

CSIRT Description for Indra

1. About this document

1.1 Date of Last Update

This is version 0.2, last update 25/09/2026.

1.2 Distribution List for Notifications

Notifications of updates are submitted to our constituency via the established communication channels.

1.3 Locations where this Document May Be Found

The current version of this CSIRT description document is available upon request to CSIRT[AT]Indra[DOT]es.
It will be updated and published soon on the Indra website.

1.4 Authenticating this Document

This document has been signed with Indra CSIRT's PGP key.
The signature is available on public keyservers with ID 0x79D7FB7C.
It will be published soon on the Indra website, as well.

2. Contact Information

2.1 Name of the Team

"Indra CSIRT": the Indra Computer Emergency Response Team.

2.2 Address

Indra CSIRT
Avenida de Bruselas, 35
28108 Alcobendas
Madrid

2.3 Time Zone

Spain (CET/GMT+0100 and CEST/GMT+0200 from April to October)

2.4 Telephone Number

Regular telephone number:
+34 914 805 002

2.5 Facsimile Number

None available

2.6 Other Telecommunication

Videoconference options available upon request.

2.7 Electronic Mail Address

Indra CSIRT electronic mail address
CSIRT[AT]Indra[DOT]es
Mail will be forwarded to the responsible persons

2.8 Public Keys and Other Encryption Information

The Indra CSIRT has the following PGP keys:

Indra CSIRT
CSIRT[AT]Indra[DOT]es
KeyID:0x79D7FB7C
Fingerprint: CF65BD70172C7AC4367DBB7DF8D8797B79D7FB7C

The key and its signature can be found at the usual large public key servers.

2.9 Team Members

This information is classified

2.10 Other Information

General information about the Indra CSIRT will be published on the Indra CSIRT website.

2.11 Points of Customer Contact

The preferred method for contacting the Indra CSIRT is via e-mail . E-mail sent to this address will "biff" the responsible human, or be automatically forwarded to the appropriate backup person, immediately. If you require urgent assistance, put "URGENT" in your subject line.

If it is not possible (or not advisable for security reasons) to use e-mail, the Indra CSIRT can be reached by telephone.

2.12. Operating hours

Incident Response Team is available 24x7x365.

3. Charter

3.1 Mission Statement

The purpose of the Indra CSIRT is to maintain the availability,

integrity and confidentiality of the stored, transmitted or processed information in its employees systems whose security they entrust to Indra CSIRT.

3.2 Constituency

The Indra CSIRT provides various information security services to all the Indra employees.

3.3 Sponsorship and/or Affiliation

The Indra CSIRT is currently requesting the membership to FIRST and CSIRT.es

3.4 Authority

The Indra CSIRT is part of the Cybersecurity department of Indra Company.

4. Policies

4.1 Types of Incidents and Level of Support

The Indra CSIRT is authorized to address all types of computer security incidents which occur, or threaten to occur, at its employees systems.

Indra CSIRT will always provide consultancy and incident response services to any employees who requires them, whatever SLA is defined,
as long as it is possible in time and resources.

4.2 Co-operation, Interaction and Disclosure of Information

Indra CSIRT will cooperate with other organizations in the field of computer security. It can exchange information regarding security incidents and vulnerabilities, when necessary.

Private information about its employees will never be shared without express consent.

4.3 Communication and Authentication

Regular e-mail or telephone are considered appropriate for transmission of low-sensitivity data, which would be most of the cases. If it is necessary to exchange confidential information, PGP (or other encryption system) will be used.

5. Services

5.1 Reactive Services

5.1.1 Incident Response

Indra CSIRT will assist its constituency in handling the technical and organizational aspects of incidents. In particular, it will provide assistance or advice with respect to the following aspects of incident management:

5.1.1.1 Incident Triage

- Investigating whether indeed an incident occurred.
- Determining the extent of the incident.

5.1.1.2 Incident Coordination

- Determining the initial cause of the incident (vulnerability exploited).
- Facilitating contact with other sites which may be involved.
- Facilitating contact with appropriate security services and/or appropriate law enforcement officials, if necessary.
- Making reports to other CSIRTs.
- Composing announcements to users (members of the constituency), if applicable.

5.1.1.3 Incident Resolution

- Removing the vulnerability.
- Securing the system from the effects of the incident.
- Evaluating whether certain actions are likely to reap results in proportion to their cost and risk, in particular those actions aimed at an eventual prosecution or disciplinary action: collection of evidence after the fact, observation of an incident in progress, setting traps for intruders, etc.
- Collecting evidence where criminal prosecution, or disciplinary action, is contemplated.

5.1.2 Artifact Handling

An artifact is any file or object found on a system that might be involved in probing or attacking systems and networks or that is being used to defeat security measures. Artifacts can include but are not limited to computer viruses, Trojan horse programs, worms, exploit scripts, and toolkits. Artifact handling involves receiving information about and copies of artifacts that are used in intruder attacks, reconnaissance, and other unauthorized or disruptive activities. Once received, the artifact is reviewed. This includes analyzing the nature, mechanics, version, and use of the artifacts; and developing (or suggesting) response strategies for detecting, removing, and defending against these artifacts. Since this service is further

categorized based on the type of activities performed and the type of assistance given as follows:

5.1.2.1 Artifact analysis

The CSIRT performs a technical examination and analysis of any artifact found on a system. The analysis done might include identifying the file type and structure of the artifact, comparing a new artifact against existing artifacts or other versions of the same artifact to see similarities and differences, or reverse engineering or disassembling code to determine the purpose and function of the artifact.

5.1.2.2 Artifact response

This service involves determining the appropriate actions to detect and remove artifacts from a system, as well as actions to prevent artifacts from being installed. This may involve creating signatures that can be added to antivirus software or IDS.

5.1.2.3 Artifact response coordination

This service involves sharing and synthesizing analysis results and response strategies pertaining to an artifact with other researchers, CSIRTs, vendors, and other security experts. Activities include notifying others and synthesizing technical analysis from a variety of sources. Activities can also include maintaining a public or constituent archive of known artifacts and their impact and corresponding response strategies.

6. Incident Reporting Forms

Use the following template and send it by email to the appropriate address. Please, provide as much detail as possible and attach any relevant file (log, email, image...):

=====

INCIDENT REPORT

Your contact information

- Name:
- Email address:
- Telephone number:

Project information

- Name of the project / program:
- Project code:
- Type of project: development / production / laboratory

- Market:
- Cross:
- Affected clients:

Incident Information

- Type of incident detected (Phishing, Malware, DDoS, Unauthorized use/access...):
- When, approximately, did the incident start? (Provide datetime and timezone):
- When was this incident detected? (Provide datetime and timezone):
- Incident Description (Please enter a brief description of the incident):
- Other relevant information:

=====

7. Disclaimers

While every precaution will be taken in the preparation of information, notifications and alerts, Indra CSIRT assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.