

Virtual SOC (vSOC)

Servicio de cumplimiento ENS



FEDERACION ESPAÑOLA DE
MUNICIPIOS Y PROVINCIAS



centro criptológico nacional

● Servicio de cumplimiento ENS

Los **vSOC** podrán contar con servicio de apoyo a las entidades en su marco normativo y de adaptación al Esquema Nacional de Seguridad (ENS).

En función de las necesidades, este apoyo servirá de refuerzo al servicio existente o bien se prestará a aquellas entidades que no dispongan del mismo.

Centro de
Operaciones de
Ciberseguridad

1

Asesoramiento normativo



2

Soporte técnico



● Servicio de cumplimiento ENS

1

Asesoramiento normativo

Definición del **ALCANCE** de los sistemas sujetos al ENS.
PRIORIZACIÓN de sistemas a la hora de afrontar el proceso de adecuación

Centro de
Operaciones de
Ciberseguridad



● Servicio de cumplimiento ENS

1

Asesoramiento normativo

Identificación de **ACTIVOS ESENCIALES**, **CATEGORIZACIÓN** de los sistemas, análisis de riesgos (**AR**) y elaboración de la **DECLARACIÓN DE APLICABILIDAD**

Centro de Operaciones de Ciberseguridad

ACT. ESENCIALES



Activos esenciales:
información y
servicios

CATEGORIZACIÓN



Balance entre la importancia
de la información y servicios
que presta y el esfuerzo de
seguridad requerido

ANÁLISIS DE RIESGOS

Salvaguarda	Identificación	Autenticación	Control de acceso	Confidencialidad	Integridad	Disponibilidad
SA-1) Se dispone de nombres de identificación y autenticación	3	1.1	1.2	1.3	1.4	1.5
SA-2) Se dispone de procedimientos para las tareas de identificación y autenticación	3	1.1	1.2	1.3	1.4	1.5
SA-3) Identificación de los usuarios	3	1.1	1.2	1.3	1.4	1.5
SA-4) La identificación del usuario no indica su función ni su nivel de privilegios	3	1.1	1.2	1.3	1.4	1.5
SA-5) Las cuentas de usuarios están sometidas a un control estricto	3	1.1	1.2	1.3	1.4	1.5
SA-6) Debido a la identificación y autenticación de usuarios	3	1.1	1.2	1.3	1.4	1.5
SA-7) Cuentas especiales (administración)	3	1.1	1.2	1.3	1.4	1.5
SA-8) Canal seguro de autenticación	3	1.1	1.2	1.3	1.4	1.5

DECLARACIÓN
DE
APLICABILIDAD

● Servicio de cumplimiento ENS

1

Asesoramiento normativo

Apoyo en la elaboración de:
la **POLÍTICA DE SEGURIDAD**, **NORMATIVA** y **PROCEDIMIENTOS**
de seguridad

Centro de
Operaciones de
Ciberseguridad

Política de Seguridad

Normativa y Procedimientos



Marco organizativo
[org.1]



Marco organizativo
[org.1], [org.2] y [org.3]

Marco operacional y medidas de seguridad
Procedimientos asociados a las medidas
técnicas.

● Servicio de cumplimiento ENS

1

Asesoramiento
normativo

Apoyo en la **AUDITORÍA DE CERTIFICACIÓN** y en la
DECLARACIÓN DE CUMPLIMIENTO

Centro de
Operaciones de
Ciberseguridad



Logo de la Entidad Certificadora con marca de certificación acreditada

CERTIFICACIÓN DE CONFORMIDAD CON EL ENS

CERTIFICADO DE CONFORMIDAD CON EL ESQUEMA NACIONAL DE SEGURIDAD

«Entidad Certificadora» certifica que los sistemas de información sometidos, todos ellos de categoría «cualquier categoría mínima aplicable (BÁSICA, MEDIA o ALTA)» y los servicios que se relacionan, de «Entidad (pública o privada), dirección postal»:

Han sido sometidos 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 «fecha» para:

«Resumen los sistemas de información y los servicios objeto de la certificación».

Fecha de certificación de conformidad inicial: «dd» de «mes» de «año».

Fecha de renovación de la certificación de conformidad: «dd» de «mes» de «año».

Número de certificado: «Número de certificación».

Fecha (localidad) de que corresponde, «dd» de «mes» de «año».

Firma: «Nombre y Apellidos del responsable competente de la Entidad Certificadora».

Rema del responsable de la Entidad Certificadora.

Nombre completo, razón social de la Entidad Certificadora y sig. web, Dirección postal, electrónica, Código Postal, Provincia, País.

Logo de la Entidad Pública declarante

Identificación inequívoca de la Unidad del declarante

dirección:

DECLARACIÓN DE CONFORMIDAD CON EL ESQUEMA NACIONAL DE SEGURIDAD

Los sistemas de información y los servicios prestados, de categoría BÁSICA, han superado un proceso de autoevaluación conforme con las exigencias del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración electrónica, según se indica en el correspondiente Informe de «fecha» para:

1. Denominación Sistema de información 1 y servicios prestados

2. Denominación Sistema de información 2 y servicios prestados

Fecha de declaración de conformidad inicial: «dd» de «mes» de «año».

Fecha de renovación de la declaración de conformidad: «dd» de «mes» de «año».

En Localidad, a día de mes de año.

Fdo. Nombre y Apellidos del titular del Órgano Superior de que se trata

Administración Pública de que se trata.



Instrucción Técnica de Seguridad de Auditoría de Seguridad de los Sistemas de Información.

Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.

● Servicio de cumplimiento ENS

1

Asesoramiento normativo

Asesoramiento para el cumplimiento del **Reglamento General de Protección de Datos (RGPD)**, a partir del Esquema Nacional de Seguridad

Centro de Operaciones de Ciberseguridad

Concepto analizado	Ubicación en el RGPD	Ubicación en el ENS	Respuesta
1. Base jurídica del tratamiento	Considerandos 10, 40, 45, 51, 65 Artículo 6	Artículo 1	Las medidas para tratar el impacto no exigen modificar el ENS más allá del nuevo conjunto de medidas relativas al RGPD que se señalan en el epígrafe 16.
2. Utilización de medios electrónicos	Considerandos 59, 141 Artículos 12, 15, 28	Artículos 31, 33 Medidas 4.2.1, 4.2.5, 4.2.7, 5.7.4	Las medidas para tratar el impacto no exigen modificar el ENS.
3. Política de Seguridad – Política de Protección de Datos	Artículo 24	Artículo 11	Es necesario incluir un nuevo párrafo 4 al art. 11 del ENS.
4. Interconexión de redes	Artículo 60, 61, 64, 67, 75	ITS de Interconexión en el ENS	Las medidas para tratar el impacto no exigen modificar el ENS.
5. Fuente (sellos) de tiempo	Considerando 59 Artículo 12	Artículo 33 Medida 5.7.5	Las medidas para tratar el impacto no exigen modificar el ENS.
6. Responsable del Tratamiento y Encargado del Tratamiento	Numerosos Considerandos y Artículos Artículo 4	Artículo 10	Nueva redacción al art. 10 del ENS.
7. Encargados de Tratamiento – Servicios Externos	Considerandos 18, 81, 95 Artículo 28	Medida 3.4, 4.3.9, 5.2.2, 4.4, 4.4.1, 4.4.2, 4.4.3	Las medidas para tratar el impacto no exigen modificar el ENS más allá del nuevo conjunto de medidas relativas al RGPD que se señalan en el epígrafe 16.



Desarrollo un **MODELO DE EVALUACIÓN CONJUNTO RGPD-ENS** que facilite la aplicación simultánea de ambas regulaciones.



ens
Esquema Nacional de Seguridad



INCREMENTALES



Información
clasificada

Infraestruc.
críticas

Regulación
Europea de
Protección
de Datos

Servicios
Esenciales

CCN
centro criptológico nacional

● Servicio de cumplimiento ENS

2

**Soporte
técnico**

Apoyo en la **PRIORIZACIÓN** en la implantación de medidas.
Apoyo en la elaboración del **PLAN DE ADECUACIÓN**

Centro de
Operaciones de
Ciberseguridad



El **PLAN DE ADECUACIÓN** es un documento en el que se recoge cómo se va a conseguir la conformidad con el ENS: qué medidas se van a implementar, con qué recursos, los plazos, las prioridades, las responsabilidades, etc...

● Servicio de cumplimiento ENS

2

**Soporte
técnico**

Apoyo en las **MEDIDAS TÉCNICAS DE SEGURIDAD**:
recomendaciones, implementación, configuración y
mantenimiento

Centro de
Operaciones de
Ciberseguridad

Recomendaciones

Implementación

Configuración

Mantenimiento



● Servicio de cumplimiento ENS

2

Soporte técnico

Planteamiento de **MEDIDAS COMPENSATORIAS** y actualización de la declaración de Aplicabilidad

Las medidas de seguridad referenciadas en el Anexo II podrán ser reemplazadas por otras compensatorias siempre que se justifique que protegen igual o mejor el riesgo sobre los activos y se satisfacen los principios básicos y los requisitos mínimos previstos en el real decreto.

*En la Declaración de Aplicabilidad se indica de forma detallada la correspondencia entre las **medidas compensatorias implantadas** y las **medidas del Anexo II que compensan**.*

Para cada medida compensatoria que pretenda adoptarse se incluirá información completa sobre la misma en la Declaración de Aplicabilidad:

1. *Ámbito de aplicación*
2. *Limitaciones o restricciones*
3. *Objetivo*
4. *Riesgo identificado*
5. *Definición de la(s) medida(s) compensatoria(s)*
6. *Validación de la medida(s) compensatoria(s)*
7. *Mantenimiento*

Centro de
Operaciones de
Ciberseguridad

Muchas

Gracias

E-mails

info@ccn-cert.cni.es

ccn@cni.es

sondas@ccn-cert.cni.es

redsara@ccn-cert.cni.es

organismo.certificacion@cni.es

Páginas web:

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es

