El ENS, confianza en el uso de medios electrónicos

El Esquema Nacional de Seguridad nace con el objetivo fundamental de impulsar la confianza en el uso de los medios electrónicos por parte de la Administración en su relación con los ciudadanos. Desde ICA invertimos en innovación y apostamos en el desarrollo de soluciones que facilitan la implantación y seguimiento de las medidas de seguridad articuladas.

POR JESÚS CASTELLANOS

Con el desarrollo del Esquema Nacional de Seguridad se consigue dar cumplimiento a lo establecido en el artículo 42 de la Ley 11/2007 de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, en lo relacionado con aspectos de la seguridad de los sistemas de tecnologías de la información. Ha sido elaborada con la participación de todas las Administraciones públicas a las que les es de aplicación, tras informes favorables de diversas entidades implicadas y de los propios ciudadanos.

Aunque el espíritu está focalizado en la protección de la información en la relación de la Administración con los ciudadanos, el verdadero alcance aplica igualmente al resto de Administraciones, aunque no tengan esa relación directa en los servicios que cada uno presta, ya que el artículo 3 del capítulo I establece como ámbito

de aplicación lo establecido en el artículo 2 de la Ley 11/2007:

La presente Ley, en los términos expresados en su disposición final primera, será de aplicación:

a.A las Administraciones Públicas, entendiendo por tales la Administración General del Estado, las Administraciones de las Comunidades Autónomas y las Entidades que integran la Administración Local, así como las entidades de derecho público vinculadas o dependientes de las mismas.

b.A los ciudadanos en sus relaciones con las Administraciones Públicas.

c.A las relaciones entre las distintas Administraciones Públicas.

Algunas Administraciones excusan el cumplimiento basado en la falta de relación directa con el ciudadano, pero, ¿existe realmente una Administración Pública que no se relacione con otra?

Los objetivos

Esta norma (en el entorno al que va dirigido su cumplimiento tiene más sentido hablar de una norma de seguridad que de un Real Decreto de seguridad) ha establecido unos objetivos marco sobre los que focalizar el esfuerzo en la gestión de la seguridad que se materializan en principios básicos y requisitos mínimos para asegurar el acceso, la integridad, la disponibilidad, la autenticidad, la confidencialidad, la trazabilidad y la conservación de los datos, información y servicios.

El capítulo II del Esquema Nacional de Seguridad establece los principios fundamentales para la implementación de la seguridad a utilizar en los medios electrónicos que gestionen las competencias de las Administraciones Públicas. Siete artículos dentro de este capítulo definen en la Política de alto nivel los principios de seguridad como esenciales para garantizar la seguridad. Estos artículos resumen, a alto nivel, el espíritu de la norma, que posteriormente se desarrolla en agrupaciones de controles, más o menos relacionados entre sí, como lo hace cualquier otra norma enfocada a la protección de la información. Véase que cualquier norma o código de buenas prácticas toma como principios fundamentales el intento de garantía de tres principios básicos, la confidencialidad, la integridad y la disponibilidad, que son complementados con algún otro según la norma que estemos utilizando como referencia.

Las medidas de seguridad

El desarrollo del resto del articulado del Esquema Nacional de Seguridad describe detalladamente cómo se deben lograr los objetivos plasmados en la política establecida en el capítulo II.

Es de especial interés que se establezcan objetivos de cumplimiento por niveles y definiendo con claridad que es lo que debe cumplir el Organismo en cuestión, en base a que se vean afectadas las dimensiones de seguridad que toda Administración Pública debe valorar: Disponibilidad; Autenticidad; Integridad; Confidencialidad y Trazabilidad.

Esto en sí mismo, ya es un paso muy importante para fijar el punto de salida, ya que, en base a la afectación de estas dimensiones, se categoriza el sistema de información y, por extensión, las medidas de seguridad que se han de adoptar de entre el catálogo de controles disponibles en el Esquema Nacional de Seguridad.

Tras la elaboración de este análisis es posible determinar qué nivel de

LogICA es una solución enfocada a la recolección, centralización y almacenamiento de información que gestiona la seguridad de forma proactiva y reactiva

implantación de un control debe una Administración desplegar en su entorno: nivel BAJO, relacionado con perjuicios definidos como limitados; nivel MEDIO, relacionado con perjuicios definidos como graves y, nivel ALTO, relacionado con perjuicios definidos como muy graves.

Aunque aparentemente esta clasificación da pie a la subjetividad, cada uno de los niveles tienen definidos indicadores que ayudan a clasificar el nivel aplicable en cada sistema de información. Estos indicadores están enfocados a la pérdida de capacidad, a daños en los activos, al incumplimiento legal, a daños y perjuicios a individuos o a otros de naturaleza análoga.

Nuestra percepción

ICA, como fabricante de soluciones de seguridad de la información, referentes en el sector de la Administración Pública, está evolucionando las funcionalidades de sus productos para permitir la ágil integración de esta Normas de seguridad.

La mejor manera de aproximarse de una forma eficiente al cumplimiento del Esquema Nacional de Seguridad es realizando el aprovechamiento de los sistemas de información existentes con los que la mayoría de las organizaciones ha empezado a cubrir sus necesidades de seguridad. Es extraño encontrar Organismos que no dispongan de tecnología relacionada con el control de acceso lógico y físico, de control de suministro energético o medioambiental, de monitorización de redes, de gestión de capacidad y disponibilidad, de inspección de contenidos, de control de código malicioso, de gestión de contenidos e información de negocio, de gestión de incidentes y otros muchos sistemas de información.

Lo que sí es más extraño es la utilización, de forma centralizada, de la información generada de forma independiente por cada uno de estos sistemas de información.

La suite LogICA (compuesta por Lógica y Cuádica) posee la certificación Common Criteria EAL2, además de ser el producto recomendado por el Centro Criptológico Nacional para la gestión de seguridad en la Administración Pública:

"Se considera que la solución evaluada es idónea para proporcionar servicios avanzados de monitorización de redes, como los contenidos en la Norma Těcnica STIC 302 de interconexión de sistemas, apartado dedicado a los Sistemas de Protección de Perímetro asociados a la gestión centralizada de logs.

Se recomienda la utilización de la solución en todos los organismos que necesiten una gestión avanzada de los registros de auditoría"

LogICA es una solución enfocada a la recolección, centralización y almacenamiento de información que, posteriormente, es gestionada desde dos puntos de vista, la gestión proactiva y la gestión reactiva de la seguridad. Dentro de estos conceptos de gestión se pueden enmarcar aspectos como el inventariado de los sistemas de información, la gestión de eventos de seguridad en Tiempo Real, la correlación de eventos de seguridad, la gestión de vulnerabilidades, la gestión de incidentes, la generación de evidencias digitales. Unas de las últimas novedades es la integración con PILAR, herramienta utilizada por la Administración Pública para la gestión de riesgos de seguridad de la información. LogICA es capaz de introducir ese grado de objetividad en los parámetros de probabilidad e impacto, hasta ahora inexistente.

CuadICA es una solución para la centralización de la información relacionada con la creación de cuadros de mando de seguridad y la evaluación del grado de cumplimiento normativo de los objetivos de la organización. Una de las últimas novedades es la incorporación de más de 600 indicadores relacionados directamente con el Esquema Nacional de Seguridad. MetrICA, versión para la Administración Pública de CuadICA, es capaz de proporcionar de manera automática indicadores que proporcionen un grado de cumplimiento de los controles establecidos en el Esquema Nacional de Seguridad.

Acerca de ICA

Informática y Comunicaciones Avanzadas, SL, es un grupo fundado en 1983, con más de 25 años de experiencia en el sector tecnológico, que desarrolla su actividad dentro en el ámbito de los servicios, la consultoría y la auditoría de las Tecnologías de la Información y de las Comunicaciones. ICA posee los Certificados en Seguridad de la Información (ISO 27001), en Gestión de la Calidad (ISO 9001), Gestión Ambiental (ISO 14001) y recientemente en Determinación de la Mejora de Proceso y de la Capacidad del Software (ISO 15504). Adicionalmente, ICA continúa su expansión de certificaciones que reflejan el compromiso de la organización con la seguridad organizativa y de productos.

Jesús Castellanos Fernández
SGSI, CISA, ITIL, Lead Auditor
Responsalbe de consultoría de Seguridad TIC y Jefe de Producto CuadICA
ICA Informática y Comunicaciones Avanzadas