RFC 2350
Cyber Incident Response Command (C.I.R.C.)
Evolution Discovery LLC

Versión: 1.3

Control de Versiones

Autor	Versión	Fecha Aprobación	Descripción
C.I.R.C.	1.0	02/03/2023	Versión inicial del documento.
C.I.R.C.	1.1	01/09/2024	Actualización de claves públicas y dirección de correo electrónico asociada.
C.I.R.C.	1.2	01/01/2025	Corrección de hipervínculos relacionados con el sitio web oficial de Evolution Discovery (evolutiondiscovery.com).

Índice

1. Difusión

1.1. Destinatarios del documento

Este documento está dirigido a clientes, socios, y partes interesadas en los servicios de ciberseguridad proporcionados por **Evolution Discovery LLC.**

1.2. Introducción

El presente documento describe el funcionamiento, servicios y políticas del **Cyber Incident Response Command (C.I.R.C.)** de **Evolution Discovery LLC**, conforme al estándar **RFC 2350** de IETF, disponible en: https://www.ietf.org/rfc/rfc2350.txt.

1.3. Fecha de la última actualización

La versión vigente de este documento corresponde a la versión 1.3, publicada el 1 de enero de 2024.

1.4. Localizaciones en las que se puede acceder al documento

- El sitio web oficial de Evolution Discovery LLC: www.evolutiondiscovery.com.
- Solicitud directa por correo electrónico a: circ@evolutiondiscovery.com.

1.5. Autenticación del documento

La autenticidad del documento puede verificarse mediante la clave PGP disponible en el sitio web oficial de **Evolution Discovery LLC.**

1.6. Identificación del documento

RFC 2350 Cyber Incident Response Command (C.I.R.C.) Evolution Discovery LLC

2. Información de contacto

2.1. Nombre del equipo

Cyber Incident Response Command (C.I.R.C.) de Evolution Discovery LLC.

2.2. Dirección Postal

7901 4th St N, STE 300, St. Petersburg, FL 33702, USA

2.3. Zona horaria

GMT-5 (Hora Estándar del Este de los Estados Unidos).

2.4. Teléfonos de contacto

Teléfono: +1 (786) 798-7222

2.5. Número de fax

Actualmente, no se dispone de un número de fax.

2.6. Direcciones de correo electrónico

Comunicación y gestión de incidentes: circ@evolutiondiscovery.com

Otras comunicaciones: contact@evolutiondiscovery.com

2.7. Otros medios de comunicación

No se han definido al momento de la publicación del presente documento.

2.8. Claves públicas y cifrado

El **C.I.R.C.** utiliza la dirección de correo electrónico **circ@evolutiondiscovery.com** para las comunicaciones relacionadas con la gestión de incidentes. Para garantizar la seguridad de dichas comunicaciones, emplea la siguiente clave PGP:

Fingerprint: A235 7B25 FEEE 15DC CEB8 E375 469A 5C79 51C6 6461

Esta clave está disponible en los servidores públicos de PGP, accesibles en **https://keys.openpgp.org**, así como en la dirección web previamente mencionada en este documento.

Se debe utilizar el cifrado PGP para todas las comunicaciones por correo electrónico que, debido a su nivel de confidencialidad, lo requieran.

2.9. Componentes del equipo

El equipo está conformado por especialistas en **respuesta a incidentes**, **análisis forense digital** y **consultoría en ciberseguridad**.

Por razones de privacidad, el listado del personal integrante no se incluye en este documento. Si requiere información adicional, le invitamos a contactarnos directamente.

2.10. Horas de funcionamiento

El **C.I.R.C.** opera bajo los siguientes horarios:

- **Área operativa:** 24 horas al día, 7 días a la semana, los 365 días del año.
- **Área administrativa:** De lunes a viernes, de 8:00 h a 17:00 h.

2.11. Información adicional

Para más información, visite nuestra página oficial o contáctenos directamente.

2.12. Puntos de contacto

Para comunicaciones no relacionadas con incidentes, se deberá utilizar el correo electrónico dirigido a:

- **Correo electrónico dirigido a:** contact@evolutiondiscovery.com

Para la comunicación y gestión de incidentes, los medios de contacto asignados son:

- **Correo electrónico dirigido a:** circ@evolutiondiscovery.com
- **Llamadas telefónicas al número:** +1 (786) 798-7222

3. Objetivos

3.1. Misión

El **Cyber Incident Response Command (C.I.R.C.)** de **Evolution Discovery LLC** es un **Equipo de Respuesta ante Emergencias Informáticas (CSIRT)** privado, dedicado a proporcionar servicios de ciberseguridad de alta calidad. Su misión es responder de manera eficaz a incidentes de seguridad, garantizando la protección de los activos digitales de sus

clientes ante eventos que puedan afectar la integridad, confidencialidad o accesibilidad de la información, así como comprometer sus operaciones o reputación.

Los servicios del **C.I.R.C.** están disponibles para clientes externos mediante suscripción, la cual puede ser realizada para la totalidad o parte de los servicios ofrecidos.

Para alcanzar estos objetivos, el **C.I.R.C.** lleva a cabo, entre otras, las siguientes tareas:

- **Recopilación y análisis de información** de diversas fuentes sobre nuevas vulnerabilidades y amenazas.
- **Comunicación a los clientes** de la inteligencia generada que sea relevante para su contexto operativo.
- **Distribución de información técnica** sobre incidentes con otros centros de respuesta a incidentes, con el fin de mejorar la respuesta conjunta ante los mismos.
- **Realización de tareas proactivas y preventivas** para mejorar la seguridad de los beneficiarios.
- **Monitorización de eventos de seguridad** y detección de incidentes.
- **Apoyo a los clientes** en la coordinación y gestión de respuestas ante incidentes de seguridad que pudieran afectarlos.

Con el objetivo de lograr estos fines, el **C.I.R.C.** se adhiere, desde su creación, a los siguientes valores fundamentales:

- **Cumplimiento de la normativa legal** aplicable a nivel nacional e internacional respecto a los servicios proporcionados.
- **Aplicación de las mejores prácticas** reconocidas en el sector, adoptándolas como referencia para sus operaciones.
- **Establecimiento de estrictos requisitos éticos y de confidencialidad** para todo el personal involucrado en el servicio.
- **Promoción del uso de buenas prácticas** entre sus clientes.
- **Provisión de una capacidad de respuesta eficaz y eficiente** frente a incidentes.

- **Definición y ejecución de procesos de auditoría continua de calidad y seguridad** sobre los servicios suministrados, tomando como referencia metodologías y estándares reconocidos en el sector.
- **Creación y mantenimiento de procesos de comunicación y evaluación periódica** de las necesidades de los clientes, internos y externos, dentro de un marco de mejora continua de los servicios.

3.2. Circunscripción

Los servicios proporcionados por el **C.I.R.C.** están dirigidos a todos los departamentos internos de **Evolution Discovery LLC**, así como a empresas e instituciones externas que se suscriban a dichos servicios.

3.3. Afiliación

El **C.I.R.C.** forma parte del grupo de operaciones de **Evolution Discovery LLC**. Además, mantiene relaciones con diversas organizaciones relacionadas en el ámbito de la ciberseguridad y la respuesta ante incidentes.

3.4. Autoridad

El **C.I.R.C.** actúa bajo la autoridad del **responsable de la seguridad de la información corporativa** de **Evolution Discovery LLC**, en coordinación con el **Área Legal y Regulatoria** cuando sea necesario, y con la **Dirección** de la empresa.

En relación con sus clientes externos, el **C.I.R.C.** actúa como asesor de los equipos de seguridad de dichos clientes y no dispone de autoridad sobre los mismos. En consecuencia, la implementación de las recomendaciones proporcionadas será exclusivamente responsabilidad del cliente.

4. Políticas

4.1. Tipos de incidentes gestionados y nivel de soporte proporcionado

El C.I.R.C. proporciona soporte para incidentes de ciberseguridad que puedan afectar la integridad, disponibilidad y confidencialidad de la información gestionada por los sistemas y procesos de los clientes suscritos al servicio.

De manera general, los tipos de incidentes soportados corresponden a las categorías establecidas por la European Union Agency for Network and Information Security (ENISA), y pueden consultarse en el documento titulado "Good Practice Guide on How to Improve CSIRT Capabilities", publicado por ENISA el 26 de enero de 2018. Este documento se encuentra disponible en el siguiente enlace:

https://www.enisa.europa.eu/sites/default/files/publications/WP2017%20O-3-1-1%20Good%20practice%20guide%20on%20how%20to%20improve%20CSIRT%20capabilities.pdf

Todos los incidentes confirmados son clasificados según su tipología y gravedad, y las respuestas se priorizan en función de esta clasificación. El **C.I.R.C.** asigna recursos y coordina esfuerzos para garantizar una respuesta efectiva y adecuada a cada situación, teniendo en cuenta el impacto potencial en las operaciones de los clientes.

El **C.I.R.C.** no proporciona soporte directo a usuarios finales externos a **Evolution Discovery LLC**, ya que se entiende que estos contactarán con sus propios servicios de seguridad. Todas las comunicaciones entre el **C.I.R.C.** y sus clientes externos serán gestionadas a través de los interlocutores definidos en el contrato de servicio.

El nivel de soporte proporcionado puede variar según las condiciones contractuales del servicio, la tipología, el impacto, la severidad y/o la complejidad del incidente. En función de estos factores, el **C.I.R.C.** ajustará los recursos y la respuesta para garantizar la protección adecuada de los activos digitales del cliente.

4.2. Cooperación, interacción y distribución de información

El **Cyber Incident Response Command (C.I.R.C.)** interactúa activamente con diversas organizaciones en el cumplimiento de su misión. Estas incluyen otros equipos CERT/CSIRT, proveedores, analistas y generadores de inteligencia, entre otros actores relevantes.

A nivel nacional, el organismo de referencia designado para la coordinación de incidentes de seguridad es el **Cybersecurity and Infrastructure Security Agency (CISA)**

(https://www.cisa.gov). CISA es responsable de coordinar la respuesta a incidentes de seguridad que afectan a ciudadanos, organismos gubernamentales y empresas del sector privado en los Estados Unidos.

Aunque hasta la fecha no se han formalizado relaciones de cooperación con otros equipos CSIRT o CERT dentro de los Estados Unidos, el **C.I.R.C.** cumple con las disposiciones de la **S.2588 - Cybersecurity Information Sharing Act of 2014 (CISA)**. Esta legislación fomenta la cooperación y el intercambio de información entre entidades privadas y gubernamentales para mejorar la defensa contra amenazas cibernéticas, garantizando la protección de los datos sensibles compartidos.

Se han iniciado esfuerzos para establecer relaciones formales con equipos CSIRT autónomos, sectoriales e internacionales, con el fin de optimizar la capacidad de respuesta y la distribución de información sobre amenazas.

El **C.I.R.C.** aplica políticas estrictas para garantizar la protección y el uso responsable de la información compartida. Estas políticas están alineadas con los principios establecidos en la **S.2588 - Cybersecurity Information Sharing Act of 2014** y se implementan mediante las siguientes directrices:

- **Protección de la privacidad y las libertades civiles**: Se desarrollan y actualizan periódicamente directrices para garantizar la protección de la privacidad y las libertades civiles, conforme a los principios establecidos en la **S.2588**.
- **Uso exclusivo para ciberseguridad**: La información compartida debe utilizarse únicamente para fines relacionados con la ciberseguridad o conforme a los objetivos legales establecidos.
- **Eliminación de datos personales no relacionados**: Antes de compartir información, se eliminan todos los datos personales que no estén directamente relacionados con amenazas cibernéticas.
- **Anonimización de datos**: Siempre que sea posible, los datos compartidos deben anonimizarse, limitándose a los elementos necesarios para abordar problemas de ciberseguridad.

- **Protección frente a divulgaciones no autorizadas**: El uso de información compartida está restringido y cualquier divulgación no autorizada conlleva sanciones.
- **Consentimiento explícito del propietario**: La información solo puede compartirse con la autorización explícita de su propietario, salvo que exista una obligación legal que lo requiera.
- **Prohibición de usos indebidos**: Se prohíbe el uso de la información para fines comerciales, discriminatorios o no relacionados con la ciberseguridad.
- **Protección de datos personales**: Se evita la divulgación de datos personales, salvo en casos estrictamente necesarios y con la autorización expresa del titular.
- **Cese inmediato de distribución**: Si el propietario de la información retira su autorización, se detiene la distribución de los datos, salvo que exista una obligación legal que lo impida.

4.3. Operaciones

El **C.I.R.C.** opera cumpliendo con la normativa legal vigente en los Estados Unidos, adhiriéndose a las disposiciones federales establecidas en la **S.2588 - Cybersecurity Information Sharing Act of 2014 (CISA)**, que regula el intercambio de información sobre amenazas cibernéticas entre entidades públicas y privadas. Además, el **C.I.R.C.** implementa las mejores prácticas y directrices establecidas en el **NIST Cybersecurity Framework** del **National Institute of Standards and Technology (NIST)**, asegurando un enfoque integral en la detección, respuesta y mitigación de incidentes cibernéticos, garantizando así una respuesta eficaz y alineada con los estándares internacionales en materia de ciberseguridad.

4.4. Comunicación y autenticación

El **C.I.R.C.** aplica las medidas de protección correspondientes a la información manejada, considerando su naturaleza y clasificación, de acuerdo con la normativa legal vigente en los Estados Unidos, particularmente en el estado de Florida. Además de cumplir con las disposiciones establecidas en la **S.2588 - Cybersecurity Information Sharing Act of 2014 (CISA)**, se toman en cuenta principios y directrices locales de ciberseguridad y

privacidad. Para la gestión de la información, el C.I.R.C. emplea el protocolo **FIRST TLP v1.1** tanto a nivel interno como externo, asegurando la correcta clasificación y etiquetado de los documentos conforme a los siguientes niveles de información:

RED: Información no distribuible, restringida exclusivamente a representantes autorizados, quienes deben haber firmado los correspondientes acuerdos de confidencialidad.
AMBER: Información con distribución limitada, accesible solo para personal autorizado con necesidad legítima de conocer y que haya suscrito los compromisos de confidencialidad.
GREEN: Información de distribución restringida a instituciones dentro de la red de confianza del servicio, con acuerdos de no distribución, pero sin acceso libre ni publicación.
WHITE: Información de libre distribución, aunque puede estar sujeta a copyright.

Dada la naturaleza de los datos manejados, el C.I.R.C. considera que las comunicaciones a través de teléfonos son suficientemente seguras para el intercambio de información no cifrada. En cambio, el correo electrónico no cifrado no se considera completamente seguro, pero es adecuado para la transmisión de datos de baja sensibilidad. En el caso de que se necesite enviar datos altamente confidenciales, se aplicará cifrado utilizando claves PGP tanto del emisor como del receptor. Las transferencias de archivos de red se tratarán de manera similar al correo electrónico, por lo que los datos confidenciales deberán ser cifrados durante su transmisión. Además, para establecer relaciones de confianza antes de revelar información confidencial, se verificará la identidad de la otra parte con un grado razonable de confianza, empleando referencias de terceras partes o organismos conocidos y confiables como medio de acreditación.

5. Servicios

5.1. Consultoría en ciberseguridad:

Asesoramiento a organizaciones para identificar y mitigar riesgos digitales, implementando medidas de seguridad adecuadas.

5.2. Auditorías de seguridad informática:

Evaluación de sistemas y redes para detectar vulnerabilidades y garantizar el cumplimiento de estándares de seguridad.

5.3. Servicios de respuesta a incidentes:

Intervención en casos de brechas de seguridad, gestionando y resolviendo incidentes cibernéticos de manera efectiva.

5.3.1. Triaje:

- Investigación inicial para confirmar si ocurrió un incidente de seguridad.
- Determinación del alcance y severidad del incidente.

5.3.2. Coordinación de Incidentes:

- Identificación de la causa raíz del incidente, incluyendo la vulnerabilidad explotada.
- Realización de adquisiciones y análisis forense digital, cuando sea necesario, abarcando forense de discos duros y memoria.
- Coordinación con contactos de seguridad y/o autoridades legales pertinentes, según se requiera.
- Notificación y colaboración con otros CSIRTs, CERTs o SOCs, si aplica.

5.3.3. Resolución de Incidentes:

- Asesoramiento y soporte para remediar las vulnerabilidades explotadas.
- Implementación de medidas para asegurar los sistemas y prevenir efectos secundarios del incidente.
- Evaluación estratégica para determinar la proporcionalidad entre el costo y riesgo de las acciones recomendadas.
- Recolección de evidencia sólida en casos donde se contemple acción penal o disciplinaria.

5.4. Capacitación en ciberseguridad:

Formación de personal en prácticas seguras y concientización sobre amenazas digitales.

5.5. Protección de datos personales:

Implementación de políticas y procedimientos para asegurar la privacidad y el manejo adecuado de la información sensible.

5.6. Análisis forense digital:

Investigación de delitos informáticos, recopilando y preservando evidencia digital para procedimientos legales.

6. Formularios de respuesta a incidentes

Para las comunicaciones relacionadas con el servicio, se utilizan formatos previamente acordados entre las partes involucradas o aquellos ampliamente reconocidos en el ámbito del sector. En los casos en que la comunicación provenga de una fuente externa y no exista un formato de notificación previamente establecido, se recomienda que dicha comunicación contenga al menos los siguientes datos:

- **Datos de identificación**: Nombre del remitente, nombre de la organización, dirección física, etc.
- **Datos de contacto**: Dirección de correo electrónico y número telefónico (si está disponible).
- **Clave PGP**: En caso de estar disponible, incluirla para la seguridad de la comunicación.
- **Resumen conciso del incidente**: Descripción breve y clara del incidente reportado.
- **Método de detección del incidente**: Indicar cómo fue identificado el incidente.
- **Sistemas afectados e impacto inicial**: Especificar qué sistemas se vieron afectados y una estimación inicial del impacto.
- **Información técnica relevante**: Incluir detalles técnicos clave sobre el incidente, como cabeceras de correo, direcciones IP involucradas, muestras y artefactos

relacionados, o cualquier otra información relevante sobre los medios disponibles para compartir estos datos.

Siempre que sea posible, se recomienda que los incidentes sean reportados por correo electrónico utilizando la dirección previamente indicada en este documento.

Adicionalmente, el C.I.R.C. ha desarrollado plantillas y formatos propios para la gestión de los incidentes, facilitando el análisis y la posterior comunicación de los resultados a los clientes de manera clara y estructurada.

7. Descarga de responsabilidad

El C.I.R.C. toma todas las precauciones necesarias en la preparación, verificación y distribución de la información, notificaciones y alertas relacionadas con la gestión de incidentes cibernéticos. Sin embargo, no asume ninguna responsabilidad por errores, omisiones, inexactitudes o cualquier daño directo o indirecto que pueda derivarse del uso de la información proporcionada.

Asimismo, el C.I.R.C. no será responsable por la interpretación incorrecta, aplicación inapropiada o consecuencias del uso indebido de los datos o alertas entregadas durante la ejecución de sus servicios, ya que la información se proporciona con fines de orientación y prevención, y depende del receptor garantizar su correcta aplicación según el contexto específico.

En ningún caso el C.I.R.C. será responsable de los daños que resulten del uso de la información contenida en los informes, comunicaciones o alertas, incluyendo, pero no limitado a, la pérdida de datos, interrupción de actividades o cualquier otro perjuicio derivado de las decisiones tomadas basadas en dicha información.

La responsabilidad sobre la correcta implementación y manejo de las recomendaciones proporcionadas recae exclusivamente en las entidades receptoras de la información, las cuales deben realizar su propio análisis y evaluación en función de sus necesidades y circunstancias específicas.