NUNSYS-CERT RFC 2350

Information Classification:

Document type	General document
Filename	Nunsys-CERT_RFC_2350_v2.4_EN.docx
Clasification	PUBLIC
Field of dissemination	Public
Responsible	Head of NUNSYS-CERT

VERSION CONTROL		
Description	**Version**	**Date**
Luis Bernal: Preliminary version.	1.0	01/04/2018
Luis Bernal: Preliminary version.	1.1	16/04/2018
Rafael Vidal: Modified 3.2 and 3.4	1.2	17/04/2018
Luis Bernal: Team member deleted	1.3	11/05/2018
Luis Bernal: Team member added	1.4	05/09/2018
Luis Bernal: Team members modified	1.5	19/12/2018
Miguel Roca: General review and adaptation	2.0	11/06/2020
Miguel Roca: Team member added	2.1	10/07/2020
Miguel Roca: Team members modified	2.2	06/10/2020
Miguel Roca: Team members modified	2.3	14/01/2021
Oscar Atienza: Modified 2.6 and 2.7	2.4	04/03/2021

Content index

1 ABOUT THIS DOCUMENT

1.1 Date of last update

This is version 2.4 and was published on March 4th, 2021.

1.2 Distribution list for notifications

Nunsys does not currently use any mailing list as a means of notification of changes to the document.

1.3 Location where this document may be found

The current versión of this document is available from the Nunsys website:

https://www.nunsys.com/rfc2350/

1.4 Authenticating this document

This document has been digitally signed with the NUNSYS -CERT's PGP key (see section 2.6).

2 CONTACT INFORMATION

2.1 Name of the team

NUNSYS-CERT
Nunsys S.L. – Computer Emergency Response Team

2.2 Address

Nunsys S.L.
Calle Gustave Eiffel, 3
46980 Paterna, Valencia
Spain

2.3 Time zone

Central Europe: CET (UTC/GMT +1), CEST (UTC/GMT +2)

2.4 Telephone number

+34 902 88 16 26

2.5 Electronic mail address

sat@nunsys.com

2.6 Public keys and encryption information

sat@nunsys.com
Key ID: 9ABFFCC4
Fingerprint 631B 7475 E00B 00D9 52F5 AC03 9648 B393 9ABF FCC4

The public PGP key is available from the Nunsys website:

https://www.nunsys.com/nunsys-cert/pgp/sat.asc

2.7 Team members

Oscar Atienza
Oscar.atienza@nunsys.com
Key ID: 104AD6A0
Fingerprint D2DDACAB8FD56098967FCFA0219D0B04104AD6A0

María José Montes
mariajose.montes@nunsys.com
Key ID: EC835DA3
Fingerprint 27781C0EA6F4B197F792F1D83BCF410BEC835DA3

Néstor Jarque
Nestor.jarque@nunsys.com
Key ID: EE3BC7CE
Fingerprint 0E6B0BEB5593CE40E87DF4D408BFEABBEE3BC7CE

Nafees Muhammad
nafees.muhammad@nunsys.com
Key ID: 2C6700C0
Fingerprint 0E6B0BEB5593CE40E87DF4D408BFEABBEE3BC7CE

Agustin Domenech
agustin.domenech@nunsys.com
Key ID: 9FBEBC5F
Fingerprint D4E482E353F9F29763E456BAA1B5148B9FBEBC5F

David Blasco
david.blasco@nunsys.com
Key ID: 732A23ED
Fingerprint 1D29F7CB9FF65E80F4035A217E3E4E5D732A23ED

Manuel del Olmo
Manuel.deolmo@nunsys.com
Key ID: 3148A951
Fingerprint EF4CDBCBE4642159AA5C504B4184D9AA3148A951

Juan Antonio Vicent
juanantonio.vicent@nunsys.com
Key ID: 5740F93C
Fingerprint 7E234B4AFE60B7048CF27F60CCACFA565740F93C

Arturo Raga
arturo.raga@nunsys.com
Key ID: CB844621
Fingerprint A1D3D617EDF58EDCA4DE1D0E966D5BFECB844621

Carlos José Hernandez
carlosjose.hernandez@nunsys.com
Key ID: E3CFDACA
Fingerprint A8C9979878C07D2925D7C4594ECDA2F4E3CFDACA

Lorena Penalba
lorena.penalba@nunsys.com
Key ID: BA6A4C0D
Fingerprint E2CF65D73B6CB98B98D3075FA2B61C41BA6A4C0D

Antonio José Escabias
antoniojose.escabias@nunsys.com
Key ID: 37B1E061
Fingerprint BFB93BE667EDDA0DE34E6F8A09D0857437B1E061

2.8 Points of customer contact

For reporting and managing security incidents preferred method is by mail.

Please write to us at sat@nunsys.com using the public key. This will create a case in our ticket system and will be handled by our staff.

3 CHARTER

3.1 Mision statement

NUNSYS-CERT is a private Security Incident Response Centre, established by the Directorate of NUNSYS S.L., which has as its mission the provision of cybersecurity services aimed at protecting against security incidents that could impact on the confidentiality, integrity or availability of its own information services, as well as external clients, affecting their processes or reputation.

3.2 Constituency

NUNSYS-CERT offers information security services for critical infrastructures, educational institutions, public institutions and corporations, in addition to analyzing events, coordinating technical solutions, ensure that the necessary information is transmitted and train other teams or individuals in the management of security incidents.

Our security services are provided to final customers, such as private companies (industry, critical infrastructure, integrators, other telecommunications providers, etc.) and public bodies (municipalities, hospitals, universities, etc.)

3.3 Sponsorship and/or affiliation

NUNSYS-CERT is part of the Systems Department of Nunsys S.L., within its operations division. It is a member of TF-CSIRT Trusted Introducer and CSIRT.ES, actively collaborating with other CSIRTs and cybersecurity organizations.

3.4 Authority

NUNSYS-CERT operates, as a department within Nunsys S.L., under the authority of the Cybersecurity Technical Manager and the Chief Operations Officer of the organization. NUNSYS-CERT relates to its external clients acting as an advisor, so it has no authority over them; it is the sole responsibility of the client to adopt the recommendations and measures proposed by this CERT.

4 POLICIES

4.1 Types of incidents and level of support

In general, NUNSYS-CERT supports the types of incidents collected by the CCN-CERT, in its document "CCN-STIC 817 Cyberincident Management", and that may impact on the confidentiality, integrity or availability of its clients' assets, both internal and external.

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

The level of support provided may vary depending on the contractual conditions of the service and the type, impact, severity and/or complexity of the incident, which may imply the need for scaling up and the intervention of higher-scope CSIRTs associated with different goverment administrations and/or services.

4.2 Cooperation, interaction and y disclosure of information

NUNSYS-CERT, in the performance of its mission, can cooperate and interact with other organizations, such as other CERT or CSIRT teams. Within the Spanish national territory, two reference CERTs have been established to which relevant information security incidents must be reported. These bodies are as follows:

- INCIBE-CERT – For citizens, organizations and companies in the private sector.
- CCN-CERT – For public bodies and enterprises.

NUNSYS-CERT is part of well-known national and international forums, whose objective is to promote cooperation and coordination between the CSIRTs in order to act against computer security problems. These forums are as follows:

- CSIRT.ES
- TF-CSIRT Trusted Introducer

If it is necessary to share information with other actors, NUNSYS-CERT will follow the following guidelines:

- Share only information relevant to the handling of incidents, respecting the level of confidentiality established by the owner.
- Apply at all times the necessary technical and legal measures for the protection of information.
- Anonimize shared information as much as possible.
- Do not share confidential information with other parties without prior agreement and authorization from the owner, unless there is a higher legal or regulatory obligation to do so.
- Do not share personal data. If necessary, it will be done taking into account the Spanish personal data protection law and requesting prior authorisation from their owner.

4.3 Communication and authentication

NUNSYS-CERT treats the information with absolute confidentiality, applying the necessary measures for its protection, as stated in its Information Classification Policy and considering, among other laws and regulations:

- Regulation EU 2016/679 General Data Protection Regulation
- Organic Law 3/2018 Personal Data Protection and Digital Rights Guarantee
- Royal Orders 3/2010 y 951/2015 National Security Scheme

- Royal Order 704/2011 Critical Infrastructure Protection

For the purposes of low-sensitivity information, transmission by e-mail or over the network, not considered as particularly secure means, shall be enough. In the case of sensitive information, the communication via email will require encryption, for which the PGP keys of the senders and recipients will be used; similarly, for the transmission of files over the network, these will be previously encrypted.

Telephone lines are considered enough secure for use even without encryption.

5 SERVICES

5.1 Incident response

NUNSYS-CERT provides 24x7x365 monitoring, detection, analysis, classification, coordination and support services in the response to security incidents, always in close collaboration with the different actors involved, with the objective of enhancing mitigation capacity.

5.1.1 Incident triage

- Investigating whether an incident actually occurred
- By identifiying its scope

5.1.2 Incident coordination

- Identifying and contacting the organizations involved
- Providing contact with third parties, including law enforcement agencies, if necessary.
- Requesting and/or writing reports based on the organizations involved, type of incident and severity.
- Where appropriate, by generating communications to stakeholders.

5.1.3 Incident resolution

- Providing technical assistance to the organizations involved
- Recommending actions aimed at eradicating the root cause of the incident and its impact.
- Conducting forensic investigations, collecting evidence and interpreting data if necessary.

5.2 Proactive services

5.2.1 Announcements and warnings

NUNSYS-CERT collects and distributes intelligence on emerging threats, engagement indicators, malicious campaigns, etc., as well as guidelines and recommendations on actions to be taken for their prevention and response.

5.2.2 Vulnerabilities management

Continuous monitoring and improvement of the security of information systems (network, applications, infrastructure, etc.) through the periodic execution of scans aimed at identifying, quantifying and classifying system vulnerabilities.

5.2.3 Security assessment/audit

Information security management review and improvement services in accordance with internationally recognized standards, frameworks and good practices, as well as pentesting services.

5.2.4 Security tools development

NUNSYS-CERT collaborates with the R&D department of Nunsys S.L. in the development of tools and services aimed at improving the information security management of its stakeholders, both internal and external.

5.2.5 Training and awareness raising

As the first defence barrier in the prevention of incidents, NUNSYS-CERT provides awareness and training services in all areas of information security, such as cybersecurity, privacy or incident response.

5.2.6 Records retention

Records of managed security incidents shall be maintained. This information will be considered confidential; however, anonymized statistical reports may be generated and shared with the community.

6 HOW TO REPORT AN INCIDENT

For reporting and managing security incidents preferred method is by mail, as set out in point 2.8 of this document.
This is done using notification formats agreed with interested parties. In the absence of such a format or an external third party communication, it shall be necessary to include in such communication at least the following information:

- Identification data (sender's name, organization, etc.)
- Contact details (email address and telephone number)
- PGP key (en caso de disponer de ella)
- Brief summary of the incident
- Afected systems and estimated initial impact
- Relevant technical information (IP addresses, email headers, etc.)

7 DISCLAIMERS

NUNSYS-CERT takes all precautions in the preparation of information, notifications, alerts and reports, assuming no responsibility for errors, omissions or for damages resulting from the use of the information provided.