Requerimientos Técnicos Del Esquema Nacional De Seguridad (ENS)

www.seguridadinformacion.com

www.esquemanacionaldeseguridad.com

AMETIC

1. INTRODUCCIÓN

Esquema Nacional de Seguridad

- El ENS es un Sistema de Gestión de Seguridad de la Información para las Administraciones Publicas.
- El ENS se desarrolla sobre las recomendaciones de la UE y los estándares internacionales en materia de seguridad de la información, especialmente la Norma ISO 27001.

2. GENERALIDADES

- Es el marco, obligatorio para las administraciones públicas, para la protección de la información y su gestión a través de los medios electrónicos.
- Su creación se contempla en la LEY 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos y se regula a través de Real Decreto del Gobierno de España 3/2010, de 8 de enero.

3. A QUIEN APLICA

La Administración General del Estado

Las Administraciones de las Comunidades Autónomas

Las Entidades que integran la Administración Local

Las entidades de derecho público vinculadas o dependientes de las mismas

4. A QUIENES AFECTA

Proveedores de Servicios TI

Productos de Seguridad de la información

- El ENS precisa que los proveedores de servicios TI de las Administraciones Públicas deberán contar con una gestión y un nivel de madurez de seguridad equivalente al que tiene implantado la entidad.
- Se valorará aquellos proveedores que tengan certificados relevantes de gestión o de productos.

5. DIMENSIONES DE LA SEGURIDAD DE LA INFORMACIÓN

Confidencialidad	• Para asegurar que sólo quienes estén autorizados puedan acceder a la información
Integridad	• Para asegurar que la información y sus métodos de proceso son exactos y completos
Disponibilidad	• Para asegurar que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran
Trazabilidad	• Para asegurar el saber quien, cuando, cómo y qué se ha hecho en un proceso telemático dentro de la Administración Electrónica
Autenticidad	• Para que no haya duda de quién se hace responsable de una información o prestación de un servicio, tanto a fin de confiar en él como de poder perseguir posteriormente los incumplimientos o errores. Fundamenta la administración electrónica, permitiendo confiar sin papeles ni presencia física.

6. CONCEPTOS BÁSICOS

Seguridad integral	La gestión de la seguridad debe ser un proceso integral.
Gestión de riesgos	Un programa de seguridad debe responder a las necesidades de reducción de riesgos de la entidad.
Prevención, reacción y recuperación	La utilización de estos tipos de medidas permitirá un enfoque integral de la seguridad.
Líneas de defensa	El sistema debe contar con sucesivas capas de protección para que si ocurre un incidente, no desarrolle todo su potencial dañino.
Reevaluación periódica	El programa de seguridad debe ajustarse a los cambios que se vayan produciendo.
Función diferenciada	Las funciones de responsable de la información, responsable del servicio y responsable de la seguridad deben estar separadas.

7. ELEMENTOS SUJETOS AL ENS

Todos los elementos técnicos, humanos, materiales y organizativos, relacionados con la Administración Electrónica, y en particular:

- Los servicios, trámites y demás relaciones que se presten a ciudadanos electrónicamente.
- Las comunicaciones electrónicas relativas a la transmisión, almacenamiento y recepción de datos.
- Las sedes y registros electrónicos.
- Procedimientos que aseguren la conservación y accesibilidad a largo plazo de los documentos electrónicos
- Toda información que, estando en un soporte físico haya sido causa o consecuencia de la información electrónica.

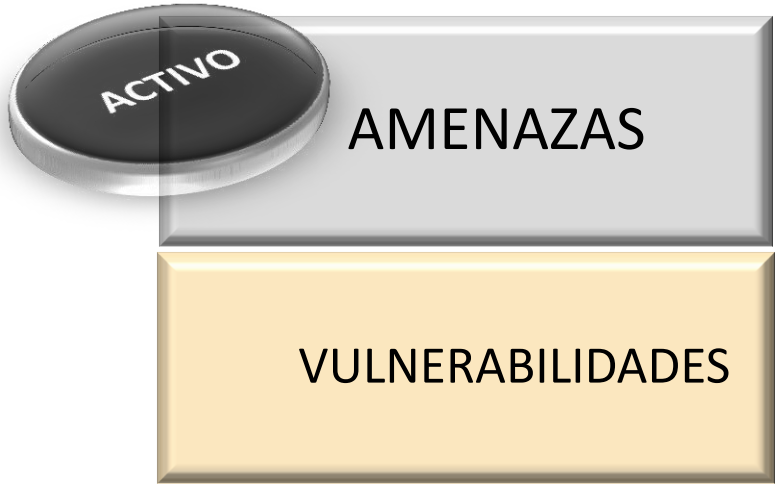
8. REQUISITOS MÍNIMOS

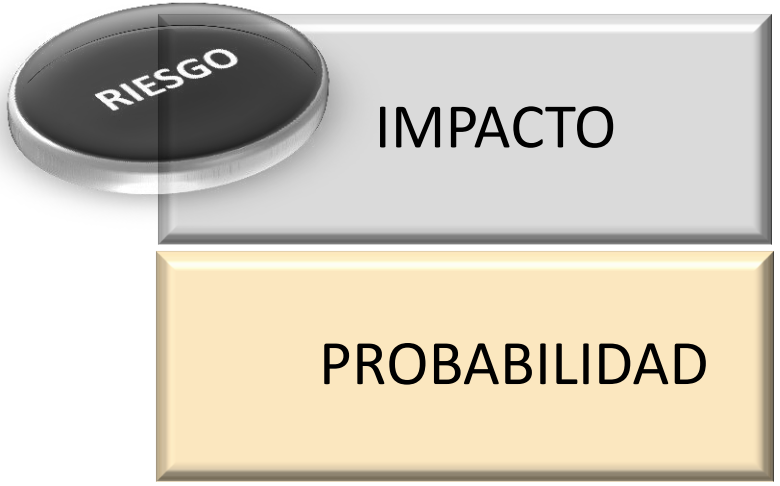
- Organización e implantación del proceso de seguridad
- Análisis y Gestión de Riesgos
- Gestión de personal
- Profesionalidad
- Autorización y control de los accesos
- Protección de las instalaciones
- Adquisición de productos
- Seguridad por defecto
- Integridad y actualización del sistema
- Protección de la Información almacenada y en tránsito
- Prevención ante otros sistemas de información interconectados
- Registro de actividad
- Incidentes de seguridad
- Continuidad de la actividad
- Mejora continua del proceso de seguridad

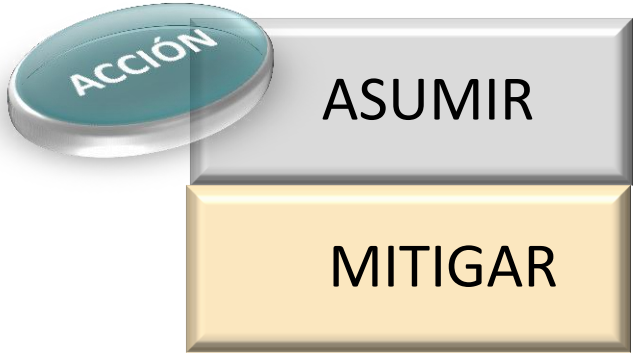
8.1 Organización e implantación del proceso de seguridad

- Nombramiento de:
  - Responsable de Seguridad
  - Responsable del Sistema
  - Responsable de la Información
  - Responsable del Servicio
- Documentar Responsabilidades y funciones de cada puesto.

8.2 Análisis y Gestión de los riesgos







8.3 Gestión de personal

- Formación en seguridad de la información y en el ENS
- Cumplimiento de las normas de seguridad de la Organización
- Identificación única en los sistemas de información

8.4 Profesionalidad

- Auditorías por personal cualificado
- Formación específica a los que cuentan con responsabilidades dentro del ENS

8.5 Autorización y control de los acceso

- Tecnologías
  - Autenticación
  - Permisos
  - Roles

8.6 Protección de las instalaciones

- Las instalaciones deben protegerse contra daños que puedan afectar a los sistemas que albergan.
- Para acceder a los sistemas deberá existir un control de acceso como mínimo mediante salas cerradas y con control de llaves.

8.7 Adquisición de productos de seguridad

- Los productos de seguridad que se adquieran deberán ser idealmente certificados en seguridad según alguna norma o estándar reconocido internacionalmente
- En este contexto, lo habitual será la certificación en Common Criteria.
- Los productos o servicios relacionados con la administración electrónica deben cumplir con los requisitos establecidos por el ENS para el nivel de seguridad definido.

8.8 Seguridad por defecto

- Mínima funcionalidad requerida para que la organización solo alcance sus objetivos, y no alcance ninguna otra funcionalidad adicional.
- Las funciones de operación, administración y auditoría del sistema serán las mínimas necesarias.
- El uso ordinario del sistema ha de ser sencillo y seguro

8.9 Integridad y actualización del sistema

- Autorización formal para la instalación de un nuevo sistema ó aplicación.
- Se gestionan las vulnerabilidades y actualizaciones de los sistemas.
- Del mismo modo, el ENS se deberá mantener actualizado de manera permanente

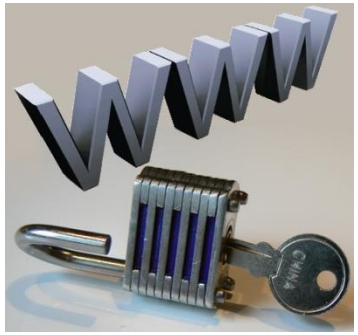
8.10 Protección de la información almacenada y en tránsito

Normas para:

- PORTÁTILES
- PDAS
- PERIFÉRICOS
- SOPORTES
- DOCUMENTACIÓN EN PAPEL

8.11 Prevención ante otros sistemas de información interconectados

- Analizar los riesgos derivados de la interconexión del sistema con otros sistemas de otras Administraciones públicas.
- **Tecnologías:**
  - Cortafuegos
  - VPN
  - Redes inalámbricas deshabilitadas.
  - Administradores de redes
  - Cableado Seguro
  - Control de accesos remotos



8.12 Registros de actividad

- Tecnologías
  - Detección de Intrusos
  - Análisis de Logs
  - Test de penetración
  - Análisis de vulnerabilidades
  - Registros de acceso a aplicaciones

8.13 Incidentes de seguridad

- Sistema de Detección y Reacción frente a Código Dañino
- Registro de incidentes y acciones a seguir
- Mejora continua
- El Centro Criptológico Nacional (CCN) articulará la respuesta a los incidentes de seguridad en torno a la estructura denominada CCN-CERT

8.14 Continuidad de la actividad

- Las Administraciones Públicas deberán de establecer los mecanismos necesarios para garantizar la continuidad de la actividad en caso de incidencia grave o contingencia que impida el uso de los mecanismos habituales de trabajo.
- Tecnologías
  - Back-Ups
  - Almacenamiento seguro
  - Copias en segunda ubicación
  - Pruebas de recuperación
  - Sistemas de replicado

9. CORRESPONDENCIA ENS-ISO 27001 (I)

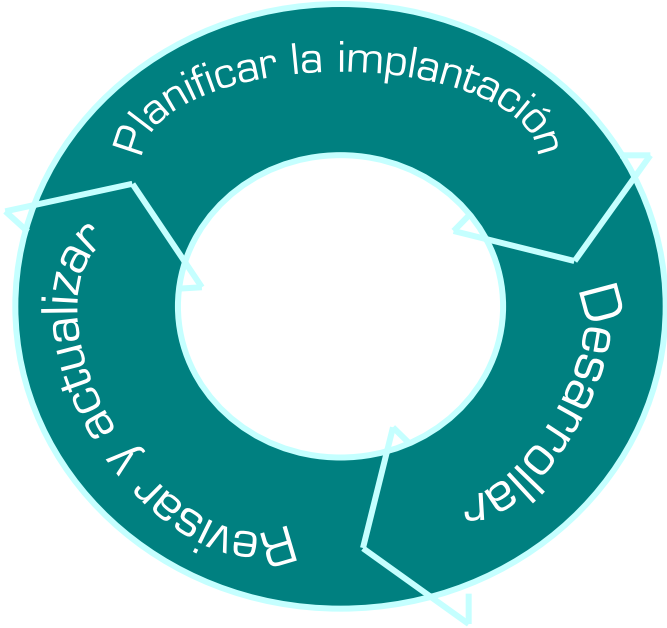
ENS	REQUISITO	ISO 27001
11	Política de Seguridad	4.2.1.b)
12	Compromiso de la dirección	5.1.c) d)
13.1 13.2	Evaluación de riesgos	4.2.1.c) d) e)
13.3	Gestión de riesgos	4.2.1.f) g)
27.1	Documento de Aplicabilidad	4.2.1.g)
14 - 15	Formación	5.2.2
34.1	Auditorías	4.2.3.e) - 6
26	Mejora continua	8.1

9. CORRESPONDENCIA ENS-ISO 27001 (II)

ENS	REQUISITO	ISO 27001
14.3	Uso aceptable de los activos	A7.1.3
14.4	Gestión de privilegios de los usuarios	A10.10.1 A11.2
15.3	Controlar los riesgos de terceros	A6.2
16	Gestión de altas y bajas de usuarios	A11.2.1
17	Control de acceso	A9.1
25	Copias de seguridad	A10.5.1 - 14.1
24.1	Política de prevención de malware	A10.4
24.2	Gestión de incidentes	A13.1 - A13.2
27.2	LOPD	A15.1.4
33.2	Firma electrónica	A12.3 A15.1.6

10. PROYECTO DE IMPLANTACIÓN

1. Planificar la implantación
   - Organizar el Comité de Seguridad
   - Realizar plan de acción
   - Establecer objetivos
   - Recopilar información
2. Desarrollar
   - Política de Seguridad
   - Inventario de activos
   - Categorización de sistemas
   - Análisis de riesgos
   - Documento de aplicabilidad
   - Normativa de seguridad
3. Revisar y actualizar
   - Verificar y validar objetivos
   - Formación
   - Planes de auditorías



11. TAREA 1: PLANIFICACIÓN

- Asignar formalmente los cargos de Responsable de Seguridad, Responsable del Servicio y Responsable de la Información.
- Crear y definir el/los Comité/s de Seguridad, responsable de velar por el cumplimiento de la política de seguridad de la organización y establecer los objetivos.
- Recopilar los servicios electrónicos e infomación que componen el/los sistemas de la entidad.

12. TAREA 2: DESARROLLO (1)

- Definir y aprobar formalmente la Política de Seguridad. Deberá ser aprobada por el titular responsable de la acción de gobierno.
- Definir el conjunto de activos sujetos al ENS, identificando los sistemas existentes en la organización y valorándolos de acuerdo a las dimensiones de seguridad especificadas en el esquema.
- Determinar la categoría del sistema o sistemas identificados.

12. TAREA 2: DESARROLLO (2)

- Determinar las **medidas de seguridad** del Anexo 1 que aplican a los sistemas según su nivel.
- Llevar a cabo el **Análisis de Riesgos**.
- Documentar la **Declaración de Aplicabilidad.**
- Definir la **Normativa de Seguridad**, detallando cómo y quien hace las distintas tareas.

13. CATEGORIZACIÓN DE SISTEMAS

ACTIVOS	SERVICIOS		INFORMACIÓN		SISTEMA
DIMENSIONES	Portal web	Gestión de Expedientes	Información web	Información de Expedientes	
Confidencialidad	Sin valorar	M	B	M	**M**
Integridad	B	M	B	M	**M**
Autenticidad	B	M	B	M	**M**
Trazabilidad	B	M	B	M	**M**
Disponibilidad	M	B	M	A	**A**

14. NORMATIVAS DE SEGURIDAD (PARTE 1)

14. NORMATIVAS DE SEGURIDAD (PARTE 2)

- Política de seguridad
- Normativa de seguridad
- Procedimientos de seguridad
- Procesos de autorización
- Órganos de gestión
- Auditorías de seguridad: Cumplimiento legal y cumplimiento técnico

14. NORMATIVAS DE SEGURIDAD (PARTE 3)

- 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 en la vida laboral

15. NORMATIVAS DE SEGURIDAD (PARTE 4)

- 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

16. TAREA 4: REVISAR Y MANTENER

- Formar a todo el personal sobre la política, normativa y procedimientos de seguridad.
- Evaluar los objetivos midiendo la eficacia de las medidas adoptadas.
- Revisar el sistema de gestión de la seguridad y mantenerlo actualizado.
- Realización de una Auditoría bienal de Seguridad que revise la política de seguridad y su cumplimiento, así como el conjunto de riesgos, normativas, procedimientos y controles establecidos.

17. CONCLUSIONES

La correcta implantación del ENS aportará:

- Confianza en la relación de los ciudadanos con la Administración.
- Aumento de la satisfacción de los usuarios.
- Mejorar la Gestión de Seguridad de la Información, favoreciendo el desarrollo de la propia Administración:
  - ✓ Mejorando la gestión de recursos y costes.
  - ✓ Aumentando la eficiencia y productividad.
  - ✓ Buscando la mejora continua.

18. GUIA AMETIC

Start Up, ha elaborado una guía práctica sobre el ENS publicada a través de la página de AMETIC.

http://www.ametic.es/projects/ens/Events/EventDetail.aspx?ID=257

Gracias por su atención

START-UP S.L.
www.seguridadinformacion.com
www.esquemanacionaldeseguridad.com

info@seguridadinformacion.com