

CAMBIOS CLAVE

NUEVO ESQUEMA NACIONAL DE SEGURIDAD (RD 311/2022)

OBJETIVOS

Reforzar la protección de los servicios y de los datos, como activo esencial para la Administración Digital frente a atacantes y/o amenazas.

Adecuar al marco normativo actual

- RGPD (UE) 2016/679 relativo a la protección de datos
- LO 3/2018 de Protección de Datos Personales y garantía de los derechos digitales.
- LO 7/2021 de LO 7/2021 de Protección de Datos Personales tratados para fines de prevención, detección, investigación, enjuiciamiento y ejecución de infracciones penales.
- RD 43/2021 por el que se desarrolla el Real Decreto-ley 12/2018 de seguridad de las redes y sistemas de información

DELEGADO DE PROTECCIÓN DE DATOS

El delegado asesora al responsable o el encargado del tratamiento de datos personales en el análisis de riesgos (art. 24, RGPD) y en la evaluación de impacto (art. 35, RGPD) desde el inicio del tratamiento.

PERFILES DE CUMPLIMIENTO ESPECÍFICOS

¿Cuál es su justificación?
Adaptar el Esquema Nacional de Seguridad racionalizando los recursos requeridos sin menoscabo de la protección exigible como consecuencia de un análisis de riesgos.

¿Qué es?
Es el conjunto de medidas de seguridad, comprendidas o no en el anexo II del RD 311/2022, que resulten de aplicación a una entidad o sector de actividad concreto para una determinada categoría de seguridad, validado y publicado por el Centro Criptológico Nacional.

PROTECCIÓN DE LA CADENA DE SUMINISTRO

Designación de un Punto o Persona de Contacto (POC) de la organización prestadora para la seguridad de la información tratada y el servicio prestado.

Nuevos requisitos:
[op.ext.3.1] [op.ext.3.2] [op.ext.3.3]
+ Refuerzo R1 (Plan de contingencia)

NUEVO PRINCIPIO DE "VIGILANCIA CONTINUA"

¿Cuál es su función?
Detección y respuesta ante actividades o comportamientos anómalos.

Evaluación permanente del estado de la seguridad de los activos, para detectar vulnerabilidades e identificar deficiencias de configuración.

NUEVAS MEDIDAS DE SEGURIDAD

- Servicios en la nube [op.nub.1]
- Interconexión de sistemas [op.ext.4]
- Protección de la cadena de suministro [op.ext.3]
- Medios alternativos [op.cont.4]
- Vigilancia [op.mon.3]
- Otros dispositivos conectados a la red [mp.eq.4]

NOTIFICACIÓN DE INCIDENTES DE SEGURIDAD

¿A quién?
Al CCN-CERT por las entidades del sector público y a la Secretaría General de Administración Digital (SGAD).

Al INCIBE-CERT por las empresas que presten servicios a las entidades públicas.

PLAZO DE ADECUACIÓN AL NUEVO ENS

A partir del 05.05.2024 dejarán de tener la condición de acreditados los certificados emitidos frente al RD 3/2010

Las entidades públicas y privadas que presten servicios o provean soluciones a las públicas disponen de 24 meses para la certificación de conformidad de los sistemas de información con el ENS.

CONCIENCIACIÓN Y FORMACIÓN

El CCN y el INAP desarrollarán programas de sensibilización y formación dirigidos al personal de las entidades del sector público.

