Implantación del Esquema Nacional de Seguridad

Alberto López

Responsable de Proyectos

Dirección de Operaciones

Índice

1 – ¿Que es el ENS?

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad 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.

- La finalidad del Esquema Nacional de Seguridad es **crear las condiciones necesarias para la 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 el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

- El Esquema Nacional de Seguridad introduce los elementos comunes que han de guiar la actuación de las Administraciones Públicas en materia de seguridad de las tecnologías de la información y **aporta un lenguaje común para facilitar la interacción de las Administraciones Públicas**, así como la comunicación de los requisitos de seguridad de la información de las mismas a la industria.

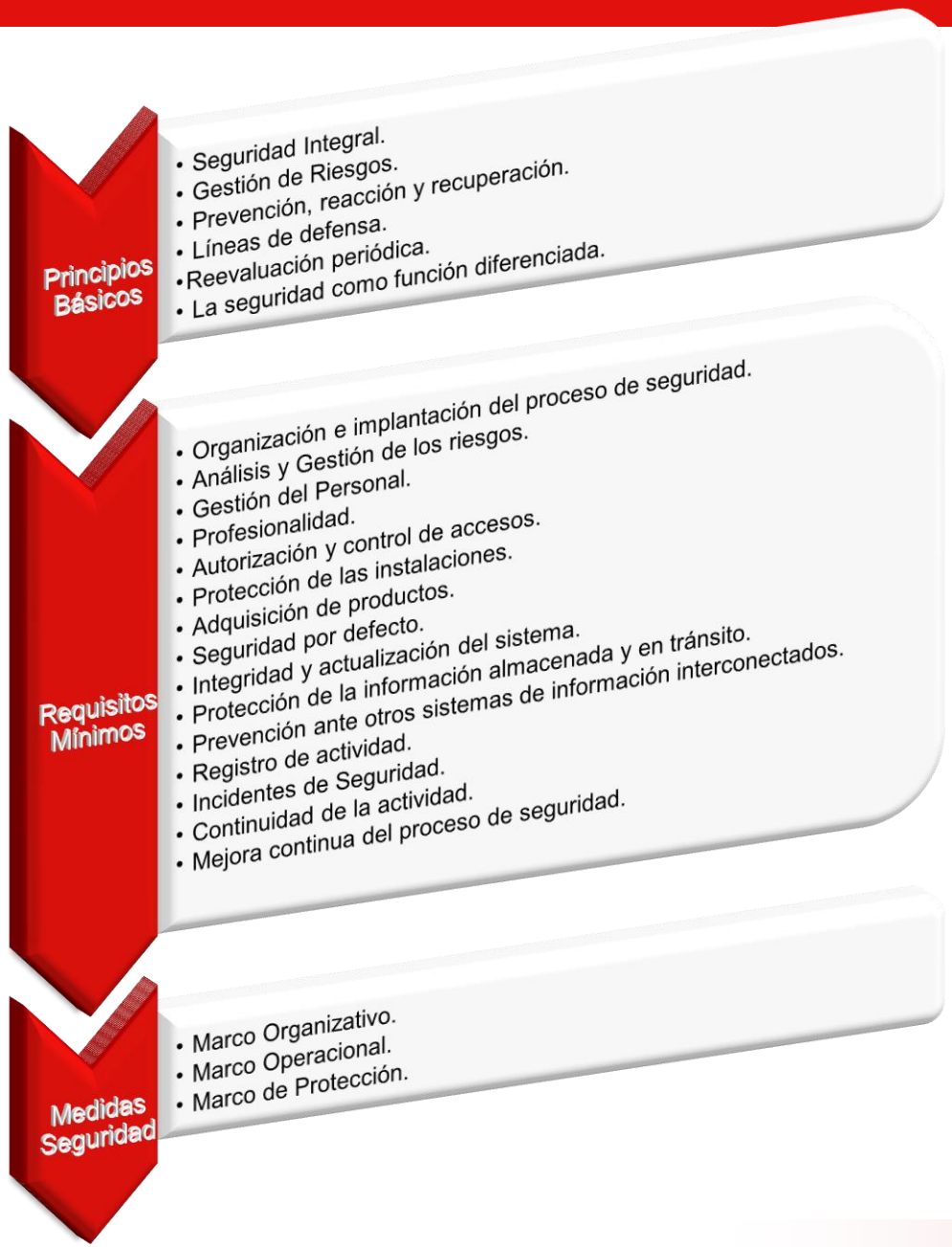
2 – Ámbito de Aplicación e Impacto

El ámbito de aplicación del Esquema Nacional de Seguridad es el establecido en el artículo 2 de la Ley 11/2007:

- A la Administración General del Estado, 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.
- A los ciudadanos en sus relaciones con las Administraciones Públicas.
- A las relaciones entre las distintas Administraciones Públicas.

✓ Todos los sistemas existentes deben adecuarse al ENS en un plazo de 12 meses desde su aprobación, aunque si hubiera circunstancias que impidieran la plena aplicación, se dispondrá de un plan de adecuación que marque los plazos de ejecución, en ningún caso superior a 48 meses desde la entrada en vigor del esquema.

3 - Visión General del Esquema



✓Cinco dimensiones de seguridad: **Disponibilidad, Autenticidad , Integridad , Confidencialidad y Trazabilidad.**

✓Gestión de la seguridad basada en los riesgos, debiendo realizarse un análisis y gestión de los mismos con el objetivo de minimizarlos hasta unos niveles aceptables. → **Categorización de los activos: BÁSICO. MEDIO Y ALTO.**

✓Necesidad de realizar reevaluaciones periódicas. → **Mejora Continua.**

3 - Visión General del Esquema

Medidas Seguridad

Marco Organizativo

- Política de Seguridad.
- Normativa de Seguridad.
- Procedimientos de Seguridad.
- Proceso de Autorización.

Marco Operacional

- Planificación.
- Control de Acceso.
- Explotación.
- Servicios Externos.
- Continuidad del servicio.
- Monitorización del sistema.

Medidas de Protección

- Protección de las instalaciones e infraestructuras.
- Gestión del Personal.
- Protección de los equipos.
- Protección de las comunicaciones.
- Protección de los soportes de información.
- Protección de las aplicaciones informáticas.
- Protección de la información.
- Protección de los servicios.

ANEXO II

D		
bajo	medio	alto
aplica	+	=

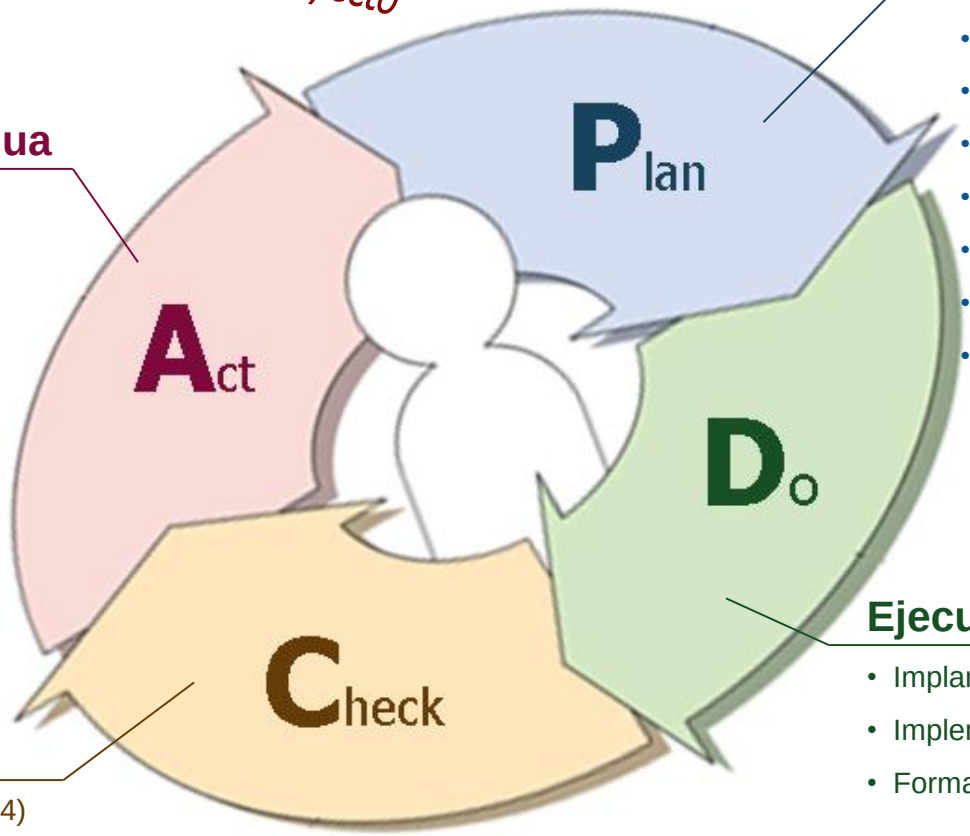
todas		
básica	media	alta
aplica	=	=

T		
bajo	medio	alto
no aplica	no aplica	aplica

4 - Implantación

Esquema Nacional de Seguridad

Comienzo del Proyecto



Planificación

- Alcance (articulo 2 11/2007)
- Organización y Responsabilidades
- Política de Seguridad
- Valoración de Información y Servicios
- Categoría del sistema y aplicabilidad.
- Análisis y Evaluación de Riesgos.
- Identificación de Insuficiencias.
- Plan de Mejora

Ejecución

- Implantar el Plan de Mejora
- Implementar los Controles
- Formación y Concienciación

Seguimiento

- Plan de auditoría (articulo 34)

Mejora Continua

- Acciones Correctivas
- Acciones Preventivas

Seguridad de la Información = Modelo en CONTINUA Evolución

PLANIFICACIÓN: Plan de Adecuación al ENS – 31 Enero de 2011

1. **Definición del Alcance.**
2. **Organización y Responsabilidades.**
   - ✓ Responsables de Seguridad, de la Información y de los Servicios
3. **Política de Seguridad de la entidad.**
   - ✓ Objetivos o misión de la organización.
   - ✓ Marco legal y regulatorio en el que se desarrollarán las actividades.
   - ✓ Roles o funciones de seguridad, definiendo para cada uno, los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación.
   - ✓ Estructura del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, los miembros y la relación con otros elementos de la organización.
   - ✓ Directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

RETOS:

- **No tengo organizadas las responsabilidades .**
- **No tenemos política de seguridad.**
- **La política de seguridad de mi organización no cumple con dicha estructura.**

PLANIFICACIÓN: Plan de Adecuación al ENS – 31 Enero de 2011

4. Valoración de Información y Servicios.

✓ Anexo I – RD 3/2010.

5. Categoría del Sistema y Aplicabilidad.

6. Análisis de Riesgos.

✓ En función de la categoría del sistema.

7. Insuficiencias del Sistema.

✓ Incumplimiento formal de las medidas de seguridad exigidas en el Anexo II para la valoración del sistema.
✓ Incumplimiento formal de las medidas de seguridad exigidas por el RD 1720/1997 para los datos de carácter personal tratados por el sistema.
✓ Existencia de riesgos no asumibles por el organismo.

Dudas:

- **¿Quién valora? → Formalmente el Responsable del Servicio y de la Información.**
- **¿Quién acepta el riesgo residual? → Formalmente los Responsables del Servicio y la Información**

PLANIFICACIÓN: Plan de Adecuación al ENS – 31 Enero de 2011

8. Plan de Mejora.

✓ Insuficiencias que subsanan.
✓ Plazo previsto de ejecución, indicando fecha de inicio y fecha de terminación, así como los principales hitos intermedios.
✓ Estimación del coste que supondrá.

Próximos pasos:

- **Implantación de controles derivados del Plan de Mejora.**
- **Formación y concienciación.**
- **Plan de Auditoría.**
- **Mejoras derivadas de Plan de Auditoría.**

Conclusiones

- Apoyo: desde arriba hacia abajo
- Definir desde el inicio un Responsable de Seguridad, encargado de llevar a cabo la adecuación.
- Establecer fases progresivas para la adecuación a través del plan de adecuación (tenemos 3 años más, pero luego seguimos).
- Reutilizar lo que ya tenemos.
- **Entender el cumplimiento como un medio y no como un fin.**

INTECO

Instituto Nacional
de Tecnologías
de la Comunicación

Muchas gracias

INTECO

Instituto Nacional
de Tecnologías
de la Comunicación