DIPUTACIÓN DE ALMERÍA

Esquema Nacional de Seguridad

Presentación ejecutiva

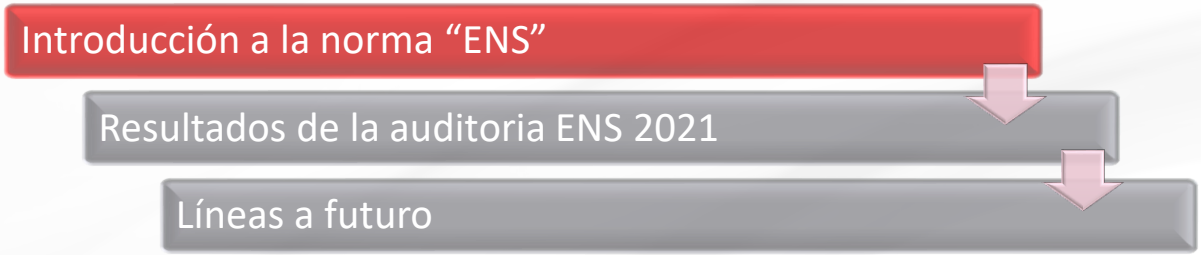
Auditoria 2021

Ingenia

INGENIERÍA E INTEGRACIÓN AVANZADAS

Presentación ejecutiva al Comité de Seguridad

Índice de Contenidos



Introducción a la norma

Esquema Nacional de Seguridad

El Esquema Nacional de Seguridad es un conjunto de **105 controles** de seguridad agrupados en **75 medidas**

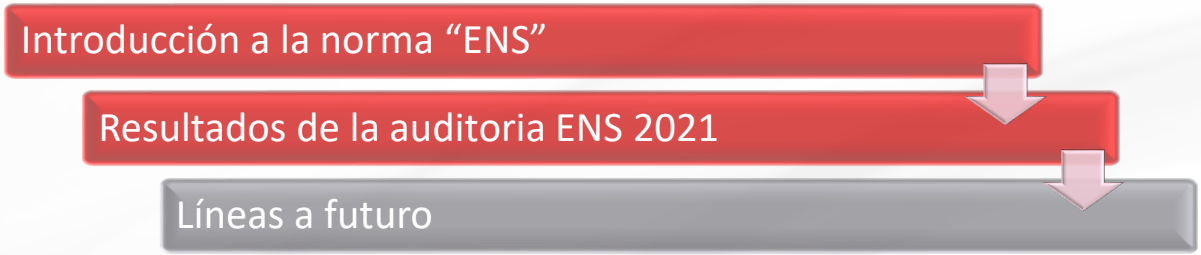
La aplicación de más o menos controles dependerá de la valoración de los servicios

La relación de controles a aplicar viene recogida formalmente en la Declaración de aplicabilidad

Fuente: https://www.ccn-cert.cni.es/ens.html

Presentación ejecutiva al Comité de Seguridad

Índice de Contenidos



Resultados de la auditoria ENS 2021

Visión general en números

Resumen de hallazgos de la Auditoría:

	No Conformidad Mayor	No Conformidad Menor	Observaciones	Sugerencia de Mejora	Conformidad
Marco Organizativo	0	1	0	0	3
Marco Operacional	0	11	0	5	9
Medidas de Protección	0	4	2	4	23
TOTAL	**0**	**16**	**2**	**9**	**35**

Resultados de la auditoria ENS 2021

Medidas de Seguridad del ENS

Marco Organizativo [org.]

Medidas relativas a la organización global de la seguridad

- [org.1] Política de Seguridad (CATEGORIA) ✓
- [org.2] Normativa de Seguridad (CATEGORIA) ✓
- [org.3] Procedimientos de Seguridad (CATEGORIA) ✓
- [org.4] Proceso de Autorización (CATEGORIA) ✗

[org.1] Política de Seguridad

[org.2] Normativa de Seguridad

[org. 3] Procedimientos de Seguridad

[org. 4] Proceso de Autorización

Se ha definido un procedimiento en la materia que incluye una matriz RACI de autorizaciones, pero no está implantado en la organización.

Resultados de la auditoria ENS 2021

Medidas de Seguridad del ENS

Marco Operacional [op.]

Proteger la operación del sistema como conjunto integral de componentes para un fin.

- [op.pl.1] Análisis de Riesgos (CATEGORIA) ✓
- [op.pl.2] Arquitectura de Seguridad (CATEGORIA) ✓
- [op.pl.3] Adquisición de nuevos componentes (CATEGORIA)
- ZA
- [op.pl.4] Dimensionamiento / gestión de capacidades (D) ✗
- [op.pl.5] Componentes certificados (CATEGORIA) **N.A**

[op.pl.1] Análisis de Riesgos

[op.pl.2] Arquitectura de Seguridad

[op.pl.3] Adquisición de nuevos componentes

Se recomienda priorizar desde ya en los pliegos de contratación los componentes presentes en la ultima versión de la guía CCN-STIC-105

[op.pl.4] Dimensionamiento / gestión de capacidades

Control sin aplicar en la actualidad.

[op.pl.5] Componentes certificados

N.A

Resultados de la auditoria ENS 2021

Medidas de Seguridad del ENS

Marco Operacional [op.]

Proteger la operación del sistema como conjunto integral de componentes para un fin

- [op.acc.1] Identificación (AT) ✗
- [op.acc.2] Requisitos de acceso (ICAT) ✗
- [op.acc.3] Segregación de funciones y tareas (ICAT) ✓
- [op.acc.4] Proceso de gestión de derechos de acceso (ICAT) ◉
- [op.acc.5] Mecanismo de autenticación (ICAT) ✗
- [op.acc.6] Acceso local (ICAT) ✗
- [op.acc.7] Acceso remoto (ICAT) ✓

[op.acc.1] Identificación

No están definidos/aprobados formalmente los periodos de retención de cuentas de usuario. No se realiza la revisión de cuentas cada 12 meses por parte de los responsables de servicio indicada en el procedimiento.

[op.acc.2] Requisitos de acceso

No hay evidencia de la aplicación de la regla del mínimo privilegio y necesidad de conocer, puesto que responsables de los sistemas de información no solicitan/aprueban previamente el acceso de los usuarios.

[op.acc.3] Segregación de funciones y tareas

[op.acc.4] Proceso de gestión de derechos de acceso

Procesos de alta y baja definidos con soporte por parte de Intranet y RPC, llega un correo a Sistemas que se encarga del alta/baja en LDAP.

Periodo máximo sin acceso a cuenta tras la cual se inhabilita.

Resultados de la auditoria ENS 2021

Medidas de Seguridad del ENS

Marco Operacional [op.]

Proteger la operación del sistema como conjunto integral de componentes para un fin

- [op.acc.1] Identificación (AT) ✗
- [op.acc.2] Requisitos de acceso (ICAT) ✗
- [op.acc.3] Segregación de funciones y tareas (ICAT) ✓
- [op.acc.4] Proceso de gestión de derechos de acceso (ICAT) 💡
- [op.acc.5] Mecanismo de autenticación (ICAT) ✗
- [op.acc.6] Acceso local (ICAT) ✗
- [op.acc.7] Acceso remoto (ICAT) ✓

[op.acc.5] Mecanismo de autenticación

Control sin aplicar en la actualidad

[op.acc.6] Acceso local

Solo está aplicada la GPO que limita el número máximo de intentos de login fallidos, el resto de las exigidas por este control están sin aplicar.

[op.acc.7] Acceso remoto

Resultados de la auditoria ENS 2021

Medidas de Seguridad del ENS

Marco Operacional [op.]

Proteger la operación del sistema como conjunto integral de componentes para un fin

- [op.exp.1] Inventario de activos (CATEGORIA) ✓
- [op.exp.2] Configuración de Seguridad (CATEGORIA) ✗
- [op.exp.3] Gestión de la configuración (CATEGORIA) ✗
- [op.exp.4] Mantenimiento (CATEGORIA) 💡
- [op.exp.5] Gestión de cambios (CATEGORIA) ✗
- [op.exp.6] Protección frente a código dañino (CATEGORIA) ✓
- [op.exp.7] Gestión de incidencias (CATEGORIA) ✗
- [op.exp.8] Registro de actividad de los usuarios (T)
- [op.exp.11] Protección de claves criptográficas (CATEGORIA) 💡

[op.exp.1] Inventario de activos

[op.exp.2] Configuración de Seguridad y [op.exp.3] Gestión de la configuración

No se aplica, no existe checklist de configuración/bastionado, ni evidencias.

[op.exp.4] Mantenimiento

No se realiza a día de hoy un escaneo activo de vulnerabilidades en estos momentos solo se controla a nivel de equipos por parte del WSUS de Microsoft y mediante las emitidas por el CCN-CERT.

Respecto al software, se adquiere con garantía a 5 años y al terminar se valora si renovarla o no, y en ese caso el equipo se da por amortizado y se gestiona conforme al control Mp.si.5.

[op.exp.5] Gestión de cambios

Procedimentado en NOR6 y PRO12, pero sin implementar.

[op.exp.6] Protección frente a código dañino

Resultados de la auditoria ENS 2021

Medidas de Seguridad del ENS

Marco Operacional [op.]

Proteger la operación del sistema como conjunto integral de componentes para un fin

- [op.exp.1] Inventario de activos (CATEGORIA) ✓
- [op.exp.2] Configuración de Seguridad (CATEGORIA) ✗
- [op.exp.3] Gestión de la configuración (CATEGORIA) ✗
- [op.exp.4] Mantenimiento (CATEGORIA) 💡
- [op.exp.5] Gestión de cambios (CATEGORIA) ✗
- [op.exp.6] Protección frente a código dañino (CATEGORIA) ✓
- [op.exp.7] Gestión de incidencias (CATEGORIA) ✗
- [op.exp.8] Registro de actividad de los usuarios (T) ✗
- [op.exp.11] Protección de claves criptográficas (CATEGORIA) 💡

[op.exp.7-9] Gestión de incidentes

Si bien se dispone de un procedimiento correctamente definido y estructurado, se comprueba durante la auditoría la carencia de soporte y responsabilidades respecto a su aplicación práctica.

[op.exp.8] Registro de actividad de los usuarios

Activado el registro de actividad de servidores Windows, Linux pero sin evidencia de revisión de los mismos.

No se dispone de servicio de SIEM.

[op.exp.11] Protección de claves criptográficas

No se generan claves criptográficas, las contraseñas de LDAP se guardan vía HASH de manera cifrada. No se dispone de HSM

Resultados de la auditoria ENS 2021

Medidas de Seguridad del ENS

Marco Operacional [op.]

Proteger la operación del sistema como conjunto integral de componentes para un fin

- [op.ext.1] Contratación y acuerdos de nivel de servicio (CATEGORIA) ✓
- [op.ext.2] Gestión diaria (CATEGORIA) ✗
- [op.ext.9] Medios alternativos (D) **N.A**

[op.ext.1] Contratación y acuerdos de nivel de servicio

[op.ext.2] Gestión diaria

No se están solicitando informes de seguimiento de SLA.

[op.ext.9] Medios alternativos

Esta medida no aplica por la categorización del sistema.

Resultados de la auditoria ENS 2021

Medidas de Seguridad del ENS

Marco Operacional [op.]

Proteger la operación del sistema como conjunto integral de componentes para un fin

- [op.cont.1] Análisis de Impacto (D) ✓
- [op.cont.2] Plan de Continuidad (D) **N.A**
- [op.cont.3] Pruebas periódicas (D) **N.A**

[op.cont.1] Análisis de Impacto

[op.cont.2] Plan de Continuidad

Esta medida no aplica por la categorización del sistema

[op.cont.3] Pruebas periódicas

Esta medida no aplica por la categorización del sistema

Resultados de la auditoria ENS 2021

Medidas de Seguridad del ENS

Marco Operacional [op.]

Proteger la operación del sistema como conjunto integral de componentes para un fin

- [op.mon.1] Detección de intrusión (CATEGORIA) 
- [op.mon.2] Sistema de métricas(CATEGORIA) 

[op.mon.1] Detección de intrusión

[op.mon.2] Sistema de métricas

Se revisa el INES 25/03/2021, firmada por CISO

Resultados de la auditoria ENS 2021

Medidas de Seguridad del ENS

Medidas de protección [mp.]

Proteger activos concretos, según su naturaleza, con el nivel requerido en cada dimensión de seguridad

- [mp.if.1] Áreas separadas y con control de acceso (CATEGORIA)
- [mp.if.2] Identificación de las personas (CATEGORIA)
- [mp.if.3] Acondicionamiento de los locales
- [mp.if.4] Energía Eléctrica (D)
- [mp.if.5] Protección frente a incendios (D)
- [mp.if.6] Protección frente a inundaciones (D)
- [mp.if.7] Registro de Entrada y Salida de equipamiento (CATEGORIA)
- [mp.if.9] Instalaciones alternativas (D)

[mp.if.1] Áreas separadas y con control de acceso

[mp.if.2] Identificación de las personas

Dispositivo de acceso biométrico para los miembros de sistemas.

[mp.if.3] Acondicionamiento de los locales

[mp.if.4] Energía Eléctrica

[mp.if.5] Protección frente a incendios

[mp.if.6] Protección frente a inundaciones

[mp.if.7] Registro de entrada y salida de equipamiento

Resultados de la auditoria ENS 2021

Medidas de Seguridad del ENS

Medidas de protección [mp.]

Proteger activos concretos, según su naturaleza, con el nivel requerido en cada dimensión de seguridad

- [mp.per.1] Caracterización del puesto de trabajo (CATEGORIA) 
- [mp.per.2] Deberes y obligaciones (CATEGORIA) 
- [mp.per.3] Concienciación (CATEGORIA) 
- [mp.per.4] Formación (CATEGORIA) 

[mp.per.1] Caracterización del puesto de trabajo

Faltaría profundizar en los otros puestos/roles que no son propiamente los indicados en el ENS pero también pueden tener incidencia en la seguridad.

[mp.per.2] Deberes y obligaciones

Ver ORG.2

[mp.per.3] Concienciación

Amplia variedad de formatos y periodicidad adecuada.

[mp.per.4] Formación

Se imparten cursos en la materia por personal interno o empresa especializada, asociados a una iniciativa/catalogo formativo de la Junta de Andalucía

Resultados de la auditoria ENS 2021

Medidas de Seguridad del ENS

Medidas de protección [mp.]

Proteger activos concretos, según su naturaleza, con el nivel requerido en cada dimensión de seguridad

- [mp.eq.1] Puesto de trabajo despejado (CATEGORIA) ✓
- [mp.eq.2] Bloqueo del puesto de trabajo (A) ✗
- [mp.eq.3] Protección de portátiles (CATEGORIA) ✓
- [mp.eq.9] Medios alternativos (D) 👁

[mp.eq.1] Puesto de trabajo despejado

[mp.eq.2] Bloqueo del puesto de trabajo

Control sin aplicar en la actualidad

[mp.eq.3] Protección de portátiles

[mp.eq.9] Medios alternativos

Se debe disponer e inventariar el material alternativo o de respaldo, en especial en lo referido a puesto de usuario.

Resultados de la auditoria ENS 2021

Medidas de Seguridad del ENS

Medidas de protección [mp.]

Proteger activos concretos, según su naturaleza, con el nivel requerido en cada dimensión de seguridad

- [mp.com.1] Perímetro seguro (CATEGORIA)
- [mp.com.2] Protección de la confidencialidad (C)
- [mp.com.3] Protección de la autenticidad y de la integridad (IA)

[mp.com.1] Perímetro seguro

[mp.com.2] Protección de la confidencialidad

[mp.com.3] Protección de la autenticidad y de la integridad

Resultados de la auditoria ENS 2021

Medidas de Seguridad del ENS

Medidas de protección [mp.]

Proteger activos concretos, según su naturaleza, con el nivel requerido en cada dimensión de seguridad

- [mp.si.1] Etiquetado (C)
- [mp.si.2] Criptografía (I C)
- [mp.si.3] Custodia (CATEGORIA)
- [mp.si.4] Transporte (CATEGORIA)

- [mp.si.5] Borrado y destrucción (C)

[mp.si.1] [mp.si.2] [mp.si.3] [mp.si.4]

[mp.si.5] Borrado y destrucción

Se formatean los equipos antes de cambio de usuario pero sin ticket/evidencia, se desmonta, se destruyen físicamente y se llevan a un punto limpio por parte de una persona interna.

Resultados de la auditoria ENS 2021

Medidas de Seguridad del ENS

Medidas de protección [mp.]

Proteger activos concretos, según su naturaleza, con el nivel requerido en cada dimensión de seguridad

- [mp.sw.1] Desarrollo de aplicaciones (CATEGORIA) ✓
- [mp.sw.2] Aceptación y puesta en servicio (CATEGORIA) ✗

[mp.sw.1] Desarrollo de aplicaciones

[mp.sw.2] Aceptación y puesta en servicio

Control sin aplicar en la actualidad.

Resultados de la auditoria ENS 2021

Medidas de Seguridad del ENS

Medidas de protección [mp.]

Proteger activos concretos, según su naturaleza, con el nivel requerido en cada dimensión de seguridad

- [mp.info.1] Datos de carácter personal (CATEGORIA)
- [mp.info.2] Calificación de la información (CATEGORIA)
- [mp.info.4] Firma electrónica (CATEGORIA)
- [mp.info.6] Limpieza de documentos (CATEGORIA)
- [mp.info.9] Copias de Seguridad (CATEGORIA)

[mp.info.1] Datos de carácter personal

DPD ejercido a través de Comité de Seguridad de la información, se reúne 1 al mes.

RAT publicado.

Varios modelos de contratos de encargado de tratamiento.

[mp.info.2] Calificación de la información

Definido en NOR02 y PRO01 pero sin aplicación en la actualidad.

[mp.info.4] Firma electrónica

[mp.info.6] Limpieza de documentos

Definido en PRO18 pero sin aplicación en la actualidad.

[mp.info.9] Copias de Seguridad

Resultados de la auditoria ENS 2021

Medidas de Seguridad del ENS

Medidas de protección [mp.]

Proteger activos concretos, según su naturaleza, con el nivel requerido en cada dimensión de seguridad

- [mp.s.1] Protección del correo electrónico (CATEGORIA)
- [mp.s.2] Protección de servicios y aplicaciones (CATEGORIA)
- [mp.s.8] Protección frente a la DoS (D)

[mp.s.1] Protección del correo electrónico

[mp.s.2] Protección de servicios y aplicaciones

[mp.s.8] Protección frente a la DoS

Presentación ejecutiva al Comité de Seguridad

Índice de Contenidos

- Introducción a la norma “ENS”
- Resultados de la auditoria ENS 2021
- Líneas a futuro

Líneas a futuro

Ejecución del Plan de Acciones Correctivas

- Para cada uno de los controles del anexo II del ENS se incluye dentro del informe de auditoría:
  - El estado actual de cumplimiento de cada uno de los controles y obligaciones
  - Las acciones sugeridas o propuestas para todos aquellos aspectos que no alcance el nivel mínimo requerido de cumplimiento.
- Ingenia recomienda a la Diputación de Almería llevar a cabo estas acciones correctivas, además de las propuestas en el Plan de Mejora de la Seguridad, en aras de alcanzar un cumplimiento íntegro el Esquema Nacional de Seguridad, así como de acometer una gestión y mejora del riesgo actual del sistema de información.

Líneas a futuro

Certificación de conformidad

Los órganos y Entidades de Derecho Público darán publicidad en las correspondientes sedes electrónicas a las declaraciones de conformidad, y a los distintivos de seguridad de los que sean acreedores, obtenidos respecto al cumplimiento del Esquema Nacional de Seguridad.

(Artículo 41. Esquema Nacional de Seguridad)

Líneas a futuro

Publicación de conformidad (EJEMPLO)

AENOR

Certificado de Conformidad
con el Esquema Nacional de Seguridad

ENS-2017/0012

AENOR, certifica que los sistemas de información reseñados todos ellos de categoría MEDIA, y los servicios que se relacionan, de:

INSTITUTO NACIONAL DE CIBERSEGURIDAD DE ESPAÑA, S.A.
INCIBE
AV. JOSÉ AGUADO, 41. 24005 LEÓN

han sido auditados y encontrados conforme con las exigencias del 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, según se indica en el correspondiente Informe de Auditoría de 2017/10/09

para: Los sistemas de información que dan soporte a los servicios de:
-Gestión de incidentes de seguridad del CERT de seguridad e Industria.
-Elaboración y difusión de contenidos de Ciberseguridad
-Desarrollo de tecnologías de Ciberseguridad.

Así como a los servicios corporativos, incluyendo la gestión de las áreas de Sistemas, recursos Huamnos, Servicios Generales, Jurídico y Económico Financiero de acuerdo al documento de determinación de la categoría vigente.

que se realizan: AV. JOSE AGUADO, 41. 24005 - LEÓN

Fecha de certificación de conformidad inicial: 2017-10-26
Fecha de renovación certificación de conformidad: 2019-10-26

Fecha: Madrid, 26 de octubre de 2017

Rafael GARCÍA MEIRO
Director General

AENOR INTERNACIONAL S.A.U.
Génova, 6. 28004 Madrid. España
Tel. 91 432 60 00 - www.aenor.com

ENAC CERTIFICACIÓN

para: Los sistemas de información que dan soporte a los servicios de:

-Gestión de incidentes de seguridad del CERT de seguridad e Industria.
-Elaboración y difusión de contenidos de Ciberseguridad
-Desarrollo de tecnologías de Ciberseguridad.

Así como a los servicios corporativos, incluyendo la gestión de las áreas de Sistemas, recursos Huamnos, Servicios Generales, Jurídico y Económico Financiero de acuerdo al documento de determinación de la categoría vigente.

Ingenia
a Babel company

DIPUTACIÓN DE ALMERÍA

Ingenia
a Babel company

les agradece su atención

JUAN I. SÁNCHEZ JIMÉNEZ

JUAN.SANCHEZ@BABELGROUP.COM

Ingenia
a Sabel company

DIPUTACIÓN DE ALMERÍA

MÁLAGA

C/ Severo Ochoa, 43
Parque Tecnológico de
Andalucía. 29590

T: +34 952 029 300

SEVILLA

Estadio Olímpico. Isla de la Cartuja,
Edificio Suroeste, puerta E,
4ª planta. 41092

T: +34 954 460 448

MADRID

Paseo de la Habana, 26
1ª planta.
28036

T: +34 918 286 211

BARCELONA

Networkia Business Center.
C/ Portal del l´Àngel, 36. 08002

T: +34 934 925 733

SANTIAGO DE CHILE

Av. Eliodoro Yáñez, 2473.
Providencia

T: +56 2 265 37000

PERÚ

C/Grimaldo del Solar, 162
Of. 901. Miraflores

T: +51 1 501 3411

www.ingenia.es  @ingenia_es  linkedin.com/company/ingenia  facebook.com/ingeniaface