INTECO

Instituto Nacional
de Tecnologías
de la Comunicación

EL ESQUEMA NACIONAL DE LA SEGURIDAD Y LA ADMINISTRACION

INTECO

Marzo 2010

Instituto Nacional
de Tecnologías
de la Comunicación

ÍNDICE

1. ¿QUÉ ES EL ESQUEMA NACIONAL DE SEGURIDAD?

El **Real Decreto 3/2010, de 8 de enero (BOE de 29 de enero), por el que se regula el Esquema Nacional de Seguridad (ENS)** en el ámbito de la administración electrónica, regula el citado Esquema previsto en el artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

Su objeto es establecer la política de seguridad en la utilización de medios electrónicos y está constituido por principios básicos y requisitos mínimos que permitan una protección adecuada de la información.

Su finalidad es crear **la confianza necesaria en el uso de la administración electrónica** por parte de los ciudadanos y **permitir el cumplimiento por parte de las Administraciones** de la obligación de prestar acceso electrónico y trámites públicos a partir de enero de 2010.

El ENS introduce los elementos comunes que han de guiar la actuación de las Administraciones Públicas en materia de seguridad de las tecnologías de la información. En particular:

- Los principios básicos a ser tenidos en cuenta en las decisiones en materia de seguridad.
- Los requisitos mínimos que permitan una protección adecuada de la información.
- El mecanismo para lograr el cumplimiento de los principios básicos y requisitos mínimos mediante la adopción de medidas de seguridad proporcionadas a la naturaleza de la información, el sistema y los servicios a proteger.

Se desarrolla teniendo en cuenta, entre otras, las recomendaciones de la Unión Europea, la situación tecnológica de las diferentes Administraciones Públicas, así como los servicios electrónicos ya existentes, y la utilización de estándares abiertos así como, en su caso y de forma complementaria, estándares que sean de uso generalizado por los ciudadanos.

En su elaboración se han manejado, entre otros, referentes en materia de seguridad tales como directrices y guías de la OCDE, recomendaciones de la Unión Europea, normalización nacional e internacional, normativa sobre administración electrónica, protección de datos de carácter personal, firma electrónica y Documento Nacional de Identidad Electrónico, así como a referentes de otros países.

1.1. OBJETIVOS

Sus objetivos principales son los siguientes:

- Crear las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita a los ciudadanos y a las administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

- Establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la Ley 11/2007, que estará constituida por los principios básicos y los requisitos mínimos para una protección adecuada de la información.
- Introducir los elementos comunes que han de guiar la actuación de las administraciones públicas en materia de seguridad de las tecnologías de la información.
- Aportar un lenguaje común para facilitar la interacción de las administraciones públicas, así como la comunicación de los requisitos de seguridad de la información a la industria.

En el **ENS se concibe la seguridad como una actividad integral**, en la que no caben actuaciones puntuales o tratamientos coyunturales, debido a que la debilidad de un sistema la determina su punto más frágil y, a menudo, este punto es la coordinación entre medidas individualmente adecuadas pero deficientemente ensambladas.

2. ¿QUIÉN DEBE DE CUMPLIR CON EL ENS?

El ENS es de obligado cumplimiento para:

- Administración General del Estado (AGE): el conjunto de departamentos, entes, sociedades públicas, organismos y agencias estatales.
- Las Administraciones de las Comunidades Autónomas: los departamentos y consejerías, fundaciones públicas, institutos, agencias, sociedades públicas, universidades y otros entes de la administración
- Las Administraciones Locales: ayuntamientos, diputaciones, mancomunidades, y otras formas de organización de la administración, fundaciones y patronatos, sociedades públicas y entes autónomos.
- Entidades de derecho público vinculadas o dependientes del conjunto de la administración española

No obstante no es obligatorio a aquellas administraciones que realicen sus actividades en régimen de derecho privado.

3. ¿CUÁNDO DEBEN DE CUMPLIR LAS ADMINISTRACIONES CON EL ENS?

Según lo recogido por el Real Decreto 3/2010, de 8 de enero, las administraciones tienen un plazo de 12 meses desde la entrada en vigor del mismo, por lo que **dicho plazo finalizaría el 8 de enero de 2011.**

4. ¿CUÁLES SON LAS OBLIGACIONES ORGANIZATIVAS Y FORMALES?

Para cumplir con el ENS, las administraciones deben cumplir al menos los siguientes puntos:

- Definir y aprobar formalmente la política de seguridad por parte del titular responsable de la acción de gobierno, documento recopilatorio del marco de seguridad objetivo.
- Definir los tipos y niveles de información administrativa a efectos de seguridad y aprobar su estructura por el órgano de dirección.
- Crear y definir comités de seguridad, responsables de velar por la política de seguridad de la entidad
- Designar la figura del responsable de seguridad por sistemas y/o departamentos.
- Definir la Normativa de Seguridad, indicando cómo y quién hace las distintas tareas y cómo se identifican y resuelven las incidencias que pudieran darse.
- Definir y escribir los procesos de autorización, formalizando autorizaciones que cubran todos los elementos de los sistemas de información: instalaciones, equipos, aplicaciones, medios de comunicación, accesos, soportes, etc.
- Establecer el cumplimiento técnico, con la revisión periódica de la normativa y los procedimientos por el personal técnico.
- Realizar auditorías bienales de seguridad, en las que se revise la política de seguridad y su cumplimiento, así como el conjunto de riesgos, normativas, procedimientos y controles establecidos.
- Formar continuamente a todo el personal sobre la política, normativa y procedimientos de seguridad.

5. PRINCIPIOS BASICOS

- **Seguridad Integral**: la seguridad de la información en las administraciones se plantea como un proceso integral, que excluye tratamientos coyunturales. Se prestará especial atención a las personas, la organización y los procedimientos de seguridad.
- **Gestión basada en riesgos**: se analizarán los riesgos donde se deberán identificar y evaluar riesgos inherentes en todos los activos de información incluyendo las personas y la infraestructura que invierten en su gestión. Este conocimiento de los riesgos servirá para gestionarlos mediante el despliegue de medidas de seguridad para mitigar su impacto.
- **Prevención, reacción y recuperación**: los sistemas de seguridad deben tener una orientación preventiva, para evitar las amenazas. Los sistemas dispondrán de medidas de recuperación que permitan restaurar la información y los servicios, sin que se ponga en peligro la continuidad de los mismos.
- **Establecimiento de barreras de defensa**: deberá existir una estrategia de protección con diversas capas de seguridad y control.
- **Evaluación periódica**: a través de auditorias y sistemas de verificación de cumplimientos.
- **Función diferenciada**: Las diversas responsabilidades inherentes a la gestión de la seguridad deberán diferenciarse de las relativas a las de gestión de los sistemas de información.

6. ¿QUÉ ELEMENTOS Y PROCESOS ESTÁN SUJETOS EN EL ENS?

Están integrados en el ámbito del ENS todos los elementos técnicos, humanos, materiales y organizativos relacionados con los sistemas de información.

De forma específica se implementarán, gestionarán e integrarán para el cumplimiento del ENS los siguientes conceptos:

- servicios, trámites y demás relaciones que se presten a ciudadanos electrónicamente
- las comunidades electrónicas relativas a la transmisión, almacenamiento y recepción de datos
- las sedes y registros electrónicos
- las notificaciones y publicaciones electrónicas
- los mecanismos de firma electrónica y certificados digitales
- las aplicaciones informáticas
- los ficheros con datos de terceros
- la gestión de las copias de seguridad
- las herramientas de hardware y software, ya sean propias o provistas por terceros
- la adquisición de nuevos componentes de los sistemas de información
- la transmisión de datos entre distintas administraciones
- el acceso y manejo de la información por el personal de las administraciones
- las redes, dispositivos periféricos, dispositivos móviles, etc.
- procedimientos que aseguren la conservación y accesibilidad a largo plazo de los documentos electrónicos elaborados por las administraciones públicas.
- el cumplimento del ENS engloba a toda información que estando en soporte físico haya sido causa o consecuencia de la información electrónica, debiendo aplicarse las mismas medidas de seguridad conforme al soporte en el que se encuentre

7. ¿CÓMO SE IMPLEMENTA EL CUMPLIMIENTO DEL ENS?

Para su implementación tendremos que disponer de los siguientes elementos:

- inventario de activos, recursos técnicos, organizativos, humanos y procedimentales sujetos al ENS
- catalogación de los tipos de información según su criticidad
- análisis de riesgos
- selección de medidas de protección en función de los tipos y niveles de la información
- elaboración de un marco organizativo de seguridad:
    - documento de política de seguridad
    - documentos de normativa de seguridad
    - documentos de procedimientos de seguridad
    - documentos de autorización
    - documentos de cumplimiento técnico
- arquitectura de seguridad
- sistemas de registro, control y resolución de incidencias
- plan de continuidad de servicio
- plan de pruebas y monitorización del sistema
- medidas de protección
- plan de formación y sensibilización del personal
- actualización del sistema
- plan de auditoría bienal

7.1. ESQUEMA DE IMPLANTACIÓN

Medidas de protección:

- protección de instalaciones e infraestructuras
- gestión del personal
- protección de equipos
- protección de las comunicaciones
- protección de soportes de información
- protección de aplicaciones
- protección de la información

- protección de los servicios

Categorización de los sistemas de información:

- dimensiones de la seguridad: disponibilidad, autenticidad, integridad, confidencialidad, trazabilidad
- determinación de los niveles de seguridad por sistema: bajo, medio, alto
- relación entre tipos de información y dimensión de la confidencialidad
- determinación de categoría de cada sistema: básica, media, alta

Marco organizativo:

- política de seguridad
- normativa de seguridad
- procedimientos de seguridad
- procesos de autorización
- órganos de gestión
- auditorías de seguridad: cumplimiento legal y cumplimiento técnico

Marco operacional:

- planificación: análisis de riesgos, arquitecturas de seguridad, componentes, etc.
- control de accesos
- explotación: inventario de activos, gestión de procesos, registros, sistemas de protección
- servicios externos
- continuidad del servicio
- monitorización del sistema
- acreditación de conocimientos de la vida laboral

8. ¿QUIÉN PUEDE DAR SOPORTE A LAS ADMINISTRACIONES EN LA ADPATACIÓN Y CUMPLIMIENTO DEL ENS?

Soporte y asesoría a la Administración desde la Administración es el servicio que el Instituto Nacional de Tecnologías de la Comunicación (INTECO) puede prestar a las distintas administraciones ofreciendo todo su equipo técnico y humano para el cumplimiento del Esquema Nacional de Seguridad.

El Instituto Nacional de Tecnologías de la Comunicación (INTECO), es referenciado en el Esquema Nacional de Seguridad como herramienta de soporte e innovación en el proceso de integración de la seguridad. INTECO, así mismo, tiene un papel relevante en el desarrollo y ejecución de las áreas de confianza, seguridad, calidad TI y accesibilidad, marcadas en el **Plan Avanza y Plan Avanza 2,** que reforzarán las políticas seguidas en esta materia en los últimos años. Mediante esta línea de actuación, se tratará de mostrar soporte y apoyo a las administraciones públicas que lo soliciten durante su proceso de adaptación y cumplimiento del Esquema Nacional de Seguridad.