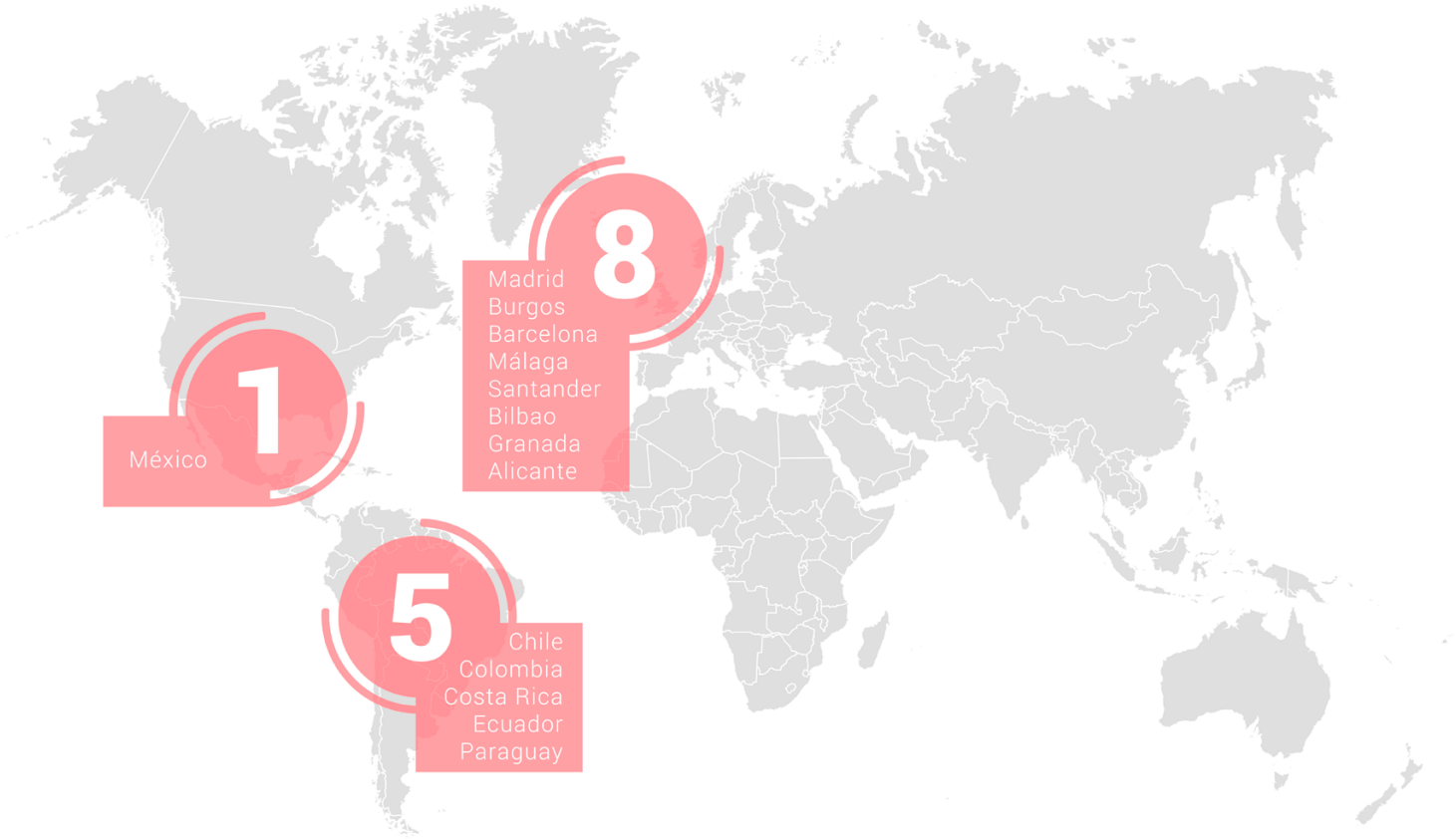
GrupoACMS
CONSULTORES

GRUPO ACMS Consultores

Esquema Nacional de Seguridad (ENS)



AENOR
ER
Empresa Registrada
ISO 9001

(ER-0772/2013)

Alcance ISO 9001

Diseño, desarrollo, implantación, formación y mantenimiento de sistemas de gestión de la calidad, medioambiental, de la prevención de riesgos laborales, protección de datos, seguridad alimentaria y de la calidad y competencia técnica en laboratorios clínicos.

Alcance ISO 27001

Los sistemas de información que dan soporte a las actividades de diseño, desarrollo, implantación, formación y mantenimiento de sistemas de gestión y el diseño, desarrollo y comercialización de software de sistemas de gestión de acuerdo con la declaración de aplicabilidad vigente.

AENOR
ER
Seguridad Información
ISO/IEC 27001

(SI-0021/2020)

Si necesita implantar el Esquema Nacional de Seguridad (ENS) enGrupo ACMS Consultores podemos asesorarle.

Índice de Contenidos

1. ¿Qué es el Esquema Nacional de Seguridad?

El Esquema Nacional de Seguridad (ENS) es un conjunto de medidas y políticas de seguridad de la información, establecido por el Gobierno de España, que tiene como objetivo principal garantizar la protección de los sistemas, datos e información gestionados por las diferentes Administraciones Públicas Españolas.

El ENS se presenta como un marco obligatorio para asegurar la confidencialidad, integridad y disponibilidad de los datos en el sector público.

Este esquema es esencial para proteger los sistemas de información de amenazas como ciberataques y accesos no autorizados, proporcionando un marco robusto para que las entidades públicas y organizaciones privadas que gestionan servicios para el sector público establezcan medidas preventivas y controlen los riesgos de manera efectiva.

A través de esta normativa, se fomenta la confianza en los servicios digitales del sector público, garantizando que la información sensible de los ciudadanos y otros datos de interés nacional se manejen de forma segura y conforme a los estándares de ciberseguridad.

La adopción del ENS permite a las organizaciones operar con mayor seguridad en el ámbito digital, respaldando un compromiso claro con la protección de la información en el contexto actual.

2. Ámbito de Aplicación del Esquema Nacional de Seguridad (ENS)

El Esquema Nacional de Seguridad (ENS) está diseñado para proteger los sistemas y datos de las entidades públicas y, en muchos casos, de organizaciones privadas que colaboran o prestan servicios a las administraciones públicas. Su ámbito de aplicación abarca diversas entidades y sectores clave:

- Administraciones Públicas: Todos los niveles de la administración pública en España, desde el gobierno central hasta los autonómicos y locales, deben cumplir con el ENS. Esto incluye organismos como ayuntamientos, diputaciones provinciales y consejerías autonómicas, que gestionan datos sensibles de los ciudadanos y operan servicios críticos para el público.

- Entidades Públicas Especializadas: Organismos específicos como universidades públicas, hospitales del sistema nacional de salud, y entidades de investigación también están obligados a implementar las medidas del ENS, dada la naturaleza sensible de los datos que manejan y su impacto en servicios esenciales.

- Empresas Privadas con Contratos Públicos: Muchas empresas tecnológicas, proveedores de software y contratistas de servicios públicos también deben cumplir con los requisitos del ENS cuando prestan servicios a entidades del sector público. Por ejemplo, una empresa de tecnología que desarrolle sistemas de gestión de datos para un ministerio o un proveedor de servicios en la nube que aloje información para una administración local necesita cumplir con el ENS para asegurar la protección adecuada de la información que gestiona.

Niveles de Gestión Afectados

El ENS establece requisitos que impactan en múltiples niveles de gestión dentro de estas entidades:

- Acceso y autenticación de usuarios: Controla quién puede acceder a los sistemas de información, estableciendo medidas de autenticación para proteger los datos sensibles y evitar accesos no autorizados.

- Gestión de la infraestructura tecnológica: Impone medidas de seguridad en servidores, bases de datos y redes, con el objetivo de blindar la infraestructura frente a ciberamenazas y ataques externos.

- Protección de datos: Asegura que la información se almacena y procesa de manera segura, garantizando la integridad y confidencialidad de los datos, especialmente en sectores críticos como la salud y la investigación.

- Mantenimiento de la disponibilidad del servicio: El ENS también se enfoca en asegurar que los sistemas y servicios estén disponibles para los usuarios cuando se necesiten, evitando caídas y asegurando la continuidad operativa.

3. ¿Por qué implementar el ENS fortalece la seguridad y la confianza?

Es importante destacar que implementar el ENS no solo protege la información y asegura el cumplimiento normativo, sino que también posiciona a la organización como un referente en seguridad digital, aumentando su competitividad y mejorando su capacidad para afrontar los desafíos de un entorno cada vez más digitalizado.

La implementación del ENS en una organización proporciona beneficios significativos que van más allá del cumplimiento normativo. Este sistema se convierte en una herramienta estratégica que refuerza la seguridad, mejora la confianza de los usuarios y protege la infraestructura tecnológica frente a amenazas digitales cada vez más complejas. A continuación, se detallan algunas de las principales ventajas de adoptar el ENS:

Mejora de la Confianza y la Reputación

Cumplir con el ENS refuerza la confianza de los usuarios y colaboradores al asegurar que la información gestionada está protegida bajo un marco riguroso de seguridad. Para las administraciones públicas, esto es clave, ya que transmite a los ciudadanos un compromiso con la protección de sus datos personales y la continuidad de los servicios digitales. En el caso de empresas privadas que trabajan con la administración, cumplir con el ENS refuerza su reputación como socios confiables, lo que puede abrir nuevas oportunidades de negocio en el sector público.

Ejemplo: Un hospital público que implemente el ENS puede comunicar a sus pacientes que sus datos de salud están resguardados bajo un sistema de protección robusto, lo cual genera mayor tranquilidad y confianza en el servicio.

- Reducción de Riesgos de Ciberataques

El ENS ayuda a las organizaciones a identificar y mitigar riesgos de ciberseguridad, reduciendo la probabilidad de sufrir incidentes como ataques de ransomware, brechas de datos o accesos no autorizados. Al establecer controles y medidas de protección, las organizaciones se blindan contra amenazas externas e internas, minimizando el impacto en caso de que ocurra un incidente.

Recomendación: Realizar evaluaciones de riesgo periódicas es clave para identificar vulnerabilidades y ajustar las medidas del ENS. Por ejemplo, una universidad pública que gestione datos de investigación puede identificar los sistemas más vulnerables y aplicar mejoras específicas en esos puntos.

- Cumplimiento de Regulaciones y Normativas Internacionales

Implementar el ENS garantiza que la organización cumple con los requisitos de seguridad obligatorios en España, lo cual es especialmente relevante para entidades públicas y empresas que trabajan con el sector público. Además, el ENS se alinea con otras normativas internacionales de seguridad, como ISO/IEC 27001, facilitando a las organizaciones cumplir con regulaciones internacionales cuando operan en mercados globales.

Ejemplo: Una empresa de tecnología que desee colaborar con administraciones públicas en proyectos internacionales puede beneficiarse del ENS, ya que facilita la adaptación a requisitos de seguridad en otros países, abriendo así las puertas a nuevos mercados.

- Optimización de la Infraestructura y Eficiencia Operativa

La implementación del ENS no solo asegura la protección de la información, sino que también contribuye a la modernización y optimización de la infraestructura tecnológica. Al estandarizar y automatizar procesos de seguridad, las organizaciones pueden reducir la carga de trabajo en los equipos de IT, optimizando la eficiencia operativa y permitiendo una gestión más efectiva de los recursos.

Recomendación: Implementar sistemas de monitoreo y alertas automáticas puede ayudar a los equipos a identificar posibles riesgos antes de que se conviertan en amenazas, asegurando una respuesta rápida y eficiente.

- Aseguramiento de la Continuidad del Servicio

El ENS incluye medidas para garantizar la disponibilidad de los sistemas críticos, lo que significa que los servicios continuarán operativos incluso en situaciones de crisis o ciberataques. Esto es crucial para organizaciones que prestan servicios públicos esenciales, ya que una interrupción puede tener un impacto severo en la población.

Ejemplo: En un ayuntamiento, contar con un plan de recuperación ante desastres basado en el ENS asegura que los servicios clave, como la atención ciudadana o el acceso a documentación pública, permanezcan accesibles incluso durante un incidente de seguridad.

4. ¿Dónde se regula?

El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad sustituye al Real Decreto 3/2010, de 8 de enero, por el que se regula el ENS en el ámbito de la Administración Electrónica.

Existen diversas medidas de seguridad recogidas en el ENS, que se dividen en 3 grupos (Anexo II del Real Decreto 311/2022):

- Marco organizativo: las medidas son acerca de la política de seguridad, Los procedimientos y normas de seguridad, los procesos sobre autorizaciones, etc.

- Dentro del marco operacionalse aprecian medidas sobre la planificación, análisis de riesgos, control de accesos, la continuidad del servicio, la monitorización de los sistemas, etc.

- Las medidas para la protecciónson varias para proteger instalaciones e infraestructuras, gestión del personal, servicios, comunicaciones, soportes de información, etc.

Es importante destacar que el cumplimiento del ENS es obligatorio para las Administraciones Públicas y sus proveedores.

5. ¿Cuáles son sus objetivos?

El objetivo principal del Esquema Nacional de Seguridad es asegurar la protección de los sistemas de información, garantizando la disponibilidad, confidencialidad, integridad y autenticidad de los mismos, así como la protección de los derechos y libertades de las personas físicas.

De esta manera, se busca establecer un marco común de seguridad para todas las administraciones públicas españolas, que permita prevenir y mitigar los riesgos de seguridad asociados al uso de las tecnologías de la información.

El Esquema Nacional de Seguridad, actualizado en 2022, pretende cumplir tres objetivos:

- Alinear el ENS con el marco normativo y el contexto estratégico existente para garantizar la seguridad en la administración digital. Se trata de reflejar con claridad el ámbito de aplicación del ENS en beneficio de la ciberseguridad y de los derechos de los ciudadanos.

- Introducir la capacidad de ajustar los requisitos del ENS, para garantizar su adaptación a la realidad de ciertos colectivos o tipos de sistemas, atendiendo a la semejanza que presentan una multiplicidad de entidades o servicios en cuanto a los riesgos a los que están expuestos sus sistemas de información y sus servicios.

- Facilitar una mejor respuesta a las tendencias en ciberseguridad, reducir vulnerabilidades y promover la vigilancia continua mediante la revisión de los principios básicos, de los requisitos mínimos y de las medidas de seguridad.

El objeto último de la seguridad de la información, como se define en el Esquema de Seguridad Nacional es garantizar que una organización podrá cumplir sus objetivos, desarrollar sus funciones y ejercer sus competencias utilizando sistemas de información.

Por ello, en materia de seguridad de la información deberán tenerse en cuenta los siguientes principios básicos:

- Seguridad como proceso integral.

- Gestión de la seguridad basada en los riesgos.

- Prevención, detección, respuesta y conservación.

- Existencia de líneas de defensa.

- Vigilancia continua.

- Reevaluación periódica.

- Diferenciación de responsabilidades.

6. ¿Necesita asesoramiento?

Si necesita asesoramiento para implantar los procedimientos y requisitos que aplica el Esquema Nacional de Seguridad, enGrupo ACMS Consultorespodemos asesorarle.

Lo primero que se debe analizar y tener en cuenta a la hora de implantar el Esquema Nacional de Seguridad es la categorización de la seguridad de los sistemas de información, tal y como se describe en el Anexo I del Real Decreto 311/2022, de 3 de mayo.

Esto se realizará teniendo en cuenta las 5 dimensiones de la seguridad: Confidencialidad, Integridad, Trazabilidad, Autenticidad y Disponibilidad de la información. Así se definen 3 niveles de Seguridad: Bajo, Medio y Alto. Y a partir de aquí, se definen tres categorías de seguridad: BÁSICA, MEDIA y ALTA.

- Un sistema de información será de categoría ALTA si alguna de sus dimensiones de seguridad alcanza el nivel de seguridad ALTO.

- Un sistema de información será de categoría MEDIA si alguna de sus dimensiones de seguridad alcanza el nivel de seguridad MEDIO, y ninguna alcanza un nivel de seguridad superior.

- Un sistema de información será de categoría BÁSICA si alguna de sus dimensiones de seguridad alcanza el nivel BAJO, y ninguna alcanza un nivel superior.

Para lograr el cumplimiento de los principios básicos y requisitos mínimos establecidos se aplicarán las medidas de seguridad indicadas en el Anexo II, en el cual se incluye una Tabla con la correspondencia de Medidas de Seguridad a aplicar por cada uno de los Marcos definidos (organizativo, operacional y medidas de protección) en función de las dimensiones de seguridad, la Categoría de seguridad del sistema.

Nos definimos como una compañía consultora independiente cuyo objetivo fundamental es suministrar servicios de consultoría en las áreas de Gestión empresarial, que representen para el cliente una solución excelente, que satisfaga sus necesidades explícitas o implícitas, tenga en cuenta las regulaciones y normas aplicables, y cumpla los objetivos de plazo y coste establecidos.

Madrid

C/ Campezo 3, nave 5 28022 Madrid

Tfno.: (+34) 91 375 06 80

Burgos

Centro de Empresas, 73 09007 Burgos

Tfno.: (+34) 947 041 645

Barcelona

C/ Plaça Universitat 3 08007 Barcelona

Tfno.: (+34) 93 013 19 49

Málaga

C/ Alejandro Dumas 17 29004 Málaga

Tfno.: (+34) 95 113 69 04

México

José González Varela 15 14700 Tlalpan

Tfno.: (+52) 5513 39 96 22

www.grupoacms.com
informacion@grupoacms.com