RFC 2350

CSIRT-RT

REALTIME CONSULTING & SERVICES

CSIRT-RT
REALTIME CONSULTING & SERVICES
https://www.rt.com.co/
soc@rt.com.co

Tabla de Contenido

RFC 2350 1
1. INFORMACIÓN DEL DOCUMENTO 3
1.1. Fecha de la última actualización 3
1.2. Lista de distribución para notificaciones 3
1.3. Ubicación del documento 3
2. INFORMACIÓN DE CONTACTO 3
2.1. Nombre del equipo 3
2.2. Zona horaria 3
2.3. Otras telecomunicaciones 3
2.4. Correo electrónico (método preferido) 3
2.5 Comunicación segura 3
2.6. Miembros del equipo. 3
2.7. Otra información 4
2.8. Puntos de contacto con el cliente 4
3. CARTA 4
3.1. Misión 4
3.2. Visión 4
3.3. Comunidad Atendida 5
3.4. Patrocinio y / o Afiliación 5
3.5. Autoridad 5
4. POLÍTICAS 5
4.1. Tipos de incidentes y nivel de soporte 5
4.2. Cooperación, interacción y divulgación de información 6
4.3. Comunicación y autenticación 6
5. SERVICIOS 6
6. FORMULARIOS DE NOTIFICACIÓN DE INCIDENTES 7
7. DESCARGOS DE RESPONSABILIDAD 8

1. INFORMACIÓN DEL DOCUMENTO

1.1. Fecha de la última actualización

La versión actual de este documento es la versión 1.0 y se lanzó el 01 de febrero del 2025.

1.2. Lista de distribución para notificaciones

Los cambios a este documento no se distribuyen por una lista de correo. Cualquier pregunta o comentario específico, por favor diríjase a la dirección de correo.

1.3. Ubicación del documento

La última versión del documento se encuentra publicada tanto en Español, como en Inglés.

2. INFORMACIÓN DE CONTACTO

2.1. Nombre del equipo

CSIRT RT

2.2. Zona horaria

UTC –5 (Bogotá Colombia)

2.3. Otras telecomunicaciones

Contacto - CSIRT RT

Central Telefónica: 5717943337 – Ext. 911

2.4. Correo electrónico (método preferido)

- Informe de incidentes: csirtrt@rt.com.co
- Información de carácter general: csirtrt@rt.com.co

2.5 Comunicación segura

PGP:

2.6. Miembros del equipo.

En la fecha de publicación de este documento el equipo se encuentra constituido por analistas de seguridad dedicados a tiempo completo.

Una lista completa de los miembros del equipo no está disponible públicamente. Los miembros del equipo se identificarán ante la parte

informante con su nombre completo en una comunicación oficial sobre un incidente.

2.7. Otra información

La información general de los servicios la podrá encontrar publicadas en el siguiente portal: https://www.rt.com.co.

2.8. Puntos de contacto con el cliente

El método preferido para comunicarse con "CSIRT-RT" en caso de incidentes cibernéticos por partes de sus clientes es mediante mensajes de correo electrónicos con csirtrt@rt.com.co. El equipo de respuesta a incidentes está disponible en función de los servicios contratados. El mensaje de correo electrónico enviado a dicha dirección será comunicado al responsable, o se reenviará automáticamente a la persona de respaldo adecuada, de inmediato.

Si necesitas asistencia urgente, agregue la palabra "URGENTE" al inicio del asunto del mensaje para poder activar los flujos de emergencia. Si no es posible o por razones de confidencialidad, puede contactar al 5717943337 – Ext. 911 por teléfono.
El horario de funcionamiento del CSIRT-RT es 24x7x365.

2. CARTA

3.1. Misión

En CSIRT RT, nuestra misión es proporcionar una respuesta inmediata, eficiente y profesional ante incidentes de seguridad cibernética, protegiendo la integridad, confidencialidad y disponibilidad de los activos digitales de nuestras organizaciones y clientes. A través de la colaboración, el monitoreo en tiempo real y el análisis continuo de amenazas, garantizamos la mitigación de riesgos y la restauración rápida de los sistemas afectados, promoviendo la resiliencia cibernética.

3.2. Visión

Ser un referente en la industria de ciberseguridad, reconocido por nuestra capacidad para anticipar, detectar y responder a incidentes de manera proactiva y eficaz. Aspiramos, una vez siendo miembros activos del FIRST, colaborar globalmente en la mejora de las mejores prácticas de seguridad y estableciendo a CSIRT-RT como un líder en la protección digital en tiempo real.

3.3. Comunidad Atendida

Atenderemos a los clientes internos y externos de Colombia, tanto del sector público como privado, que hayan suscrito o formalizado algún acuerdo de servicios de los clientes externos pueden estar físicamente localizados dentro del territorio, así como también atenderemos a clientes de otros países de la región latinoamericana.

3.4. Patrocinio y / o Afiliación

CSIRT-RT está patrocinado por RealTime Consulting & Services y busca estar afiliado a instituciones alrededor del mundo para colaborar, compartir información y dar soporte a incidentes de ciberseguridad.

3.5. Autoridad

CSIRT-RT colabora estrechamente con los administradores y usuarios de los sistemas de COLCERT, y con los clientes internos y externos, promoviendo relaciones de cooperación y no de autoridad cuando sea posible. Sin embargo, si las circunstancias lo justifiquen, el apelará a para ejercer su autoridad directa o indirecta, según sea necesario.
Adicionalmente, realiza las acciones que requieran sus clientes a nivel operativo y técnico, teniendo siempre la potestad principal y última decisión sobre las acciones a realizar.

Se deja la potestad de que los clientes o miembros de la comunidad puedan apelar a las acciones del poniéndose en contacto con el Coordinador del SOC. En caso de que no se encuentre disponible o se requiere un escalamiento, se debe comunicar con el Gerente del. En cualquier caso, la comunicación se debe iniciar a través del canal de comunicación establecido.

4. POLÍTICAS

CSIRT-RT definirá sus políticas y procedimientos para la operación y la gestión de incidentes a lo largo de todo su ciclo de vida. No obstante, conforme a lo establecido en el RFC 2350, se describe lo siguiente:

4.1. Tipos de incidentes y nivel de soporte

El CSIRT-RT puede abordar cualquier incidente de seguridad de la información dentro de su comunidad atendida o área de alcance, si está dentro de los servicios que ofrece. Puede intervenir cuando los miembros de su comunidad lo soliciten o cuando alguno de ellos esté involucrado en un

incidente de seguridad informática.

El nivel de asistencia proporcionado por CSIRT-RT variará según la naturaleza y la gravedad del incidente, el tipo de interesado dentro de su comunidad a entidad, el tamaño de la comunidad de usuarios afectados y los recursos disponible en ese momento.

4.2. Cooperación, interacción y divulgación de información

CSIRT-RT colabora con otros equipos especializados en la mejora de la seguridad, para ello puede compartir la naturaleza de los incidentes detectados en el ejercicio de sus funciones y los métodos de actuación llevados a cabo para su resolución. No obstante, se considera información confidencial cualquier dato que pueda comprometer los sistemas de información o identificar a nuestros clientes no compartiendo ningún tipo de información relevante a los mismos, salvo consentimiento previo, en cuyo caso se utilizará un método seguridad para garantizar su confidencialidad e integridad.

4.3. Comunicación y autenticación

El método preferido de comunicación es por correo electrónico. La utilización de correos electrónicos no cifrados no se valora como un medio seguro de comunicación. No obstante, resulta adecuado para la transmisión de datos de baja sensibilidad o información no delicada. Es importante tener en cuenta que los datos sensibles, que abarcan información de carácter altamente confidencial (restringido, confidencial, secreto o estrictamente secreto), deben ser cifrados antes de su transmisión, lo cual también aplica para la transferencia de archivos.

5. SERVICIOS

El nuevo departamento realizará las siguientes funciones según los tipos de servicios descritos a continuación:

1. **Servicios Proactivos:**
    a. Monitoreo de alertas-notificaciones de seguridad y análisis de amenazas.
    b. Gestión y administración de herramientas y soluciones de seguridad, que incluye su configuración y soporte que incluye las actualizaciones de versiones y aplicación de parches.

c. Búsquedas y alertas de vulnerabilidades cuando sea parte del servicio contratado.
d. Validación de amenazas (threat hunting) cuando sea parte del servicio contratado.
e. Evaluación de riesgos tecnológicos.
f. Difusión de información y boletines relacionados a la ciberseguridad.

2. **Servicios reactivos**
   a. Gestión de eventos de seguridad (identificación, análisis, respuesta, soporte y coordinaciones).
   b. Respuesta a incidentes (análisis, contención y remediación), y coordinación interna y externa.
   c. Evaluación forense cuando sea parte del servicio contratado.

3. **Evaluación de Seguridad**
   a. Descubrimiento de activos en la infraestructura de los clientes.
   b. Escaneo de vulnerabilidades TI OT, análisis y recomendaciones sobre actualizaciones, configuraciones en equipo de seguridad.
   c. Seguimiento de acciones preventivas para robustecer la postura de seguridad

4. **Concientización**
   a. Concientización para reducir el riesgo de ciberataques ocasionados por errores humanos.

5. **Boletines de Seguridad**
   a. Publicación y envío regularmente de boletines de ciberseguridad, con los avisos de las últimas vulnerabilidades de los principales fabricantes de soluciones con que cuentan nuestros clientes.

6. FORMULARIOS DE NOTIFICACIÓN DE INCIDENTES

Para reportar incidentes, por favor envié un correo electrónico a la dirección csirtrt@rt.com.co.
Al notificar un incidente, es necesario proporcionar la siguiente información:

- Nombre de usuario
- Nombre del cliente
- Número de contacto
- Descripción del incidente

7. DESCARGOS DE RESPONSABILIDAD

Si bien se tomarán todas las precauciones en la preparación de la información, notificaciones y alertas, CSIRT-RT no asume ninguna responsabilidad por errores u omisiones, ni por daños resultantes del uso de la información proporcionada durante la ejecución de sus servicios.