RFC 2350

1. Document Information

This document adheres to RFC 2350 - Expectations for Computer Security Incident Response

1.1 Last update date

1.0 Version August 8, 2024, publishing date

1.2 Notification distribution list

When created, the new versions will replace the previous ones, so the updated version will be in:
https://www.grupoice.com/wps/portal/ICE/Transparencia/informacionn

and in:
https://www.kolbi.cr/wps/portal/kolbi_dev/terminosycondiciones/

Update notifications will be sent to all CSIRT-ICE members' e-mail.

1.3 Document

The last document version is publicly available in the web site:

https://www.grupoice.com/wps/portal/ICE/Transparencia/informacionn

and in:

https://www.kolbi.cr/wps/portal/kolbi_dev/terminosycondiciones/

2. Contact Information

2.1 Team name

CSIRT-ICE, CSIRT Instituto Costarricense de Electricidad

2.2 Address

Instituto Costarricense de Electricidad, ICE, Edificio Jorge Manuel Dengo, Sabana Norte, San José, Costa Rica.

2.3 Time Zone

CST (Central Standard Time) in Costa Rica: UTC-6

2.4 Telephone Number

Not publicly disclosed.

2.5 Fax Number

None

2.6 Other media

None

2.7 E-mail addresses

Incidents Management and Reports related to CSIRT-ICE scope: csirt@ice.go.cr

Other general issues:
https://www.grupoice.com/wps/portal/ICE/contactenos/inicio-contactenos

2.8 Public keys and information encryption

PGP encryption is used by CSIRT-ICE in each and all its e-mail communications related to information security incidents management and reports, so required due to its confidentiality level. Contact: csirt@ice.go.cr

See public key below:

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

mDMEZU6irBYJKwYBBAHaRw8BAQdAkUO/PL1wHpECvKNAMthf2MAo87TDz+tKq8bb
82XjsVC0QEVxdWlwb3MgZGUgUmVzcHVlc3RhIGEgSW5jaWRlbnRlcyBkZSBTZWd1
cmlkYWQgPGNzaXJ0QGljZS5nby5jcj6ImQQTFgoAQRYhBLmyiNO8g0l25MQgCTFo
p/NdTCPxBQJlTqKsAhsDBQkFpLj0BQsJCAcCAiICBhUKCQgLAgQWAgMBAh4HAheA
AAoJEDFop/NdTCPxBwIA/i2iTrYW369mBqtxX3N8V+HdNtgPktOtxhyhYDKPNwQw
AP0TEcMKj9s0qWDR8V/XJWf0XQ7rfG9z5Nht1E9bwWAZA7g4BGVOoqwSCisGAQQB
l1UBBQEBB0Dy5NqwFTlwxvLBns9pnqwuCjbYxkFzMkPlNM1dy1jiVgMBCAeIfgQY
FgoAJhYhBLmyiNO8g0l25MQgCTFop/NdTCPxBQJlTqKsAhsMBQkFpLj0AAoJEDFo
p/NdTCPx25gA/3HeQWiyKu4dwwnxEeydhHfyKxt0TDKmPv7C9B4wNVdmAQCJysOY
FIBufmNEDhFD1z65WIiEcL5LoZbE09OuNiN2CA==
=7fRi
-----END PGP PUBLIC KEY BLOCK-----

2.9 Team members

Not publicly disclosed

2.10 Supplementary Information

Additional cybersecurity information in:
https://www.kolbi.cr/wps/portal/kolbi_dev/negocios/kolbi-empresas/seguridad/ciberseguridad/

2.11 Customer Care Contacts

E-mail is the main communication tool.

For general inquiries: csirt@ice.go.cr
For information security incidents management and reports:

1) from 7:00 – 16:36: csirt@ice.go.cr
2) out of office hours: slico@ice.go.cr
3) For Corporate (Business) Customers: 800-Empresa (800-367 7372) or through the means referred to in the Agreement

CSIRT-ICE operates 24/7/365

3. Organization

3.1 Mission

ICE, Instituto Costarricense de Electricidad is a government owned company created by Decree under the Law No 449, April 8, 1949.

More than eleven (11) years of cyberspace and cybersecurity issues experience characterizes CSIRT-ICE, ICE 'specialized response leading area, responsible of handling information security incidents. Consequently, this experience and leadership grant it an outstanding role, both nationally and internationally.

CSIRT-ICE mission is to provide ICE and its customers with a reliable and secure network and digital environment for their activities and services development as well as to give an effective handling of the response and recovery when facing information security incidents (which allows a high level of cyber resilience)

3.2 Scope

CSIRT-ICE scope is to provide tactical and technical support to the technological Infrastructure (IT or Operational field) managers with the purpose of solving IT security incidents.

Besides, CSIRT-ICE provides specific services to a group of external customers, particularly to those in the corporate context. Task which is considered confidential pursuant to the in-force agreements.

CSIRT-ICE structure is made on a Governmental, public and private basis

3.3 Sponsorship and/or Affiliation

CSIRT-ICE, the area that belongs to Instituto Costarricense de Electricidad, stands out as a national leader that provides electricity, connectivity and sustainable secure digital services to the Costa Rican population.

It is a well-established company responsible of providing convergent solutions duly aligned to **Revolución 4.0** version.

3.4 Authority

CSIRT-ICE, with headquarters in the facilities of Instituto Costarricense de Electricidad, has the appropriate know how to coordinate all the issues related to information security, and whose responsibility is to prevent as well as to respond to the cybersecurity incidents, which may affect not only the digital context but also ICE´s assets.

4. Policies

4.1 Incident types and support level

Support level offered by CSIRT-ICE may vary according to the incident type and severity or security problem, the component type, the infrastructure impact relevance or crucial or essential service and availability, at that time, of CSIRT-ICE resources.

All potential cyber security incidents reported are labeled as normal priority unless they are explicitly labeled as Emergency, Urgent or Highly Crucial, or in case CSIRT-ICE team classifies them as relevant.

Services provided by CSIRT-ICE are described in section 5.

4.2 Information disclosure, cooperation and integration

CSIRT-ICE cooperates, in the cyber security sector and pursuant to an agreement, with other national and international organizations and entities, such as security providers, governmental entities, national security teams, national law enforcement entities, academic and technological partners and customers.

The aforementioned cooperation includes threat, vulnerabilities and incidents information exchange.

By sharing information with third parties, the principles of minimum necessary information are fulfilled, so that only the required information, which allows to prevent an incident and amend its negative effects, is provided.

All the information handled by CSIRT-ICE, related to cybersecurity, is treated as confidential, pursuant to ICE´s policies and procedures as well as with the applicable Costa Rican regulation. Therefore, data security and liability handling are resolutely protected through encryption, policies and data access controls as well as by using other up to date cybersecurity methodologies and state of the art technology.

CSIRT-ICE supports Sharing Traffic Light Protocol (ISTLP, see ISTLP-v1.1-approved (trusted-introducer.org) which guarantees the appropriate labeled information handling.

When exchanging sensitive information or reporting a sensitive incident you are kindly required to explicitly indicate it, by using the appropriate label in the e-mail "Subject line", and preferably through encryption. ICE also must use the settled and communicated mechanisms for this purpose.

4.3 Communication and Authentication

CSIRT-ICE communication channels are detailed in 2.8

In case of non-confidential information (public information) CSIRT-ICE uses the regular methods, generally non encrypted e-mails. Otherwise, to guarantee sensitive information communications confidentiality, PGP encrypted e-mails will be used.

5. Services

CSIRT-ICE services are available 24/7/365.

Besides, find commercial and corporate services/solutions in https://www.kolbi.cr/wps/portal/kolbi_dev/negocios/kolbi-empresas/seguridad/ciberseguridad

5.1 Incident Response

All IT and operations incidents are assessed, then, a professional and technical experts' team will provide the incidents detailed analysis.

5.1.1 Triage

It refers to Incident severity assessment and the coordination with the involved parties to block and respond, pursuant to the pertinent priority, including when applicable escalating. If necessary, and the opportune communication (crisis handling).

5.1.2 Coordination

Incident information classification (file/records, information contacts and so on) pursuant to the information disclosure policies.

5.1.3 Solution

Technical and operational support for the different stages in the information security incidents handling process.

5.2 Proactivity

Based on those services provided to reduce the occurrence, on the one, of an information security incident probability and on the other hand, to increase its detection probability. It considers all the activities/tasks created to be prepared for potential threats, by improving current controls and security baselines.

- ✓ Awareness raising and training
- ✓ Security assessments (ethical hacking audits)
- ✓ Vulnerabilities Detection (vulnerabilities analysis and handling)
- ✓ Cybersecurity warnings/alerts

6. Notification Incidents

A PGP encrypted e-mail is required to notify cybersecurity incidents.

7.Liability disclaimer

The guidelines for the pertinent sensitive information handling, be it as notifications, reports, warnings and general information submitted to CSIRT-ICE, as well as the stated mechanisms and formats for the pertinent transfer, are stated herein. All the above is for the purpose of guaranteeing information protection. Therefore, CSIRT-ICE is exempted for faults or omissions therein.