

Esquema Nacional de Seguridad, ¿seguridad en Administraciones Públicas?

Ya han pasado las duras navidades y es hora de ponerse manos a la obra. 2010 se presenta como el año de la consolidación de la ISO 27001 como la norma de gestión "de moda" y como no podía ser de otra manera la Administración Pública no quiere quedarse atrás, y más si tenemos en cuenta los tiempos que corren, en los que la e-Administración empieza a tener peso entre los ciudadanos y los problemas de seguridad derivados de su uso masivo aún no han despertado.

¿Cómo se puede ser proactivo en lugar de reactivo?: adelantándose a los acontecimientos, por supuesto. Para ello ya tenemos el proyecto de Real Decreto que nos da un borrador de lo que será en un futuro muy muy próximo el **Esquema Nacional de Seguridad** (ENS), aprobado ya en Consejo de Ministros y esperemos que publicado en el B.O.E. cuando uds. lean este artículo.

¿Lo qué?, si si, el **Esquema Nacional de Seguridad**. Pero... ¿y eso qué es lo que es?, pues... por decirlo así llanamente es la ISO 27001 personalizada para las administraciones públicas (AAPP). Am... ¿ISO 27000 qué? Mejor que lo explique el propio ENS:

"La finalidad del Esquema Nacional de Seguridad es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones Públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios. El Esquema Nacional de Seguridad persigue fundamentar la confianza en que los sistemas de información prestarán sus servicios y custodiarán la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar al conocimiento de personas no autorizadas".

Ahora si.

Se podrían escribir ríos de tinta sobre el ENS, pero hoy nos centraremos en conocer su contexto, a quién aplica y las



principales diferencias con la ISO 27001. En próximos artículos desgranaremos punto por punto aquello que se considere más interesante.

Su contexto ya lo conocemos, nace con el objetivo de implantar un sistema de gestión de seguridad de la información (SGSI) en las AAPP. Para ser más exactos, el propio ENS en su artículo 1 nos lo aclara mucho mejor:

"1. El presente real decreto tiene por objeto regular el Esquema Nacional de Seguridad establecido en el artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, y determinar la política de seguridad que se ha de aplicar en la utilización de los medios electrónicos a los que se refiere la citada ley.

2. El Esquema Nacional de Seguridad está constituido por los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información. Será aplicado por las Administraciones Públicas para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias".

El artículo 2 consta de definiciones y el 3 del ámbito de aplicación. En el 4 (dentro ya del capítulo II de "Principios básicos") se referencian los principios básicos de seguridad del ENS, detallados entre los artículos 5 y 10. En el capítulo 3 ("Requisitos mínimos") se dice que todas las AAPP deben tener una política de seguridad que contenga una serie de apartados, que son desarrollados entre los artículos 11 y 30. Lo apartados son:



- a) Organización e implantación del proceso de seguridad.
- b) Análisis y gestión de los riesgos.
- c) Gestión de personal.
- d) Profesionalidad.
- e) Autorización y control de los accesos.
- f) Protección de las instalaciones.
- g) Adquisición de productos.
- h) Seguridad por defecto.
- i) Integridad y actualización del sistema.
- j) Protección de la información almacenada y en tránsito.
- k) Prevención ante otros sistemas de información interconectados.
- l) Registro de actividad.
- m) Incidentes de seguridad.
- n) Continuidad de la actividad.
- o) Mejora continua del proceso de seguridad.

Buena pinta tiene, no parece que se haya olvidado nada.

El capítulo IV versa sobre cómo se deben gestionar de forma segura las comunicaciones electrónicas y el capítulo V aporta una de las principales novedades: deben hacer auditorías cada 2 años (como cuando tenemos nivel medio o alto en LOPD). El informe debe contener la misma estructura que el de LOPD.

En el capítulo X se establecen diversos niveles de "Información administrati-



va" en función del perjuicio que tendría sobre el procedimiento administrativo o sobre los intereses de las personas afectadas una revelación no autorizada de la misma. Tenemos nivel alto, nivel medio, nivel "no divulgable" y nivel "público".

En el Anexo I tenemos las pautas para clasificar, otra vez en tres niveles (bajo, medio y alto) un sistema de información en función de la información administrativa (vista antes) que posea.

En el Anexo II tenemos las anheladas medidas de seguridad, que se organizan por niveles, algo muy acertado. Así, una AAPP que tenga un sistema de información clasificado como "Bajo" no tendrá que implantar las mismas medidas de seguridad que uno clasificado como "Alto" y las que tenga que implantar serán menos exhaustivas. Ejemplo: en nivel bajo no hará falta tener un plan de continuidad de negocio.

El Anexo III nos explica todo lo relativo a las auditorías bienales que hay que realizar. Lo más destacable es que para nivel "Bajo" no hay que realizar una auditoría, pero si un informe de auto-evaluación.

Y ahora, como opinión personal y teniendo en cuenta la experiencia en Audisec durante estos años, me parece que el ENS es un acierto se mire como se mire, incluso tiene partes que la propia ISO 27001 debería envidiar y adoptar cuanto antes. Ahora sólo falta que las AAPP lo acojan con los brazos abiertos, ya que ganaremos todos y como decía al principio, es la mejor forma de ser proactivos y no reactivos. Y además, gracias al ENS haremos las cosas de forma gradual y coherentemente respecto al tipo de información que manejemos. Todo un acierto. Y será una forma más de impulsar la cultura de seguridad en el resto de sectores.

Hasta aquí la parte menos técnica del ENS, el mes que viene más y posiblemente mejor. Hablaremos sobre las medidas de seguridad del anexo II y su aplicación práctica. No os lo perdáis, promete.

Mientras tanto quiero consultas en mi buzón. 