Identifier
[RFC 2350]

2025/05/11 RFC 2350

TLP:CLEAR

Description of Services

1. Document Information

1.1. Last updated: Version 2.0, released on May 15, 2025.
1.2. Distribution Lists: There is no distribution channel to notify changes to this document. Changes are updated and posted on the website.
https://www.colcert.gov.co/800/w3-channel.html
1.3. Location of the Document: The current version of the document is available on the website.
https://www.colcert.gov.co/800/w3-channel.html
1.4. Authentication of the Document: This document has been digitally signed by the Coordinator of the ColCERT Group.

2. Contact Information

2.1. Team Name: Colombian Cyber Emergency Response Team ColCERT, National CERT, attached to the Ministry of Information and Communications Technologies (MinTIC).
2.2. Address:
Ministry of Information and Communications Technologies
Colombia Cyber Emergency Response Team ColCERT
Edificio Murillo Toro Cra. 8a between 12A and 12B streets
Bogotá D.C., Colombia
2.3. Time Zone: GMT/UTC -5
2.4. Phone Number: +57 601 344 2222
2.5. Fax Number: Non-existent
2.6. Other Communications: Non-existent
2.7. Email Addresses:
Exchange of information relating to incidents: contacto@colcert.gov.co
Malware Report: malware@colcert.gov.co

Phishing Report: phishing-report@colcert.gov.co

2.8. Public Keys and Information Encryption: Contact emails and associated PGP keys are published in
https://www.colcert.gov.co/800/w3-article-198656.html
2.9. Team Members: Not available
2.10. More Information: General information on the services provided by ColCERT and on the organisation itself is published on the website:
https://www.colcert.gov.co/800/w3-channel.html
2.11. Hours of Operation: The incident response team is available at the following times:
Services and consultations: Monday to Friday from 8:00 – 12:30 and from 14:00 – 17:00.
Incidents classified as very serious and serious: 7x24
2.12. Points of contact for the community: Communication between the ColCERT Team and the community to which it offers its services is mainly carried out through:

- Mailbox associated with the topic to be consulted
- Telephone numbers provided during the subscription process or incident management support.

3. Constitution

3.1. Mission
The ColCERT has the mission of leading and coordinating incident management, the identification of vulnerabilities, risks and threats against national digital security. We act as a central point of contact and collaboration between public and private entities and the international community, strengthening the resilience of the State through information sharing, capacity building, dissemination of guidelines, identification of critical infrastructures and promotion of a culture of security, through national and international cooperation.
+Responsibility Statement
3.2. Community to which it provides Services
All public entities of the branches of the executive, legislative and judicial branches, private sector and civil society in Colombia.
3.3. Sponsorship / Affiliation
The ColCERT Team is an internal working group attached to the Vice Ministry of Digital Transformation of the Ministry of Information and Communication Technologies – MinTIC
3.4. Authority
ColCERT operates under the shared authority model in which it either exercises unilateral or "command and control" authority over its target community. Instead, its authority and effectiveness are based on the collaboration, coordination, technical expertise, and trust it generates within that community.

4. Policies

4.1. Type of Incidents and level of support: The typology of Digital Security incidents classified by ColCERT are described in the taxonomy published on the website
https://www.colcert.gov.co/800/articles-198656_taxonomia.pdf

As a National CERT, it collaborates, supports and coordinates with all public and private sector entities in incident management and offers additional services for vulnerability management, situational analysis and knowledge transfer.

4.2. Cooperation, Interaction and Disclosure of Information: The information managed by ColCERT is treated with absolute confidentiality in accordance with the policies and procedures of the Ministry of Information and Communications Technologies MinTIC.

Information Security and Privacy Policy
Personal Data Processing Policies of the ICT Ministry

https://www.mintic.gov.co/portal/inicio/Secciones-auxiliares/Politicas/2627:Politicas-de-Privacidad-y-Condiciones-de-Uso

4.3. Communication and Authentication: The communication channels available for ColCERT reporting and consultations are:

Bogotá Hotline: +57 601 344 22 22
Exchange of information relating to incidents: contacto@colcert.gov.co
Malware Report: malware@colcert.gov.co
Phishing Report: phishing-report@colcert.gov.co
The contact emails and associated PGP keys are published in
https://www.colcert.gov.co/800/w3-article-198656.html
Social Network X: @colCERT

5. Portfolio of Services

The ColCERT Service Portfolio is an integrated and dynamic set of specialized capabilities, designed to **proactively strengthen the nation's cyber resilience.** Through **Situational Awareness**, we provide timely intelligence on the threat landscape. Through **Vulnerability Management**, we identify and mitigate weaknesses in systems. With **Incident Management**, we offer a coordinated and effective response to security events. And through **Knowledge Transfer**, we empower stakeholders with the skills and information needed to protect themselves. Together, our portfolio seeks to **create a safer and more reliable Colombian digital ecosystem.**

5.1. Service Line: Situational Awareness.

It is a fundamental service area of the ColCERT, focused on the ability to anticipate and understand the evolution of the landscape of threats and vulnerabilities that affect national digital security. This requires the identification, processing, and analysis of critical information, as well as its timely dissemination to stakeholders to facilitate preventive and reactive decision-making. ColCERT integrates information from various sources and from your other service areas to provide a clear and actionable view, thereby strengthening the responsiveness and resilience of your community.

5.1.1. Collection:

This ColCERT service focuses on the comprehensive collection of strategic, tactical and operational intelligence, relevant to national digital security. The process encompasses the identification, search, filtering, organization and storage of key information from a variety of sources (Feeds, CSIRTAmericas Dashboards, CERTs, PSIRTs, SOCs, news, social networks, instant messaging groups, reports, CTI tools, etc.), complementing the automated feeds. The main objective is to improve the understanding of the threat landscape, increase the visibility of the security posture of public and private entities, and in general of the country and provide the necessary information (risks, threats, vulnerabilities, IoCs, IoAs, etc.) for the analysis, communication and substantiation of preventive and reactive decisions, thus supporting incident management and risk mitigation.

5.1.2. Data processing and preparation.

Given the diversity of sources and formats of cybersecurity data, this service focuses on its transformation, standardization and exhaustive validation to ensure its reliability. The combination of current and historical data allows for richer contextual understanding. In addition, advanced processing techniques (such as natural language analysis) are applied to extract valuable information from unconventional sources, enriching the intelligence landscape of ColCERT and improving its ability to anticipate and respond to threats at the national level.

5.1.3. Analysis.

ColCERT uses this service to transform data into contextualized intelligence on national digital security. Through the assessment of the current situation in relation to expected patterns, potential risks to critical assets are identified. In-depth analysis of current and historical data reveals the nature and origin of events, as well as their present and future implications. The incorporation of diverse sources of information enriches understanding and allows ColCERT to generate actionable knowledge for threat prevention and response.

5.1.4. Communication.

Through its communication service, ColCERT generates and disseminates processed and analyzed intelligence to improve understanding of the digital security landscape in Colombia. A fundamental component is the generation of alerts and warnings, through which critical information about threats, attacks, new vulnerabilities and digital security risks is communicated, including alerts from threat intelligence monitoring. The purpose is to increase the preparedness and responsiveness of stakeholders, providing mitigation recommendations to strengthen their safety and reduce their exposure.

5.2. Vulnerability Management

ColCERT, through its Vulnerability Management Service Area, is responsible for the discovery, analysis and proactive management of security vulnerabilities, both new and existing, in information systems. A crucial component is coordinated detection and response to known vulnerabilities to prevent their exploitation. It is important to distinguish that, although "Vulnerability Response" is a fundamental activity (such as scanning and patching), it is part of a broader Vulnerability Management service that can involve different teams and processes within ColCERT.

5.2.1. Discovery of Vulnerabilities from Public Sources.

A proactive function of the ColCERT to identify known early and new security vulnerabilities by gathering information through various public and third-party sources. The information collected by specialized personnel is organized and analyzed, integrating with data from fingerprint and brand protection tools, to feed the ColCERT Vulnerability Management and Early Warning services.

5.2.2. Reception of Vulnerability Reports.

ColCERT facilitates the reporting of security vulnerabilities through defined channels to receive reports from a wide range of sources, including its constituents, the security research community, technology vendors, PSIRTs, and other CSIRTs. The information received can range from the affected devices and operating requirements to the potential impact and proposed solutions. This service ensures that valuable vulnerability information is captured and used effectively in ColCERT's management and response processes, complementing the information obtained through the receipt of incident reports.

5.2.3. Vulnerability Analysis (On Demand).

Through this service, ColCERT performs vulnerability analysis at the request of organizations to discover weaknesses in various technological environments: on-premise infrastructure, cloud, Active Directory, and web services. Using licensed and open source tools, the level of analysis is adapted to the security capacity of the applicant, offering a basic report for entities with CISO/Processor and a more in-depth analysis for those without this figure.

5.2.4. Vulnerability Reporting:

ColCERT service that delivers reports derived from the receipt of reports and vulnerability analysis requested by public and private entities. The main objective is to provide information on the identification of critical, high, medium and informational vulnerabilities, to facilitate the establishment of mitigation plans, improve your security posture, close the gap in the attack surface and avoid incidents that may impact your operations and the continuity of services to citizens, through the established communication channels and guaranteeing the confidentiality of information.

5.3. Digital Security Incident Management

ColCERT, with its unique position and expertise, offers a fundamental Digital Security Incident Management service. This involves the collection, evaluation, and in-depth technical analysis of incidents and artifacts. From this analysis, mitigation and recovery recommendations are generated, providing support in their application and coordinating with external entities for an effective response and the prevention of future incidents. ColCERT's specialized expertise is also crucial to support digital security crisis management in the country.

5.3.1. Receipt of reports of Digital Security Incidents.

ColCERT service dedicated to receiving reports of digital security incidents classified as Very Serious or Serious, according to the ColCERT incident management procedure and the MSPI incident management guidelines, from public and private entities. These reports are received through the communication channels established by ColCERT.

5.3.2. Triage and Processing of Digital Security Incidents.

This service focuses on the initial review and classification of digital security incident reports to understand their nature and impact on information assets at the national level, also considering the classification provided by the affected organization. After this preliminary assessment, the incident is prioritized and the follow-up action is defined, which can be the convening of a context meeting to gather more details.

5.3.3. Mitigation and Recovery

ColCERT offers this service to effectively contain digital security incidents, minimizing and reducing operational and economic losses. The goal is to achieve timely recovery of impacted services, prevent the recurrence of attacks by eliminating root causes, and strengthen the overall cybersecurity posture in public and private entities. The service includes the execution and monitoring of the necessary actions until the resolution of the incident or the identification of new information that requires a review of the response strategy.

5.3.4. Establishment of the Response Plan.

ColCERT service to define and implement a coordinated plan with the affected entity, in order to restore the integrity of the compromised systems and return the data, systems and networks to a normal operational state. The plan seeks to restore the full functionality of the impacted services, avoiding the recreation of the conditions that allowed the initial operation. Business impact, mitigation and recovery requirements are considered, and the plan is continually reviewed as new information is obtained, ensuring an effective and coordinated response at the national level.

ColCERT offers comprehensive nationwide protection through two key capabilities: **Domain Protection and DNS Investigation**, which acts as a preventative layer by analyzing DNS traffic

to detect and predict threats, as well as mitigating ongoing attacks by restricting malicious connections. In addition, the **EDR Malware Detection and Response** capability provides continuous monitoring and active response to threats that reach the endpoints and networks of public and private entities, supporting recovery after incidents and strengthening their security.

5.3.5. Coordination of Digital Security Incidents.

ColCERT offers this service to manage the response to digital security incidents at the national level, ensuring effective and timely communication between all stakeholders (Cyber Instances). This involves receiving and distributing relevant information, tracking the progress of mitigation and recovery actions, ensuring implementation of the response plan, and addressing modifications needed due to new information or delays. Likewise, and according to the digital security governance model (Decree 338 of 2022), report digital security incidents that have a national impact or that affect critical cyber infrastructure.

5.3.6. Crisis Management Support

The ColCERT acts as a critical resource for public and private entities in digital security crisis situations, offering its valuable experience, established services and network of contacts with other experts and CSIRTs, in its role as Colombia's National CERT. This support seeks to facilitate the mitigation of the crisis and ensure the availability of the country's digital ecosystem and its network of allies for the recovery of operations.

5.3.7. Artifact Analysis

ColCERT offers two services related to malware analysis:

1. **Sandbox Analysis:** For digital security incident management, ColCERT analyzes files in a sandbox, generating detailed technical reports on the behavior of potentially malicious software and identifying Indicators of Compromise (IoCs).
2. **Web Analysis (DetectIC):** To facilitate the detection of threats by the general public and the technical teams of public entities, ColCERT offers the online web analysis tool DetectIC. This service scans files and URLs for malicious payloads, generally notifying them of their dangerousness.

6. Knowledge transfer

It is an essential service area of ColCERT, leveraging its privileged position to collect relevant data, perform detailed analysis, and identify threats, trends, and risks. ColCERT generates and disseminates current operational best practices to raise awareness and train organizations in the detection, prevention, and effective response to security incidents, thus contributing to raising the overall level of cybersecurity in Colombia.

6.1. Digital Security Awareness in the General Community

To provide citizens with the tools and education essential to strengthen the security of their personal, family and professional environments, as well as that of their entities and organisations, through an awareness strategy based on risk management.

6.2. Basic, Intermediate and Advanced Incident Management Training

Training program designed to equip digital security incident response teams and IT managers of public and private entities with the necessary skills to carry out preventive and reactive actions. This includes analysis, identification, classification, containment, eradication, recovery and post-incident management.

6.3. Digital Security Awareness Managers

Strategic programme to raise awareness among senior management of public and private entities about the cross-cutting nature of digital security in all organisational processes. The importance of establishing a robust security strategy and posture to mitigate the materialization of risks and prevent incidents that may generate significant legal, financial, and reputational impacts is emphasized.

7. Forms of incident reporting

Incident reporting can be done by:

Bogotá Hotline: +57 601 344 22 22
Exchange of information relating to incidents: contacto@colcert.gov.co
Malware Report: malware@colcert.gov.co
Phishing Report: phishing-report@colcert.gov.co
The contact emails and associated PGP keys are published in
https://www.colcert.gov.co/800/w3-article-198656.html

8. Disclaimer

The COLCERT Team is not responsible for any misuse that may occur of the information contained herein.

Service Channels

If you wish to report a digital security incident, you can contact COLCERT, through the following channels:

Bogota: +57 601 344 22 22

contacto@colcert.gov.co.

@colCERT