COINSOC INFORMATION
RFC 2350

April 2025

1. Information about the document

1.1 Version 2: Published April 2025

1.2 Distribution list:

There is no distribution list for notification of the change of version of this document, in case of new version, it will be published on the COINSA S.A.S. website, CoinSOC section.

1.3 Location of the document:

Español:

https://coinsasas.com/wp-content/uploads/COINSOC_RFC_2350_ESP.pdf

Inglés:

https://coinsasas.com/wp-content/uploads/COINSOC_RFC_2350_ENG.pdf

1.4 Document Authentication:

The document is signed by the user authorized by COINSA S.A.S.

2. Contact information

2.1 Team name:

COINSOC, Security Operations Center, which is part of the COMPAÑIA DE INGENIEROS DE SISTEMAS ASOCIADOS - COINSA S.A.S.

2.2 Direction:

Administrative Headquarters: Carrera 35 No. 46-48 - Bucaramanga

Operating Headquarters: Calle 119 #13-51, Piso 4, Bogotá

2.3 Time Zone:

America / Bogota (GMT-5), there is no daylight saving time in this time zone.

2.4 Contact numbers:

(57) 3157750178 - (57) 3174276422

2.5 E-mail address:

- To exchange incident information: analistasoc@coinsalt.com
- General information: info@coinsalt.com

2.6 PGP public keys

To send encrypted mail to the incident response account analistasoc@coinsalt.com, download the public key found at the bottom of the page, at the link: https://coinsasas.com/why-us/ and download it at the link:

https://coinsasas.com/wp-content/uploads/CSIRTCoinsa_public.asc

2.7 Team members:

The names of team members are not published for security reasons. In a formal CoinSOC review process or in a contractual process with clients, this information may be provided.

2.8 SOC working hours:

7 days a week, 24 hours a day, 365 days a year, 24-hour hotline

2.9 Information about COINSOC:

General information about COINSA S.A.S. SOC, can be consulted at https://coinsasas.com/why-us/

2.10 Community Contact Points:

The communication between COINSOC and the clients or those interested in the services is done through:

- Cellular numbers (57) 3157750178 - (57) 3174276422

- Send e-mail to analistasoc@coinsalt.com

3. Constitution

3.1 Mission

COINSA SAS.[1] is a company that provides computer goods and services, offering a complete, real and effective solution to the needs of systematization and technological updating of our customers, seeking to increase their business competitiveness through the effective appropriation of technology.[2]

CoinSOC (COINSA's NOC-SOC) provides clients and the company with horizontal cybersecurity, information security and technology operations monitoring services in a more agile and timely manner.

3.2 Community served[3]

The community to which the services are provided are: COINSA S.A.S. internal target customer and the different external customers of the company that require the service, defined in a contract.

3.3 Scope

Through the management of cybersecurity, information security and monitoring of technological operations, we seek to apply containment or mitigation measures and response to threats, events and incidents, which are carried out with the services offered by COINSOC:

- IT Event and Security Incident Management and Monitoring - SOC
- Digital Surveillance

[1] COMPANY OF ASSOCIATED SYSTEMS ENGINEERS - COINSA S.A.S.

[2] SC-O-PL-22-007_STRATEGIC PLANNING

[3] To whom the services are provided (electoral district)

- Threat Intelligence / Threat Hunt
- Computer Forensic Analysis
- Vulnerability Assessment, Intrusion Testing and Social Engineering
- Cybersecurity and Technology Infrastructure Development, Research and Education

3.4 Sponsoring organization

CoinSOC, belongs to Compañía de Ingenieros de Sistemas Asociados - COINSA S.A.S. and is part of the Operations Vice-Presidency.

4. Policies

4.1 Incident management and level of support

The clients: external (with subscribed contract) as the internal client (COINSA S.A.S. through CoinSOC (NOC/SOC) reports the events or security incidents that occur along with the records or supports that they have, in order to make a correct identification, collection, acquisition and preservation.[4]

COINSA S.A.S., as sponsor of COINSOC (NOC/SOC), establishes the responsible persons and channels for the management of information security incidents (See the following paragraphs of this document: "2.5 E-mail address" and "2.10 Points of contact for the community").

The responsible personnel must immediately attend to the reported events, after analyzing the events, determine whether they are categorized as a cybersecurity and/or information security incident and perform the corresponding escalation according to their level of criticality, determined by means of the impact levels described in section "6.2.2 Impact levels", which is part of SC-O-PR-22-003_PROCEDURE INFORMATION SECURITY INCIDENT MANAGEMENT PROCEDURE.

[4] SC-O-PR-22-003_INFORMATION SECURITY INCIDENT MANAGEMENT PROCEDURE.

The incidents reported to COINSOC are catalogued according to the incident classification taxonomy, described in document SC-O-PR-22-003_PROCEDURE INFORMATION SECURITY INCIDENT MANAGEMENT PROCEDURE, in section "6.2.1 Incident classification taxonomy".

CoinSOC (NOC-SOC) has the authority and is responsible for ensuring that potential cybersecurity and information security incidents are properly identified, analyzed, defended, investigated and reported.

Security bulletins are periodically sent from CoinSOC with the description of vulnerabilities, their impact, the level at which they can be exploited, affected software resources, risks, remediation and COINSOC contact information.

4.2 Cooperation, interaction and dissemination of information

In the disclosure of information, from CoinSOC (NOC-SOC) of COINSA S.A.S. it is determined that all or part of the confidential information must be kept under reserve and not propagate, disclose or use for their own benefit or for the benefit of third parties.

Protect the information created, processed, transmitted or safeguarded by its processes, in order to minimize financial, operational or legal impacts due to its incorrect use.[5]

Share with the community the events and incidents identified in the areas of technology monitoring, operations security and information security in order to create synergies of knowledge in these areas.

5. Services

COINSA S.A.S. CoinSOC (NOC-SOC) offers the following services:

COINSOC SERVICE	DESCRIPTION
IT Event and Security Incident Management	Permanent monitoring of the activity of information assets

[5] SC-O-MO-22-002_INFORMATION SECURITY POLICY MANUAL

COINSOC SERVICE	DESCRIPTION
and Monitoring - SOC	aimed at identifying events or incidents that may impact the security, integrity, availability, identity and access to the client's business processes. In order to make early warnings, apply containment and/or prevention actions, make process improvements based on lessons learned, and document the knowledge base.
Digital Surveillance	Activities are carried out for the proactive detection of abuses that threaten the company's brand and reputation. Identification of digital events in order to avoid disruptions in the business. COINSA's SOC capacity lines for the digital surveillance service are: a) Digital Content Research: All content related to intellectual property abuse, patents, copyrights, trademarks. b) Reputational impact: Events of (criminal conduct, threats, slander), obfuscation of demonstrations, protests, strikes disclosed, all events or subjects identified in digital environments that may affect the integrity of our customers. c) Leakage of information: All personal and/or institutional information and/or data found in public digital environments. d) Impersonation: Evidence of deception or computer fraud of the technological infrastructure or assets. digital customer. e) Technological Security: Exposure of digital assets or technological infrastructure

COINSOC SERVICE	DESCRIPTION
	of the customer
Threat Intelligence/Threat Hunting	With the collection of detailed information on cybersecurity threats that have been directed at organizations, described in Cyber Threat Intelligence (CTI) reports ([6]), analysis and filtering is performed in order to identify potential threats to the infrastructure and apply containment and/or impact mitigation measures to reduce risks to the systems.
Computer Forensic Analysis	It is a set of techniques aimed at extracting valuable information from systems without altering their status (chain of custody). These allow the identification of data that is previously known, to find a certain pattern or behavior, or to discover information that was hidden Information that is part of a process of computer fraud or cybercrime and that is delivered for disciplinary or legal processes.
Vulnerability Assessment, Penetration Testing and Engineering Social	It is the exercise of identifying the weaknesses of technologies, people or processes.
Cybersecurity and Technology Infrastructure Development, Research and Education	Conduct laboratories for threat simulation, review of vulnerabilities and verification of affectation and impact on technologies.

6. Notification of incidents

- **E-mail:** analistasoc@coinsalt.com
- **Cellular number:** + 57 3157750178

7. Disclaimer of Liability

[6] Cyber Threat Intelligence

COINSA S.A.S. is not responsible for the possible misuse of the information contained in this document.

Firmado digitalmente por Analista Soc
Nombre de reconocimiento (DN): cn=Analista Soc, o=Coinsa, ou=CU, email=analistasoc@coinsalt.com, c=CO
Fecha: 2025.04.08 14:21:19 -05'00'