CBPOL
OPOSICIONES POLICIALES

ACTUALIZACIONES 2021

TEMA 14

ESQUEMA / RESUMEN DEL RD 43/2021 de 26 de enero por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

AFECTA A TEMA 14: INFRAESTRUCTURAS CRÍTICAS

ESQUEMA /RESUMEN DEL RD 43/2021 por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

ORIGEN : Directiva NIS(Security of Network and Information Systems) traspuesta al ordenamiento jurídico español mediante el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. El RD 43/2021 de 26 de enero desarrolla ese RD.

INNOVACIÓN (AFECTA A TEMA 14) :

CREACIÓN PLATAFORMA NACIONAL DE NOTIFICACIÓN Y SEGUIMIENTO DE CIBERINCIDENTES

ÓRGANOS INVOLUCRADOS: CSIRT (CCN-CERT/ INCIBE-CERT) / CONSEJO SEGURIDAD NACIONAL / CNPIC / OFICINA OFICINA DE COORDINACIÓN DE CIBERSEGURIDAD

Ámbito de aplicación.

a) Los **servicios esenciales dependientes de las redes y sistemas de información comprendidos en los sectores estratégicos** definidos en el anexo de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las Infraestructuras críticas.

b) Los servicios digitales que sean mercados en línea, motores de búsqueda en línea y servicios de computación en nube.

CREACIÓN PLATAFORMA NACIONAL DE NOTIFICACIÓN Y SEGUIMIENTO DE CIBERINCIDENTES

La cooperación entre los CSIRT de referencia, y entre estos y las autoridades competentes, se instrumentará a través de la **esta PLATAFORMA.**

SI HAY INCIDENTE DE SEGURIDAD : COORDINARÁ CCN-CERT Y SE CALIFICARÁ:

1.º La clasificación del incidente. 2.º La peligrosidad del incidente. 3.º El impacto del incidente.

b) Plan de acción del CSIRT para abordar la resolución técnica del incidente, si procede.

Punto de contacto único.

1. **SI INCIDENTE INTERNACIONAL: Consejo de Seguridad Nacional, a través del Departamento de Seguridad Nacional**

En su función de enlace para garantizar la cooperación transfronteriza de las autoridades competentes designadas conforme al artículo 9 del Real Decreto-ley 12/2018, de 7 de septiembre, con las autoridades competentes de otros Estados miembros de la Unión Europea, así como con el grupo de cooperación contemplado en el artículo 11 de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, y la red de CSIRT

CONTACTO OPERADORES SERVICIOS ESENCIALES:
Responsable de la seguridad de la información.

Los operadores de servicios esenciales designarán una persona, unidad u órgano colegiado, responsable de la seguridad de la información que ejercerá las **funciones de punto de contacto y coordinación técnica con la autoridad competente y CSIRT**

2. **Actuaciones ante incidentes con carácter presuntamente delictivo.**
3. En cumplimiento de lo dispuesto en el artículo 262 de la Ley de Enjuiciamiento Criminal, la OCC (Oficina de Coordinación de Ciberseguridad) comunicará a la mayor brevedad posible al Ministerio Fiscal y, en su caso, a las Unidades orgánicas de Policía Judicial competentes, aquellos incidentes de seguridad que le sean notificados y que revistan carácter presuntamente delictivo, trasladando al tiempo la información que posea en relación con ello. A dicho fin podrá requerir de los operadores afectados o de los CSIRT de referencia cuanta información relacionada con el incidente se estime necesaria.

CONCEPTOS IMPORTANTES DE LA LEY 12/2018 (Recordatorio)

Artículo 11. Equipos de respuesta a incidentes de seguridad informática de referencia.

1.CSIRT_ Son equipos de respuesta a incidentes de seguridad informática (CSIRT) de referencia en materia de seguridad de las redes y sistemas de información, los siguientes:

a) En lo concerniente a las relaciones con los operadores de servicios esenciales:

1.º El CCN-CERT, del Centro Criptológico Nacional (CNI) , al que corresponde la comunidad de referencia constituida por las entidades del ámbito subjetivo de aplicación de la Ley 40/2015, de 1 de octubre. (ADMINISTRACIÓN PÚBLICA y organismos públicos)

2.º El INCIBE-CERT, del Instituto Nacional de Ciberseguridad de España, al que corresponde:

A.- la comunidad de referencia constituida por aquellas entidades no incluidas (SECTORES no Admón. pública)

B.- los proveedores de servicios digitales que no estuvieren comprendidos en la comunidad de referencia del CCN-CERT.

C.- Tb INCIBE-CERT para , equipo de respuesta a incidentes de referencia para los ciudadanos, entidades de derecho privado y otras entidades no incluidas anteriormente en este apartado 1.

El INCIBE-CERT será operado conjuntamente por el INCIBE y el CNPIC en todo lo que se refiera a la gestión de incidentes que afecten a los operadores críticos.

3.º El ESPDEF-CERT, del Ministerio de Defensa, que cooperará con el CCN-CERT y el INCIBE-CERT en aquellas situaciones que éstos requieran en apoyo de los operadores de servicios esenciales y, necesariamente, en aquellos operadores que tengan incidencia en la Defensa Nacional y que reglamentariamente se determinen.

COORDINACIÓN CSIRT en respuesta a INCIDENTES SEGURIDAD

CCN (Centro Criptológico Nacional)-CERT:

1.- COORDINADOR EN incidentes especial gravedad

2.- COORDINADOR Sector público

1. Los CSIRT de referencia se coordinarán entre sí y con el resto de CSIRT nacionales e internacionales en la respuesta a los incidentes y gestión de riesgos de seguridad que les correspondan. En los supuestos *de especial gravedad* que reglamentariamente se determinen y que requieran un nivel de coordinación superior al necesario en situaciones ordinarias, el CCN (Centro Criptológico Nacional)-CERT ejercerá la coordinación nacional de la respuesta técnica de los CSIRT. Y EN GENERAL en respuesta a incidentes de seguridad informática (CSIRT) en materia de seguridad de las redes y sistemas de información del SECTOR PÚBLICO comprendido en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

2.- SI AFECTA A OPERADOR CRÍTICO (Infraestructuras críticas):

a.- LOS CSIRT de referencia se coordinarán con el Ministerio del Interior, a través de la Oficina de Coordinación de Ciberseguridad del Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC), de la forma que reglamentariamente se determine.

ENLACE INTERNACIONAL: El CCN ejercerá la función de enlace para garantizar la cooperación transfronteriza de los CSIRT de las Administraciones Públicas con los CSIRT internacionales, en la respuesta a los incidentes y gestión de riesgos de seguridad que les correspondan.