o servicio que gestiona las notificaciones recibidas por los emisores, las presenta a los ciudadanos y recoge los eventos correspondientes (puesta a disposición, lectura, rechazo, etc) para comunicarlo a los emisores. Este servicio se denomina Notificaciones Telemáticas (NT).

Componentes del sistema

El Servicio de Notificaciones Telemáticas Seguras y la Dirección Electrónica Única constan de una serie de componentes. En primer lugar, los emisores, que son los órganos, organismos públicos, ministerios, CCAA, entidades locales, etc. Publican y establecen los procedimientos a los que los ciudadanos se pueden suscribir para la recepción de las notificaciones telemáticas; preguntan al sistema

Alfonso Berral López.

"Se pone a disposición de los interesados un único buzón electrónico: la Dirección Electrónica Única del ciudadano".

sobre los ciudadanos suscritos a sus procedimientos; emiten las notificaciones telemáticas al prestador del servicio, Correos, para su posterior puesta a disposición de los ciudadanos a través del Portal del Ciudadano; reciben la acreditación de la entrega de sus envíos; y requieren de información de retorno, acerca del acceso de los ciudadanos al contenido de sus notificaciones telemáticas.

A continuación, vienen los ciudadanos. Solicitan la creación de su DEU en el Portal del Ciudadano, ya sea directamente o encaminado a través de la web del organismo que gestiona dicho procedimiento administrativo; se suscriben a los procedimientos asociados a órganos u organismos públicos, de los que deseen recibir notificaciones por vía telemática, por los mecanismos que éstos habiliten; y acceden al contenido de las notificaciones telemáticas, a través del buzón electrónico personal que proporciona Correos. Las notificaciones se presentan ordenadas en carpetas que se corresponden con los órganos y organismos públicos, a las que han dado su consentimiento para la recepción de notificaciones, por vía telemática, los ciudadanos y empresas que se adhieren voluntariamente al servicio y sin coste alguno. Éstos requieren estar en posesión de un certificado digital X.509 v.3 individual o de empresa para acceder a los servicios de Notificaciones Telemáticas.

En tercer lugar, tenemos el Portal del Ciudadano. Ofrece información general del servicio, inclusive descarga de SW y enlace para la solicitud del certificado de la Autoridad de Certificación, que genera los certificados admisibles; así como creación, modificación o revocación de una DEU; suscripción voluntaria a los procedimientos publicados por emisor determinado; información acerca de la suscripción a los procedimientos de los órganos y organismos públicos; y acceso al buzón electrónico particular de la DEU correspondiente.

En cuarto lugar, está Correos, SNTS y DEU. Gestiona el directorio del MAP con todas las Direcciones Electrónicas Únicas de los ciudadanos; proporciona un buzón electrónico a cada ciudadano a partir de su solicitud de la DEU; recibe las notificaciones telemáticas y las pone a disposición del destinatario en su buzón y remite a cada órgano notificador certificación electrónica de los eventos producidos: recepción de la notificación del órgano notificador, puesta a disposición en buzón, lectura o rechazo de la notificación por el interesado, posibles incidencias y caducidad de la notificación telemática dentro del plazo de diez días señalados por ley. Correos-Soporte desarrolla las funciones de soporte operativo al ciudadano y a los órganos u organismos públicos emisores de notificaciones telemáticas.

Otras entidades que intervienen en el proceso son las Autoridades de Certificación, que generan los certificados digitales de componentes, empresas o particulares empleados por emisores, Correos y usuarios finales. El sistema basa los procesos de seguridad en la aplicación de certificados X.509 v.3 de las CAs integradas en el servicio.

El Real Observatorio de la Armada (ROA) interviene como proveedor de referencias para sellado de tiempo aplicable en las diferentes transacciones del sistema.

Solución técnica

La solución técnica del sistema se basa en una arquitectura, con tecnología Microsoft .NET, en tres capas; presentación con Servidores Web Microsoft IIS; Aplicación con Servidores COM+ (se ha incluido el servicio de Fechado electrónico); datos con Buzones Exchange, SQL Server 2000, Microsoft Biztalk; Sistema OperativoWindows 2000 Advanced Server y Directorio Activo de Microsoft; e intercambio de información entre Emisores y Sistema de Notificaciones Telemáticas basado en XML, con protocolo de comunicación HTTPS.

En cuanto a seguridad del sistema, la firma electrónica avanzada de ciudadanos y emisores, basada en PKCS#7, proporciona integridad, autenticación y no repudio. Se emplea certificado digital particular X.509. v.3. La confidencialidad se realiza mediante el cifrado y empleo de canales seguros SSL1 a 128 bits, con HTTPS entre SNTS y el emisor, y entre SNTS y el ciudadano. Y el fechado electrónico de los mensajes que lo requieran se realiza vía ROA (Real Observatorio de la Armada).

Los requisitos que han de tener los puestos de los usuarios son los siguientes: Navegador MS Internet Explorer versión 5.5 o superior, Netscape 6.x o superior y Mozilla 1.6 o superior, así como tener activadas las opciones de seguridad para https; Acrobat Reader 5.0 o superior, para leer las notificaciones en formato PDF; descarga e instalación de los módulos de seguridad y certificado digital estándar X.509 v.3.

El organismo emisor genera una notificación a un usuario, que ha manifestado su voluntad para recibir notificaciones por medios telemáticos. Éstas son cifradas con una clave simétrica única y remitidas al Servicio de Notificaciones cifradas, mediante mecanismos de clave pública. ☒

Centro Criptológico Nacional.

Certificación de la seguridad de las TIC

Los productos y sistemas de TI deben llevar a cabo sus funciones, ejerciendo un control apropiado de la información que manejan, para asegurar su protección contra sucesos, como revelación no deseada, modificación o pérdida. El término seguridad de TI se utiliza, generalmente, para referirse tanto a la prevención como a la reducción de este tipo de sucesos.

Jaime Gotor, subdirector general adjunto del Centro Criptológico Nacional, explica que la Seguridad de las TIC agrupa al conjunto de medidas de seguridad (controles, salvaguardas, servicios o funciones, y mecanismos) para proteger la información almacenada, procesada o transmitida (manejada), por productos o sistemas de las tecnologías de la información. También incluye aquellas medidas que permiten la detección, documentación y contabilidad de las amenazas a la información y a los sistemas, de manera que no sólo se permita detectar los ataques sino también oponerse activamente o, en último caso, recuperarse de ellos.

Así, la seguridad de las TIC abarca los productos o sistemas de tecnologías de la información utilizados en los sistemas de comunicaciones y en los sistemas de información. También se incluye otro tipo de sistemas electrónicos como, por ejemplo, sensores, equipos de medida, sistemas de identificación, de navegación, etc, que manejan información muy específica.

La Seguridad de las TIC puede conseguirse protegiendo, adecuadamente, cada uno de los recursos y componentes de la configuración de los sistemas de información y comunicaciones. "La seguridad de los productos y sistemas de TI, por afectar y preocupar a diversos sectores de la sociedad, dispone de una amplia oferta de soluciones. Sin embargo, lo que es difícil, realmente, es saber si las soluciones de seguridad que existen son adecuadas. Pocas personas o entidades tienen la posibilidad de llegar a valorar la calidad de un sistema de seguridad. De la misma forma que los sistemas que manejan la información, los productos y sistemas de seguridad se han convertido en elementos populares pero, en general, no se conoce gran cosa de su composición, ni de su fiabilidad".

Gotor indica que muchos usuarios de TI carecen del conocimiento, experiencia y, sobre todo, de los medios necesarios para juzgar si su confianza en la seguridad de los productos o sistemas está justificada y pueden no querer confiar sólo en las afirmaciones de los fabricantes. "Los usuarios necesitan, cada vez más, incrementar su confianza en las propiedades de seguridad de un producto o sistema de TI, ordenando un análisis de su seguridad, es decir, una Evaluación de Seguridad". Una Evaluación de la Seguridad de las TI es un análisis, realizado mediante un proceso metodológico, de la capacidad de un producto o sistema de las tecnologías de la información, para proteger las condiciones de la información, de acuerdo a unos criterios establecidos, todo ello con objeto de determinar si puede ser certificado.


Jaime Gotor.

Existen cuatro posibles certificaciones: Seguridad funcional de las TIC, Seguridad Criptológica, Seguridad de Emanaciones y Seguridad Física de los propios productos de seguridad de las TIC.

Una Certificación de la Seguridad de las TI es la determinación, realizada mediante un proceso metodológico, de la capacidad de un producto o sistema de las tecnologías de la información para proteger en profundidad las condiciones de la información, de acuerdo a unos criterios preestablecidos.

Certificaciones

Gotor señala que, en este ámbito, se pueden distinguir cuatro tipos de certificaciones: Certificación de la Seguridad funcional de las TI, Certificación de la Seguridad Criptológica, Certificación de la Seguridad de Emanaciones (TEMPEST) y Certificación de la Seguridad Física de los propios productos de seguridad de las TI.

La Certificación de la Seguridad de un producto o sistema de TI podrá requerir, dependiendo de la finalidad del propio producto, la obtención de una o varias certificaciones. Aquellos productos que deban ser certificados y no incluyan componentes criptológicas entre sus elementos, no requerirán la obtención de la certificación de la seguridad criptológica. Sin embargo, los productos que incluyan componentes criptológicas deberán obtener ambos certificados y en el orden correlativo en el que se han relacionado. En los casos en que se considere necesario, la certificación de la Seguridad de Emanaciones es requerida de forma explícita.

La certificación de la Seguridad Criptológica determina la capacidad de un sistema de cifra para proteger la información, con el nivel de seguridad adecuado, en todo momento de su vida útil. Esta certificación incluye verificar que el sistema de cifra implementa un algoritmo de cifra de robustez contrastada, que se manejan claves de calidad adecuada, que el sistema maneja correctamente el algoritmo y las claves, y que el sistema mantendrá estas características durante toda su vida útil.

La certificación de la Seguridad de Emanaciones (Tempest) determina la capacidad de un producto o sistema de TI de proteger la información que maneja contra la amenaza que supone la captación de las emanaciones electromagnéticas que cualquier producto de TI emite de forma involuntaria en su normal funcionamiento. Esta certificación supone verificar que las emanaciones del producto o sistema de TI están dentro de unos márgenes de seguridad establecidos en los criterios o normas de evaluación y, además, que el entorno físico, donde el producto o sistema es instalado, ofrece una atenuación de dicha emanación, dentro de unos márgenes de seguridad.

La certificación de la seguridad Física de los productos de las TI proporciona las evidencias necesarias sobre la seguridad del diseño e implementación hardware de los mecanismos de seguridad. "Dichas evidencias son fundamentales para la integridad de los mecanismos de seguridad, pilar clave en todo el edificio de seguridad asociado a un producto o sistema de TI." Uno de los estándares de referencia para llevar a cabo la evaluación de este aspecto específico de la STI es la norma americana FIPS Pub. 140-2 (ISO 19790, en desarrollo).

Luis Jiménez, responsable de la Unidad de Políticas de Seguridad de las TI del Centro Criptológico Nacional, explica que España tiene, razonablemente, buenas capacidades técnicas: evaluación *Common Criteria* de la seguridad, evaluación y certificación de la seguridad criptológica, evaluación y certificación de la seguridad de emisiones y valoración y acreditación de la STI

Básicamente, estas capacidades se concentran en el INTA, la primera de ellas, y en el Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI) el resto. "Sin embargo, la aplicación de estas capacidades y el uso del beneficio que pueden y deben generar en nuestro país no es tan amplio como sería deseable". ☒