cipher

a Prosegur company

CIPHER-CSIRT / RFC2350

Reference: CIPHER-CSIRT_RFC2350_EN_V3.1

CONTROL PAGE

SECURITY CLASSIFICATION	TLP-WHITE

Title:	CIPHER-CSIRT / RFC2350
Reference:	CIPHER-CSIRT_RFC2350_EN_V3.1

VERSION CONTROL		
Version	**Revision date**	**Change description**
1.0	10/12/2019	Document creation – Certified team
2.0	05/05/2022	Team name changed with all the changes that come with it. In addition, the Constituency
2.1	12/05/2022	Small changes included
3.0	19/12/2025	Full revision of the document including the Constituency
3.1	14/05/2026	Revision of the constituency list

Index of Contents

1 Introduction

1.1 Abstract

This document describes the CIPHER-CSIRT, the Cipher CSIRT team, according to RFC 2350. The RFC 2350 is an RFC (Request for Comments) which describes the structure, the procedures and the policies of a CSIRT (Computer Security Incident Response Team). The RFC 2350 can be downloaded from http://www.ietf.org/rfc/rfc2350.txt.

1.2 Locations where this document can be found

The current version of this document is available from the CIPHER-CSIRT site:

https://www.cipher.com/why-choose-cipher

This document has been signed with the CIPHER-CSIRT PGP key.

2 Contact Information

2.1 Name of the Team

CIPHER-CSIRT: the Cipher Computer Security Incident Response Team.

2.2 Address

CIPHER - CONSULTORIA EM SEGURANÇA DE INFORMAÇÃO, PORTUGAL, UNIPESSOAL LDA

Torre de Monsanto, Rua Afonso Praça, 30, 7º Piso

1495-061 Miraflores - Algés – Lisboa

Portugal

2.3 Time Zone

Portugal/WEST (GMT+0 and GMT+1 from April to October).

2.4 Telephone Number

+351 966 389 221

2.5 Electronic Mail Address

irt@cipher.com

2.6 Public Keys and Other Encryption Information

The CIPHER-CSIRT has a PGP key for secure communication.

CIPHER-CSIRT: irt@cipher.com

Fingerprint: 5BC9E9C4F9835585057E7C8B3DD1C76FDFC8914D

2.7 Team Members

(Ordered alphabetically)

Adail Domingues Da Silva De Oliveira – adoliveira@cipher.com

Andreia Nascimento Santos - asantos@cipher.com

Antonio Javier Montes - amontes@cipher.com

Antonio Xavier Ferreira Correia - axcorreia@cipher.com

Bryan Silvestre Matias - bmatias@cipher.com

Daniel António Sousinha - daniel.sousinha@cipher.com

Daniel Martins Mata - daniel.martins-mata@cipher.com

Enrique Sebastian Arambulo Rubbini - enrique.arambulo@cipher.com

Henrique Pessôa Pessôa Leo - henrique.leo@cipher.com

Jose Carlos Navarrete Armada - jose.navarrete-armada@cipher.com

Miguel De Almeida Martins Libânio - mlibanio@cipher.com

Teresa Leal Ferreira - teresa.leal@cipher.com

Tiago José Rodrigues Costa - Tiago.rodrigues@cipher.com

Yaser Rimawi - yaser.rimawi@prosegur.com

2.8 Other Information

Information regarding activities and structure of the CIPHER-CSIRT, as well as links to various recommended security resources can be found at https://www.cipher.com/why-choose-cipher

2.9 Points of Customer Contact

The preferred method for contacting CIPHER-CSIRT is via e-mail at irt@cipher.com. If it is not possible (or not advisable for security reasons) to use e-mail, the CIPHER-CSIRT can be reached by telephone at +351 966 389 221.

3 CHARTER

3.1 Mission Statement

The purpose of the CIPHER-CSIRT is to respond to security incidents in its own infrastructure as well as its client's infrastructure, assuring a high degree of availability and the business continuity of affected clients.

3.2 Constituency

The CIPHER-CSIRT constituency is its own infrastructure as well as the infrastructure of its clients. Currently, the following IP addresses are part of our constituency:

18.201.88.141/32	148.69.133.56/32	4.226.19.32/32
34.247.4.201/32	148.69.133.57/32	4.226.19.47/32
34.248.117.39/32	75.2.70.75/32	4.226.23.32/32
34.248.191.171/32	89.114.154.65/32	4.226.25.251/32
34.248.235.169/32	99.83.190.102/32	4.226.28.128/32
34.254.99.141/32	31.221.12.128/26	4.226.33.108/32
52.50.137.244/32	62.38.57.224/27	4.226.37.207/32
52.51.121.116/32	80.17.182.144/28	4.226.50.40/32
54.155.137.224/32	81.0.71.0/26	4.226.50.158/32
54.155.249.211/32	81.93.77.120/29	4.226.53.186/32
54.195.45.72/32	82.141.141.136/29	13.69.131.89/32
54.195.182.247/32	88.118.136.8/29	13.70.194.204/32
99.80.211.186/32	89.44.246.0/24	13.74.36.102/32
108.128.194.197/32	89.204.165.96/27	20.33.18.3/32
41.76.144.0/24	91.199.57.0/24	20.33.18.4/32
41.76.145.0/24	188.119.9.112/28	20.33.18.5/32
197.235.1.0/24	193.85.207.32/29	20.33.18.6/32
197.235.2.0/24	193.126.27.160/27	20.33.18.7/32
197.235.3.0/24	194.224.217.176/28	20.54.61.111/32
148.69.131.126/32	195.29.38.64/27	20.54.101.37/32
148.69.133.50/32	195.65.194.0/27	20.67.174.86/32
148.69.133.51/32	213.190.49.0/28	20.93.60.0/32
148.69.133.52/32	217.23.199.48/29	20.107.130.154/32
148.69.133.53/32	4.208.16.245/32	20.107.147.189/32
148.69.133.54/32	4.209.228.113/32	20.166.37.211/32
148.69.133.55/32	4.210.105.236/32	20.166.222.109/32

20.199.146.86/32
20.250.160.99/32
20.250.169.164/32
20.250.184.12/32
20.250.199.255/32
20.250.203.70/32
40.67.248.173/32
40.67.251.242/32
40.67.254.76/32
40.67.254.77/32
40.67.254.82/32
40.127.188.244/32
51.138.235.175/32
52.137.25.50/32
52.155.163.65/32
65.52.147.251/32
74.161.75.174/32
74.161.104.202/32
74.161.114.62/32
74.242.193.77/32
74.242.214.243/32
135.236.225.254/32
137.116.234.109/32
172.161.140.17/32
172.161.161.30/32
172.162.241.62/32
172.205.122.139/32

Currently, the following domains are part of our constituency:

cipher.com

cipherxmdr.io

bondalti.com

bondaltiwater.com

lifthiumenergy.com

3.3 Authority

The CIPHER-CSIRT expects to work cooperatively with system administrators and users of the client infrastructures, to the extent possible, to ensure the necessary authority to respond to security incidents.

4 POLICIES

4.1 Types of Incidents and Level of Support

The CIPHER-CSIRT restricts its support and incident handling activities to incidents that fall within its constituency.

Incident classification and reporting follow the RNCSIRT Common Taxonomy[1] (v3.3), aligned with the RSIT WG Reference Security Incident Taxonomy (v1003). Incidents may be classified using a primary classification (main intent/impact) and secondary classifications (e.g., delivery vector or enabling activity) when applicable.

4.1.1 Incident Classes Supported

Within its constituency, CIPHER-CSIRT provides support for incidents that fall under the following RNCSIRT incident classes:

- **Abusive Content:** Spam (unsolicited bulk email), harmful speech/policy violations, sexual/violent prohibited content.
- **Malicious Code:** Infected systems, command-and-control (C2) activity, malware distribution, malware configuration artefacts.
- **Information Gathering:** Scanning, sniffing, social engineering (non-technical means such as lies, tricks, bribes, threats).
- **Intrusion Attempts:** Exploitation of known vulnerabilities, login attempts (e.g., brute-force), new/unknown attack signatures.
- **Intrusions:** Privileged account compromise, unprivileged account compromise, application compromise, system compromise.
- **Availability:** DoS, DDoS, sabotage, misconfiguration, outage (no malice).
- **Information Content Security:** Unauthorized access to information, unauthorized modification of information (e.g., defacement/ransomware encryption), data loss, leak of confidential information.
- **Fraud:** Unauthorized use of resources, copyright infringement, masquerade/impersonation, phishing.
- **Vulnerable:** Weak cryptography, DDoS amplifiers, exposed/unwanted services, information disclosure, vulnerable systems.
- **Other:** Uncategorized, undetermined, test (used when the incident cannot be reliably classified at intake).

4.1.2 Level of Support Provided

Depending on the type of incident and available information, CIPHER-CSIRT may provide one or more of the following:

[1] *https://www.redecsirt.pt/files/RNCSIRT_Taxonomia_v3.3.pdf*

- **Intake, triage and classification** according to the RNCSIRT taxonomy (including primary/secondary classifications where relevant).
- **Analysis support** (validation, scoping guidance, and interpretation of indicators/observables provided by the reporter).
- **Coordination and facilitation** with relevant internal parties within the constituency and, where appropriate, external entities (e.g., providers, other CSIRTs) to support containment and mitigation actions.
- **Mitigation and containment guidance** (advisory recommendations to limit impact and reduce recurrence).
- **Information sharing** within applicable information handling rules and agreed disclosure constraints.

Unless otherwise agreed, CIPHER-CSIRT does not provide full remediation, on-site response, or complete forensic investigation; it provides guidance and coordination support as appropriate.

4.1.3 Response Time

Under normal operating conditions, CIPHER-CSIRT will acknowledge and respond to incident reports within 24 hours.

4.1.4 Exclusions / Special Handling

Reports that primarily fall outside CSIRT handling (e.g., certain abusive content categories) may be redirected to the appropriate channels and/or competent authorities, as applicable. Notification to CNCS does not replace any mandatory reporting to judicial or law enforcement authorities when an incident also constitutes a criminal offense.

4.2 Co-operation, Interaction and Disclosure of Information

The CIPHER-CSIRT applies to the information that manages the protection measures corresponding to its nature and classification, taking as a reference, among others, the General European Data Protection Regulation (GDPR) and the European NIS directive.

Likewise, in communications and documentation, the FIRST TLP v1.1 protocol is used internally and externally for the classification and labelling of documents, according to which the following levels of information classification have been established:

- RED. Information is not distributable and is restricted to representatives authorized to participate directly in the exchange of information and who have signed the corresponding confidentiality commitments.
- AMBER. Information of limited and restricted distribution to authorized personnel, belonging to the service or its beneficiary organizations, who have a legitimate need to know to exercise their functions, and who have signed the corresponding confidentiality commitments.
- GREEN. Information of limited distribution and restricted to personnel and institutions within the service's trusted network, with which non-distribution agreements are established, but cannot be freely published or freely accessible.

- WHITE. Information that is freely distributed and not restricted but that may be subject to Copyright

Information tagged with identifiers in the TLP will be handled accordingly.

When reporting a sensitive incident, please indicate so appropriately, using the appropriate TLP label in the subject line, and please consider using encryption as specified in section 2.6

The CIPHER-CSIRT will handle all information that is provided as confidential. However, statistical data can be generated from some of this information as long as full confidentiality and anonymization can be ensured.

All confidentiality and privacy customer rights are safeguarded by a non-disclosure agreement, which is part of the standard incident handling service contract.

4.3 Communication and Authentication

In view of the types of information that the CIPHER-CSIRT will likely be dealing with, telephones and unencrypted e-mail will be sufficiently secure for low-sensitivity data. Any sensitive data should be encrypted with PGP.

5 SERVICES

5.1 Incident Response

CIPHER-CSIRT provides incident response support only for incidents affecting its constituency. Activities are performed in accordance with recognized CSIRT best practices and relevant guidance from organizations such as CERT/CC, ENISA, Trusted Introducer and FIRST.

The service typically includes intake and validation of reports, incident classification, coordination support, and mitigation guidance. Unless otherwise agreed, CIPHER-CSIRT provides advisory and coordination services and does not perform full remediation, on-site response, or comprehensive digital forensics.

Where applicable, CIPHER-CSIRT leverages its security monitoring and response capabilities, including the CIPHER xMDR platform, to support incident intake, correlation, enrichment and investigation workflows. Automation is used to accelerate initial assessment; final incident handling decisions remain under human responsibility.

5.2 Incident Triage

CIPHER-CSIRT performs an initial triage to validate the report and determine priority/severity based on available information, including (where applicable): incident type/classification, impact, scope/extent, urgency, confidence level, and potential for ongoing harm.

For incidents originating from monitored environments, triage is supported by automated workflows (e.g., alert correlation, enrichment and scoring). The assigned priority/severity is reviewed and, if necessary, adjusted by an analyst based on the evidence available and the operational context.

Each reported incident is recorded and assigned a unique incident identifier, and relevant information is documented to support tracking, coordination and reporting.

5.3 Incident Coordination

CIPHER-CSIRT coordinates the handling of incidents by facilitating communication and actions among relevant parties within the constituency and, when appropriate, external entities (e.g., service providers, vendors, other CSIRTs).

During analysis, CIPHER-CSIRT may identify likely causes, contributing factors and attack paths based on available evidence. Coordination activities are supported by case management and traceability features (e.g., timelines, artefact tracking and documented actions) to ensure continuity throughout the incident lifecycle.

When an incident is outside CIPHER-CSIRT's scope or authority, the report may be referred/forwarded to the appropriate responsible entity, and CIPHER-CSIRT may support coordination as appropriate.

5.4 Incident Resolution

CIPHER-CSIRT supports incident resolution by guiding containment, eradication and recovery, and for improving security posture to reduce recurrence. Where legal or disciplinary action is contemplated, CIPHER-CSIRT may guide preservation of relevant evidence and recommended documentation practices.

An incident may be considered resolved when one or more of the following conditions apply (as appropriate to the case):

- Affected services/systems have returned to an agreed normal operational state;
- Containment/mitigation actions have been implemented, and risk is reduced to an acceptable level;
- Responsibility has been formally transferred to another competent entity;
- The constituency confirms closure or accepts residual risk.

Non-confidential and/or sanitised data may be retained for statistical purposes, service improvement, and, where relevant, for information sharing with involved CSIRTs under applicable information handling rules.

5.5 Post-Incident Activities

After incident closure, CIPHER-CSIRT may support post-incident activities to strengthen prevention and readiness, such as:

- Post-incident review/lessons learned, including validation of what happened, what worked well, and what should be improved.
- Recommendations for corrective and preventive actions, including hardening measures, detection improvements, and process adjustments.
- Control and monitoring enhancements, where applicable (e.g., detection logic improvements, alert tuning guidance, indicator sharing).
- Reporting and metrics, using non-confidential or sanitised information for service quality, trend analysis, and (where applicable) structured information sharing with relevant CSIRTs.

Post-incident activities may be executed as part of normal CSIRT support or as additional services, depending on scope, complexity and agreement with the constituency.

5.6 Proactive Activities

The CIPHER-CSIRT provides consulting services. Detailed descriptions of these services are available at: https://www.cipher.com

6 DISCLAIMER

While every precaution will be taken in the preparation of information, notifications and alerts, CIPHER-CSIRT assumes no responsibility for errors or omissions, or for damage resulting from the use of information contained within.

Furthermore, several contractual obligations are included in the standard service contract, which only cover the parties involved.