

ENS. Tengo el plan de adecuación. ¿Qué me falta?

COMO casi todo el mundo sabe para el día 30 de enero todas aquellas Administraciones Públicas (AAPP) que estaban bajo el alcance del paraguas del Esquema Nacional de Seguridad (ENS) debían, al menos, haber elaborado el famoso plan de adecuación para demostrar al mundo que esto del ENS se lo van (y hablo en futuro) a tomar en serio.

No es muy difícil saber qué debe tener el plan de adecuación, si consultamos la web del Centro Criptológico Nacional (<https://www.ccn-cert.cni.es>) y nos vamos a la parte del ENS, y dentro de él a la guía de implantación "CCN-STIC-806" veremos con detalle qué debemos hacer para elaborar dicho plan. A grandes rasgos es lo siguiente:

- 1.- La política de seguridad
- 2.- Información que se maneja, con su valoración
- 3.- Servicios que se prestan, con su valoración
- 4.- Datos de carácter personal
- 5.- Categoría del sistema
- 6.- Análisis de riesgos
- 7.- Declaración de aplicabilidad de las medidas del anexo II del ENS
- 8.- Insuficiencias del sistema
- 9.- Plan de mejora de la seguridad.

Todo ello bien detallado en la propia guía 806 y en el resto, que prestan gran ayuda a la hora de abordar la implantación real del ENS.

¿Cómo debe ser ese plan? Lo mínimo que se debería pedir a aquellas AAPP que lo hagan es que lo hagan con plazos e hitos REALISTAS; que se tomen en serio el ENS y piensen bien qué capaci-

dad tanto técnica como humana van a tener hasta el 30 de enero de 2014 (plazo final para todo el mundo para cumplir con todos los requisitos).

Pensemos ahora que ya hemos elaborado nuestro plan.

¿Qué tenemos que hacer ahora? Esa pregunta mucho me temo que aún no se la ha planteado casi nadie.

Hay dos opciones:

1.- Esperar. No cumplir el plan al menos de momento y ver si la situación económica mejora y hay más recursos para en el último año hacer un gran sprint e implantar todas las medidas de seguridad y gestión detalladas en el plan.

2.- Actuar. Hacer un plan realista y colocar en primera posición aquellas medidas que son asumibles en tiempo y recursos y en años sucesivos aquellas que a día de hoy son inabordables. La mayoría de medidas a implantar son técnicas, aunque hay algunas de carácter organizativo, que darán forma a todo el ENS en su conjunto.

¿Sólo quedaría eso?, ¿cumplir el plan? Si somos puristas prácticamente sí, aunque faltaría dar cumplimiento a los artículos que están fuera de lo que serían las medidas del Anexo II, que representan un porcentaje de proyecto pequeño respecto al cumplimiento de esas medidas, y que incluso podrían incorporarse como hitos a cumplir dentro del plan de adecuación, matando dos pájaros de un tiro.

Pero como he comentado en otras ocasiones debería perseguirse otro obje-



tivo que no fuese sólo el cumplimiento del plan de adecuación: implantar, además de los requisitos del ENS, un Sistema de Gestión de Seguridad de la Información (SGSI) cogiendo lo mejor del estándar internacional ISO 27001. No es más costoso ni mucho menos que la



¿Todo el mundo ha hecho ya su plan de adecuación? Me temo que no... y el tiempo, aunque parezca mentira, se nos echará encima una vez más...

mayoría de requisitos del ENS, ya que simplemente se trata de reforzar con una "capa de gestión" algunos controles que quedan un tanto inmaduros si se les compara con los que podemos encontrar en el estándar ISO. Prácticamente sería transparente y los beneficios obtenidos serían mucho mayores que con un ENS "a secas".

¿Todo el mundo ha hecho ya su plan de adecuación? Me temo que no... y el tiempo, aunque parezca mentira, se nos echará encima una vez más...

En enero de 2014 os lo digo. ●