RFC-2350
ENOC-CSIRT

Versión 1.2

Version control

Autor	versión	Fecha de aprobación	Cambios realizados
ENOC-CSIRT	1.0	September 13th 2019	Document creation
ENOC-CSIRT	1.1	May 20th 2020	ednon.com web link corrections
ENOC-CSIRT	1.2	Jul 13th 2020	Public Keys corrections

Index

1. Broadcasting 5
1.1. Document recipient 5
1.2. Introduction 5
1.3. Date of last update 5
1.4. Notification distribution list 5
1.5. Where the document could be found 5
1.6. Document authentication 5
1.7. Document ID 5
2. Main Contact information 6
2.1. Team name 6
2.2. Addresses 6
2.3. Timezone 6
2.4. Telephone contacts 6
2.5. Fax number 6
2.6. Mail addresses 6
2.7. Other media 6
2.8. Public key and encription 6
2.9. Team members 7
2.10. Operating hours 7
2.11. Aditional Information 7
2.12. Contact points 7
3. Goals 8
3.1. Mission 8
3.2. District 9
3.3. Membership 9
3.4. Authority 9
4. Policies 10
4.1. Types of incidents managed and level of support provided 10
4.2. Cooperation, interaction and distribution of information 10
4.3. Operations 11
4.4. Communication and authentication 11
5. Services provided 13
5.1. Awareness and awareness 13
5.2. Alerts and notices 13

5.3. Security reviews and audits 13
5.4. Incident monitoring and management 13
5.5. Development of security solutions 13
6. Incident response forms 14
7. Disclaimer 14

1. Broadcasting

1.1. Document recipient

This document has as target audience the clients of the ENOC-CSIRT, other established CSIRTs, organizations with a legitimate interest in the services provided and the general public. In view of this, it can be freely distributed, being subject exclusively to copyright controls.

1.2. Introduction

In the present document services provided by ENOC-CSIRT are described in accordance with the RFC 2350 IETF's model accessible in: https://www.ietf.org/rfc/rfc2350.txt

1.3. Date of last update

Current version of this document is 1.1 and was released on may 20th 2020.

1.4. Notification distribution list

A private distribution list was created to report ENOC-CSIRT services suscribers on document changes.

1.5. Where the document could be found

Current versión of this document could be retrieved from ENOC-CSIRT public web page:

https://ednon.com/enoc-csirt/

1.6. Document authentication

This document was signed with ENOC-CSIRT PGP key. ENOC-CSIRT key signature could be found at:

https://ednon.com/enoc-csirt/

1.7. Document ID

Title: RFC 2350 ENOC-CSIRT
Version: 1.1
Document date: 20/05/2020
Expiration date: This document will be valid untill a new versión was released.

2. Main Contact information

2.1. Team name

ENOC-CSIRT

2.2. Addresses

Rúa dos Postes numero 10
15703 Santiago de Compostela
A Coruña (Galicia)
España

2.3. Timezone

Central Europe (CET/CEST)

2.4. Telephone contacts

Landline: +34 981552700 extension number otros medios de comunicación 272

2.5. Fax number

No fax numbers available.

2.6. Mail addresses

Comunication and incident Management: csirt@ednon.com
Other comunications: enoc_csirt@ednon.com

2.7. Other media

Not defined for the present document.

2.8. Public key and encription

ENOC-CSIRT uses for communications related to incident management the address csirt@ednon.com with PGP key:

Fingerprint 2E0F 80F8 A08F 4801 B558 F483 6ED9 AD2C 6D24 B356

This key is available on freely accessible PGP servers and at the web address mentioned above in this document. PGP encryption must be used in all email communications that, due to their level of confidentiality, require it.

The address enoc_csirt@ednon.com associated with the following PGP key is used for administrative communications:

Fingerprint: 7301 6FC9 C4D7 8CA0 1221 271D 067E ACDC 7D39 82AB

2.9. Team members

At the date of publication of this document, the team is made up of full-time security analysts.

For privacy reasons the list of personnel belonging to the team is not published in this document, please contact us directly if you need more information

2.10. Operating hours

ENOC-CSIRT works following the scheduling:

Usually. Monday to Thursday from 8:00 h to 17:30 h and friday, from 8:00 h. to 15:00 h
Summer timetable. Monday to Friday, from 8:00 h a 15:00 h

Service not available during oficial holidays.

2.11. Aditional Information

More information related to the ENOC-CSIRT can be found on the website:

https://ednon.com/enoc-csirt

2.12. Contact points

The following means of contact have been established during the hours of operation of the service. For communications not related to incidents, the email addressed to:

enoc-csirt@ednon.com

For communication and incident management, the assigned means of contact are email addressed to:

csirt@ednon.com

And / or phone calls to the numbers indicated above.

3. Goals

3.1. Mission

ENOC-CSIRT is a private CSIRT dedicated to public and private organizations and companies, created by mandate of the EDNON SL Management, with the mission of providing security services and protecting the information systems of the different departments of the organization and external customers to it, both being referred to hereinafter as the beneficiaries, in the event of security incidents that could affect the integrity, confidentiality or accessibility of the information and / or damage the operations or reputation of those affected.

These services are available to clients outside EDNON S.L. by subscription, which can be carried out to all or part of the services offered.

To achieve this goals ENOC-CSIRT performs, among others, the following tasks:

- Collection and analysis of information from different available sources regarding new vulnerabilities and threats.
- Communication to the beneficiaries of the intelligence generated that is relevant to their context of operations.
- Distribution of technical information on incidents with other incident response centers to improve joint response to them
- Carrying out proactive and preventive tasks to improve the safety of its beneficiaries.
- Monitoring of security events and incident detection.
- Support beneficiaries in coordinating and managing responses to security incidents that could affect them.

To achieve these objectives, ENOC-CISRT adheres since its creation to the following values:

- Compliance with the legal regulations applicable to the services provided.
- Application of best practices commonly recognized in the sector, adhering to and taking the CSIRT Code of Practice version 2.4 as a reference for its operations, available at *https://www.trusted-introducer.org/TI-CCoP.pdf.*
- Establishment of strict ethical behavior and confidentiality requirements for all personnel belonging to the service.
- Promote the use of good practices among its beneficiaries.
- Provide an effective and efficient response capacity in case of incidents.
- Definition and execution of continuous Quality and Safety audit processes on the services provided, taking as a reference for the same methodologies and standards commonly recognized in the sector.
- Creation and maintenance of communication processes and periodic evaluation of the needs of the internal and external clients of the services within a process of continuous improvement of the same.

3.2. District

The services provided by ENOC-CSIRT are directed to all the internal departments of EDNON S.L. and to companies and institutions outside the company that subscribe to them.

3.3. Membership

ENOC-CSIRT is part of the EDNON S.L. It also maintains relationships with different CSIRTs and related organizations within the Spanish and European national sphere.

3.4. Authority

ENOC-CSIRT operates, within EDNON S.L. under the authority of the Head of Corporate Information Security and the Company's Management.

Regarding its external clients, ENOC-CSIRT acts as an advisor to the security teams of said clients and does not have authority over them, therefore the implementation of the recommendations provided will be exclusively the responsibility of the client.

4. Policies

4.1. Types of incidents managed and level of support provided

The ENOC-CSIRT supports information incidents that may affect the integrity, availability and confidentiality of the information managed by the systems and processes of the beneficiaries of its services.

In general, the types of incidents supported correspond to the types of security incidents published by the National Cryptological Center of Spain, CCN-CERT, which can be consulted among others in the document:

https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file.html

All confirmed incidents are classified according to their typology and severity according to the recommendations of the CCN-CERT, prioritizing responses based on the results of said classification.

The ENOC-CSIRT does not give direct support to end users external to EDNON S.L., considering that they will contact their own security services. All communications between ENOC-CSIRT and its external beneficiaries will be channeled through the interlocutors defined in the service contract.

The level of support provided may be subject to variation depending on the contractual conditions of the service and the typology, impact, severity and / or complexity of the incident, as a result of which the intervention of CSIRT of higher scope may be necessary, associated with different administrations and / or state services.

4.2. Cooperation, interaction and distribution of information

During the execution of its mission, the ENOC-CSIRT can interact with other organizations, such as other CERT or CSIRT teams, providers, analysts and intelligence generators, etc.

Within the Spanish national scope, two reference CERTs have been established to which relevant incidents of information security and systems must be reported, limiting their powers according to the typology of the organizations affected by accidents. These organisms are the following:

- For citizens, organizations and private sector companies, INCIBE-CERT has been designated as a reference *https://incibe-cert.es*
- For public bodies and companies, the CCN-CERT has been designated as a reference. *https://ccn-cert.cni.es*

As of the date of approval of this document, no cooperative relationships have been formally established with other CSIRT / CERTs at the Spanish or European level, beyond those that are mandatorily established by Spanish legal regulations. Even so, the necessary contacts have been initiated and in the medium term the establishment of formal relationships with different regional and sectoral CSIRTs at the Spanish level is foreseen to improve response services and the distribution of information on threats.

In reference to the information that can be shared with other actors, the ENOC-CSIRT applies the following guidelines for its management and selection:

- Apply at all times the technical and legal measures indicated in this document for the protection of information.
- Anonymize the shared information as much as possible and within it select exclusively relevant data for the resolution of incidents.

- Respect the level of confidentiality assigned to the information by its owner.
- Do not share confidential information with other parties without the prior agreement and authorization of its owner. This guideline applies in all cases in which there is no higher legal or regulatory obligation that requires the sharing of information.
- Protect the privacy of personal information. Although in general, personal data will never be shared, if necessary, and within the assumptions contained in the European and Spanish regulations on the protection of personal data, express authorization is requested from the owner thereof.
- Stop the distribution of information at the moment in which the client who owns it notifies the denial of permission to do so. This guideline applies in all cases in which there is no higher legal or regulatory obligation that requires the sharing of information.

4.3. Operations

The ENOC-CSIRT operates in accordance with Spanish legal regulations and adheres to the CSIRT Code of Practice version 2.4, available at *https://www.trusted-introducer.org/TI-CCoP.pdf*.

4.4. Communication and authentication

The ENOC-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), the National Security Scheme of the Government of Spain 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 labeling of documents, according to which the following levels of information classification have been established:

- ✓ **RED.** Information not distributable and 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 in order 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 and 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.

Considering the types of information the ENOC-CSIRT deals with, the phones will be considered secure enough to be used even without encryption. Unencrypted email will not be considered particularly secure, but will be sufficient for low-sensitivity data transmission.

If it is necessary to send highly confidential data by email, they will be encrypted using the PGP keys of the senders and receivers of the same. Network file transfers will be considered similar to email for these purposes, so confidential data must be encrypted for transmission.

When it is necessary to establish a relationship of trust, and before revealing confidential information, the identity of the other party shall be determined with a reasonable degree of trust, using, to the extent possible, the references of third parties and / or known bodies and of trust as a means of accreditation. Otherwise, appropriate methods will be used, such as searching for FIRST members or the **Trusted Introducer** database and performing a phone callback or email to ensure the identity of the other parties.

5. Services provided

5.1. Awareness and awareness

The ENOC-CSIRT provides these services by participating in training and information days together with sending communications to its beneficiaries where news on good practices regarding information security, recent security incidents, new vulnerabilities, analyzes and reports are addressed. about malware etc.

5.2. Alerts and notices

The ENOC-CSIRT distributes intelligence information in relation to detected malicious campaigns, new threats, indicators of commitment, etc., as well as recommendations on the actions to be taken in response to them.

5.3. Security reviews and audits

The ENOC-CSIRT provides services for reviewing and improving information security management based on recognized frameworks, as well as vulnerability analysis and pentesting.

5.4. Incident monitoring and management

The ENOC-CSIRT provides motorization, detection, analysis, classification, coordination and support services in response to security incidents.
These services are provided through the support and collaboration with other IT groups of the beneficiaries.

5.5. Development of security solutions

The ENOC-CSIRT collaborates with the solutions development department of EDNON SL, **EDNON labs_** for the development of services and tools, for internal use and commercialization, with the aim of achieving improvements in the management of the information security of its beneficiaries.

6. Incident response forms

For the communications of the service, formats agreed between the participating parties and / or generally recognized by the sector are used. In cases where the origin of a communication is external and there is no previously agreed notification format, it is recommended to include at least the following information in it:

- Identification data. Sender name, organization, address, etc.
- Contact details. Email address and phone if available.
- PG PGP key if available.
- Brief summary of the reported incident.
- Incident detection means.
- Affected systems and estimated initial impact.
- Relevant technical information about the incident. Mail headers, IP addresses, samples and artifacts associated with the incident or information on the means available to share them.

Whenever possible, incidents should be communicated by email using the address previously indicated in this document.
Furthermore, ENOC-CSIRT has developed its own reporting models for the management and analysis of incidents and the communication of results to its beneficiaries.

7. Disclaimer

Although all precautions will be taken in the preparation of information, notifications and alerts, ENOC-CSIRT assumes no responsibility for errors or omissions, or for damages resulting from the use of the information provided during the execution of its services.