Interreg
España – Portugal

Cofinanciado por la Unión Europea

IBERUS SMART

Ayuntamiento Ponferrada

ENS: Pilar Fundamental de la Protección Digital

Introducción

El Esquema Nacional de Seguridad (ENS) es la norma básica de referencia en España para garantizar la protección de los sistemas, servicios y datos en el ámbito de la administración electrónica. Su cumplimiento es obligatorio para todas las administraciones públicas y también para empresas que prestan servicios tecnológicos a éstas.

En este seminario exploraremos qué es el ENS, por qué es esencial en el contexto actual de digitalización, cómo se estructura, y cómo se puede implementar de forma práctica en el ámbito local.

Qué es el ENS

El ENS se estableció por el artículo 156 de la Ley 40/2015 y se desarrolla reglamentariamente en el Real Decreto 311/2022. Su **objetivo es crear las condiciones necesarias para garantizar la seguridad en el uso de medios electrónicos por parte del sector público**, estableciendo una política de seguridad común basada en principios, requisitos mínimos y medidas de protección.

Conceptos clave

- **Seguridad de la información**: Conjunto de medidas destinadas a proteger la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información.
- **Sistema de información**: Conjunto de recursos organizativos, humanos y tecnológicos que procesan y gestionan información.
- **Categoría del sistema**: Clasificación del sistema según el nivel de impacto que tendría una amenaza sobre los servicios esenciales, pudiendo ser **Básica**, **Media** o **Alta**.
- **Responsables del sistema**: Distintas figuras que asumen la responsabilidad de implementar y garantizar la seguridad del sistema, como el Responsable de Seguridad, el Responsable del Servicio, el Responsable de la Información y el Responsable del Sistema.
- **Medidas de seguridad**: Controles y actuaciones establecidos por el ENS para garantizar la protección adecuada de los sistemas de información.

Marco normativo

El ENS se desarrolla en el ámbito de la legislación española y europea para garantizar la protección de los sistemas de información públicos:

- Ley 39/2015, del Procedimiento Administrativo Común.
- Ley 40/2015, de Régimen Jurídico del Sector Público.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (reemplaza al RD 3/2010).
- Reglamento (UE) 2016/679 (RGPD).
- Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).
- Normas técnicas de interoperabilidad (NTI).
- Directrices del CCN-CERT y el Centro Criptológico Nacional (CCN).

El ENS **es obligatorio para todas las Administraciones Públicas y para los proveedores** que prestan servicios vinculados a sistemas de información públicos.

Interreg
España – Portugal

Cofinanciado por la Unión Europea

IBERUS SMART

Ayuntamiento Ponferrada

Entender el ENS

Entender el ENS

Está regulado por el Real Decreto 311/2022 y establece las normas y medidas de **ciberseguridad obligatorias** para las administraciones públicas y sus proveedores tecnológicos. Su objetivo es garantizar la **protección de la información, la continuidad de los servicios digitales y la resiliencia ante ciberataques**.

El ENS se estructura en **10 principios** básicos, **3 niveles** según el impacto que tendría un problema de seguridad. Además, detalla las **75 medidas** (medidas organizativas, técnicas y operativas), destinadas a para proteger la confidencialidad, integridad y disponibilidad de los datos públicos.

Principios básicos (I)

los fundamentos que orientan el diseño, implantación y gestión del sistema de seguridad de la información en las Administraciones Públicas. Están recogidos en el artículo 10 del **Real Decreto 311/2022**, y funcionan como una **filosofía de actuación** que debe impregnar todas las medidas técnicas, organizativas y procedimentales y su objetivo asegurar que **la seguridad no sea una capa añadida**, sino una parte intrínseca, transversal y sostenible de cualquier sistema de información público.

Principios básicos (II)

Seguridad como proceso integral :
La seguridad no es solo un tema tecnológico o de TI. Abarca procesos, personas, tecnología, datos, instalaciones, proveedores, decisiones políticas y operativas. Es transversal.

> Una administración no puede limitarse a tener un antivirus actualizado; debe formar a los usuarios, definir políticas de uso, clasificar la información y auditar servicios externos

Gestión de riesgos:
Todas las medidas de seguridad deben responder a un análisis de riesgos previo: qué puede fallar, qué consecuencias tendría y cómo prevenirlo o mitigarlo

> En un ayuntamiento pequeño, quizá no es viable implantar una infraestructura de ciberseguridad compleja, pero sí se puede priorizar el refuerzo de la autenticación y las copias de seguridad

Principios básicos (II)

Prevención, detección, respuesta y recuperación:
El ciclo de seguridad debe ser completo: prevenir incidentes, detectarlos rápidamente, responder eficazmente y restaurar los sistemas afectados.

> Un ransomware entra por un correo. Si se detecta tarde y no hay plan de recuperación, el sistema queda bloqueado

Líneas de defensa:
La seguridad debe estructurarse en capas: multicapa o defensa en profundidad. Si una falla, otra la compensa

> Aunque haya una VPN segura, también es necesario usar doble factor de autenticación, limitar accesos, y monitorizar la actividad.

Principios básicos (II)

Reevaluación periódica:
La seguridad no es estática. Cambian los sistemas, los usuarios, las amenazas… Por eso hay que revisar y actualizar el análisis de riesgos y las medidas.

> Un ayuntamiento que digitaliza expedientes debe reevaluar su ENS al cambiar su infraestructura o al contratar una nueva solución SaaS

Función diferenciada :
Debe haber una clara separación entre quienes usan, gestionan y supervisan la seguridad. Evita conflictos de interés y fortalece el control

> No es adecuado que el técnico informático que administra el sistema sea también el que se audita a sí mismo

Principios básicos (II)

Minimización :
Solo debe recopilarse, tratarse y conservarse la información necesaria. También se debe minimizar el número de personas con acceso, los privilegios, los servicios expuestos.

> No mantener bases de datos históricas con DNIs y direcciones de antiguos usuarios de un servicio de guardería si ya no son necesarias

Proporcionalidad :
Las medidas de seguridad deben estar ajustadas a los riesgos y al valor del activo. Ni quedarse corto ni pasarse.

> Un servidor con datos sensibles debe tener cifrado, autenticación robusta y monitoreo. Una web informativa pública puede tener medidas básicas

Principios básicos (II)

Responsabilidad :
La seguridad es una responsabilidad que no se puede delegar sin control. Cada actor debe asumir su parte: técnicos, responsables políticos, proveedores

Un alcalde o secretario debe firmar la política de seguridad y entender su contenido y obligaciones

Auditoría y mejora contínua :
La seguridad no se da por sentada: se evalúa mediante auditorías, se detectan desviaciones, se aplican mejoras.

Una entidad que ha implantado un sistema de notificaciones electrónicas debe auditar el cumplimiento de las medidas ENS cada 2 años

Niveles de seguridad

Nivel Básico: Requisitos mínimos de seguridad para sistemas con **bajo impacto** si ocurre un fallo.

- Medidas como: control de accesos básicos, copias de seguridad simples

Nivel Medio: Mayor protección porque el impacto de un fallo sería **moderado**

- Medidas como: Autenticación de doble factor para accesos, cifrado de datos personales, registro de actividad y auditoría, planes de recuperación ante desastres.

Nivel Alto Máximo nivel de seguridad porque una brecha puede generar **graves consecuencias**.

- Medidas como Cifrado de toda la información, seguridad avanzada de redes y sistemas y supervisión continua, planes de contingencia

Medidas de seguridad

Las medidas de seguridad son el conjunto de controles técnicos, organizativos y operacionales que deben aplicarse a los sistemas de información para garantizar los principios de confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad. Están definidas en el Anexo II del Real Decreto 311/2022 y se aplican según la categoría del sistema (Básica, Media o Alta).

Las medidas se agrupan en cuatro bloques:

- **Medidas organizativas**: Relacionadas con la gobernanza y gestión de la seguridad (políticas, roles, formación…).
- **Medidas operacionales**: Relativas a la operación diaria del sistema (registro de actividad, gestión de incidentes, backups…).
- **Medidas de protección**: Tecnológicas, para proteger los activos ante amenazas (firewalls, cifrado, antivirus…).
- **Medidas específicas para entornos externos**: Aplicables a servicios cloud, subcontratación y proveedores TIC.

Medidas de seguridad

Medidas organizativas

- Política de seguridad
- Organización de la seguridad
- Control de acceso físico
- Gestión de personal

Medidas operacionales

- Protección de la información
- Seguridad por defecto
- Gestión de incidentes
- Copias de seguridad
- Registro de actividad

Medidas de seguridad

Medidas de protección

- Protección frente a código malicioso
- Protección de comunicaciones
- Gestión de vulnerabilidades
- Monitorización continua
- Cifrado y control de medios

Requisitos adicionales para entornos cloud o servicios externalizados

- Gestión del ciclo de vida del servicio
- Evaluación continua del proveedor
- Garantía de ubicación y control del dato

Interreg
España – Portugal
Cofinanciado por la Unión Europea
IBERUS SMART
Ayuntamiento Ponferrada

Otros aspectos del ENS

Relación entre las normas de seguridad (I)

	RGPD	LOPDGDD	ENS
Ámbito de aplicación	Toda la UE (empresas y administraciones públicas)	España (complementa el RGPD)	Administraciones públicas y empresas que trabajen con ellas en España
Objetivo principal	Proteger los datos personales y garantizar la privacidad	Adaptar el RGPD al contexto español y regular derechos digitales	Garantizar la seguridad de los sistemas de información públicos
Obligatoriedad	Obligatorio para cualquier entidad que trate datos personales	Obligatorio en España para entidades que traten datos personales	Obligatorio para administraciones y proveedores de servicios
Protección de datos personales	Sí, regula el tratamiento y los derechos de los ciudadanos	Sí, detalla normas y derechos digitales específicos	No regula protección de datos personales, pero los protege mediante medidas técnicas
Seguridad de la información	No regula medidas técnicas específicas, pero exige seguridad	No regula medidas técnicas, pero establece directrices	Sí, establece medidas técnicas y operativas obligatorias

Relación entre las normas de seguridad (II)

	RGPD	LOPDGDD	ENS
Medidas de seguridad	Principios generales de seguridad y protección de datos	Regulación específica en ámbitos laborales, educativos y de videovigilancia	75 medidas de seguridad organizativas, operacionales y técnicas
Notificación de brechas de seguridad	Obligatoria en 72 horas en caso de filtración de datos personales	Amplía la regulación del RGPD y la coordinación con la AEPD	Obligatoria según nivel de seguridad del sistema (Básico, Medio, Alto)
Roles y responsabilidades	Responsable del Tratamiento, Encargado del Tratamiento, Delegado de Protección de Datos (DPD)	Incluye derechos digitales y normas sobre tratamiento en distintos sectores	Responsable de Seguridad, Responsable del Sistema, Delegado de Seguridad
Niveles de seguridad	No establece niveles, solo exige seguridad adecuada al riesgo	No establece niveles, pero exige medidas adecuadas	Tres niveles: Básico, Medio y Alto
Sanciones por incumplimiento	Multas hasta 20 millones de euros o el 4% de la facturación anual	Sanciones similares al RGPD según la AEPD	No establece sanciones económicas directas, pero puede haber restricciones en contratos públicos

ENS en la contratación pública

La contratación pública debe incluir aspectos de seguridad alineados con el ENS. Se recomienda:

- Incluir **cláusulas específicas ENS** en pliegos técnicos y administrativos
- Exigir **certificado de conformidad ENS** para categoría media o alta
- Evaluar la **adecuación de los servicios externalizados** a las medidas ENS
- Establecer controles de seguimiento y auditoría

Elementos clave en los pliegos:

- Definición de roles y responsabilidades
- Requisitos de seguridad en la prestación del servicio
- Obligaciones en caso de incidentes de seguridad
- Garantía de continuidad del servicio
- Mecanismos de control y supervisión

Resumen de principios del ENS

Principio	¿Qué busca?	Cómo aplicarlo
Seguridad integral	Ver la seguridad como algo transversal	Afecta a procesos, personas, tecnología y datos
Gestión de riesgos	Decidir basándose en análisis de impacto	Usar metodologías como MAGERIT
Ciclo de seguridad	Prevenir, detectar, responder, recuperar	Tener planes y herramientas en cada fase
Líneas de defensa	Redundancia en la protección	Seguridad por capas (lógica, física, humana)
Reevaluación	Adaptación continua	Revisar cada vez que cambie el entorno o la amenaza
Función diferenciada	Separación de roles y responsabilidades	No mezclar supervisión y ejecución
Minimización	Menos es más	Reducir información, acceso, datos y privilegios
Proporcionalidad	Ajustar la seguridad al riesgo	Ni infra ni sobreproteger
Responsabilidad	Que cada actor asuma lo que le toca	Designar y documentar responsables
Auditoría/mejora continua	Revisar para mejorar	Auditorías periódicas, planes de mejora, seguimiento

Resumen medidas de seguridad

Grupo	Tipo de control	¿Qué cubre?	Medidas
Organizativas	Políticas y gobernanza	Roles, formación, gestión de riesgos	9
Operacionales	Gestión diaria del sistema	Accesos, incidentes, backups, continuidad	11
Protección	Tecnologías defensivas	Criptografía, software, comunicaciones, malware	12
Externos/Cloud	Relación con terceros	Servicios cloud, SLAs, evaluación de proveedores	4
TOTAL			36

Proceso de adecuación al ENS en una EE.LL

Implementar el ENS en una entidad local no es una tarea inmediata, sino un proceso que debe planificarse en fases. Estas son las etapas más habituales:

1. Diagnóstico inicial: identificar los sistemas de información, procesos afectados, y estado actual de la seguridad.
2. Categorización de sistemas: analizar el impacto sobre la confidencialidad, integridad y disponibilidad.
3. Análisis de brechas: comparar la situación actual con los requisitos del ENS para el nivel correspondiente.
4. Plan de adecuación: definir las medidas necesarias, responsables, plazos y recursos.
5. Implementación progresiva: desplegar las medidas organizativas y técnicas.
6. Evaluación y auditoría: verificar el cumplimiento mediante revisión interna o auditoría externa.

Enlaces

Real Decreto 311/2022 – BOE
https://www.boe.es/eli/es/rd/2022/05/03/311
Portal del ENS – CTT
https://administracionelectronica.gob.es/ctt/ens
Guías CCN-STIC del ENS
https://www.ccn-cert.cni.es/es/guias.html
Guía CCN-STIC 808 – Verificación del cumplimiento del ENS
https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/3677-ccn-stic-808-verificacion-del-cumplimiento-del-esquema-nacional-de-seguridad/file.html
Guía CCN-STIC 830 – Ámbito de aplicación del ENS
https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/3706-ccn-stic-830-el-ambito-de-aplicacion-del-ens/file.html
FAQ oficial del ENS (CCN-CERT)
https://ens.ccn-cert.cni.es/faqs/