RFC 2350

CYBER INCIDENT RESPONSE CENTER

1. Document Information

1.1. Last updated:
Version 1.0, released October 22, 2025.

1.2. Distribution List:
Changes to this document will be communicated via official notification on the Radical Group's institutional portal:
https://gruporadical.com

1.3. Document Location:

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

1.4. Document Authentication:
This document is digitally signed by CERT RADICAL GRD RADICAL CORPORATION CL

2. Contact Information

2.1. Team Name:
CERT RADICAL – GRD RADICAL CORPORATION CL

2.2. Address:
Diego de Almagro Avenue and Pedro Ponce Carrasco, Almagro Plaza Building .
Quito, Ecuador.

2.3. Time Zone:
GMT -5 (Ecuador Time)

2.4. Telephone:
+593 (02) 2-909-088

2.5. Fax:
Not applicable .

2.6. Other Communications:
Through the institutional web portal: https://gruporadical.com/contact anos

2.7. Emails:

- Incident Report: **incidencia@gruporadical.com**
- General inquiries: **info@gruporadical.com**

2.8. Public Keys and Encryption:
The team's PGP keys and digital certificates are available upon request via email **at cert@gruporadical.com**

2.9. Team Members:
For security and confidentiality reasons, team member names are not published.

2.10. More Information:
General information about the services of the RADICAL CERT and the Radical Group can be found at https://gruporadical.com

2.11. Opening Hours:

- Service inquiries: Monday to Friday , 9:00 a.m.–6:00 p.m. (GMT -5)
- Critical or high-risk incidents: **24x7x365**

2.12. Community Contact Points:
Community contact is made through the official email and telephone channels assigned during the support and incident management processes.

3. Constitution

3.1. Mission:
The RADICAL CERT is the **Computer Security Incident Response Capability (CSIRT)** of **GRD RADICAL CORPORATION CL** , whose objective is **to protect the digital assets, information and operational continuity** of its clients and strategic allies.
Its mission is **to detect, analyze, contain and respond effectively to cybersecurity incidents** , promoting a more secure digital environment through the application of international standards (ISO 27001, NIST, ENS, CIS Controls) and coordination with national and international organizations.

3.2. Community served:
CERT RADICAL provides services to:

- Public and private organizations that maintain contracts with Grupo Radical.
- Critical infrastructure and strategic sectors in Ecuador and the region.
- Financial institutions, telecommunications, energy and associated multilateral organizations.

3.3. Sponsorship:
The RADICAL CERT is part of the **Radical Group (GRD RADICAL CORPORATION CL)** , an Ecuadorian company specializing in **advanced cybersecurity, telecommunications, and digital transformation technologies.**

3.4. Authority:
The authority of the RADICAL CERT emanates from the internal policies of the Radical Group, from its cybersecurity service provision contracts with clients, and from its recognition in coordination with national and international cybersecurity organizations.

4. Policies

4.1. Incident Type and Support Level:

CERT RADICAL manages incidents involving:

- Intrusions, malware , ransomware , DDoS, information leaks.
- Credential compromises or unauthorized access.
- Digital fraud and phishing.
- Critical vulnerabilities and insecure configurations.
  The level of support and response depend on the **criticality of the incident** , its impact, and the type of customer affected.

4.2. Cooperation and Disclosure of Information:

All information processed by CERT RADICAL is handled under strict principles of **confidentiality, integrity and availability** , in accordance with the **Organic Law on the Protection of Personal Data (Ecuador)** and the security policies of Grupo Radical.

4.3. Communication and Authentication:

All communication is carried out through secure channels (encrypted email, VPN, multi-factor authentication) and verifiable PGP keys.

5. Services

5.1. Prevention:

- Proactive vulnerability management.
- Issuance of security alerts and bulletins.
- ENS/ISO27001 Risk and Compliance Assessments.
- Training, drills and awareness campaigns.

5.2. Incident Response:

- Incident identification, analysis and containment.
- Technical advice and coordination with clients.
- Preparation of forensic reports and lessons learned.

5.3. Forensic Analysis:

- Acquisition and preservation of digital evidence.
- Forensic analysis of systems, networks and mobile devices.
- Technical support in judicial or expert processes.

5.4. Cyberintelligence:

- Monitoring threats on the surface, deep , and dark web.
- Identification of threat actors and targeted campaigns.

- Strategic and technical analysis of indicators of compromise (IoC).

5.5. Penetration Tests:

- Controlled assessment of technical and human vulnerabilities.
- Attack simulation (Red Team / Blue Team / Purple Team).

5.6. Consulting:

- Consulting in regulatory compliance with ENS, ISO 27001, NIST CSF.
- Design and implementation of security policies and frameworks.

5.7. Training and Awareness:

- Technical and executive training programs.
- Practical workshops on incident response, digital forensics , and crisis management.

6. Incident Notification

Incidents can be reported via:

- Email: **incidencia@gruporadical.com**
- Emergency telephone (24x7)

It is recommended to include in the notification:

- Description of the incident and its impact.
- Approximate date and time of the event.
- Contact details of the technical manager.
- Initial evidence or relevant records (if possible).

7. Disclaimer

The RADICAL CERT is not responsible for any misuse or unauthorized use of the information contained in this document.
All information shared with the RADICAL CERT will be treated confidentially and used exclusively for cybersecurity incident management and mitigation purposes.