La seguridad como un proceso integral

ADECUACIÓN AL ESQUEMA NACIONAL DE SEGURIDAD DE LOS SERVICIOS DE ADMINISTRACIÓN-E DE LA DIRECCIÓN GENERAL DE MODERNIZACIÓN ADMINISTRATIVA

El Esquema Nacional de Seguridad tiene como principal objetivo "...la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de la información gestionada por los servicios de administración electrónica.....". Todos los profesionales TIC conocemos en detalle el concepto de seguridad, y también somos conscientes de sus implicaciones prácticas y, por lo tanto, de la debilidad del propio concepto, entendido como referencia de un objetivo a conseguir.

POR PILAR VIÑADO

Por eso el ENS enfoca su atención y expone como un principio básico contemplar la seguridad como un proceso integral, "…constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. La aplicación del Esquema Nacional de Seguridad estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural".

Por otro lado el ENS, en su Artículo 39, nos indica claramente, como un requisito mínimo, que la seguridad se debe de implementar integrada con el Ciclo de Vida de los Servicios de Administración Electrónica con los correspondientes procedimientos de control, que se integren con el marco metodológico de desarrollo de aplicaciones (media mp.sw.1).

También como punto importante señala el ENS, aunque en mi opinión de una manera discreta, que la articulación de la seguridad pasa por disponer de un Sistema de Gestión de la Seguridad de la Información (SGSI) que se deberá estructurar, según el Artículo 26, mediante un ciclo de mejora continua.

Con el enfoque que este marco legislativo nos ofrece, nos es fácil encontrar uno metodológico que nos permita llevar a la práctica la implantación del ENS.

Como pilar importante contamos con la norma ISO/IEC 27001 que enfoca la atención en cómo abordar la implementación del SGSI, basado en el Ciclo de Deming: PDCA (Planificar, Hacer, Control y Evaluación, Mantener). Cada una de las fases de PDCA identifican una serie de actividades a llevar a cabo para conseguir la Planificación, Definición, Desarrollo y Despliegue del SGSI, así como su puesta en Operación a través de las fases de Control y Evaluación y la de Mantenimiento.

En la definición del SGSI aportada por el ENS, en la línea de la propia definición recogida en la norma ISO/IEC 27001, se especifica claramente el tipo de componentes que constituyen el SGSI: La estructura organizativa, Las Políticas, las actividades de Planificación, las Responsabilidades, las prácticas Los procedimientos Los procesos y Los recursos.

Vemos como el SGSI, entendido como tal Sistema de Gestión, está constituido por activos que corresponden a capacidades (Estructura Organizativa, Políticas, Planificación, Responsabilidades, Prácticas, Procesos, Procedimientos) y recursos (Herramientas Preventivas, Reactivas, y Reductivas, integradas en un Sistema de Información propio) y personas.

A su vez, los Servicios de Administración Electrónica a proteger bajo el marco del ENS, están organizados, si tomamos como referencia buenas prácticas como ITIL, en sus propias capacidades (Organización, Sistemas de Gestión del Servicio, etc.), recursos (Información, Instalaciones e Infraestructuras, Comunicaciones, Equipos, Aplicaciones, Servicios TI de apoyo, Soportes, etc.) y personas.

Si vemos la estructuración del ENS, las medidas de seguridad están orientadas a:

- Regular las Capacidades del SGSI mediante medidas de seguridad del marco organizativo (org) y del marco operacional (op).
- Especificar requisitos para los Recursos del propio SGSI, mediante medidas operacionales y medidas de protección (mp).
- Protección de los diferentes tipos de Recursos propios de los Servicios Regular Responsabilidades y Capacidades de las Personas que gestionan la seguridad (principalmente en mp.per).

Adecuación en la DG de Modernización

Con la amplia visión anteriormente descrita ¿Cómo se ha enfocado en la Dirección General de Modernización Administrativa, Procedimientos e Impulso para la Administración Electrónica el proyecto de adecuación al ENS?

Partiendo de unos índices de buen nivel de cumplimiento en las medidas de protección de los Recursos de los Servicios de Administración Electrónica, el enfoque se ha basado en dar prioridad a la Planificación, Definición e Implantación del SGSI, basado en las siguientes directrices:

1.- Estructurar el SGSI según la ISO/IEC 27001 identificando así los Tipos de Actividad requeridos para la construcción, mantenimiento y mejora continua del mismo.

2.- Considerar al SGSI como un elemento más del Ciclo de Vida del Servicio de acuerdo a las buenas prácticas de ITIL v3.0, teniendo muy en cuenta que las actividades requeridas ISO/IEC 27001 deben de estar adecuadamente integradas con las actividades propias de gestión del ciclo de vida del servicio.

3.- Articular dichas actividades en procesos y procedimientos identificando claramente:

- Procesos y Procedimientos Centrales del propio SGSI.
- Interfaces que estos Procesos y Procedimientos tiene con los Proceso del Ciclo de Vida del Servicio (ITIL v3.0)
- Interfaces con Procesos Soporte
- Interfaces con Procesos del Negocio.

4.- Analizar detalladamente el »

ENS (incluidas las Guías CCN-STIC correspondientes) y trazar su contenido con el fin de identificar los requisitos propios del ENS a tener en cuenta en la definición del SGSI, yendo así a una actuación de definiciones de un SGSI específico para el ENS, contemplando sólo como referencia modelos de SGSI existentes basadas en otro marco de controles o medidas de seguridad ya conocidos en el mercado.

5.- Dar prioridad en la definición e implementación del SGSI al desarrollo del Marco Normativo, como componente estratégico de las capacidades del mismo, a la vez que se convierte en la definición propia del SGSI, a nivel de:

•Políticas que marcan el funcionamiento del SGSI

•Procesos y Procedimientos en los que se estructura el SGSI.

6.- Identificar claramente en el nivel de detalle requerido por el ENS, las responsabilidades de todos los componentes de la estructura organizativa de seguridad con el fin de:

•Difundir y Concienciar al equipo de la estructura organizativa, que actualmente está gestionando el ciclo de vida de los servicios, sobre esta normativa de seguridad, haciendo especial hincapié en las responsabilidades que asumen.

•Producir de esta forma el marco para una integración práctica, de la normativa y actividad requerida por el SGSI, por los profesionales de esta Dirección General, que ya siguen unas buenas prácticas de la gestión TIC.

7.- Una vez consolidado a nivel normativo en la práctica el SGSI, se puede ya abordar su nivel operativo, para así integrar herramientas de protección en un sistema de gestión integrado de información, que de soporte al SGSI.

El ENS nos ha aportado un marco legislativo común para la protección de los Servicios de Administración Electrónica. También nos ha requerido una Plan de Adecuación al mismo que cada organismo debe de ejecutar. Pero todos coincidiremos en la obviedad de que hay muchos de los elementos requeridos por el ENS que pueden ser compartidos. Entre ellos, un modelo de marco normativo. E inevitablemente, según la coyuntura económica actual en la que se encuentran las AAPP, es necesario por responsabilidad legal y profesional, seguir protegiendo nuestros servicios de amenazas gobernadas por grupos de interés que es posible que cuenten con muchos más recursos de los que nosotros contamos. Por ello, se hace imprescindible enfocar la seguridad de los Servicios de Administración Electrónica, de una manera global, y llegar así a normativas e infraestructuras operativas de protección de la seguridad comunes.

Uno de los escritores que me inspiran en el día a día, J. Krishanmurti, dijo que la seguridad sólo es posible desde una vivencia de unidad. ¿Podemos hacer algo al respecto?

Por mi parte, y por parte de esta Dirección General, estamos abiertos a generar esa Unidad en este objetivo tan importante de ofrecer servicios confiables a los usuarios de la Administración Electrónica.

Pilar Viñado Villuenda
Consejera Tēcnica
SG Modernización Administrativa, Procedimientos e Impulso a la Administración Electrónica