1 DOCUMENT INFORMATION

This document complies with RFC 2350: https://www.ietf.org/rfc/rfc2350.txt

1.1 Date of Last Update

This Document last update was made on October 11th, 2023.

1.2 Distribution List

All the distribution lists, and emails included in this document, have been created in a completely confidential manner.

This list has been created for the purpose of providing information to those subscribed to this SEIDOR | CSIRT, and the services to which it refers and, especially, in everything relating to this document and the changes made therein.

1.3 Location of the Document

The latest version of this document is available at:

https://www.seidor.com/seidor-csirt-rfc-2350

1.4 Authenticating this Document

This document has been signed with the SEIDOR | CSIRT PGP key, which can be found on the SEIDOR | CSIRT website:

https://www.seidor.com/seidor-csirt-rfc-2350

1.5 Document Specifications

Title: CS_NC27.01_RFC2350.PDF

Version. 2.0

Document date: October 11th, 2023

Expiration date: The last known version of this document will be considered valid.

2 CONTACT INFORMATION

2.1 Name of the Team

SEIDOR - CSIRT

2.2 Address

Carrer Pujades, 350. PL.2

08019 – Barcelona

Spain

2.3 Time Zone

Central European Time - CET (GMT+0100, and GMT+0200 from April to October).

2.4 Telephone Number

- +34 93 304 3222

2.5 Electronic mail addresses

Incident Management: incidentes.csirt@csirt.seidor.com

- Incident Notification from the circumscribed community.

Notifications/Communications: notificaciones.csirt@csirt.seidor.com

- Relevant Information Notification to the CSIRT.

CSIRT Contact: csirt@csirt.seidor.com

- Communications addressed to the SEIDOR | CSIRT organisation.

2.6 Public keys and encryption

The PGP key corresponding to the SEIDOR | CSIRT incident management will be the following:

csirt@csirt.seidor.com

FINGERPRINT: A8D4 7E73 E9F6 6FD1 76E5 0A14 E9B0 AE77 EC87 3208

incidentes.csirt@csirt.seidor.com

FINGERPRINT: 6A38 05B6 A500 74F2 1CBC 23C6 D925 7F75 4833 3452

notificaciones.csirt@csirt.seidor.com

FINGERPRINT: 3553 0A15 E500 E3C8 8056 6D19 F165 ADD0 531F 774F

Its location will be freely accessible and will be located at the URL stated above. A special reminder is made on the need to use PGP encryption in all outgoing and incoming communication from/to SEIDOR | CSIRT.

2.7 Team Members

Information on team members, and any other data regarding their identity or that of third parties linked to them, is to be considered totally confidential. If you require information regarding this point, please send an email to: csirt@csirt.seidor.com.

2.8 Operating Hours

The SEIDOR | CSIRT operates 24/7, 365 days a year.

2.9 Additional Contact Info

If you require further information, the procedure must be started through the following URL:

https://www.seidor.com/cybersecurity/csirt

In the event of requiring more information during service operating hours, any request should be made through the following email address:

csirt@csirt.seidor.com

3 CHARTER

3.1 Mission Statement

SEIDOR | CSIRT is a private Incident Response Centre created by the SEIDOR Company to coordinate and respond to cybersecurity threats from the company itself, subsidiaries and clients, whether public or private entities. Its main mission is to implement the human, technical and technological means necessary to reduce the risk of security incidents and provide a response, when required, in all those infrastructures, systems and services within its scope.

SEIDOR | CSIRT was born with the strong commitment to support the CSIRT community for a global response to threats that jeopardize the security of all actors providing services to companies, institutions and citizens.

To achieve those objectives, the SEIDOR-CSIRT performs the following tasks, among others:

- Definition of security alerts based on customised requirements.
- Continuous vulnerability analysis and management.
- Service progress Dashboards.
- Security Improvement Recommendations.
- Data collection and analysis from different available sources regarding new vulnerabilities and threats.
- Communication to the beneficiaries of the intelligence generated that is relevant to the context of their operations.
- Distribution of technical information on incidents with other CSIRT.
- Security Event Monitoring and Incident detection.

To achieve these objectives, SEIDOR-CSIRT has adhered, from its creation to the following values.

- Compliance with legal regulations.
- Monitoring and application of Best Practices associated with each productive and operating environment. Continuous improvement in this described area and located in the designated repository.

- Thoroughly conducting specific risk management audits for the services offered, involving the rest of the CSIRT community in the status of these risks, and facilitating the collaboration of all members to enhance the community.
- Providing the greatest sense of well-being to service beneficiaries, creating an optimal, assessable, and modifiable environment of trust and security.
- Strict and timely execution of defined audits, both internal and external, achieving excellent compliance with quality and security standards in each of the catalogued services.
- Creation and maintenance of regular communication and evaluation processes for the needs of both internal and external costumers of the services within a continuous improvement process.

3.2 Constituency

The services provided by SEIDOR | CSIRT are aimed to all departments of SEIDOR and external companies and institutions subscribing to them.

3.3 Affiliation

SEIDOR | CSIRT is sponsored by SEIDOR S.A.

3.4 Authority

SEIDOR | CSIRT operates within SEIDOR under the sponsorship and authority of the Corporate Bureau of Cybersecurity and the Corporate Chief Information Security Officer.

Regarding external clients, modifiable according to client/company agreements, SEIDOR | CSIRT acts as a security consultant for said clients and does not have any authority over them, therefore, the implementation of the recommendations provided are the sole responsibility of the client.

4 POLICIES

4.1 Types of Incidents and Level of Support

The SEIDOR | CSIRT supports information incidents that may affect the integrity, availability and confidentiality of the information managed by the systems and processes of its service beneficiaries. The types of incidents supported correspond to the typologies of security incidents published by Spain's National Cryptology Centre, CCN-CERT:

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 by type and severity, and responses are prioritised based on the results of said classification.

SEIDOR | CSIRT does not provide direct support to external end-users outside SEIDOR, as these individuals will contact their own security services. All communications between the SEIDOR | CSIRT and its external beneficiaries will be channelled through the designated points of contact defined in the service contract.

The level of support provided will depend on the contractual terms of the service and the type, impact, severity and/or complexity of the incident, which may require the involvement of higher-level CSIRTs associated with different governmental administrations and/or state services.

4.2 Co-operation, Interaction and Disclosure of Information

SEIDOR | SIRT may interact with other organisations, such as other CERT or CSIRT teams, providers, analysts and intelligence generators, etc.

Within Spain borders, the referenced CERT bodies are the following:

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

The necessary contacts have been initiated for a two-way collaboration and communication with the different national and international CSIRTs, and there is a schedule of actions in place to reach the goal as soon as possible.

SEIDOR | CSIRT applies the following guidelines for handling and selection of shared information:

- Apply the technical and legal measures always outlined in this document for the protection of information.
- Anonymize shared information and select only relevant data for the incident resolution.
- Respect the confidentiality level assigned based on the information classification.
- Do not share confidential information with other parties without prior agreement and authorization from the information owner. This guideline applies in all cases where there is no higher legal or regulatory obligation to share the information.
- Protect the privacy of personal information. While personal data will generally not be3 shared, if it becomes necessary, and within the scenarios referred to in GDPR, explicit authorization will be sought from the data subject.
- Cease the distribution of information when its owner notifies the denial of permission to do so, this is also based on the GDPR.

4.3 Communication and Authentication

SEIDOR | CSIRT applies the protection measures corresponding to the nature and classification of the information it handles, using as a reference, among others, GDPR, the National Security Framework of the Spanish Government, the European NIS directive, Royal Decree 12/2018, of September 7th and Royal Decree 43/2021, of January 26th.

Additionally, both internally and externally, the FIRST TLP v2.0 protocol is used for the classification and labelling of documents in communications and documentation:

https://www.first.org/tlp/

Considering the types of information handled by SEIDOR | CSIRT, phones will be considered secure enough to be used even without encryption. Unencrypted email will not be deemed particularly secure but will be sufficient for low-sensitivity data transmission.

As previously mentioned in sections regarding the encryption of shared information, data will be encrypted using the PGP keys of the senders and recipients.

When it is necessary to establish a trust relationship, and before disclosing any confidential information, the identity of the other party will, whenever possible, rely on references from third parties and/or known and trusted bodies as a means of accreditation. In cases where this is not feasible, appropriate methods will be employed, such as searching for FIRST members or the Trusted Introducer database and conducting a callback or sending an email to ensure the identity of the other parties.

5 SERVICES

5.1 Reactive Activities

5.1.1 Cybersecurity Monitoring

SEIDOR | CSIRT provides monitoring, detection, analysis, classification, and support services for early response to Security Incidents.

These services are delivered through collaboration and support with other IT groups of the beneficiaries.

5.1.2 DFIR – Incident Response Team

SEIDOR | CSIRT has a specialized Incident Response Team (DFIR) to act whenever an incident is declared.

5.2 Proactive Activities

5.2.1 Alerts and Notifications

SEIDOR | CSIRT distributes intelligence information related to detected malicious campaigns, new threats, Indicators of Compromise, etc., along with recommendations for actions to be taken in response to them.

5.2.2 Security reviews and audits of CSIRT Scope Services

SEIDOR | CSIRT offers services or reviewing and improving information security management complying with recognized frameworks. This includes vulnerability analysis, risk monitoring and intelligence management to prevent threats.

The scope of the service will only cover the systems within CSIRT's jurisdiction.

5.2.3 Sensitisation and awareness-raising

SEIDOR | CSIRT provides these services through informative workshops, combined with the sharing of news to its beneficiaries, in everything related to good practices, information security, news, discovery of new vulnerabilities, etc.

5.2.4 Security Solutions Development

SEIDOR | CSIRT will carry out developments aimed at enhancing the monitoring and response to security incidents, mainly in SAP and Microsoft Corp environments.

These tools, along with other CSIRT-relevant developments, are intended to achieve improvements in the information security management of its beneficiaries.

6 INCIDENT REPORTING FORMS

For service communications, agreed-upon formats are used among the participating parties and/or those generally recognised by the sector.

An Incident Report form is available at the following location:

https://www.seidor.com/seidor-csirt-rfc-2350

7 DISCLAIMER

While every precaution will be taken in the preparation of information, notifications and alerts, SEIDOR | CSIRT assumes no responsibility for errors or omissions, nor for damages resulting from the use of the information provided during the execution of its services.