

Luces y sombras en el Esquema Nacional de Seguridad

Mucho se ha escrito ya sobre el Esquema Nacional de Seguridad (de aquí en adelante el ENS) pero pocos son los que se lo han leído y menos los que se han parado a comprenderlo.

Recuerdo que cuando nos explicaban técnicas de estudio nos decían que había varios tipos de lecturas: una primera lectura exploratoria, para enterarte de qué va el tema; una segunda lectura comprensiva, reflexionando sobre lo que leemos; una tercera en la que enlazaremos ideas y conceptos, haremos esquemas mentales y analizaremos detalladamente cada párrafo; y así todas las veces que quieras...

Pues bien, no hace falta leer tanto el esquema, que son muchas páginas y seguro que hay cosas mejores que hacer. Para eso estamos esta vez aquí, para aportar luz (y sombra, ya veréis) sobre el

ENS, resaltar lo más importante y explicar esos factores clave para charlar con los colegas en los eventos DINTEL sobre el ENS y parecer que hemos llegado a esa cuarta lectura ;)

Lo primero el plazo, que ya se ha dicho, pero conviene recordarlo: para finales de **enero de 2011** los sistemas de las administraciones públicas que presen servicios de e-Administración deben cumplir con los requerimientos del ENS. Sí, hay una **moratoria de tres años más**, que debe ser debidamente justificada, por ejemplo, habiendo realizado ya un plan de adecuación. Para los nuevos sistemas que se estén creando ya aplica el ENS en todo su esplendor.

Para saber más sobre temas jurídicos (o no técnicos) remitirse a artículos anteriores, donde se explicaron muy detalladamente todos los pormenores. Hoy toca tema técnico, y además del bueno. Iremos repasando cada dominio, punto por



Dominio “Planificación”

Análisis de riesgos	Se debe hacer un análisis de riesgos, que será más formal a medida que subamos de nivel. En nivel básico sólo es necesario “un análisis informal, realizado en lenguaje natural”.
Arquitectura de seguridad	Tener documentado nuestro sistema de información desde todos los puntos de vista: estructura de la red, procedimientos y medidas de seguridad, controles internos, equipos, etc.
Adquisición de nuevos componentes	--
Componentes certificados	--

punto, destacando las medias más significativas. Hay que tener presente que aplican en función de los niveles de seguridad (ver artículos anteriores) y que en consecuencia, nos aplicarán sólo las medidas del nivel de seguridad que tenga nuestro sistema o el nivel de seguridad que tengamos en una dimensión de seguridad en concreto.

Por resumir, decir que hay **tres niveles de seguridad: básico, medio y alto;** y tendremos **cinco dimensiones de se-**

Dominio “Control de accesos”

Identificación	Identificador singular para cada usuario/proceso que accede al sistema.
Requisitos de acceso	Que los recursos estén protegidos de accesos no autorizados previamente.
Segregación de funciones y tareas	Serán diferentes las personas que autorizan, usan y controlan el uso de recursos.
Proceso de gestión de derechos de acceso	Documentar a qué se debe acceder, con qué derechos y con qué autorización.
Mecanismo de autenticación	--
Acceso local (local logon)	--
Acceso remoto (remote login)	--

Para finales de enero de 2011 los sistemas de las administraciones públicas que presten servicios de e-Administración deben cumplir con los requerimientos del ENS

Dominio “Explotación”

Inventario de activos	Tener un inventario de todos los elementos del sistema.
Configuración de seguridad	Aplicar ciertas medidas de seguridad por defecto antes de poner un sistema en producción.
Gestión de la configuración	Mantener la configuración idónea de los sistemas.
Mantenimiento	Mantener el hardware y el software de los componentes del sistema.
Gestión de cambios	Gestionar los cambios de los componentes del sistema, analizándolos y planificándolos.
Protección frente a código dañino	Protección contra virus, gusanos, troyanos, etc.
Gestión de incidencias	--
Registro de la actividad de los usuarios	--
Registro de la gestión de incidencias	--
Protección de los registros de actividad	--
Protección de claves criptográficas	--

seguridad: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad. En conclusión, una medida de seguridad nos aplicará en función de la categoría de nuestro sistema (básica, media o alta) y en función del nivel al que hayamos llegado en cada una de las cinco dimensiones anteriores.

Y ahora sí, entremos en materia, que si no, no vamos a tener de qué hablar en “los jueves con DINTEL” y de lo que se trata ahí es de “hacer networking”:

Tenemos **75 medidas de seguridad** en el Anexo II, dividiendo éstas medidas en tres categorías:

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

Esas 75 medidas a su vez se suelen dividir en varias medidas de menor im-

portancia, y a su vez tiene diferentes intensidades o "niveles de madurez". Por lo tanto para saber si una medida nos aplica o no y para saber en qué grado tenemos que implantarla hay que fijarse en tres puntos:

1. Ver si la medida aplica en general a la categoría del sistema o bien sólo aplica a una o varias dimensiones de seguridad.
2. Ver la categoría de nuestro sistema.
3. Ver el nivel que tenemos en cada dimensión de seguridad.

Con esos tres datos sabremos si la medida de seguridad nos aplica o no y sabremos también la intensidad o nivel de madurez que debe tener.

Y ahora, las famosas medidas de seguridad. No se explicarán todas, ya que no os objeto de un artículo, simplemente se hará una introducción para dar una visión mucho más realista a todo aquel que le interese.

marco organizativo

Tenemos cuatro controles que hablan sobre tener una política, normativa y procedimientos de seguridad y un proceso de autorizaciones que cubra el uso de cualquier tipo de sistema de información (equipos, soportes, información, etc.). Aplica a todos los sistemas de información, independientemente de su nivel y de los niveles que tenga en cada dimensión de seguridad.

marco operacional

Quedan muchas por comentar, dentro de la categoría "Medidas de protección", donde se encontraremos controles sobre seguridad física, protección de los equipos, soportes, información, redes de comunicación, etc.

En el próximo artículo se presentará un caso práctico, que seguro que es del interés de todo el mundo.

A pasar un feliz verano, desconectando, descansando y leyendo mucho sobre el ENS, que en septiembre vendrá de vacaciones con mucha fuerza y habrá que estar a la altura. ●

Dominio "Servicios Externos"

Contratación y acuerdos de nivel de servicio	Detallar previamente las características de recursos y servicios contratados a terceros para prestar servicios de calidad.
Gestión diaria	Revisar la calidad de los servicios prestados por terceros.
Medios alternativos	Prever la provisión de servicios contratados a través de recursos alternativos en caso de indisponibilidad.

Dominio "Continuidad del servicio"

Análisis de impacto	Establecer requisitos de disponibilidad del servicio en base al análisis del impacto que tendría la interrupción del mismo durante un periodo de tiempo.
Plan de continuidad	Tener un plan de actuación en caso de interrupción de los servicios prestados.
Pruebas periódicas	--

Dominio "Monitorización del sistema"

Detección de intrusión	Monitorizar la actividad de los sistemas en búsqueda de intrusiones, para prevenirlas o en su caso detectarlas.
Sistema de métricas	Medir el desempeño real del sistema en cuanto a su seguridad.



GOBIERNO DE ESPAÑA

MINISTERIO DE LA PRESIDENCIA





El Esquema Nacional de Seguridad

22 abril 2010

Miguel A. Amutio
Ministerio de la Presidencia



GOBIERNO DE ESPAÑA

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO





1