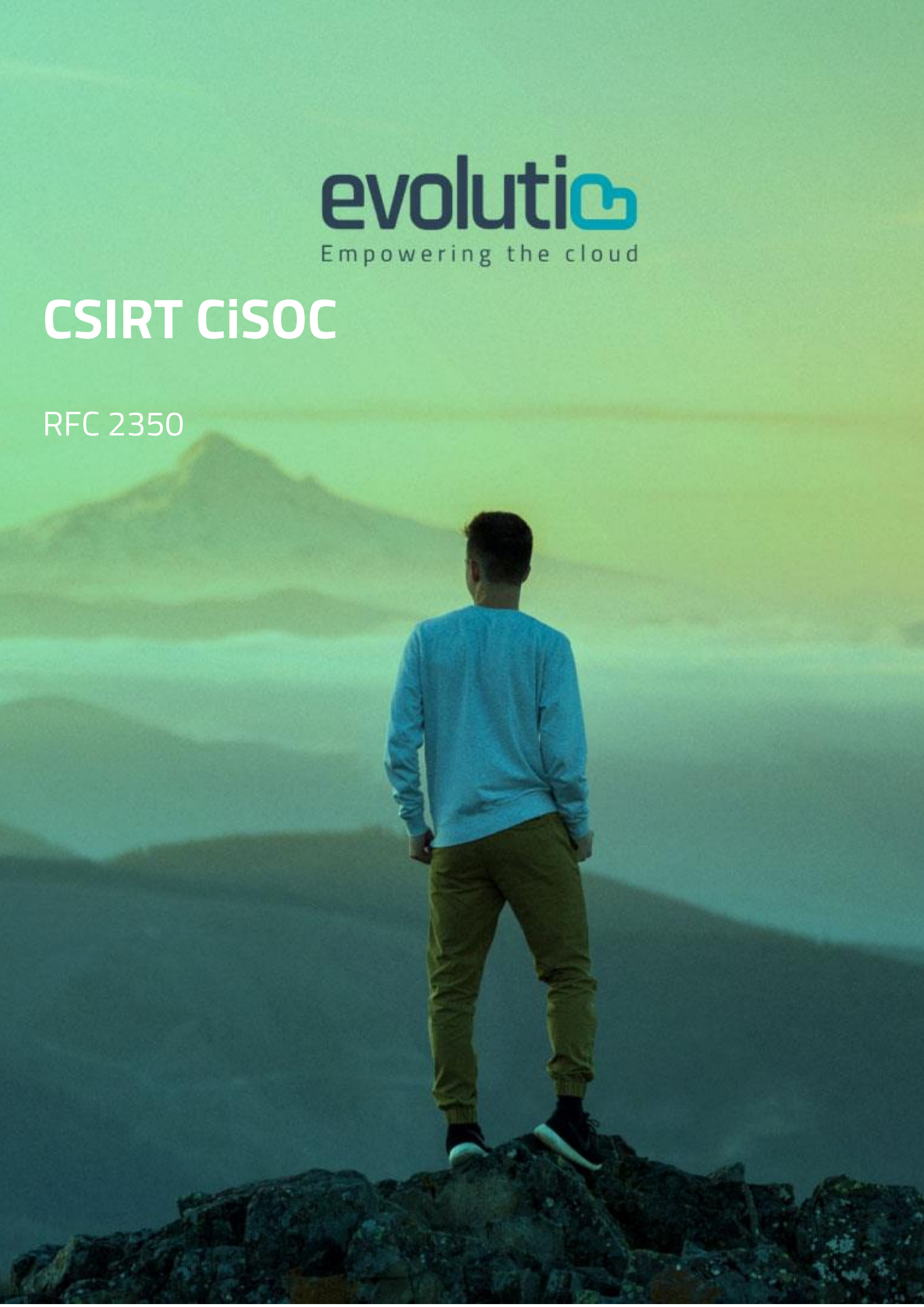
evolutio

Empowering the cloud

CSIRT CiSOC

RFC 2350



1. Información del Documento

1.1. Fecha de la última actualización: Versión 3.0, publicada el 26 de julio de 2021

1.2. Listas de Distribución: No existe un canal específico de distribución. Los cambios son anunciados en la página web de evolutio (https://www.evolutio.com/sobre-nosotros/cert/)

1.3. Ubicación del Documento: La última versión del documento se encuentra publicada en https://www.evolutio.com/wp-content/uploads/2021/07/RFC2350.pdf

1.4. Autenticación del Documento: Este documento ha sido firmado digitalmente por el evolutio cert

2. Información de Contacto

2.1. Nombre del Equipo: Evolutio CERT. CERT de la compañía Evolutio Cloud Enabler, S.A

2.2. Dirección:

Evolutio-CERT, Evolutio Cloud Enabler, S.A.

Calle Isabel Colbrand, 8.

28050 Madrid

España

2.3. Zona Horaria: CET / CEST

2.4. Número de Teléfono: No divulgado públicamente.

2.5. Número de Fax: No existe.

2.6. Otras Comunicaciones: No existen.

2.7. Direcciones de Correo Electrónico:

- Intercambio de información relativa a incidentes: **evolutio.cert@evolutio.com**
- Consultas de carácter general: **info.cert@evolutio.com**

2.8. Claves Públicas y cifrado de información: https://www.evolutio.com/sobre-nosotros/cert/Claves-Publicas/

2.9. Miembros del Equipo: No disponible públicamente.

2.10. Más Información: La información sobre los servicios que se prestan por parte del Cert de Evolutio y su CiSOC puede encontrase en la página de su portal de internet:

https://www.evolutio.com/sobre-nosotros/cert/

https://www.evolutio.com/sobre-nosotros/soc/

2.11. Horario de Atención: Muestro equipo de respuesta a Incidentes se encuentra disponible en los siguientes horarios:

- Consultas sobre servicios: horario de oficina (9.00h-18.00h) CET
- Incidentes catalogados con peligrosidad baja o media: horario de oficina (9.00h18.00h) CET
- Incidentes catalogados con peligrosidad alta o Crítica: 24x7x365.

2.12. Puntos de contacto para la comunidad: Los puntos de contacto para la comunidad son los descritos en el apartado 2.7.

3. Constitución

3.1. Misión:

Perteneciente al CiSOC de Evolutio Cloud Enabler, S.A, Evolutio CERT nace con la misión de proteger los sistemas de información de nuestros clientes, monitorizado sus sistemas de control y activos digitales existentes para detectar actividades e intrusiones no autorizadas, vulnerabilidades y violaciones de los procedimientos y políticas y uso aceptable. Proporcionar soporte directo a nuestros clientes en caso de un incidente de ciber seguridad para contener, erradicar y restaurar los sistemas de información a su situación original.

Nuestro objetivo es ser reconocidos como punto de encuentro y liderar iniciativas colaborativas, posicionando así a nuestros servicios y clientes en la aplicación de tecnologías de ciberseguridad.

Para estar a la altura de todos estos retos, y con el objetivo de garantizar una respuesta eficaz a los posibles incidentes relacionados con la seguridad dirigidos a nuestros clientes, trabajaremos con diferentes grupos de interés de España y Europa. También colaboramos con INCIBE-CERT y CCN-CERT desarrollando confianza, operativas eficaces y promoviendo la adopción y uso de prácticas comunes o estandarizadas para esquemas de clasificación de incidentes, riesgos e información.

3.2. Comunidad a la que brinda servicios:

Evolutio-cert como parte del CiSOC de Evolutio, presta servicios específicos a los clientes de evolutio y además somos el CERT y el SOC nuestra propia compañía. Adicionalmente, se realizan tareas divulgativas sobre amenazas y tendencias de carácter público y abierto al entono empresarial en España.

3.3. Patrocinio / Afiliación:

Evolutio CERT forma parte de la compañía Evolutio Cloud Enabler, S.A.

3.4. Autoridad:

Evolutio CERT opera bajo la autoridad de la dirección de Customer Solutios dentro de la estructura organizativa de Evolutio Cloud Enabler S.A.

4. Políticas

4.1. Tipo de Incidentes y nivel de soporte: la tipología d ellos incidentes de seguridad gestionados por Evolutio-cert están alineados con los indicados por el Esquema Nacional de Seguridad de España (ENS):

- Contenido Abusivo
- Contenido Dañino
- Obtención de información
- Intento de Intrusión
- Intrusión
- Disponibilidad
- Compromiso de la información
- Fraude
- Vulnerabilidad
- APTs

El nivel de soporte variará dependiendo de la severidad de del incidente y de su potencial impacto, circunscrito a los sistemas de detección, contención y remediación gestionados y/o administrados por el CiSOC de Evolutio. En los casos en los que el CiSOC de Evolutio no gestiones o administre los sistemas de control necesarios, colaborará con los equipos de IR de los clientes.

4.2. Cooperación, Interacción y divulgación de la Información: Evolutio-CERT considera que es de vital importancia la coordinación y el intercambio de información entre CERTs y SOCs, ya que fruto de esta cooperación mejorar la eficacia y la eficiencia en la resolución de incidentes de ciberseguridad. Evolutio-CERT opera dentro del marco legal

de España y de la Unión Europea en el tratamiento y confidencialidad de la información que gestiona y posee políticas y normas para el tratamiento de la información clasificada.

4.3. Comunicación y Autenticación: El medio disponible para la comunicación es principalmente el correo electrónico cifrado con claves publicas dedicadas y publicadas en nuestro portal: https://www.evolutio.com/sobre-nosotros/cert/Claves-Publicas/

Evolutio-CERT reconoce y sigue el FIRTS TLP (Traffic Light Protocol) versión 1.0 en el intercambio de información.

5. Servicios

5.1. Consultoría y Auditoria

El objetivo inicial de este servicio es poder realizar un análisis que nos muestre de una forma precisa la postura de ciberseguridad de nuestros clientes, la elaboración de un informe que incluye un plan de actuación y una hoja de ruta con posibles mejoras y recomendaciones y poder ser además *compliant* con otros marcos de referencia y estándares de seguridad.

Otro servicio de consultoría prestado a clientes se enfoca en el análisis de las tácticas, técnicas y procedimientos utilizados por los ciberdelincuentes y atacantes que afectan a una organización en base a sus características (tamaño, países en los que opera y sector de actividad) para obtener una matriz ofensiva de amenazas. Adicionalmente, se analizarán los controles establecidos (matriz defensiva) en base a dicha matriz ofensiva para poder de esta manera detectar que Gaps se deben de cubrir para reducir el riesgo de ataque.

5.2. Preventivos

Evolutio-CERT junto con el CiSOC proporciona servicios orientados a la prevención de incidentes de seguridad tales como:

- Detección y análisis de anomalías de tráfico de red corporativa (NTA: Network Traffic analysis)
- Detección y análisis de anomalías o posibles amenazas de endpoint
- Detección y análisis de anomalías o posibles amenazas de Infraestructura de cloud pública o privada o SaaS (Casb)
- Vulnerability assessment.

- Boletines informativos sobre nuevas vulnerabilidades, campañas y amenazas emergentes
- Divulgación de buenas prácticas en ciberseguridad
- Realización de campañas de concienciación de phishing.
- Búsqueda proactivas y análisis de amenazas en Clear Web, Deep Web y Dark Web

5.3. Respuesta a Incidentes:

- Evolutio-CERT ofrece apoyo técnico y operativo en las distintas etapas del proceso de gestión de incidentes: preparación, detección, respuesta y post incident. Dentro de estas etapas, el CiSOC de Evolutio realiza el triaje de las alertas de las amenazas detectadas, la clasificación y el análisis de las mismas. En aquellas que se identifican como incidentes, se trabaja dentro de la disciplina del CERT en la contención, la mitigación y seguimiento hasta la recuperación. Pare ello, nos apoyamos en los sistemas y controles administrados por el CiSOC de Evolutio.
- Finalmente se realiza el reporte del incidente y las lecciones aprendidas como parte del proceso de mejora continua establecido.
- Mantenemos en todo momento la coordinación con los equipos de respuesta a incidentes de nuestros clientes durante todas las fases del proceso de gestión de incidentes.
- El ámbito de respuesta a incidents cubrirá los siguientes ámbitos:
    - Endpoint, a través de acciones ejecutadas en base a soluciones basadas en tecnologías de EDR (TrendMicro, Microsoft, PaloAlto y CrowdStrike)
    - Red, a través de acciones ejecutadas en base a soluciones basadas en tecnologías de NDR y en acciones ejecutadas directamente sobre tecnologías de infraestructura de red perimetral como por ejemplo Proxies, WAF, Firewalls de nueva generación etc

5.4. Monitorización:

Evolutio-CERT apoyándose en las capacidades de monitorización de amenazas del CiSOC de Evolutio, realiza la monitorización permanente de las alertas sobre amenazas apoyándonos tanto en la infraestructura de SIEM de Evolutio, desplegado sobre la infraestructura Pública y virtual de Evolutio multiclientes centralizado, como en los SIEM que administramos para nuestros clientes, sobre los que procesamos toda la información y eventos generados por los diferentes controles implementados.

Desarrollamos permanentemente nuevos casos de uso para la mejora en la detección de amenazas. Este Servicio de SIEM se enriquece, a parte de la configuración de casos de uso propiedad de Evolutio, de las Fuentes de inteligencia de amenazas con las que trabaja el equipo de analistas de Evolutio, así como con las capacidades en continua evolución de SOAR.

5.5. Vigilancia Digital:

A través del CiSOC de Evolutio, préstamos servicios de vigilancia Digital sobre activos sensibles de nuestros clientes, identificando las amenazas externas sobre los mismos tanto en la clear, Deep y dark web.

6. Formas de notificación de incidentes

La notificación de incidentes puede realizarse mediante:

Buzón de correo específico: **evolutio.cert@evolutio.com**

Los teléfonos de contacto se comunicarán durante el incidente.

7. Disclaimer

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