ISO/IEC 27001:2005 & LOPD

ISO-27000 ES UN PILAR FUNDAMENTAL E IMPRESCINDIBLE PARA ACOMETER TODOS LOS CAMBIOS

Alejandro Corletti

DIRECTOR DIVISIÓN SEGURIDAD INFORMÁTICA

NCS

Carmen de Alba Muñoz

RESPONSABLE ISO-27000

NCS

El desarrollo tecnológico que estamos viviendo (y a veces sufriendo) en los últimos años, ha obligado al gobierno a modificar de forma importante algunos aspectos del derecho, al producirse situaciones desconocidas hasta ahora y que cada vez se repiten más a menudo. A día de hoy, la utilización de datos de carácter personal es uno de los pilares fundamentales para el desarrollo de las Administraciones Públicas.

En el Consejo de Ministros del 21 de diciembre del pasado año, se aprobó, entre muchas otras cosas, un Real Decreto por el que se ratifica el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre de protección de datos de carácter personal. Es evidente, que con este nuevo Reglamento, lo que se persigue es aumentar el nivel de protección de los datos personales, tratando de cubrir ciertas lagunas que han aparecido en estos últimos años.

Hay dos puntos que, si los tratamos de relacionar con la familia ISO-27000 debemos considerar especialmente: el primero es que hay una serie de **datos que suben de nivel básico a medio o a alto**.

El segundo punto, es que **todos los ficheros no automatizados (soporte papel) deberán disponer de medidas de seguridad**. Revisemos cómo se clasifican los ficheros en los diferentes niveles de seguridad existentes (básico, medio y alto) según éste nuevo Reglamento.

> El hecho de tener que revisar y reclasificar todos los ficheros es una tarea pesada

Los ficheros de **nivel básico**, son aquellos que contengan datos de carácter personal.

Los ficheros que pasan a ser de **nivel medio** son:

- Comisión de infracciones administrativas o penales.
- Hacienda Pública.
- Servicios financieros cuyo funcionamiento se rija por el artículo 29 *Presentación de Servicios de Información Sobre Solvencia Patrimonial y Crédito* de la Ley Orgánica 15/1999.
- Ficheros de las Entidades Gestoras y Servicios Comunes de la Seguridad social que tengan relación con sus competencias y las mutuas de accidentes de trabajo y de enfermedades profesionales de la Seguridad Social. **¡¡¡NUEVO!!!**
- Ficheros que contengan datos de carácter personal sobre características o personalidad de los ciudadanos que permitan deducir su comportamiento. **¡¡¡NUEVO!!!**
- Ficheros de los que son responsables los operadores de servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas sobre datos de tráfico y localización, exigiéndose a los operadores el establecimiento de un registro de acceso a tales datos para determinar quien ha intentado acceder a dichos datos, fecha u hora en que se ha intentado el acceso, y si ha sido autorizado o denegado. **¡¡¡NUEVO!!!**

Los Ficheros de **nivel alto**, son aquellos que contienen datos relativos a:

- Ideología, religión, creencias, origen racial, salud o vida sexual.
- Datos recabados para fines policiales sin consentimiento de las personas afectadas.

ISO-27000 va más allá de "cumplir" una medida, es un SGSI completo

■ Datos derivados de la violencia de género. **¡¡¡NUEVO!!!**
■ Todos los ficheros de nivel alto que estén almacenados en dispositivos portátiles deben ser cifrados. **¡¡¡NUEVO!!!**

Dependiendo del tipo de datos de carácter personal que contengan los ficheros, se deben adoptar una serie de medidas de seguridad que especifica el Real Decreto 994/1999 *Reglamento de Medidas de Seguridad de los Ficheros Automatizados que Contengan Datos de Carácter Personal*. Una de las novedades de este nuevo Reglamento, es que las medidas de seguridad se extienden también a los ficheros no automatizados (en soporte papel), fijando medidas de seguridad específicas para tratar dichos ficheros que se resumen en:

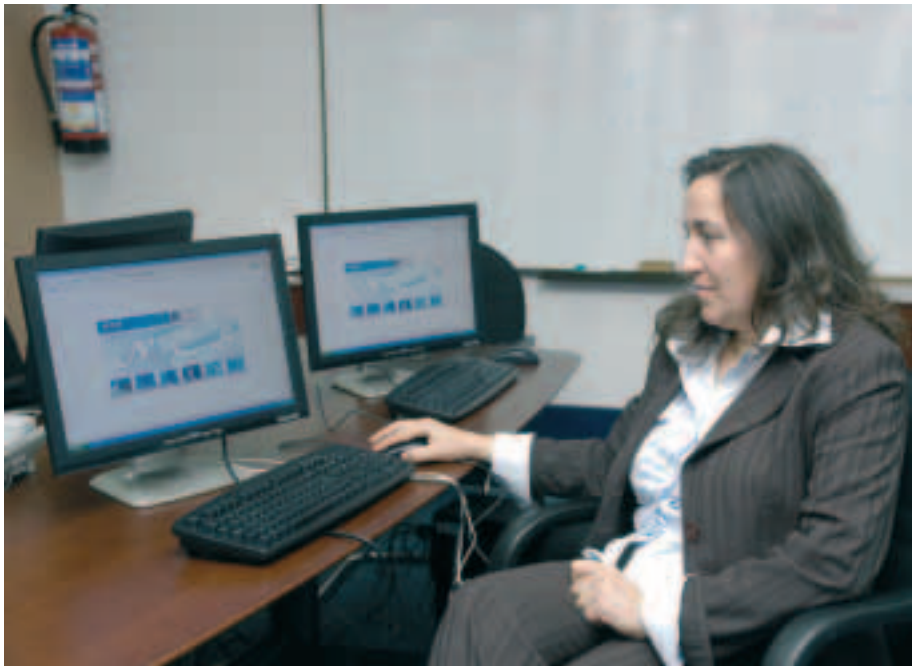
■ Se exigirá la aplicación de unos criterios de archivo que garanticen la correcta conservación de los documentos y el ejercicio del derecho de oposición al tratamiento, rectificación y cancelación de los datos.
■ Los armarios, archivadores y demás elementos de almacenamiento, deberán disponer de mecanismos adecuados de cierre (llave) que impidan el acceso a la documentación por personas no autorizadas. Mientras esa documentación no esté archivada, la persona que esté a su cargo deberá custodiarla, impidiendo que acceda a ella quien no esté autorizado.
■ Cuando estos ficheros contengan datos incluidos en un nivel de seguridad alto (ideología, afiliación sindical, religión, creencias, origen racial, salud, vida sexual, datos recabados por la policía sin consentimiento de los afectados o actos derivados de violencia de género), deberán estar en áreas cerradas con el dispositivo de seguridad pertinente (puertas con llave), pero, si por las características de los locales, no puede cumplirse esta medida, se permite aplicar otra alternativa que impida a las personas que no están autorizadas el acceso a esta documentación.

¿Qué debemos hacer para adaptarnos a este nuevo Reglamento?, ¿Qué relación tiene esto con la ISO-27000? Comencemos tratando de responder a la primera pregunta: ¿Qué hacer? La respuesta

Artículo del mes que viene:

"Tabla de controles ISO-27002 que aplican a LOPD"

En este artículo desarrollaremos con todo detalle, la explicación y requisitos de cada control, relacionado a los tres niveles de archivos de la LOPD.



parece sencilla a priori, habrá que revisar y reclasificar todos los ficheros (automatizados o no automatizados), e implementar las medidas de seguridad necesarias a aquellos ficheros que no cumplan con lo que establece el Reglamento.

El hecho de tener que revisar y reclasificar todos los ficheros tanto los automatizados como los no automatizados, es una tarea pesada tediosa, pero que no conlleva mayor complicación. Lo "entretenido" llega una vez que se han reclasificado los ficheros, ya que identificar los controles oportunos que aplican en función del nivel de seguridad que tenga el fichero no es tarea sencilla.

En NCS entendemos que **un mismo control tendrá requisitos diferentes dependiendo del nivel de seguridad que requiera el fichero.** Por ejemplo, cualquier fichero (ya sea de nivel básico, medio o alto), requiere que se efectúen procedimientos de copias de respaldo y restauración de los datos (artículo 14 y 25 del Real Decreto 994/1999); el control a aplicar de la norma ISO/IEC 27002:2005 sería el *10.5.1 Copias de Seguridad de la Información*. Mientras que un fichero de nivel alto exige guardar una copia de respaldo junto con sus procedimientos de recuperación de datos en un lugar diferente en el que se encuentran los equipos informáticos que procesan los datos del fichero, a los ficheros de nivel básico y medio no se le exige este requisito.

> Los ficheros de nivel básico, son aquellos que contengan datos de carácter personal

Este control que acabamos de citar, como mero ejemplo, representa claramente la importancia de "pensar" como ISO–27000. Si nos quedáramos sencillamente con el cumplimiento de esta novedad de LOPD, tal vez estaríamos cumpliendo con la misma. Pero ISO–27000 va más allá de "cumplir" una medida. ISO–27000, es un SGSI completo, por lo tanto, no nos basta con considerar un control aislado, sino que el mismo, como buena pieza de un verdadero ciclo dentro de un sistema, debe "cerrar" toda la maquinaria. Es decir, no nos basta considerar solamente "guardar la copia de respaldo en otro sitio y sus procedimientos", sino que además un SGSI completo, para una copia de respaldo de un archivo "CRITICO" debe:

- Llevar el registro de las personas que acceden a esta copia.
- Evaluar y llevar el control de las personas que deberían o no acceder al mismo.
- Dejar constancia del ciclo de vida de cada copia (creación, mantenimiento, modificaciones, destrucción, etc).
- Ejecutar ejercicios y simulaciones de recuperación, con las medidas de seguridad adecuadas.
- Realizar auditorías periódicas de su estado.
- Salvaguardar sus claves de acceso, y mantener actualizadas las mismas (este tema es muy vigente, por el acelerado avance en técnicas de criptoanálisis).

Lo que tratamos de ejemplificar en el párrafo anterior, es que en definitiva, para cada una de estas nuevas medidas, ISO–27000, va más allá de lo que dice la LOPD, por lo tanto, nos asegura, que no presentará flancos, ni debilidades a futuro por ser un "sistema completo".

Así como acabamos de desarrollar un control de la norma, podríamos abordar de la misma forma todos los que se relacionan con este nuevo reglamento relacionado a la LOPD. En este artículo, no podemos hacerlo con todo el detalle que quisiéramos (La tabla completa, se presentará en el artículo del mes que viene), pero como punta pie inicial, desde NCS queremos presentaros al menos la forma en que nosotros consideramos que se relacionan con estos cambios de la LOPD. El primero de los artículos a considerar es el siguiente:

FICHERO NIVEL BÁSICO	CONTROL DE LA ISO 27002	FICHERO NIVEL MEDIO	CONTROL DE LA ISO 27002	FICHERO NIVEL ALTO	CONTROL DE LA ISO 27002
Copias de Respaldo y Recuperación (ART. 14)		**Copias de Respaldo y Recuperación (ART. 14)**		**Copias de Respaldo y Recuperación (ART. 14, 25)**	
El Responsable del Fichero se encargará de verificar la definición y correcta aplicación de los procedimientos de realización de las copias de respaldo y recuperación de datos. **(1)**	**10.7.3** Procedimientos de Manipulación de la Información. **(2)** **ATRIBUTOS:** Auditorías de los procedimientos. Revisión de los procedimientos. Pruebas de recuperación de las copias. **(4)**	**Idem (1)** **Idem (3)**	**10.7.3** **Idem (2)** **ATRIBUTOS:** **Idem (4)**	**Idem (1)** **Idem (3)**	**10.7.3** **Idem (2)** **ATRIBUTOS:** **Idem (4)**
Los procedimientos establecidos deben garantizar su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción. **(3)**					
Se deben realizar copias de respaldo al menos semanalmente, salvo que en dicho periodo no se haya producido ninguna actualización de los datos. **(5)**	**10.5.1** Copias de Seguridad de la Información. **(6)** **ATRIBUTOS:** Copias efectuadas. **(7)**	**Idem (5)**	**10.5.1** **Idem (6)** **ATRIBUTOS:** **Idem (7)**	**Idem (5)**	**10.5.1** **Idem (6)** **ATRIBUTOS:** **Idem (7)**
				Se debe conservar una copia de respaldo y los procedimientos de recuperación de datos en un lugar diferente de aquél en que se encuentran los equipos informáticos que los tratan, cumpliendo siempre las medidas de seguridad exigidas	**10.7.1** Gestión de Soportes Extraíbles. **ATRIBUTOS:** Total copias existentes. Copias actualizadas. **10.7.2** Retirada de Soportes. **ATRIBUTOS:** Soportes eliminados.

Lo importante, para nosotros, es analizar cada tipo de archivo como parte de un SGSI, y por lo tanto, aplicar los pasos y controles, como cualquier otro de los 11 grupos de controles de la norma.

No nos cabe duda, de que ISO–27000 es un pilar fundamental e imprescindible para acometer todos estos cambios. La decisión de elevar el rango de ciertos datos de los ciudadanos, **obliga a las Administraciones Públicas a comprometerse con el estándar ISO/IEC 27001:2005** ya que son éstas las principales usuarias de los mismos (datos de violencia de género, datos relativos a la salud, fiscales, judiciales, etc…). Esto no hace más que reafirmar lo que escribimos en el artículo del mes pasado, pues evidentemente todos estos cambios, son planteados y diseñados por personas muy afines a esta norma y que saben muy, pero muy bien, que la seguridad de un mero archivo, no puede ser tratada como algo aislado, sino que forma parte de toda una infraestructura de seguridad, sino no tiene sentido, y cualquier infraestructura de seguridad hoy debe ser SÍ o SÍ bajo el esquema de ISO/IEC 27001:2005.