**Dognædis**
IPN Incubadora
Rua Pedro Nunes 3030-199 Coimbra - Portugal
E-Mail: info@dognaedis.com
Tel. +351 239 047 756, +351 239 300 700

Innovation Centre
Gallows Hill, Warwick CV34 6UW - UK
E-Mail: info@dognaedis.co.uk

**Nível de Acesso do Documento**: Public

# DGS-IRT, RFC 2350

26th May 2014
v1.0

www.dognaedis.com

## **Document Access Level**: Public

# Contents

**Abstract**

This document describes the DGS-IRT, the DOGNÆDIS CSIRT team, according to RFC 2350. The RFC 2350 is a 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 About this document

## 1.1 Date of Last Update

This is version v1.0, published 26th May 2014.

## 1.2 Locations where this document can be found

The current version of this document is available from the DGS-IRT site:
https://www.dognaedis.com/irt/rfc/
There are two documents both in portuguese and english of this document.
You also have the option of reading it in two formats: PDF and TXT.

## 1.3 Authenticating this Document

This document has been signed with DGS-IRT PGP key. The signature is also available at:
https://www.dognaedis.com/irt/rfc

# 2 Contact Information

## 2.1 Name of the Team

**DGS-IRT**: the DOGNÆDIS Incident Response Team.

## 2.2 Address

Dognædis
Rua Pedro Nunes, edifício IPN Incubadora
3030-199 Coimbra - Portugal

## 2.3 Time Zone

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

## 2.4 Telephone Number

+351 239 047 756

## 2.5 Electronic Mail Address

irt @ dognaedis.com

## 2.6 Public Keys and Other Encryption Information

The DGS-IRT has a PGP key for secure communication.
*DGS-IRT:* irt @ dognaedis.com
*KeyID:* 0xA0C22F72
*Key Fingerprint:* 1E69 58F6 365F 94F1 4048 3CC1 FB38 07B7 A0C2 2F72

### 2.7 Team members

(ordered alphabetically)
André Pinheiro - ampp @ dognaedis.com
Francisco Nina Rente - frente @ dognaedis.com
Hugo Trovão - htrovao @ dognaedis.com
Leandro Braguês - lbragues @ dognaedis.com
Rui Gonçalo Amaro - ramaro @ dognaedis.com
Sérgio Alves - salves @ dognaedis.com

### 2.8 Other Information

Information regarding activities and structure of the DGS-IRT, as well as links to various recommended security resources can be found at http://www.dognaedis.com/irt/

### 2.9 Points of Customer Contact

The preferred method for contacting DGS-IRT is via e-mail at irt@dognaedis.com. If it is not possible (or not advisable for security reasons) to use e-mail, the DGS-IRT can be reached by telephone at +351 239 047 756 during regular office hours.

## 3 Charter

### 3.1 Mission Statement

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

### 3.2 Constituency

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

88.157.200.81
88.157.200.82
88.157.200.83
88.157.200.84
88.157.200.85
88.157.200.86
88.157.200.87
88.157.200.88
88.157.200.89
88.157.200.90
88.157.200.91
88.157.200.92
88.157.200.93
206.125.169.26
62.28.122.242
80.172.255.131
80.172.255.105
62.28.62.86
94.46.248.110

213.228.179.8

### 3.3 Authority

The DGS-IRT expects to work cooperatively with the system administrators and users of the client infrastructures, in so far as possible, to guaranty the necessary authority to respond to security incidents.

## 4 Policies

### 4.1 Types of Incidents and Level of Support

The DGS-IRT restricts its support and incident handling to incidents that fall under its constituency. The following list represents the type of incidents to which the DGS-IRT will provide support. However different clients will have different levels of service. The service level of the various clients can be viewed in the file mentioned in section 3.2.
The following list follows the classification guidelines used by the National CSIRT network[1] of which the DGS-IRT were founding member and are still members.

- **Computer forgery** - Intentional act of introducing, modifying, deleting or suppressing of computer data, or by any other way interfering with the functioning of a computer system without right, resulting in inauthentic data or documents, with the intent that it be considered or acted upon for legal purposes as if it were authentic. Includes the use of *phishing* web sites for credential theft and the distribution of *phishing* emails.
- **Computer system interference** - Intentional action or attempt to prevent or gravely disrupting the functioning of a computer system by introducing, transmiting, damaging, deleting, deteriorating, alterating, suppressing or rendering inaccessible any software component or hardware without right. Includes denial of service attacks.
- **Illegal access to a computer system** - Intentional access or attempt to the whole or any part of a computer system without right. Includes the theft of information, namely business secret, industrial secret or confidential data protected by statute.
- **Data interference** - Intentional act or attempt to delete, damage, deteriorate, alterate, suppresse or render inaccessible computer data without right. Includes malware and its distribution by email.
- **Unauthorized gathering of data** - Intentional act of gathering information about networks and computer systems without right.
- **Copyright infringement** - Copyright infringement, regardless of its content being information, source code, graphical projects or any other elements of computer systems protected by copyrights.
- **Unsolicited electronic mail** - Unsolicited reception/sending of e-mail, whether produced for direct marketing purposes ou with no aparent purpose. *Malware* distribution or *phishing* attacks are not included.
- **Other security infringement** - Other infringement to the IT security policy.

Under normal conditions the DGS-IRT will reply to any of the above described incidents within 24 hours.

[1] http://www.cert.pt/index.php/pt/rede-nacional-csirts/documentos/1489-classificacao-de-incidentes

### 4.2 Co-operation, Interaction and Disclosure of Information

The DGS-IRT will handle all information it is provided as confidential. However statistical data can be generated from some of this information as long as full confidentiality and anonimization 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 DGS-IRT 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

The DGS-IRT only responds to incidents that affect its constituency and follows the best practices published by entities like CERT-CC[2], *ENISA*[3], *Trusted Introducer*[4] and *FIRST*[5].

### 5.2 Incident Triage

This stage will prioritize incidents according to a initial analysis which will take into account the type of incident, impact and others characteristics. All incidents will be assigned a unique identifier.

### 5.3 Incident Coordination

The analysis and investigation of an incident will identify the root causes of the incident and if needed the involved entities or persons will be contacted. If the incident is outside the scope of action of the DGS-IRT the information will be forwarded to the responsible entity.

### 5.4 Incident Resolution

The incident is considered to be resolved when all affected system have resumed normal operation.
Non-confidential data can be gathered to generate statistical information or if needed to report to other involved CSIRT.

### 5.5 Proactive Activities

The DGS-IRT provides consulting services. Detailed descriptions of these services are available at (https://www.dognaedis.com).

## 6 Disclaimer

While every precaution will be taken in the preparation of information, notifications and alerts, DGS-IRT assumes no responsibility for errors or omissions, or for damages resulting from the use of information contained within.
Furthermore several contractual obligations are included in the standard service contract, which only cover the involved parties.

[2] http://www.cert.org
[3] http://www.enisa.eu
[4] http://www.ti.terena.nl
[5] http://www.usfirst.org