CCN-CERT

La Capacidad de Respuesta a Incidentes de Seguridad, tal y como recoge el RD3/2010, que regula el **Esquema Nacional de Seguridad,** es otro de los servicios del Centro Criptológico Nacional puesto en marcha en 2006 a través del CCN-CERT.

El CERT Gubernamental español tiene como principal objetivo contribuir a la mejora del nivel de seguridad de los sistemas de información de las AAPP (general, autonómica y local), ofreciendo entre otros servicios:

- Soporte y coordinación para el tratamiento de vulnerabilidades y la resolución de incidentes de seguridad
- Investigación y divulgación de las mejores prácticas sobre seguridad de la información
- Formación destinada al personal de la Administración especialista en el campo TIC
- Información sobre vulnerabilidades, alertas y avisos de nuevas amenazas

CCN
CENTRO CRIPTOLÓGICO NACIONAL

Centro Criptológico Nacional

Centro Criptológico Nacional

www.ccn.cni.es
ccn@cni.es

www.ccn-cert.cni.es
info@ccn-cert.cni.es

www.oc.ccn.cni.es
organismo.certificacion@cni.es

GOBIERNO DE ESPAÑA | MINISTERIO DE DEFENSA

ESPAÑA CNI CENTRO NACIONAL DE INTELIGENCIA

Centro Criptológico Nacional

El CCN, adscrito al Centro Nacional de Inteligencia, es el organismo responsable de proporcionar una garantía razonable sobre la seguridad de las tecnologías de la información, sus productos y sistemas en toda la Administración. Así lo recoge el **RD 421/2004**, 12 de marzo, que regula y define su ámbito y funciones:

- Elaborar y difundir **normas, instrucciones, guías** y recomendaciones para garantizar la seguridad de las TIC en la Administración.
- **Formar** al personal de la Administración especialista en el campo de la seguridad de las TIC.
- Constituir el **Organismo de Certificación** del Esquema Nacional de Evaluación y Certificación de aplicación a productos y sistemas de su ámbito.
- **Valorar y acreditar** capacidad productos de cifra y Sistemas de las TIC (incluyan medios de cifra) para manejar información de forma segura.
- Coordinar la promoción, el desarrollo, la obtención, la adquisición y puesta en explotación y la utilización de la tecnología de seguridad de los Sistemas antes mencionados.
- Velar por el cumplimiento normativa relativa a la protección de la **información clasificada** en su ámbito de competencia (Sistemas de las TIC)
- Establecer las necesarias **relaciones** y firmar los **acuerdos** pertinentes con organizaciones similares de otros países.

Formación y asesoramiento

El CCN tiene la potestad de formar al personal de la AAPP especialista en el campo de las Tecnologías de la Información. Por este motivo, a lo largo de todo el año, ofrece una amplia variedad de cursos STIC:

- Informativos y Concienciación en Seguridad
- Básicos de seguridad
- Específicos de gestión de seguridad
- Especialización en seguridad
- Cursos On-line

Según recoge el RD 421/2004 y el RD3/2010, que regula el **Esquema Nacional de Seguridad**, el CCN debe elaborar y difundir las correspondientes normas, instrucciones, guías y recomendaciones que garanticen la seguridad de los sistemas de la Administración. Son las denominadas **Guías CCN-STIC**:

- Políticas (Serie 000),
- Procedimientos (Serie 100),
- Normas (Serie 200),
- Instrucciones técnicas (Serie 300)
- Guías generales (Serie 400)
- Guías entornos Windows (Serie 500)
- Guías otros entornos (Serie 600)
- Informes técnicos (Serie 900)

Organismo de Certificación

El OC del CCN viene operando desde finales del año 2004 con diversas formas de evaluación y certificación de la seguridad de las TIC, entre ellas:

- RD 421/2004 que regula el CCN
- Orden PRE/2740/2007 Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información y las Comunicaciones (TIC).
- Normativa interna adaptada a los requisitos necesarios para ser reconocido tanto a nivel nacional, según la norma EN45011, como a nivel internacional, de acuerdo con el "Arreglo de Reconocimiento de Certificados de Criterios Comunes" (CCRA), como entidad de certificación de la seguridad de las TIC.
- "Common Criteria" (ISO-15408) de la cuál se han venido recibiendo y tramitando diversas solicitudes de certificación de productos para su posible uso en la Administración electrónica española.

SOGIS MRA V3

Coincidiendo con la Presidencia española de turno del Consejo de Ministros de la Unión Europea, el Esquema Nacional de Evaluación y Certificación de la Seguridad TIC se ha incorporado al acuerdo europeo SOGIS MRA v3 de reconocimiento de certificados (principal referencia europea de calidad de la seguridad de los productos TIC).