CCN-CERT RFC 2350

1. Información del Documento

1.1. Fecha de la última actualización: versión 1.0, publicada el 15 de octubre de 2019

1.2. Listas de Distribución: No existe un canal de distribución para notificar cambios en este documento. Los cambios son anunciados por medio de notificación en

https//www.ccn-cert.cni.es

1.3. Ubicación del Documento: La última versión del documento se encuentra publicada en:

- Español: https://www.ccn-cert.cni.es/sobre-nosotros/rfc2350.html
- Inglés: https://www.ccn-cert.cni.es/en/about-us/rfc2350.html

1.4. Autenticación del Documento: Este documento ha sido firmado digitalmente por el CCN-CERT.

2. Información de Contacto

2.1. Nombre del Equipo: CCN-CERT, CERT Gubernamental Nacional del Centro Criptológico Nacional (CCN).

2.2. Dirección:

CCN-CERT, Centro Criptológico Nacional

Centro Nacional de Inteligencia

C/Argentona, 30, 28023

Madrid

2.3. Zona Horaria: CET / CEST

2.4. Número de Teléfono: No divulgado en medios públicos.

2.5. Número de Fax: No existente

2.6. Otras Comunicaciones: No existente

2.7. Direcciones de Correo Electrónico:

- Intercambio de información relativa a incidentes: incidentes@ccn-cert.cni.es
- Consultas de carácter general: info@ccn-cert.cni.es

- Otras direcciones de correo electrónico para contactar con el CCN-CERT: https://www.ccn-cert.cni.es/sobre-nosotros/contacto.html

2.8. Claves Públicas y cifrado de información: los correos de contacto y claves PGP asociadas se encuentran publicadas en https://www.ccn-cert.cni.es/sobre-nosotros/contacto.html

2.9. Miembros del Equipo: No disponible

2.10. Más Información: La información general sobre los servicios proporcionados por el CCN-CERT y sobre el propio organismo se encuentra publicada en el portal web:

https//www.ccn-cert.cni.es.

2.11. Horario de Atención: El equipo de respuesta a incidentes está disponible en los siguientes horarios:

- Consultas sobre servicios: horario de oficina (8.00h-18.00h)
- Incidentes catalogados con peligrosidad[1] baja, media o alta: horario de oficina (8.00h-18.00h)
- Incidentes catalogados con peligrosidad muy alta o crítica: 24x7x365.

2.12. Puntos de contacto para la comunidad: La comunicación entre el Equipo CCN-CERT y los organismos a los que da soporte se realiza principalmente a través de:

- Buzón de correo asociado a la temática a consultar: https://www.ccn-cert.cni.es/sobre-nosotros/contacto.html
- Teléfonos proporcionados durante el proceso de adhesión o el apoyo a incidentes.

3. Constitución

3.1. Misión: El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Este servicio se creó en el año 2006 como CERT Gubernamental Nacional español en base a la legislación recogida en la Ley 11/2002 reguladora del CNI, el RD 421/2004 de regulación del CCN, el RD 3/2010 regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015, y el Real Decreto 12/2018 de seguridad de las redes y sistemas de información.

Su misión es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel nacional de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes para incidentes de especial relevancia.

Todo ello, con el fin último de conseguir un ciberespacio más seguro y confiable, preservando la información clasificada y la información sensible, formando al personal experto, aplicando políticas y procedimientos de seguridad y empleando y desarrollando las tecnologías más adecuadas a este fin.

[1] Peligrosidad: según definición incluida en la guía CCN-STIC 817.

3.2. Comunidad a la que brinda servicios:

De acuerdo a la normativa anteriormente citada, y la Ley 40/2015 de Régimen Jurídico del Sector Público a la que hace mención el Real Decreto 12/2018 , es competencia del CCN-CERT la gestión de ciberincidentes que afecten a sistemas del Sector Público o empresas de interés estratégico, así como a cualquier otro sistema en el que se procese información clasificada.

En el caso de servicios esenciales, la gestión de ciberincidentes se realizará por el CCN-CERT en coordinación con el Centro Nacional de Protección de Infraestructuras Críticas (CNPIC)

3.3. Patrocinio / Afiliación: El CCN-CERT forma parte del Centro Criptológico Nacional (CCN), adscrito al Centro Nacional de Inteligencia (CNI).

3.4. Autoridad: La autoridad del CCN-CERT emana de la siguiente legislación:

- Real Decreto 3/2010, actualizado en el R.D. 951/2015, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (artículo 37)
- Real Decreto 12/2018, de seguridad de las redes y sistemas de información (artículo 19. Obligación de notificar)

4. Políticas

4.1. Tipo de Incidentes y nivel de soporte:

La tipología de ciberincidentes sobre los que actúa el CCN-CERT quedan reflejadas en la guía CCN-STIC-817, en su apartado 6.1 “Clasificación de los ciberincidentes”

CCN-CERT, como CERT Gubernamental Nacional, colabora con todos los organismos públicos y empresas de interés estratégico en la detección, notificación, evaluación, respuesta, tratamiento y aprendizaje de incidentes de seguridad de información o ciberincidentes que puedan sufrir sus sistemas.

El nivel de apoyo que brinda el CCN-CERT y el tiempo de respuesta del mismo, dependerá de del nivel de peligrosidad del incidente y de otros factores fijados en la Guía CCN-STIC-817 Gestión de Ciberincidentes, de acuerdo a los siguientes criterios:

- Tipo de amenaza (código dañino, intrusiones, fraude, etc.)
- Origen de la amenaza: interna o externa.
- La categoría de seguridad de los sistemas afectados.
- El perfil de los usuarios afectados, su posición en la estructura organizativa de la entidad y, en su consecuencia, sus privilegios de acceso a información sensible o confidencial.
- El número y tipología de los sistemas afectados.
- El impacto que el incidente puede tener en la organización, desde los puntos de vista de la protección de la información, la prestación de los servicios, la conformidad legal y/o la imagen pública.
- Los requerimientos legales y regulatorios.

CCN-CERT también ofrece información sobre el estado de la ciberseguridad a su Comunidad, con el fin de reducir tanto las vulnerabilidades técnicas (de hardware y software), como humanas y de organización. Para ello, notifica periódicamente la siguiente información:

- Avisos: amenazas/vulnerabilidades detectadas por el propio CCN-CERT u otros CSIRT.
- Alertas: igual que el epígrafe anterior, pero con una criticidad más alta.
- Vulnerabilidades: diariamente de los principales fabricantes.
- Informes de código dañino.
- Informes de buenas prácticas.
- Informes de amenazas.

4.2. Cooperación, Interacción y divulgación de la Información: La información manejada por CCN-CERT es tratada con absoluta confidencialidad de acuerdo a las políticas y procedimientos para la Gestión de Incidentes establecidos para el CCN-CERT, las políticas y normas del CCN y las normas de seguridad para la protección de la información clasificada.

4.3. Comunicación y Autenticación: Los medios disponibles para la comunicación con el CCN-CERT son:

- Correo electrónico cifrado con las claves públicas dedicadas para ello y publicadas en el portal web: https://www.ccn-cert.cni.es/sobre-nosotros/contacto.html
- Teléfonos proporcionados durante el proceso de adhesión o el apoyo a incidentes.

5. Servicios

5.1. **Prevención**

El CCN-CERT realiza distintas actividades con el fin de sensibilizar y prevenir frente a cualquier incidente. Entre ellas destacan:

a) Definición de políticas de seguridad
b) Soporte y coordinación para el tratamiento de vulnerabilidades
c) Informes, alertas y avisos sobre nuevas amenazas y vulnerabilidades de los sistemas de información, recopiladas de diversas fuentes de reconocido prestigio, incluidas las propias.
d) Investigación y divulgación de las mejores prácticas sobre seguridad de la información.
e) Desarrollo de Guías de Seguridad con normativas, procedimientos y buenas prácticas.
f) Formación y sensibilización en materia de ciberseguridad a profesionales cualificados, con distinto perfil y nivel de formación. Cuenta con una formación básica y dos itinerarios: de gestión y de especialización. Dicha formación se realiza tanto de forma presencial, como online y con cursos específicos en streaming.
g) Organización y participación en Jornadas y congresos de ciberseguridad.
h) Auditorías web a los sistemas del Sector Público.

5.2 Respuesta a Incidentes

El CCN-CERT ofrece apoyo técnico y operativo en las distintas etapas del proceso de gestión de incidentes: detección, análisis, notificación, contención, erradicación y recuperación. En este proceso se incluye la evaluación de la información disponible y su priorización (triaje), la validación y verificación de la misma; la recopilación de las pruebas adicionales necesarias; la comunicación con las partes pertinentes y, por último, la resolución del incidente.

Asimismo, asesora a los equipos sobre las acciones más adecuadas; realiza un seguimiento de la gestión del incidente y solicita los informes pertinentes (los responsables del organismo emiten un Informe del Ciberincidente en el que deben detallar su causa originaria, su coste y las medidas que la organización debe tomar para prevenir futuros ciberincidentes de naturaleza similar).

5.3. Coordinación de Incidentes

El CCN-CERT coordina los incidentes y ejerce además la coordinación a nivel nacional de las distintas Capacidades de Respuesta a Incidentes (CERT/CSIRT) o Centros de Operaciones de Seguridad (SOC) del sector público.

En los supuestos de especial gravedad concernientes a operadores de servicios esenciales que requieran un nivel de coordinación superior al necesario en situaciones ordinarias, el CCN-CERT ejercerá la coordinación nacional de la respuesta técnica de los CSIRT.

5.4. Monitorización

CCN-CERT ha desarrollado un Sistema de Alerta Temprana (SAT) para la detección de incidentes en organizaciones de su comunidad. Actualmente el SAT cuenta con tres vertientes:

- SAT-SARA. Monitorización de la Intranet de la Administración Pública
- SAT-INET. Monitorización de las conexiones a Internet de las organizaciones adscritas al servicio
- SAT-ICS. Monitorización de Sistemas de Control Industrial.

5.5 Desarrollo de soluciones y herramientas de ciberseguridad

CCN-CERT coordina y promueve el desarrollo de soluciones que garanticen la seguridad de los sistemas y contribuyan a una mejor gestión de la ciberseguridad en cualquier organización. Dichas soluciones se centran, principalmente, en la detección, análisis, auditoría e intercambio de información.

Relación completa actualizada de estas herramientas puede encontrarse en:
https://www.ccn-cert.cni.es/soluciones-seguridad.html

5.6 Análisis forense y de malware

CCN-CERT dispone de equipamiento y personal especializado para realizar el análisis forense de equipos implicados en incidentes complejos.

Del mismo modo, el CCN-CERT tiene la capacidad de realizar análisis estáticos y dinámicos de muestras de código dañino para generar patrones de detección.

6. Formas de notificación de incidentes

La notificación de incidentes puede realizarse mediante:

- Buzón de correo específico: incidentes@ccn-cert.cni.es
- LUCIA: Herramienta de notificación de incidentes.
- Teléfonos proporcionados durante el proceso de adhesión o el apoyo a incidentes.

7. Disclaimer

El Equipo CCN-CERT no se responsabiliza del mal uso que pueda darse de la información aquí contenida.