El Real Decreto que regula el Esquema fue publicado el viernes 28 de enero en el Boletín Oficial del Estado y será aplicable por todas las administraciones públicas

La coordinación nacional e internacional y la respuesta a incidentes de seguridad de la información, a través del CCN-CERT, funciones del Centro Criptológico Nacional fijados en el nuevo Esquema Nacional de Seguridad

- **El CCN ha colaborado activamente en la redacción del Esquema cuyo objeto es el establecimiento de los principios básicos y requisitos mínimos de una política de seguridad en la Administración que permita la adecuada protección de la información**

- **El RD establece el papel de coordinador del CCN con el resto de capacidades de respuesta a incidentes de seguridad que se creen en las administraciones públicas, a las que ofrecerá un programa de información, formación, recomendaciones y herramientas necesarias para su desarrollo**

Madrid, 2 de febrero de 2010.- El Real Decreto 3/2010, de 8 de enero, publicado el viernes 29 de enero en el Boletín Oficial del Estado, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, dedica todo su Capítulo VII a la Capacidad de Respuesta a Incidentes de Seguridad, CCN-CERT, del Centro Criptológico Nacional (CCN), adscrito al Centro Nacional de Inteligencia (CNI). Así, en su artículo 36, el real decreto señala que el CCN *"articulará la respuesta a los incidentes de seguridad en torno a la estructura denominada CCN-CERT (Centro Criptológico Nacional-Computer Emergency Reaction Team), que actuará sin perjuicio de las capacidades de respuesta a incidentes de seguridad que pueda tener cada administración pública y de la función de coordinación a nivel nacional e internacional del CCN".*

El nuevo texto legal, que 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, viene a recoger los servicios que el CCN-CERT ya prestaba, desde su creación en 2006 (en parte recogidos en el RD 421/2004 de regulación del CCN), y que ahora quedan establecidos en el artículo 37 de este RD:

- **Soporte y coordinación** para el tratamiento de vulnerabilidades y la resolución de incidentes de seguridad o agresiones recibidas por las distintas administraciones públicas (general, autonómica y local) y las Entidades de Derecho público con personalidad jurídica propia dependientes de éstas.
- **Investigación y divulgación de las mejores prácticas** sobre seguridad de la información entre todos los miembros de la Administración.
- **Formación** destinada al personal de la Administración especialista en el campo de la seguridad de las tecnologías de la información.

- **Información sobre vulnerabilidades, alertas y avisos** de nuevas amenazas a los sistemas de información, recopiladas de diversas fuentes de reconocido prestigio, incluidas las propias.

Asimismo, el nuevo texto legal establece el papel de coordinador a nivel público estatal del CCN con el resto de capacidades de respuesta a incidentes de seguridad que se creen en el resto de administraciones públicas, a las que ofrecerá un programa de información, formación, recomendaciones y herramientas necesarias para dicho desarrollo.

Guías CCN-STIC

Tal y como se reconoce en su Capítulo II, el CCN ha colaborado activamente en la elaboración del Esquema, en el que se ha atendido *"a la normativa nacional sobre Administración electrónica, protección de datos de carácter personal, firma electrónica y documento nacional de identidad electrónico, Centro Criptológico Nacional, …"*). De igual forma, las Guías CCN-STIC de Seguridad de los Sistemas de Información y Comunicaciones (elaboradas y actualizadas periódicamente por el propio CCN) han inspirado la articulación del RD.

De hecho, tal y como recogen los artículos 29 y 36, para el mejor cumplimiento de lo establecido en el Esquema y garantizar la seguridad de los sistemas de tecnologías de la información en la Administración, el CCN elaborará y difundirá las correspondientes normas, instrucciones, guías y recomendaciones. Entre otras, el propio texto menciona, las guías de autenticación frente al sistema (Anexo II) o la instrucción técnica CCN-STIC de auditorías de seguridad (Anexo III).

Organismo de Certificación

El Esquema también destaca la importancia de la certificación a la hora de adquirir productos por parte de la Administración. Así, el artículo 18 del real decreto señala que se valorarán positivamente aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición. En este sentido se cita al Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las TIC (el propio Centro Criptológico Nacional) como aquel encargado de determinar el criterio a cumplir en función del uso previsto del producto, en relación con el nivel de evaluación, otras certificaciones de seguridad que se requieran adicionales, así como en aquellos casos en los que no existan productos certificados.

Asimismo, en numerosas ocasiones, el Esquema señala la recomendación y/o obligación de utilizar algoritmos certificados por el Centro Criptológico Nacional a la hora de utilizar diferentes productos o características de los sistemas, como en el caso de utilización de dispositivos físicos (tokens), de la protección de claves criptográficas, protección de la confidencialidad, la autenticidad y de la integridad o en los medios utilizados en la firma electrónica (*Anexo II*).

En cuanto a la adecuación de los sistemas de las administraciones, la disposición transitoria del texto señala que se deberán adecuar al Esquema en doce meses, aunque si hubiese circunstancias que impidan la plena aplicación, se dispondrá de un plan de adecuación que marque los plazos de ejecución (en ningún caso superiores a 48 meses)

Sobre CCN-CERT

El servicio de Respuesta ante Incidentes de Seguridad de la Información, CCN-CERT, fue creado en 2006 por el Centro Criptológico Nacional del Centro Nacional de Inteligencia, con el fin de contribuir a la mejora del nivel de seguridad de los sistemas de información de las administraciones públicas españolas (general, autonómica y local).

El CERT gubernamental español asesora a todas ellas en la implantación de medidas tecnológicas que mitiguen el riesgo de sufrir cualquier ataque, colabora en la resolución de cualquier incidente, facilita cursos de formación y proporciona información sobre vulnerabilidades, alertas y avisos de amenazas a los sistemas de información.

Para desempeñar de forma óptima estas funciones, el CCN-CERT cuenta con un portal en Internet (www.ccn-cert.cni.es), desde donde ofrece los servicios mencionados. Además, forma parte de prestigiosos organismos internacionales (como el FIRST –Forum of Incident Response and Security Team- o el Trusted Introducer), con quienes comparte objetivos, ideas e información relevante sobre seguridad informática.

MÁS INFORMACIÓN

Clara Baonza/ José Herranz
comunicacion@tb-security.com
TB·Security
(+34) 91 301 34 95

Centro Criptológico Nacional
Avda. del Padre Huidobro, Km. 8,500
28023 Madrid
www.ccn-cert.cni.es
info@ccn-cert.cni.es