



ESQUEMA NACIONAL DE SEGURIDAD.

SERVICIO DE EVALUACIÓN DE LA ADECUACIÓN EN LAS ADMINISTRACIONES PÚBLICAS, AAPP, RD 3/2010.

91 109 05 11

info@controlaltsup.com

C/ Puerto de la Cruz Verde, 26. 28045 - Madrid

Verificación del cumplimiento del ENS en organismos y AAPP.

El Servicio de CONTROLALTSUP tiene como propósito verificar el cumplimiento del Esquema Nacional de Seguridad establecido en el artículo 42 de la Ley 11/2007, de 22 de junio y determinar la política de seguridad que se aplica en la utilización de los medios electrónicos a los que se refiere la citada ley.

Base legal.

- 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.
- Real Decreto 951/2015, de 23 de octubre, de modificación 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.

¿Qué es el ESQUEMA NACIONAL DE SEGURIDAD, ENS?

Se trata de un Sistema de Gestión de Seguridad de la Información, regulado por ley y por tanto de obligado cumplimiento, cuyo objeto es el establecimiento de los principios y requisitos de una política de seguridad en la utilización de medios electrónicos que permita la adecuada protección de la información.

¿Cuál es la finalidad del ENS?

La creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

El ENS persigue fundamentar la confianza en que los sistemas de información prestarán sus servicios y custodiarán la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control y sin que la información pueda llegar al conocimiento de personas no autorizadas.

Se desarrollará y perfeccionará en paralelo a la evolución de los servicios y a medida que vayan consolidándose los requisitos de los mismos y de las infraestructuras que lo apoyan.



¿Quién debe aplicar el ENS?

El Esquema Nacional de Seguridad está constituido por los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información. Será aplicado por las Administraciones públicas para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias.

En el ámbito de las Administraciones públicas, la consagración del derecho a comunicarse con ellas a través de medios electrónicos comporta una obligación correlativa de las mismas, que tiene, como premisas, la promoción de las condiciones para que la libertad y la igualdad sean reales y efectivas, y la remoción de los obstáculos que impidan o dificulten su plenitud, lo que demanda incorporar las peculiaridades que exigen una aplicación segura de estas tecnologías.



¿Qué se entiende por adecuación al ENS?

Según el Real Decreto 3/2010, del ENS, ANEXO IV. GLOSARIO:

Política de seguridad. Conjunto de directrices plasmadas en documento escrito, que rigen la forma en que una organización gestiona y protege la información y los servicios que considera críticos.

Sistema de información. Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.

ADMINISTRACIONES PÚBLICAS (AAPP)



Según el Real Decreto 3/2010, del ENS, ANEXO IV. GLOSARIO:

Principios básicos de seguridad. Fundamentos que deben regir toda acción orientada a asegurar la información y los servicios.

Requisitos mínimos de seguridad. Exigencias necesarias para asegurar la información y los servicios.



¿Cuál es el proceso para la Evaluación de la Adecuación al ENS?

La Evaluación se realiza presencialmente en las instalaciones de las AAPP y consta de cuatro apartados:

- CUMPLIMIENTO DE LOS ARTÍCULOS DEL RD 3/2010 DEL ENS:

Art. 29. Instrucciones Técnicas de Seguridad y Guías de Seguridad.
 Art.35. Informe del Estado de la Seguridad.
 Art.36. Capacidad de Respuesta a Incidentes de Seguridad de la Información.
 Art 43 y Art 44 Categorías y Facultades.

- MARCO ORGANIZATIVO.

Dimensiones				MEDIDAS DE SEGURIDAD	
Afectadas	B	M	A	org	Marco organizativo
categoria	aplica	=	=	[org.1]	Política de seguridad
categoria	aplica	=	=	[org.2]	Normativa de seguridad
categoria	aplica	=	=	[org.3]	Procedimientos de seguridad
categoria	aplica	=	=	[org.4]	Proceso de autorización

- MARCO OPERACIONAL.

Dimensiones				MEDIDAS DE SEGURIDAD	
Afectadas	B	M	A	op	Marco operacional
				[op.p]	Planificación
categoria	aplica	+	++	[op.pl.1]	Análisis de riesgos
categoria	aplica	+	++	[op.pl.2]	Arquitectura de seguridad
categoria	aplica	=	=	[op.pl.3]	Adquisición de nuevos componentes
D	n.a.	aplica	=	[op.pl.4]	Dimensionamiento / Gestión de capacidades
categoria	n.a.	n.a.	aplica	[op.pl.5]	Componentes certificado

NOTA: en la imagen se muestra un extracto. Puede verse la tabla completa en ANEXO II Medidas de seguridad\2 Selección de medidas de seguridad del RD 3/2010.

- MEDIDAS DE PROTECCIÓN.

Dimensiones				MEDIDAS DE SEGURIDAD	
Afectadas	B	M	A		
			mp	Medidas de protección	
			[mp.com]	Protección de comunicaciones	
categoria	aplica	=	+	[mp.com.1]	Perimetro seguro
C	n.a.	aplica	+	[mp.com.2]	Protección de la confidencialidad
IA	aplica	+	++	[mp.com.3]	Protección de la autenticidad y de la integridad
categoria	n.a.	n.a.	aplica	[mp.com.4]	Segregación de redes
D	n.a.	n.a.	aplica	[mp.com.9]	Medios alternativos
				[mp.si]	Protección de los soportes de información
C	aplica	=	=	[mp.si.1]	Etiquetado
IC	n.a.	aplica	+	[mp.si.2]	Criptografía
categoria	aplica	=	=	[mp.si.3]	Custodia
categoria	aplica	=	=	[mp.si.4]	Transporte
C	aplica	+	=	[mp.si.5]	Borrado y destrucción

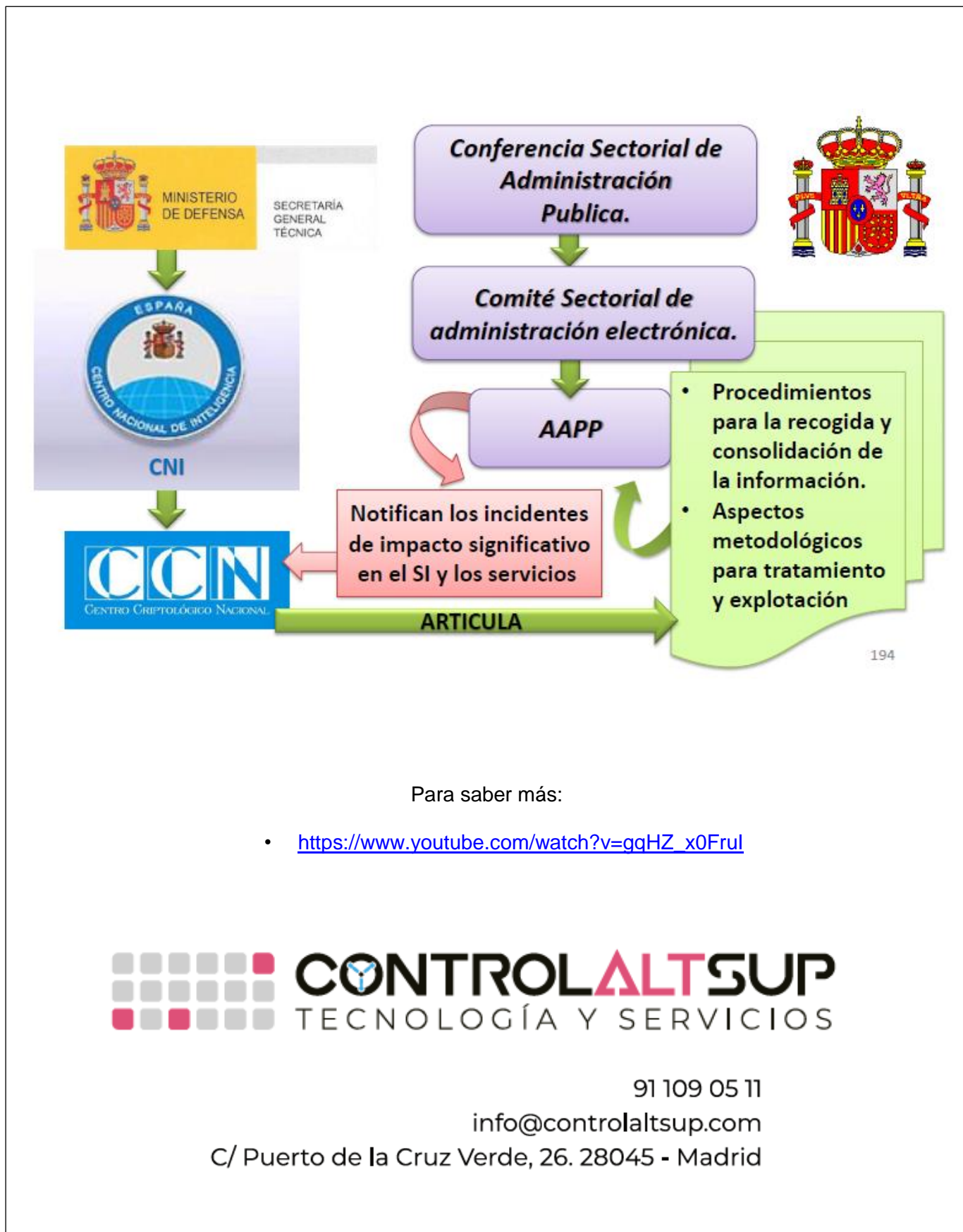
NOTA: en la imagen se muestra un extracto. Puede verse la tabla completa en ANEXO II Medidas de seguridad\2 Selección de medidas de seguridad del RD 3/2010.

- La necesaria generalización de la sociedad de la información es subsidiaria, en gran medida, de la confianza que genere en los ciudadanos la relación a través de medios electrónicos.

Real Decreto 3/2010, de 8 de enero.

Preámbulo I.





Para saber más:

- https://www.youtube.com/watch?v=gqHZ_x0FruI