1. Document Information

1.1 Date of last update

This is version 1.0 as of November 10, 2023

1.2 Mailing list for notifications

Changes to this document are not distributed by a mailing list. If you have any specific questions or comments, please contact us at csirt@micitt.go.cr

2. Contact Information

2.1 Team Name

Computer Security Incident Response Center
(CSIRT-CR)

2.2 Time zone

UTC / GMT -6 hours

2.3 Other telecommunications

No

2.4 Email

Incident Reporting: csirt@micitt.go.cr
Public Key: Download through this ***link***
Public Key Fingerprint: FF7A 4868 967E 0C46 3835 B1F5 DC3C 835A AF08 90FD

General information: csirt@micitt.go.cr

2.5 Team Members

A full list of CSIRT-CR team members is not publicly available. Team members will identify themselves to the reporting party by their full name in an official communication about an incident.

2.6 Other information

Information related to cybersecurity issues and by the CSIRT-CR and about the organization itself is published on the web portal www.micitt.go.cr

2.7 Customer contact information

In any case, please use the email address csirt@micitt.go.cr. Our regular response hours are 24/7.

3. Letter

3.1 Mission

The CSIRT-CR is the Computer Security Incident Response Center, created by Decree No. 37052-MICIT on March 9, 2012. Its mission is to promote science, technology, innovation and telecommunications through public policies for the benefit of Costa Rican society. "https://www.micitt.go.cr/micitt/mision-y-vision#:~:text=Impulsar%20la%20ciencia%2C%20tecnolog%C3%ADa%2C%20innovaci%C3%B3n,beneficio%20de%20la%20sociedad%20costarricense."

3.2 Community Served

The incidents dealt with by the CSIRT-CR will be those that affect Public Sector systems or Companies of strategic interest, as well as any other system in which classified information is processed.

3.3 Sponsorship and/or affiliation

CSIRT-CR is the Costa Rican government's Computer Security Incident Response Center. Aimed at preventing incidents related to ICT and the internet. It is part of the Ministry of Science, Innovation, Technology and Telecommunications, it is made up of the director of cybersecurity and cybersecurity analysts.

3.4 Authority

The main objective is the coordination of the response to incidents and the proper management that the constituents must have, as such we advise.

4. Policies

4.1 Types of incidents and level of support

The CSIRT-CR handles different types of incidents and their hazard determination criteria, the level of support will depend on both factors and the severity determined by the CSIRT-CR staff.

4.2 Cooperation, interaction and dissemination of information

CSIRT-CR handles all information confidentially regardless of its priority. Information of a highly sensitive nature is only communicated and stored in a secure environment and, if necessary, using encryption technologies. All information provided to CSIRT-CR will be used to help resolve security incidents. Information will only be distributed to other teams and members on a need-to-know basis and preferably anonymously. The CSIRT-CR uses the TLP for information exchange.

4.3 Communication and authentication

The preferred method of communication is via email.

5. Services

5.1 Incident response provides 24/7 readiness to coordinate recovery from all types of ICT-related incidents and consists of expertise, tools and other capabilities to act, analyze and communicate with stakeholders and the media.

5.1.1 Incident Classification

- Investigate whether an incident did occur.
- Determination of the extent of the incident.
- Evaluation and comparison of the incident with historical data.

5.1.2 Incident Coordination

- Determine the initial cause of the incident.
- Facilitate contact with other sites that may be involved.
- Communicate with stakeholders and the media.

5.1.3 Incident Resolution

- Provide advice to the reporting party that will help eliminate the vulnerabilities that caused the incident and protect systems from the effects of incidents.

- Evaluate what actions are most appropriate to provide the desired results with respect to incident resolution.

- Provide assistance in gathering evidence and interpreting data when necessary.

5.2. Proactive activities

5.2.1 Prevention and preparedness consist of all activities aimed at reducing the likelihood or impact of an incident on constituents. CSIRT-CR provides constituents with current information and advice on new threats and attacks that may have an impact on their operations and seeks to build awareness and skills in employees. CSIRT-CR provides alerts and actionable advice to the public and small businesses through the Technical Alerts service.

6. Incident Reporting Forms

To report incidents, please send communication: csirt@micitt.go.cr.

7. Disclaimer

CSIRT-CR takes every precaution in the preparation of information, notifications, alerts and reports, but assumes no responsibility for errors or omissions, or for damages resulting from the use of the information provided.