1. About this document

1.1 Date of Last Update

This is version 1.0, published 2020-11-30.

1.2 Distribution List for Notifications

Currently Intec-CSIRT does not use any distribution lists to notify about changes in this document.

1.3 Locations where this Document May Be Found

The current version of this CSIRT description document is available from the Intec-CSIRT website at: *https://cert.intec2.com/RFC2350.pdf*.

Please make sure you are using the latest version.

2. Contact Information

2.1 Name of the Team

Intec-CSIRT.

2.2 Address

Edificio Naorte B, 1º piso

07121 Palma de Mallorca, Baleares

ESPAÑA

2.3 Time Zone

GMT+0100/+0200 DST

2.4 Telephone Number

+34 971 439 846

2.5 Mobile Number

+34 664 379 745

2.6 Electronic Mail Address

cert@intec2.com

2.7 Public Keys and Other Encryption Information

The Intec-CSIRT has a PGP key, whose fingerprint is 77E8 61CC DB10 8AF4 5A88 AD18 41B0 B0EE 5C1C FEEE.

It can be found at the usual large public key servers.

2.8 Team Members

Juan José Fuster is the Intec-CSIRT Manager.

Other members of the team are Víctor Pujadas and Ángel Reyero.

2.9 Other Information

General information about the Intec-CSIRT can be found at https://intec2.com.

2.10 Points of Customer Contact

The preferred method for contacting the Intec-CSIRT is via e-mail at <cert@intec2.com>. If it is not possible (or not advisable for security reasons) to use e-mail, the Intec-CSIRT can be reached by telephone (+34 971 439 846) during regular office hours.

The Intec-CSIRT's hours of operation are generally restricted to regular business hours (09:00-18:00, Monday to Friday except holidays).

3. Charter

3.1 Mission Statement

Intec-CSIRT offers cybersecurity management, forensic analysis, incident response and monitoring services to large companies, SME and Public Administration.

3.2 Constituency

Intec-CSIRT is formed by private capital without having financing of any kind.

3.3 Sponsorship and/or Affiliation

Intec-CSIRT maintains affiliations with various other CSIRTs on an as needed basis, being member of the 'Polo Tecnológico del INCIBE' and the 'AEI Ciberseguridad'.

Intec-CSIRT also has the CERT certification of the Carnegie Mellon University and collaborates with Spanish Enforcement Agencies.

3.4 Authority

Intec-CSIRT hopes to work collaboratively with the system administrators of the companies that require its services. There is no authority above Intec-CSIRT other than that of providing good service.

4. Policies

4.1 Types of Incidents and Level of Support

The Intec-CSIRT is authorized to address all types of computer security incidents which occur.

The level of support given by Intec-CSIRT will vary depending on the type and severity of the incident or issue, the type of constituent and the size of the user community affected.

Incidents will be prioritised according to their apparent severity and extent. These incidents will be assessed as to their relative severity at Intec-CSIRT's discretion.

Direct support will be given to end users; they are expected to contact their system administrator, network administrator, or department head for assistance, but Intec-CSIRT will be the point of support to guarantee the correct handling of the security incidents that occur. However, Intec-CSIRT can also be the entity that manages security if the end user considers it appropriate.

4.2 Co-operation, Interaction and Disclosure of Information

Intec-CSIRT defaults to keep all information relative to incidents confidential. While appropriate measures will be taken to protect the identity of members of our constituency and members of neighbouring sites where necessary, the Intec-CSIRT will otherwise share information freely when this will assist others in resolving or preventing security incidents, without disclosing any personal information.

4.3 Communication and Authentication

In view of the types of information that the Intec-CSIRT will likely be dealing with, telephones will be considered sufficiently secure to be used even unencrypted. Unencrypted e-mail will not be considered particularly secure but will be sufficient for the transmission of low-sensitivity data.

If it is necessary to send highly sensitive data by e-mail, PGP will be used. Network file transfers will be like e-mail for these purposes: sensitive data should be encrypted for transmission.

It is necessary to establish trust before relying on information given to the Intec-CSIRT, or before disclosing confidential information. Otherwise, other methods will be used to establish trust, such as a search of FIRST members, the use of WHOIS and other Internet registration information…, along with telephone call-back or e-mail mail-back to ensure that the party is not an impostor.

Incoming e-mail whose data must be trusted will be checked with the originator personally, or by means of digital signatures (PGP is supported and recommended).

Intec-CSIRT PGP Public Key

Fingerprint: 77E8 61CC DB10 8AF4 5A88 AD18 41B0 B0EE 5C1C FEEE

PGP Public Key:


```
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQGNBF+pSIEBDAD2DFnxORKUQXMI9UxYDxdQxYbO+ukIrxymjSFHvTM7NOQsY0yu
31EPZvYLkrwzDEQMrSbmnL85s66btuJN/5dg7+p3Jl/3ScOVfvHm1iLQgrZ7ovAT
p0yoavk0nyFz2MuUa+zBRuq20PWNJTYEOTfVWjp7b5QMXFoHazBYL2asSijw4O0q
74hGHvQXoyb8t1D/rL0PKnd5XdvlmbXm+2GBMdfT4zhmv8sAQ8Ir7ncOzSIiaO/I
VgQ3TZPDEhmfQhw2HLGIyaO5bYD7pRo0f4tcNVXZBKBgW7vPqhFTiDIn/gxKAZa4
uyrznpYfINu6wqcIS4DX7XwUbq6aBgI2eiFORm7xZA6rKc1TiQLauOKSwehyXdQt
XDmE7998NhlBxJPYwHPu/EfZE1vUqGoP1cBK+qMgabPHX9dGOmFeyVGevCaXouEV
KjtmNAkynBRR0Cq+05P+HWHnemnLHE9TmlbKzQ2EhryXSu2xUg1+lVRnLo8YahE4
MtQV1Dkn2YQRMCUAEQEAAbQdSW50ZWMtQ1NJUlQgPGNlcnRAaW50ZWMyLmNvbT6J
AdQEEwEKAD4WIQR36GHM2xCK9FqIrRhBsLDuXBz+7gUCX6lIgQIbAwUJA8JnAAUL
CQgHAgYVCgkICwIEFgIDAQIeAQIXgAAKCRBBsLDuXBz+7mMtC/0YSMrIkV+N4sB3
cPijn9quOSMItWC4iEQ+w0AdjzG2urqIgqZHoBMNOkAnD3UrrMqUERafL8AfrFjt
lTK43579bchVAqJYxnW17gDeOtEUQa48x1V1gnKWHjfQ1NnHZTo7ddZ0Mrrj4ic7
Md14dLhp53eI32iw3VW3pcfexbvQ4GGKEFwl2Bg0b8DurKAbuagbMdxDOuYJER+0
8qIQAQrRxYM9vGt7nUxtZvs2DxZm3qVGMmKnz6P6kRgoYHdZ+eYBtBXUMmeZxbV8
0fQFghWyOjKbKnqMl9yKlcXAHgFj50SyDgbl8WCeiV4CzJtXcUaaz4B5dJy9mBSI
4Keaaq4VBZXdtOtkYwIrPPA+1rpH/SbtoOy8ob85WurL5vDuKkBpMXRDumjKgxd3
FtpIy5cdZpQzwf5qEtSdMkUGHgN1JRAFxnuc6vksQCC5iHjpSQlVb9YHLrklviBW
qeLLvyyWj8iz7FXcKtegjX3lboJLZMIKKp/05HhEhKQQxW+GnEa5AY0EX6IlgQEM
AOHfrBL0S7PZqEeALI90JFT0IgAMvGWXf41idBiY2MofVe6GH0RVUuLwt+gFMGWG
6cNrUYmUWRZ1duwLbQDU9Bdre5lVXCo9Xtrc/2ex8BPS6KqkDWicg0Go+3r7ENjy
vBjP5snX+xbjjxR5sLiDrZYGh/F+FVnaPZfIlLgxjoHOkA1YWnqI5ldwu4JWzLm0
hdzMJSlpqUz3itCH7ubvRzK+crRFUlhPCU5HIfywSk5faSsj0CtJzXpg7MtSmLgb
0q1oJNTwb7ZFOd9rXgnlv6Sx1fNBTEFjBD3AhtCMsQbNjVV/jNGBvWud2BrZKX4e
aOL2Bllr6dWSsJuhG5dWjnmFJqx8joI9UJynN1PgDjcr9hbkCwKsNFcqCTsH4MtB
qQxAPiwMp8adxdL2Lh4CzIealcgvzR6hnthU9lvX43uXDPqvu9ojuTQ/LoF/ow2O
f/v80/06nP85zRwX5bDfRveaCZEndyVIZ5R0U/yPY35tjfMcS7vlUusnr1HK4dpu
awARAQABiQG8BBgBCgAmFiEEd+hhzNsQivRaiK0YQbCw7lwc/u4FAl+pSIECGwwF
CQPCZwAACgkQQbCw7lwc/u5elgwAot7r/lREIeVfKKfZMIywzhLzLk/khVRu4PqI
uCzyndajFrz/t5Tubk3VKY66iL6UdArY2GxA3RvtgxxwsAkWSqhhym7F2M1Zb+B9
0hO+bXVL0ciP7huUjpMsqxKDcowuxEAqE0gJQ3sKsaqdZtK1tI8ic+vxVHSe6o7F
eljtBzZnJCr8C+KZZgLfXNchmrDIGOcKJxZt7uY7KwuYPo6HEkgeEUhHCCIzLbh2
3PgUXDWVcg8BFzVByWanvFjP/gJukQQXTyJU+BSV+eIQqad53hvUlYjjYxKbNIr2
```

QbdBZjsDOCtmvscJNo7SX685ftpCZObetA6wRvi4ZW3Gd4J9ufEb5j7ouA8XoIvd
AtYGBxgjkyDjNcXuXJ0oll0TfTPn4bUhSDTSml1WJuGgoXhLwm6bNsSsdAPUXoif
NhfC5GyorqDHF22SPhkZXlCIBYQUk22fCrQBWdCvq4KNnqVPYH5tv+6RwKwjGIUL
iAtFTEzFNSlFfs6/drc9smy9uUUd
=7VGn
-----END PGP PUBLIC KEY BLOCK-----

5. Services

5.1 CSIRT / SOC Services

Intec-CSIRT has its own SOC where it monitors its customers, helping to prevent incidents, investigate whether an incident occurred and to determine the extent of the incident. It includes the following related services:

- **Security monitoring:** Security monitoring, which is different from networks and systems, is a service that allows the state of a system to be monitored at all times and helps prevent attacks by anticipating them.
- **Incident response:** The objective of this service is to attend, in the shortest possible time and in the most efficient way, any security incident in order to neutralize it and restore the proper functioning of the system.
- **Vulnerability management:** The objective of this service is to search, identify and remedy vulnerabilities in information systems.
- **Anti-fraud:** Analyse the information of attacks to locate the origin, the methods and the technology used in order to prevent more fraud in the future.
- **Threat hunting:** Based on Intec-CSIRT experience and with the help of specialized tools, it is about finding any threat within a system or infrastructure.
- **Data Leak Prevention:** This service is focused on preventing the exfiltration of sensitive information, regardless of its location, towards unauthorized persons.
- **Cyber-intelligence:** It allows to collect information from several different sources to be analysed and evaluated together, finding information that would not be possible otherwise.

5.2 Cybersecurity Lab

Intec-CSIRT has the equipment and specialized personnel to perform the forensic analysis of malware involved in complex incidents. Similarly, the Intec-CSIRT has the ability to perform static and dynamic analysis of code samples to detect harmful code.

It includes the following related services:

- **Malware analysis:** Given a sample of malware, its behavior is analyzed in a controlled environment to determine its scope and origin.
- **Forensic analysis:** The task of a forensic analysis is to analyse a system that has been compromised or that has been used for some illegal activity, in search of information.
- **Data recovery:** An attempt is made to access and extract the information stored on a device that can no longer be accessed, either due to a breakdown or due to accidentally deleting that information.
- **Source code analysis:** Source code is statically and dynamically scanned for security flaws.
- **Reversing:** Reversing allows you to analyse a software sample to know its behaviour and determine its functionality.

5.3 Professional Services

Intec-CSIRT also offers the following related services:

- **Penetration test:** Pentesting, also known as ethical hacking, consists of trying to find security flaws in a system by carrying out controlled attacks against it, acting as an attacker would.
- **Security audit:** Systems are audited for design and implementation errors.
- **Expert services:** The objective is to study in depth a concrete fact, preparing a valid report for a judge with the conclusions obtained.
- **Hardening:** Hardening implies the review and securitization of computer systems to make them more secure and resistant to attacks.
- **Consulting:** Both in a general advice to answer any questions, as for a specific consulting on something specific, the work of an expert in the field is essential to help make the right decisions.
- **Online reputation:** Search, prevent, solve and report on any type of information that affects the online reputation of a client.
- **Deep & Dark web searches:** An investigation and search is carried out throughout the Internet (clear, deep and dark) for information about a specific asset, such as a person, company or concept.
- **Stress and resilience tests:** A system is attacked at the same time that its behaviour is analysed to find out how it would respond to a real attack and to improve its resistance and performance.

6. Incident Reporting Forms

There are no forms to report a security incident. The preferred methods for reporting an incident are defined in point 2.10 of this document or on the web page *<cert.intec2.com>*.

7. Disclaimers

The Intec-CSIRT is not responsible for the misuse that may occur of the information contained herein.