

Protección de datos, política de seguridad, buenas prácticas y estándar ISO 17799 en el cumplimiento del RD 994/99

Fuente:

http://www.madrid.org/comun/datospersonales/0,3126,457237_458340_127535941_12489813_12489303_1,00.html

El empleo extendido de Internet y de las nuevas tecnologías en la sociedad actual ha dado lugar a una serie de nuevos riesgos que deben ser analizados y prevenidos adecuadamente, lo cual, junto al desarrollo de la administración electrónica, ha dado lugar al desarrollo de un importante número de normativas, estándares y recomendaciones de seguridad que inciden en la implantación de las buenas prácticas aplicadas a los procesos de desarrollo, gestión de los sistemas de información y control de los datos objeto de tratamiento.

Mar Martínez. Business Development Manager de SIA. Ex Subdirectora Gral. Registro General de Protección de Datos de la AEPD.

Tanto la Directiva 95/46/CE como la Ley Orgánica 15/99, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), prevén la obligación del *responsable del fichero* y del *encargado del tratamiento* de adoptar las medidas de índole técnica y organizativas que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que estén expuestos, ya provengan de la acción humana o del medio físico o natural, estableciéndose en el artículo 44.3.h) de la LOPD, que mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen constituye infracción grave en los términos previstos en la propia Ley.

El Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal (en adelante Reglamento), tiene por objeto el desarrollo de lo dispuesto en el artículo 9 de la LOPD y determina las medidas de índole técnicas y organizativas que garanticen la confidencialidad, integridad y disponibilidad de la información y establece las previsiones que deberán cumplirse en el tratamiento de datos personales, determinando la necesidad de adoptar las medidas de índole técnica y organizativas, calificadas de nivel básico, medio y alto, necesarias para garantizar la seguridad de los datos y evitar su alteración, pérdida, tratamiento o acceso no autorizado.

Para garantizar el cumplimiento de la normativa de Protección de Datos los responsables de ficheros y tratamientos, así como los encargados de tratamiento, en su caso, deben controlar quién accede a los datos y qué uso se hace de los mismos para garantizar el principio de finalidad e idoneidad. Asimismo, un nivel adecuado de seguridad es un requisito previo para poder implantar un sistema de información (SI) con las debidas garantías jurídicas.

Tanto el sector privado como el sector público han sido conscientes de la importancia de las Tecnologías de la Información (TI) para mejorar las relaciones entre todos los agentes que interactúan con sus SI y de esta manera aumentar la calidad de los servicios prestados, facilitando el acceso de los usuarios (Clientes, ciudadanos) a estos servicios interactivos por nuevos canales de comunicación. Por este motivo, es esencial fomentar el desarrollo de nuevos servicios de seguridad, que permitan dotar de confianza a las operaciones que se realicen por estos medios y garantizarlas en los términos de confidencialidad, disponibilidad, exactitud y auditabilidad requeridos por el marco jurídico.

La mayoría de los agentes que participan en las distintas actividades de la sociedad son conscientes de que no pueden seguir funcionando de forma aislada. La necesidad de compartir información en la nueva sociedad global, es otro de los indicadores que hace necesario que los

organismos públicos y las empresas actúen colaborando y cooperando y para ello es necesario integrar e intercomunicar la información y los servicios con las garantías necesarias de seguridad.

En este aspecto, Internet ha facilitado el acceso a la información, pero precisamente el uso de las nuevas tecnologías no puede incidir negativamente en otros derechos fundamentales como es el de la seguridad y la protección de datos. Asimismo, los responsables del tratamiento deben ser muy cuidadosos con los datos que tratan o comunican a terceros y deben garantizar en todas las fases del tratamiento el cumplimiento de medidas de seguridad en el tratamiento de los datos personales de los ciudadanos.

Asimismo, se deberán garantizar a todos los ciudadanos que los datos especialmente protegidos que tratan las Administraciones Públicas, únicamente se utilicen y cedan para aquellos fines para los que fueron recogidos y dentro de las previsiones que las leyes establecen, garantizando que los Sistemas de Información (SI) cumplen con todas las medidas de seguridad establecidas en la LOPD y en el Reglamento de seguridad con el fin de evitar la lesión de derechos fundamentales.

Por otro lado, el ciudadano debe encontrar la información que demanda de los poderes públicos, poder tramitar sus peticiones y cumplir con sus obligaciones con un grado de fiabilidad y garantías en la utilización de estos nuevos canales de comunicación. Así lo ha determinado a su vez nuestro Tribunal Constitucional indicando que la Administración no debe verse ajena a esta nueva realidad.

La existencia de autoridades de protección de datos en cada uno de los estados miembros de la UE garantiza a los ciudadanos sus derechos en relación con el uso de sus datos personales. Estas entidades son independientes de los poderes públicos y velan por que se cumpla las garantías exigidas por el marco jurídico en el tratamiento de datos personales.

Asimismo, las funciones de verificación y control que las autoridades de protección de datos tienen asignadas por las leyes vienen a reforzar y afianzar la confianza de los ciudadanos respecto al tratamiento de sus datos personales y especialmente aquellos datos que por su especial sensibilidad tienen que ser especialmente protegidos por las Administraciones Públicas y entidades que los usen, y garantizar que - únicamente se utilicen y cedan para aquellos fines para los que fueron recogidos y dentro de las previsiones que las leyes establecen, garantizando que los Sistemas de Información (SI) cumplen con todas las medidas y previsiones establecidas - con el fin de evitar la lesión de derechos fundamentales.

Los ciudadanos deben conocer sus derechos, entre estos está la posibilidad de ejercer el derecho de acceso y poder conocer los datos personales que sobre ellos pueda estar tratando una empresa o administración pública.

La incorporación de las TIC en todos los entornos de la sociedad favorecen la universalidad y la equidad en el acceso a los servicios, mejora la atención continua al ciudadano y amplía la eficacia de los recursos públicos y privados disponibles, lo que permite nuevos modelos de relación entre las personas y las organizaciones. El tratamiento de datos personales, exige el cumplimiento de unas garantías que permita afirmar que los datos de los ciudadanos están protegidos y cumplen el marco jurídico que la normativa europea y española establece.

Para garantizar el cumplimiento de la normativa de Protección de Datos los responsables de ficheros y tratamientos deben controlar quién accede a los datos y qué uso se hace de los mismos para garantizar el principio de finalidad. Asimismo, un nivel adecuado de seguridad es un requisito previo para poder implantar un sistema de información (SI) que trate datos personales.

Claramente la sociedad plantea nuevas demandas que deben de tratarse desde una perspectiva más amplia. No se solicita un cambio de la cobertura de los servicios al ciudadano sino que se esperan nuevos y mejores servicios. Para el funcionamiento real de este pilar básico, se necesita disponer de un soporte de comunicaciones seguro y de suficiente capacidad para abastecer a todos los Sistemas de Información en los grandes sectores de los servicios públicos, salud, cultura, justicia, etc.

Todas estas circunstancias han incidido en los últimos años para que la seguridad de los SI esté requiriendo una atención especial. El uso generalizado de Internet, como comentamos, produce nuevos riesgos, inherentes a los nuevos canales de comunicación, a las herramientas informáticas utilizadas y a su uso malintencionado. Estos riesgos deben ser analizados y prevenidos adecuadamente ya que pueden causar graves trastornos y daños en las organizaciones. En este sentido, y paralelamente al desarrollo de la administración electrónica, han surgido un número muy importante de normativas, estándares y recomendaciones de seguridad que inciden en la implantación de las buenas prácticas aplicadas a los procesos de desarrollo, gestión de los sistemas de información y control de los datos objeto de tratamiento.

Un sistema basado en **normativas y estándares** reconocidos, que sea aplicable, que se pueda mantener, evaluar en la operación del día a día y que al final de proceso, permita obtener la certificación, **es una garantía del cumplimiento** de los principios de seguridad en el tratamiento de datos personales. Dicho sistema refuerza a su vez, la confianza del responsable del tratamiento en sus obligaciones del cumplimiento del resto de los principios de protección de datos.

Las medidas de seguridad deberán garantizar, un nivel apropiado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse. Como es conocido por todos, en la reglamentación Española, las medidas se clasifican en los tres niveles de seguridad: básico, medio y alto.

Cuando los sistemas incluyan, comuniquen o traten datos calificados por la LOPD como datos sensibles (datos de salud, vida sexual, origen racial, filiación política o sindical, convicciones filosóficas o políticas), las medidas tendrán que ser reforzadas dependiendo no solo de la sensibilidad de los datos tratados sino del número de afectados que se incluyen en el sistema, así como del grado de distribución y comunicación de los datos entre distintos agentes o responsables de su tratamiento (interoperabilidad entre redes, redes paneuropeas, usos y finalidades para garantizar derechos de terceros, federación de identidades). En suma, sistemas de información compartidos o en el límite de lo que podía considerarse compatible con el principio de finalidad en la recogida de los datos.

Podemos citar a modo de ejemplo casos tan paradigmáticos como los sistemas de información que tratan datos relativos a la historia clínica electrónica compartida y sus mecanismos de acceso, datos genéticos, identificación por radiofrecuencia, video vigilancia, seguridad y prevención de delitos, acceso por autoridades de terceros países en las bases de datos de reservas en transportes, retención de datos en telecomunicaciones, etc.

En este tipo de sistemas, además de cumplir con las previsiones legales, será recomendable implantar medidas tecnológicamente robustas, que los marcos normativos no pueden regular o aplicar recomendaciones y buenas prácticas aceptadas de facto por las organizaciones sectoriales y por las autoridades de protección de datos en sus Grupos de Trabajo (GT ART. 29), Foros y Conferencias de Autoridades de Protección de Datos internacionalmente reconocidas, así como adoptar sectorialmente las denominadas "políticas de privacidad" o códigos de buenas prácticas en materia de seguridad y privacidad. En este sentido, es muy recomendable la utilización de los estándares en materia de buenas prácticas de gestión de la seguridad de la información ISO 17799.

Por este motivo, el sector de las tecnologías están potenciando y fomentando, junto con la implantación de medidas tecnológicas de seguridad, el desarrollo de nuevos servicios de seguridad, entre los que se encuentran : **Planes Directores de Seguridad, Sistemas de Gestión de la Seguridad de la Información (SGSI), Oficinas de Seguridad, Herramientas Automatizadas de cumplimiento**, que permitan garantizar a todos los sujetos que interactúan con sistemas de información (servicios públicos, empresas, profesionales, ciudadanos) los principios de seguridad en términos de confidencialidad, disponibilidad, exactitud y auditabilidad requeridos por el marco jurídico, y a su vez, faciliten el acceso autorizado de éstos sujetos a la información y a los servicios interactivos a través de Internet.

A continuación se expondrá una breve introducción a los **Sistema de Gestión de la Seguridad de la Información (SGSI)** con el objeto de dejar esbozados las bases que permitan afirmar que existe un paralelismo entre la fase de Análisis de Riesgos y Cumplimiento UNE-ISO/IEC 17799 con las previsiones establecidas en el Reglamento de Seguridad RD 994/99.

El SGSI conforma el ciclo de mejora continua de la Gestión de la Seguridad de la Información para dar cobertura al marco jurídico de obligado cumplimiento y a los requerimientos y necesidades de las políticas de privacidad aprobadas en la organización, ya sea en el ámbito de un sector determinado o de un gran grupo multinacional, y de esta manera establecer los controles y procedimientos para su continua actualización. A su vez, como objetivo final la definición de un Sistema de Gestión de la Seguridad prepara a una organización para abordar la certificación de su sistema conforme a la UNE 71502.

El objetivo de la Gestión de la Seguridad es conseguir alinear la seguridad de la Información con los Planes Estratégicos de la Organización .Al mismo tiempo, se incluye como objetivo final la posibilidad de que la dirección de la organización, posea una herramienta de mejora continua que permita la continuidad de la aplicación de las políticas y objetivos de Seguridad de la Información.

El SGSI aporta las siguientes ventajas a una Organización:

- Establece una **metodología** de seguridad clara y estructurada.
- **Reduce riesgos** y proporciona mecanismos de reacción temprana ante ataques.
- **Automatización** de actividades de SI (Workflows, procedimientos).
- Incremento de la **concienciación** respecto a la seguridad de la Información.
- La seguridad de la información queda alineada con el **marco jurídico** exigible, la **estrategia de la organización** y con normas y buenas prácticas reconocidas.
- Garantiza el **valor añadido** de las actividades de seguridad así como de la inversión realizada (ROI).
- Conformidad con los **requisitos legales**.
- Reconocimiento y mejora de la imagen corporativa (Aumento de Confianza).
- Mejora de la gestión de la **continuidad del negocio**.
- Incorpora actividades para la **mejora continua** (procesos y actividades de revisión, auditorias, etc.).

La implantación de un SGSI se estructura en un conjunto de fases y tareas que comprende, entre otros aspectos: La política de seguridad, la estructura organizativa, los procedimientos, los procesos, los recursos necesarios y los planes de formación y concienciación.

Una vez definidos el entorno y preparada la definición del Plan se inicia la fase de Análisis de Riesgos y Cumplimiento UNE-ISO/IEC 17799. En esta fase, se debe tener en cuenta las previsiones establecidas en el Reglamento de Seguridad RD 994/99.

- Se realizará una evaluación periódica del nivel de adecuación a la UNE-ISO/IEC 17799 y al RD 994/99 según se vayan desarrollando las distintas fases de construcción del sistema. Esta tarea se basará en el análisis de la información obtenida en las entrevistas, cumplimentación de cuestionarios, así como estudio de documentación existente.

- El análisis de vulnerabilidades, además de comprobar el cumplimiento de las medidas establecidas en la normativa jurídica de obligado cumplimiento, comprueba la utilización de las recomendaciones, normas, procedimientos y políticas de la organización así como de las buenas prácticas que indica el estándar UNE-ISO/IEC 17799.

En este sentido, se puede establecer un paralelismo entre las previsiones del Reglamento de Seguridad en vigor y las secciones que marca la norma UNE-ISO/IEC 17799:

- **Política de Seguridad:** la política de seguridad existente en la organización, así como su alcance, objetivos, etc. ***Se podría alinear con la previsión del documento de seguridad establecido en el Art. 8 RD 994/99.***

- **Aspectos organizativos para la seguridad:** la estructura organizativa y su implicación en la gestión de la seguridad de la información. ***Art. 8.2 b) Medidas, normas, procedimientos reglas y estándares***

- **Clasificación y control de activos:** inventarios y la clasificación de la información existente para proteger los activos. ***Art.8.2 a) Ámbito de aplicación y recursos protegidos***

- **Seguridad ligada al personal:** medidas existentes para evitar los riesgos de errores humanos, robos, fraudes o mal uso de instalaciones y servicios. ***Art.9 Funciones y obligaciones del personal***

- **Seguridad física y del entorno:** las medidas existentes para el control del acceso a las instalaciones, locales y recursos. ***Art.19 Control Acceso Físico***

- **Gestión de comunicaciones y de operaciones:** este apartado cubre el estudio de las tareas, responsabilidades y procedimientos necesarios para la correcta utilización de los recursos de tratamiento de la información. ***Art.5 Acceso a datos a través redes comunicaciones, Art.26 Telecomunicaciones***

- **Control de accesos:** qué medidas se toman en la organización para controlar el acceso la información sobre la base de los requisitos de negocio. ***Art.11,12 y 18 Identificación y Autenticación, Control de acceso, Art. 24 Registro de accesos***

- **Desarrollo y mantenimiento de sistemas:** se analizará hasta que nivel la seguridad se encuentra imbuída en todas las fases del ciclo de vida de los sistemas de información. ***Art.22 Pruebas datos reales, Ficheros temporales***

- **Gestión de la continuidad del negocio:** se estudiarán las medidas que se tienen previstas con vistas a mantener las operaciones ante interrupciones imprevistas, así como las que

permitirán volver a la situación normal. **Art. 14 y 25 Copias respaldo y recuperación. Art. 13 y 20 Gestión de soportes**

- **Conformidad legal y de normativas:** la normativa ISO-17799 contempla el análisis de las medidas existentes para el cumplimiento de las obligaciones legales y normativas de la organización. **RD 994/99**

Conclusiones

Es obvio resaltar que el uso de los medios y técnicas telemáticas se tiene que hacer de conformidad con lo dispuesto en la LOPD y en el Reglamento de Seguridad. Lógicamente, implantar medidas de protección de datos y de seguridad por fichero o tratamiento en organizaciones complejas, además de ser caro y complicado, no permite garantizar la seguridad de los sistemas e infraestructuras de red, servidores de aplicaciones, bases de datos y directorios activos.

Estos elementos forman parte de un todo y cada uno de ellos es de vital importancia en la seguridad. La protección de datos y la seguridad se deben diseñar conjuntamente en un producto que se pueda integrar con las infraestructuras y Sistemas de Información.

Los sistemas van a necesitar de un proyecto integral y continuo de adecuación a la normativa de protección de datos y seguridad. Hay que recordar que la seguridad no es un estado sino un proceso.

La tecnología debe ayudar a garantizar la intimidad de los datos personales en todo el ciclo de vida: desde su obtención, tratamiento, archivo, custodia y transmisión de la información y la documentación. De ahí que, los responsables de tratamiento y los encargados garanticen que sus SI se desarrollan y explotan con las medidas de seguridad y pautas de conducta que permitan confirmar el cumplimiento de las obligaciones en materia de protección y seguridad de los datos personales, que debe asegurarse en condiciones de respeto a la intimidad personal y a la libertad individual de las personas, garantizando la confidencialidad de sus datos personales.