

OneCyber	OneCyber – RFC 2350	14-05-2024 Page. 1 of 8
Classification: Public		Version 1

ONECYBER
RFC 2350

OneCyber	OneCyber – RFC 2350	14-05-2024 Page. 2 of 8
Classification: Public		Version 1


DOCUMENT CONTROL SHEET

TITLE	RFC 2350
CLASSIFICATION	Public
AUTHOR	OneCyber

MADE BY	DATE	VERSION	REASON
OneCyberSec	15/05/2024	1.0	
REVIEWED BY	DATE	VERSION	REASON
APPROVED BY	DATE	VERSION	REASON
Address			

VERSION CONTROL


VERSION	DATE	REVISER	SUMMARY OF CHANGES
1.0	15/05/2024	OneCyber	First Version

	OneCyber – RFC 2350	14-05-2024 Page. 3 of 8
Classification: Public		Version 1

Copyright


This document contains restricted information. Any distribution, reproduction or disclosure of such information by any means is prohibited.

This document may not be used for any purpose other than that for which it was created and all reasonable measures must be taken to ensure the confidentiality of the information provided in its contents.

	OneCyber – RFC 2350	14-05-2024 Page. 4 of 8
Classification: Public		Version 1

Content

1. DOCUMENT INFORMATION	5
2. CONTACT INFORMATION	5
2.1. TEAM NAME	5
2.2. ADDRESS.....	5
2.3. TIME ZONE.....	5
2.4. CONTACT TELEPHONE	5
2.5. FAX NUMBER.....	5
2.6. CONTACT ADDRESSES	5
2.7. OTHER MEANS OF COMMUNICATION	5
2.8. PUBLIC KEYS AND ENCRYPTION	5
2.9. TEAM COMPONENTS.....	6
2.10. POINTS OF CONTACT.....	6
3. OBJECTIVES.....	6
3.1. MISSION	6
3.2. CONSTITUENCY.....	6
3.3. AFFILIATION.....	6
3.4. AUTHORITY.....	6
4. POLICIES	7
4.1. Types of incidents handled and level of support provided.....	7
4.2. Cooperation, interaction and distribution of information.....	7
4.3. Communication and authentication	7
5. SERVICES PROVIDED	8
5.1. Vulnerability analysis and management	8
5.2. Event detection and analysis.....	8
5.3. Awareness-raising and training.....	8
5.4. Ethical Hacking Audits	8
5.5. EDR management.....	8

	OneCyber – RFC 2350	14-05-2024 Page. 5 of 8
Classification: Public		Version 1

1. DOCUMENT INFORMATION

This document contains information about CSIRT-OneCyber and its structure is based on RFC 2350. The information shared in this document outlines the responsibilities, services, and other relevant information about CSIRT-OneCyber.

2. CONTACT INFORMATION

2.1. TEAM NAME

CSIRT-OneCyber

2.2. ADDRESS

Camino San Lázaro, 174 - Los Rodeos - Edificio Binter 1
38206 San Cristóbal de La Laguna - Santa Cruz de Tenerife

2.3. TIME ZONE

UTC +0 / Western European Time (WET)

2.4. CONTACT PHONE

+34 922 985082

2.5. FAX NUMBER

A fax number is not available.

2.6. CONTACT ADDRESSES

- Incident reporting and management: csirt@onecyber.es
- Enquiries: info@onecyber.es
- Others: <https://onecyber.es/contacto/>

2.7. OTHER MEDIA


No means of communication other than those indicated are available

2.8. PUBLIC KEYS AND ENCRYPTION

CSIRT-OneCyber uses the address csirt@onecyber.es with the following PGP key for communications related to incident response:

- Fingerprint: 901B B323 FBCD F272 6D41 6896 74B8 06D5 B600 9029

This key is available at the web address <https://onecyber.es/csirt>

	OneCyber – RFC 2350	14-05-2024 Page. 6 of 8
Classification: Public		Version 1

2.9. TEAM COMPONENTS

The names and information of the members that make up the CSIRT-OneCyber are not publicly disclosed. In the event that a report is made, staff will be identified by their full name through formal communication.

2.10. POINTS OF CONTACT

The main channel of contact with CSIRT-OneCyber for communication and management of security incidents is email, through the address: csirt@onecyber.es.

The telephone number is also enabled as an alternative means, the number being as indicated above: +34 922 985082

For other types of communications, the following address can be used: info@onecyber.es

3. OBJECTIVES

3.1. MISSION

CSIRT-OneCyber's mission is to position itself as a neutral point of reference for systematic response to cyber incidents, with the goal of supporting the development and improvement of cybersecurity. OneCyber will also strengthen communication between cybersecurity stakeholders and other CSIRT teams in the region.

CSIRT-OneCyber will provide assistance to any party that reports an incident with maximum effort and continuously carry out activities that increase cybersecurity capabilities.

3.2. CIRCUMSCRIPTION


The services offered by CSIRT-OneCyber are intended for all companies and/or organizations, both public and private, that subscribe to them.

3.3. AFFILIATION

The CSIRT-OneCyber is located within the Directorate of Operations in the OneCyberSec organizational chart.

3.4. AUTHORITY

CSIRT-OneCyber will act voluntarily to provide assistance to any party that requires assistance with cybersecurity-related issues.

	OneCyber – RFC 2350	14-05-2024 Page. 7 of 8
Classification: Public		Version 1

4. POLICIES

4.1. Types of incidents handled and level of support provided

CSIRT-OneCyber offers services for detecting, analysing and responding to security incidents that affect the integrity, availability and/or confidentiality of the information handled by its clients' systems and processes. The classification of incidents is based on the guidelines of the National Cryptologic Center of Spain (CCN-CERT) according to the ICT Security Guide CCN-STIC 817 of the National Security Scheme (ENS). These incidents are categorized and prioritized according to their typology and criticality, establishing response times in accordance with this classification. The level of support provided depends on the contractual agreements with each client. The interaction during incident management, the communication channels used and the exchange of information with other actors, such as CSIRTs, are contractually defined, respecting the legal regulations and regulations in force.

4.2. Cooperation, interaction and distribution of information


The CSIRT-OneCyber interacts daily with various actors, exchanging information according to the role they play in their network of relationships. These actors include other CSIRTs, legal authorities, information and intelligence sources, customers, suppliers, manufacturers, and within each of these groups, communicate with a variety of roles such as security engineers and analysts, system administrators, legal experts, security officers, human resources managers, and end users.

Due to their relevance at the national level, the following are identified:

- **CCN-CERT** (<https://ccn-cert.cni.es>): Relevant information and systems security incidents affecting public bodies and companies are notified.
- **INCIBE-CERT** (<https://incibe-cert.es>): Relevant information and systems security incidents affecting citizens, organizations and companies in the private sector are notified.
- **AEPD** (Spanish Data Protection Agency - <https://www.aepd.es/es>): You are notified of incidents in the event that it has put at risk or caused the leakage of personal data protected by the Regulation.
- **ESPDEF-CERT** (<https://emad.defensa.gob.es/unidades/mcce/>): You are informed of relevant security incidents that could affect the field of national defense.

4.3. Communication & Authentication

As previously established in this document, the communication channels between CSIRT-OneCyber and its clients are fundamentally 2, email and telephone, the former being used as the main channel and for the exchange of information with a certain degree of confidentiality.

	OneCyber – RFC 2350	14-05-2024 Page. 8 of 8
Classification: Public		Version 1

In the case of e-mail, PGP keys will be used to sign emails and to encrypt information that must be protected due to its degree of confidentiality.

The telephone will be used unencrypted, for communications in which the information exchanged has a low degree of confidentiality and therefore does not require special protection. This type of information can also be exchanged by email without the use of PGP key encryption.

5. SERVICES PROVIDED

5.1. Vulnerability analysis and management

Vulnerability lifecycle management by continuously analyzing the configuration of our customers' infrastructure in relation to known threats and vulnerabilities.

5.2. Event detection and analysis

Early warning through real-time monitoring, event correlation, analysis, and notification of security incidents.

5.3. Awareness and training

Simulation of personalized phishing campaigns and analysis of user responses to assess their level of awareness of these attacks. The service is complemented by educational material for users, in order to improve their ability to detect and react to this type of threat.

5.4. Ethical Hacking Audits

In-depth analysis of the vulnerabilities of the client's systems, where a cybersecurity expert attempts to access the systems by taking advantage of existing vulnerabilities and issues a detailed report.

5.5. EDR Management

OneCyber specializes in managing multiple EDRs (Endpoint Detection and Response) from various manufacturers. We monitor, manage, and optimize these security solutions to protect our customers' endpoints against advanced threats. By managing a variety of EDRs, we are able to offer comprehensive and personalized protection, adapting to the specific needs of each client and ensuring a quick and effective response to any security incident.