

El Esquema Nacional de Seguridad ya está con nosotros

En el BOE del pasado viernes 29 de enero se publicó del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad, que como ya hemos dicho otras veces, es la **ISO 27001** orientada a las administraciones públicas (AAPP).

Hay bastantes cambios de redacción si lo comparamos con el borrador, y hay cambios más profundos, destacando el hecho de que ya no habrá que definir niveles de "información administrativa", que se relacionaban directamente con la valoración de la confidencialidad, lo cual derivaba en la clasificación del sistema de información. Lo que habrá que hacer será clasificar el sistema de información basándose en "el impacto que tendría sobre la organización un incidente que afectara a la seguridad de la información o de los sistemas".

Ámbito de aplicación: en el artículo 30 se especifica claramente que los sis-

temas no afectados serán aquellos "no relacionados con el ejercicio de derechos ni con el cumplimiento de deberes por medios electrónicos ni con el acceso por medios electrónicos de los ciudadanos a la información y al procedimiento administrativo, de acuerdo a lo previsto en la Ley 11/2007, de 22 de Junio". Traducción: **no será de aplicación para aquellas AAPP que no hagan e-Administración.**

En cuanto a los plazos, los nuevos sistemas que se vayan a implantar en las AAPP y que estén dentro del alcance de este Real Decreto tendrán que estar adecuados al ENS "desde su concepción". **Para los sistemas ya existentes habrá un plazo de adecuación de 12 meses, prorrogable a 48 meses** (cuatro años) por causas que deberán ser debidamente justificadas.

Entrando en materia técnica, que es para lo que se ha escrito este artículo, tenemos un fenomenal Anexo II con todas las medidas de seguridad divididas en tres categorías:



Alejandro Delgado Gallego
Responsable de Proyectos ISO 27001
Audisec

				mp.si	Protección de los soportes de información
C	aplica	=	=	mp.si.1	Etiquetado
I	n.a.	aplica	+	mp.si.2	Criptografía
categoria	aplica	=	=	mp.si.3	Custodia
categoria	aplica	=	=	mp.si.4	Transporte
C	n.a.	aplica	=	mp.si.5	Borrado y destrucción

- Marco organizativo.
- Marco operacional.
- Medidas de protección.

En total **75 medidas de seguridad**. Pueden parecer pocas si se comparan con las 133 de la ISO 27001, pero hay que especificar que cada una de esas 75 medidas a su vez se suelen dividir en varias, y a su vez tienen diferentes intensidades o "niveles de madurez" en función de la categoría del sistema de información que estemos tratando. Lo podemos ver con un ejemplo para las medidas que el ENS establece para los soportes de información:

Podemos ver en primer lugar que se trata del dominio de medidas de protección ('mp') y que estamos en el objetivo de control "Protección de los soportes de información", que tiene cinco controles de seguridad. El 1, 3 y 4 afectan a todos los sistemas de información; el 2 (criptografía) afecta a partir de nivel medio y se intensifica para nivel alto; el 5 aplica por igual a nivel medio y a nivel alto, no aplicando a nivel bajo (que no 'básico' como en la LOPD). Además vemos que el 1 afecta a la confidencialidad ('C'), al igual que el 5. El 2 afecta tanto a la confidencialidad como a la integridad ('I'). El 3 y el 4 afectan a todas las dimensiones, de ahí que ponga un genérico 'categoría'.

En este caso concreto la intensificación del control de criptografía es:

- Usar algoritmos acreditados por el Centro Criptológico Nacional.
- Que se empleen, preferentemente, productos certificados.

De este modo hemos visto como trabaja el ENS con las diferentes categorías de sistemas de información y como divide y subdivide los 75 controles y sus apartados en función de esos niveles.

¿Qué diferencias podemos encontrar respecto a los controles de la 27001?

- Nuevos controles que la 27001 no contempla específicamente, como son los de custodia y transporte de soportes, que si bien pueden ser extrapolados de

otros controles, no están tan claramente definidos. También nos encontramos con la necesidad de hacer un BIA (análisis de impacto en el negocio) o de montar un IPS (sistemas de prevención de intrusiones) a partir de nivel medio y alto respectivamente. No es que estas medidas de seguridad no se implanten con ISO 27001, es que no eran obligatorias y ahora sí lo son, lo cual cambia bastante la situación. Podemos destacar también como novedades controles de firma electrónica, de gestión de la configuración (¿CMDB de ISO 20000?) y un sospechoso "Instalaciones alternativas" que ya analizaremos más despacio. Hay más novedades, y algún control de la 27001 que en principio se echa de menos, pero que seguro que como he dicho antes, podremos extrapolar de otros controles.

- El hecho de que los controles tengan niveles de madurez o de intensidad en función del nivel del sistema de información sobre el que deben aplicarse.
- Las auditorías (en nivel medio y alto) son cada dos años.

Hay más diferencias de menor importancia; ya las descubriremos poco a poco.

Para el mes que viene haremos un repaso general a los dominios y objetivos de control, desgranando cada uno de ellos en los aspectos más interesantes, centrándonos sobre todo en aquellos que resulten novedosos y/o particulares.

Así que ya sólo queda una cosa por hacer: ponerse a trabajar. ●

¿Qué diferencias podemos encontrar respecto a los controles de la 27001?

