RFC 2350

CENTRO DE RESPUESTA A INCIDENTES CIBERNÉTICOS

1. Información del Documento

1.1. Fecha de la última actualización:
Versión 1.0, publicada el 22 de octubre de 2025.

1.2. Lista de Distribución:
Los cambios en este documento se comunicarán mediante notificación oficial en el portal institucional del Grupo Radical:
https://gruporadical.com

1.3. Ubicación del Documento:

- Español: https://gruporadical.com/servicios/cert/
- English: https://gruporadical.com/servicios/cert/

1.4. Autenticación del Documento:
Este documento se encuentra firmado digitalmente por el CERT RADICAL GRD RADICAL CORPORATION C.L.

2. Información de Contacto

2.1. Nombre del Equipo:
CERT RADICAL – GRD RADICAL CORPORATION C.L.

2.2. Dirección:
Av. Diego de Almagro y Pedro Ponce Carrasco, Edificio Almagro Plaza.
Quito – Ecuador.

2.3. Zona Horaria:
GMT -5 (Hora de Ecuador)

2.4. Teléfono:
+593 (02) 2-909-088

2.5. Fax:
No aplica.

2.6. Otras Comunicaciones:
A través del portal web institucional: https://gruporadical.com/contactanos

2.7. Correos Electrónicos:

- Reporte de incidentes: **incidente@gruporadical.com**
- Consultas generales: **info@gruporadical.com**

2.8. Claves Públicas y Cifrado:
Las claves PGP y certificados digitales del equipo están disponibles bajo solicitud a través del correo **cert@gruporadical.com**

2.9. Miembros del Equipo:
Por razones de seguridad y confidencialidad, los nombres de los miembros no se publican.

2.10. Más Información:
Información general sobre los servicios del CERT RADICAL y del Grupo Radical se encuentra en https://gruporadical.com

2.11. Horario de Atención:

- Consultas sobre servicios: Lunes a Viernes, 09h00–18h00 (GMT -5)
- Incidentes críticos o de alta peligrosidad: **24x7x365**

2.12. Puntos de Contacto para la Comunidad:
El contacto con la comunidad se realiza por los canales oficiales de correo electrónico y teléfono asignados durante los procesos de soporte y gestión de incidentes.

3. Constitución

3.1. Misión:
El CERT RADICAL es la **Capacidad de Respuesta ante Incidentes de Seguridad Informática (CSIRT)** de **GRD RADICAL CORPORATION C.L.**, cuyo objetivo es **proteger los activos digitales, la información y la continuidad operativa** de sus clientes y aliados estratégicos.
Su misión es **detectar, analizar, contener y responder eficazmente a los incidentes de ciberseguridad**, promoviendo un entorno digital más seguro mediante la aplicación de estándares internacionales (ISO 27001, NIST, ENS, CIS Controls) y la coordinación con organismos nacionales e internacionales.

3.2. Comunidad a la que brinda servicios:
CERT RADICAL brinda servicios a:

- Organizaciones públicas y privadas que mantienen contratos con Grupo Radical.
- Infraestructuras críticas y sectores estratégicos en Ecuador y la región.
- Entidades financieras, telecomunicaciones, energía y organismos multilaterales asociados.

3.3. Patrocinio:
El CERT RADICAL forma parte del **Grupo Radical (GRD RADICAL CORPORATION C.L.)**, compañía ecuatoriana especializada en **tecnologías avanzadas de ciberseguridad, telecomunicaciones y transformación digital.**

3.4. Autoridad:
La autoridad del CERT RADICAL emana de las políticas internas de Grupo Radical, de los contratos de prestación de servicios de ciberseguridad con clientes, y de su reconocimiento en coordinación con organismos nacionales e internacionales de ciberseguridad.

4. Políticas

4.1. Tipo de Incidentes y Nivel de Soporte:

CERT RADICAL gestiona incidentes que involucran:

- Intrusiones, malware, ransomware, DDoS, fugas de información.
- Compromisos de credenciales o accesos no autorizados.
- Fraudes digitales y phishing.
- Vulnerabilidades críticas y configuraciones inseguras.
  El nivel de soporte y la respuesta dependen de la **criticidad del incidente**, su impacto y el tipo de cliente afectado.

4.2. Cooperación y Divulgación de Información:

Toda la información tratada por CERT RADICAL se maneja bajo estrictos principios de **confidencialidad, integridad y disponibilidad**, conforme a la **Ley Orgánica de Protección de Datos Personales (Ecuador)** y las políticas de seguridad de Grupo Radical.

4.3. Comunicación y Autenticación:

Toda comunicación se realiza mediante canales seguros (correo cifrado, VPN, autenticación multifactor) y claves PGP verificables.

5. Servicios

5.1. Prevención:

- Gestión proactiva de vulnerabilidades.
- Emisión de alertas y boletines de seguridad.
- Evaluaciones de riesgo y cumplimiento ENS/ISO27001.
- Capacitaciones, simulacros y campañas de concienciación.

5.2. Respuesta a Incidentes:

- Identificación, análisis y contención de incidentes.
- Asesoría técnica y coordinación con clientes.
- Elaboración de informes forenses y de lecciones aprendidas.

5.3. Análisis Forense:

- Adquisición y preservación de evidencias digitales.
- Análisis forense de sistemas, redes y dispositivos móviles.
- Soporte técnico en procesos judiciales o periciales.

5.4. Ciberinteligencia:

- Monitoreo de amenazas en superficie, deep y dark web.
- Identificación de actores de amenaza y campañas dirigidas.

- Análisis estratégico y técnico de indicadores de compromiso (IoC).

5.5. Pruebas de Penetración:

- Evaluación controlada de vulnerabilidades técnicas y humanas.
- Simulación de ataques (Red Team / Blue Team / Purple Team).

5.6. Consultoría:

- Asesoría en cumplimiento normativo ENS, ISO 27001, NIST CSF.
- Diseño e implementación de políticas y marcos de seguridad.

5.7. Formación y Sensibilización:

- Programas de entrenamiento técnico y ejecutivo.
- Talleres prácticos en respuesta a incidentes, forensia digital y gestión de crisis.

6. Notificación de Incidentes

Los incidentes pueden reportarse a través de:

- Correo electrónico: **incidente@gruporadical.com**
- Teléfono de emergencia (24x7)

Se recomienda incluir en la notificación:

- Descripción del incidente y su impacto.
- Fecha y hora aproximada del evento.
- Datos de contacto del responsable técnico.
- Evidencias iniciales o registros relevantes (en caso de ser posible).

7. Disclaimer

El CERT RADICAL no se responsabiliza del uso indebido o no autorizado de la información contenida en este documento.
Toda información compartida con el CERT RADICAL será tratada de forma confidencial y utilizada exclusivamente para fines de gestión y mitigación de incidentes de ciberseguridad.