Esquema Nacional de Seguridad, se lanzó la "cuenta atrás".

En el año 2008, escribí un artículo que se llamó "**La Ley 11 ....¿J?**" (puede descargarse desde la Revista Auditoría y Seguridad Nº 24 en: http://www.revista-ays.com/Archivo/popup2408.htm, y también en www.darFE.es en la sección "Descargas"). En ese artículo, pasado un año de la publicación de esta Ley, ponía de manifiesto que la falta de interés demostrada por la masa de los Organismos Oficiales Españoles sobre los datos personales de sus ciudadanos, pues estaba y estoy aún seguro que la filtración de muchos de estos datos (Médicos, hacienda, judiciales, policiales, etc..) podían desencadenar en una "catástrofe Informática de Estado".

El Artículo 42 de la Ley 11 mencionaba textualmente:

"Esquema Nacional de Interoperabilidad y Esquema Nacional de Seguridad.

3. *Ambos Esquemas se elaborarán con la participación de todas las Administraciones y se aprobarán por Real Decreto del Gobierno.....*
4. *En la elaboración de ambos Esquemas se tendrán en cuenta las recomendaciones de la Unión Europea, la situación tecnológica de las diferentes Administraciones Públicas....*

En el mes de enero de 2010 se publicaron el **RD 03/2010 "Esquema Nacional de Seguridad**" (**ENS**) y el **RD 04/2010 "Esquema Nacional de Interoperabilidad"**. Sobre el tema ya se ha escrito bastante y es de público conocimiento su propuesta, la cual debo felicitar personalmente pues esto ya empieza a tomar forma tanto técnicamente como en todos sus aspectos. Tal cual dice el artículo anterior se han tenido en cuenta todos los aspectos y se ha basado fuertemente en estándares reconocidos internacionalmente lo cual merece todos los aplausos.

Como suele suceder muy a menudo en las AAPP, los plazos no son los mismos que en el ámbito privado y han pasado ocho meses en los cuales tal vez no se hayan hecho del todo bien los deberes, y los doce meses de plazo que impone este **ENS** ya han quedado cortos para casi todos. Tal vez pueda citarse la excepción de los Organismos que se encuentran certificados con **ISO/UNE 27001**, pero de los que yo conozco, están convencidos que al contar con esta certificación, el **ENS** se cumple al 100 % y más aún, lo cual no es cierto, pues aunque en realidad en la mayoría de los aspectos se cumple al 150 %, quedan algunos pequeños detalles que no tienen por qué ser así (Alcance, dimensiones, categorización, niveles, firma electrónica, etc.). Salvados estos Organismos creo que no hay ninguno (y tal vez pueda estar equivocado) que esté en condiciones de llegar a este plazo.

No sé por dónde, ni quién, ni cómo, ni.... pero algunos hilos se están moviendo (si alguien los conoce por favor desveladme esta incógnita) y el resultado es que hay un gran número de AAPP que se han puesto las pilas recientemente para empezar a hacer algo. Por supuesto que en los cuatro meses que quedan es imposible, por esa razón están jugándose "la cuenta atrás" de la segunda carta de la Disposición Transitoria del RD 03/2010:

Disposición transitoria. Adecuación de sistemas.

1. Los sistemas existentes a la entrada en vigor del presente real decreto se adecuarán al Esquema Nacional de Seguridad de forma que permitan el cumplimiento de lo

establecido en la disposición final tercera de la Ley 11/2007, de 22 de junio. Los nuevos sistemas aplicarán lo establecido en el presente real decreto desde su concepción.

*2. Si a los doce meses de la entrada en vigor del Esquema Nacional de Seguridad hubiera circunstancias que impidan la plena aplicación de lo exigido en el mismo, se dispondrá de un **plan de adecuación** que marque los plazos de ejecución los cuales, en ningún caso, serán superiores a 48 meses desde la entrada en vigor.*

Bajo estas líneas todo parece indicar que esta segunda carta puede ser la ganadora, pero al final de esta Disposición Transitoria está el secreto:

El plan indicado en el párrafo anterior será elaborado con la antelación suficiente y aprobado por los órganos superiores competentes.

Ningún auditor que posea más de tres nanosegundos de experiencia podría dejarse caer en el engaño de una IMPROVISACIÓN. Es decir un "Plan de adecuación" elaborado con "antelación suficiente" **deja ¡huellas imborrables!**: Fechas de documentos, borradores, registros de modificaciones, reuniones, identificación de activos, descripción, inventarios, valoraciones, designación de roles, responsables, actas de reunión de seguimiento y aprobación, etc, etc, etc.... y si este "Plan de adecuación" se improvisa el resultado es evidente.

Ya hemos empezado a trabajar sobre este tema y creedme las cosas no cuelan así. Para que un "Plan de adecuación" sea "Adecuado", antes de poder redactarlo (que en definitiva es llegar a darse cuenta que no se llega en doce meses) debe seguir una serie de pasos inevitables que permitan demostrar sin lugar a dudas que no se llega al primer término y por esa razón (luego de estos pasos), se planifica todo a cuatro años, no existe otro camino o atajo.

Básicamente la secuencia es natural y no es complicada, pero hay que hacerla, dicha en términos sencillos, los pasos son:

1. Proponerse empezar, reunirse el grupo que asumirá las responsabilidades y "ponerse las pilas".
2. Organizar los roles, y responsables (tal cual lo dice el **RD**), de aquí surge un organigrama, una serie de funciones y responsabilidades que será el punto de partida de un muy próximo documento de "**Organización de la Seguridad**".
3. Comenzar el trabajo sobre los activos.

   Este tema llevará mucho tiempo y dolores de cabeza, pero las AAPP lo tienen bastante "masticado" y "servido en bandeja", pues cuentan gratuitamente con la metodología MAGERIT y su herramienta PILAR, y ahora también con la **guía 803** de CCN (Que forma parte del **ENS**).

   De todo esto los pasos son:

   - Identificación de Activos: Según **PILAR**: {Redes de Comunicaciones (COM), Datos/Información (D), Hardware (HW), Instalaciones (L), Personal (P), Servicios (S), Soportes de Información (SI), Equipamiento Auxiliar (AUX) y Software (SW)} y la **Guía 803** - Punto 2.1. IDENTIFICACIÓN en el Artículo 19. dice: Para cada elemento de información, se debe determinar: · su nombre que la identifica unívocamente, su responsable que establece sus requisitos de

seguridad, otras características que se consideren relevantes a efectos operacionales, de asociación de vulnerabilidades, de estimación de riesgos o de auditoría.

Es decir, la pólvora y la rueda ya están inventadas, sólo usémosla. Empecemos por aquí, cada activo deberá estar INVENTARIADO e identificado, tal cual lo expresa el párrafo anterior.

- Valoración de activos: El RD 03/2010: Artículo 17. dice:

  *"Aunque información es cualquier conjunto de datos que tienen significado, el Esquema Nacional de Seguridad se limita a **valorar** aquellos tipos de información que son relevantes para el proceso administrativo y pueden ser tratados en algún servicio afecto a la ley 11/2007 de acceso electrónico de los ciudadanos a los servicios públicos.*

  Si yo poseo sólo monedas de oro, ¿Cómo sé que valen más que las de plata o níquel?. Primero debo identificar TODOS los activos para luego determinar cuáles entran en juego con el **ENS** (que los acota bien claramente a aquellos que guardan relación con servicio electrónico al ciudadano).

  Nuevamente PILAR nos facilita la tarea ofreciendo cinco parámetros sobre los que valorar: Autenticación/Autenticidad, Confidencialidad, Integridad, Disponibilidad y Trazabilidad.

- Dimensión y Categorización de los Sistemas de Información (IMPORTANTE DETALLE PARA **JUSTIFICAR** HACER UN ALTO EN EL CAMINO:

  Según el RD 03/2010: Categorización de los sistemas de información

  Artículo 43. Categorías.

  1. *La **categoría** de un sistema de información, en materia de seguridad, modulará el equilibrio entre la importancia de la información que maneja, los servicios que presta y el esfuerzo de seguridad requerido, en función de los **riesgos** a los que está expuesto, bajo el criterio del principio de proporcionalidad.*
  2. *La determinación de la categoría indicada en el apartado anterior se efectuará en función de la valoración del **impacto** que tendría un incidente que afectara a la seguridad de la información o de los servicios con perjuicio para la disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad, como dimensiones de seguridad, siguiendo el procedimiento establecido en el Anexo I.*

  Según la Guía 803. Valoración de sistemas:

  - determinar la valoración del sistema en cada dimensión
  - determinar la categoría del sistema
  - determinar el conjunto mínimo de medidas de seguridad del Anexo II que son de aplicación en el sistema aplicando las condiciones indicadas en dicho anexo.

  Según el RD, ANEXO I Categorías de los sistemas

Dimensiones de la seguridad. serán identificadas por sus correspondientes iniciales en mayúsculas: Disponibilidad [D], Autenticidad [A], Integridad [I], Confidencialidad [C] y Trazabilidad [T].

NOTA IMPORTANTE: Si en el trabajo con "Activos" hemos llegado hasta aquí (Demostrado con estas actividades y documentos) es el momento de empezar a redactar el "**Plan de adecuación**", pues lo más adecuado para "Dimensionar y Categorizar" los sistemas es finalizar, el Análisis de Riesgo, tal cual dice el citado Artículo 43, cosa que aún falta un buen trecho según MAGERIT.

4. Comenzar la redacción de los documentos imprescindibles para dar comienzo a un Sistema de Gestión de la Seguridad (SGSI), pues en definitiva de esto estamos hablando. En este paso podríamos tener algunas variantes y/o aprovechar documentos existentes, pero no pueden faltar:
   - "Organización de la Seguridad" (Que se mencionó en el paso 2, y tiene gran parte ya hecha).
   - "Obligaciones del personal".
   - Al menos un primer borrador de la "Política de Seguridad".

5. Formación: Se debería dar al menos una charla de información sobre el ENS, y de ser posible llegar a hacer otra informando al personal sobre la documentación con que se cuenta.

6. "Reciclado de lo realizad hasta hoy": Todo organismo al día de hoy tiene implantadas un conjunto al menos mínimo de medidas (Antivirus, firewalls, proxies, autenticación, control de accesos, seguridad física, copias de respalda, registros o logs, etc...). Se trata de empezar a "Gestionar" integralmente todo ello, es decir, que forme parte de un único mecanismo. Insertarlo y coordinarlo con el resto de medidas y acciones, por medio de un análisis, rediseño y eventuales modificaciones.

Cualquier AAPP que haya realizado esta secuencia de pasos, podrá diseñar un "Plan de adecuación" con la conciencia tranquila del deber cumplido y con la garantía que será bien visto por cualquiera.

Nos vemos en el 2011 para ver por dónde seguimos!!!

Alejandro Corletti Estrada
acorletti@darFE.es

Madrid, Octubre de 2010