RFC 2350

1. Información del documento

Este documento cumple con RFC 2350 - Expectations for Computer Security Incident Response

1.1. Fecha de la última actualización

Versión 1.0, publicada el 1 marzo 2024.

1.2. Lista de distribución para notificaciones

Las nuevas versiones, cuando se generen, sustituirán a la anterior y se mantiene actualizado en https://www.grupoice.com/wps/portal/ICE/Transparencia/informacionn y https://www.kolbi.cr/wps/portal/kolbi_dev/terminosycondiciones/

Las notificaciones de actualizaciones se remitirán por correo electrónico a todos los miembros del CSIRT-ICE.

1.3. Ubicación del documento

La última versión del documento es accesible públicamente a través del sitio web https://www.grupoice.com/wps/portal/ICE/Transparencia/informacionn y https://www.kolbi.cr/wps/portal/kolbi_dev/terminosycondiciones/

2. Información de contacto

2.1. Nombre de equipo

CSIRT-ICE, CSIRT Instituto Costarricense de Electricidad

2.2. Dirección

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

2.3. Zona horaria

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

2.4. Número de teléfono

No divulgado en medios públicos

2.5. Numero de fax

No existente

2.6. Otras comunicaciones

No existente

2.7. Direcciones de correo electrónico

Reporte y gestión de incidentes que se relacionan con la circunscripción de CSIRT-ICE: csirt@ice.go.cr

Otras comunicaciones generales: https://www.grupoice.com/wps/portal/ICE/contactenos/inicio-contactenos

2.8. Claves públicas y cifrado de información

El CSIRT-ICE emplea el cifrado PGP en todas las comunicaciones por correo electrónico referente a reporte y gestión de incidentes de seguridad de la información que, dado su nivel de confidencialidad, así lo requieren; para ello dispone csirt@ice.go.cr

Ver clave pública aquí:

-----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. Miembros del equipo

No divulgado en medios públicos

2.10. Otra información

Puede encontrar más información sobre ciberseguridad en: https://www.kolbi.cr/wps/portal/kolbi_dev/negocios/kolbi-empresas/seguridad/ciberseguridad/

2.11. Puntos de contacto del cliente

El canal de comunicación principal es el correo electrónico.

Para consultas generales, puede enviar correo a csirt@ice.go.cr
Para reporte y gestión de incidentes de seguridad de la información csirt@ice.go.cr, en horario 7:00 – 16:36, fuera de este horario se dispone de slico@ice.go.cr.

El horario de funcionamiento del CSIRT-ICE es 24/7/365.

Cliente empresarial (Negocios) puede solicitar asistencia llamando a 800-Empresa (800-3677372), o bien los medios indicados contractualmente.

3. Constitución

3.1. Misión

El CSIRT-ICE es la unidad de respuesta a incidentes de seguridad de la información regente y especializada adscrita al Instituto Costarricense de Electricidad (ICE); con más de 11 años de experiencia en temas del ciberespacio y ciberseguridad. Es un referente a nivel nacional e internacional.

Su misión es propiciar a la Institución y clientes un entorno de red y espacio digital seguro y confiable para el desarrollo de sus actividades y servicios, brindando una gestión efectiva en la respuesta y recuperación ante eventos e incidentes de seguridad de la información, permitiendo alcanzar un alto nivel de ciber resiliencia.

3.2. Circunscripción

La circunscripción del CSIRT-ICE está comprendida a nivel Institucional, brindando el apoyo táctico y técnico a los administradores de infraestructura tecnológica, sea esta tecnología de la información u operativa, para la resolución de incidentes de seguridad informática.
CSIRT-ICE brinda servicios específicos a un gran grupo de clientes externos, particularmente en el ámbito empresarial, se mantiene confidencial debido a los contratos vigentes.

3.3. Patrocinio y/o Afiliación

El CSIRT-ICE es una unidad que forma parte del Instituto Costarricense de Electricidad (ICE), referente nacional en brindar energía, conectividad y servicios digitales seguros y sostenibles a los habitantes de Costa Rica.

Empresa consolidada en soluciones convergentes alineadas a la **Revolución 4.0.**

3.4. Autoridad

CSIRT-ICE, con sede en las instalaciones del Instituto Costarricense de Electricidad (ICE), posee las facultades suficientes para coordinar todo lo relacionado con la materia de seguridad informática, el cual trabaja para prevenir y responder ante los incidentes de seguridad cibernética que afecten al entorno digital y patrimonio del ICE.

4. Políticas

4.1. Tipos de incidentes y nivel de soporte

El nivel de soporte brindado por CSIRT-ICE variará según el tipo y la gravedad del incidente o problema de seguridad, el tipo de componente, la importancia del impacto en la infraestructura o servicio crítico o esencial y nuestros recursos disponibles en el momento.

Todos los posibles incidentes de seguridad cibernética reportados se consideran prioridad normal a menos que estén etiquetados explícitamente como Emergencia, Urgente, o Criticidad Alta, o bien que nuestros equipos los clasifiquen como importantes.

Los servicios ofrecidos por CSIRT-ICE se describen en la sección 5.

4.2. Cooperación, interacción y divulgación de información

CSIRT-ICE coopera con otras organizaciones y entes nacionales e internacionales en el campo de ciberseguridad, como proveedores de seguridad, entidades gubernamentales, equipos de seguridad nacionales, fuerzas del orden nacional, socios tecnológicos y académicos, y clientes donde medie un contrato.

Esta cooperación incluye el intercambio de información sobre el panorama de amenazas, vulnerabilidades, eventos/incidentes.

Al compartir información con terceras partes, se siguen los principios de mínima información necesaria, para proporcionar solo la información absolutamente necesaria que permitan prevenir un incidente y remediar sus consecuencias adversas.

TODA la información manejada por el CSIRT-ICE concerniente al ámbito de ciberseguridad es tratada con absoluta confidencialidad en congruencia con las políticas y procedimientos del Instituto Costarricense de Electricidad y la regulación nacional aplicable.

El manejo de los datos es de forma segura y confiable, están protegidos sólidamente mediante cifrado, políticas y controles de acceso a los datos y mediante la aplicación de otras metodologías modernas de ciberseguridad y tecnología de punta.

CSIRT-ICE admite el Sharing Traffic Light Protocol (ISTLP, ver detalle en ISTLP-v1.1-approved (trusted-introducer.org)), por lo que la información etiquetada se manejará de manera apropiada.

Se solicita encarecidamente que al intercambiar información de carácter sensible o al informar un incidente de naturaleza sensible indicarlo explícitamente, utilizando la etiqueta correspondiente en el campo de asunto del correo electrónico, y en la medida de lo posible, emplear la encriptación. A nivel Institucional, circunscripción interna, debe utilizar el mecanismo establecido y comunicado para tal fin.

4.3. Comunicación y autenticación

Los medios disponibles para la comunicación con CSIRT-ICE se detallan en el punto 2.8.

CSIRT-ICE utiliza métodos convencionales, principalmente correo electrónico sin cifrar cuando la información sea pública, es decir, no confidencial. En contraste, para garantizar la seguridad de las comunicaciones que involucren información sensible se utilizará correo electrónico cifrado con PGP.

5. Servicios

Los servicios del CSIRT-ICE están disponibles 24/7/365 para nuestra circunscripción.

CSIRT-ICE también ofrece servicios y soluciones comerciales/empresariales que se describen en https://www.kolbi.cr/wps/portal/kolbi_dev/negocios/kolbi-empresas/seguridad/ciberseguridad

5.1. Respuesta a incidentes

Se evalúan todas las incidencias relacionadas con las tecnologías de la información y operativas. Expertos técnicos y profesionales proporcionan un análisis en profundidad.

5.1.1. *Triaje*

Evaluación de la gravedad del incidente y la articulación con las partes involucradas para la contención y respuesta; acorde a la priorización. Incluye los escalamientos en caso de ser necesarios y la comunicación que corresponda (manejo de la crisis).

5.1.2. Coordinación

Categorización de la información relativa con el incidente (archivos de registro, contactos de información, entre otros) conforme a las políticas de divulgación de la información.

5.1.3. Resolución

Apoyo técnico y operativo en las distintas etapas del proceso de manejo de incidentes de seguridad informática.

5.2. Actividades proactivas

Radica en servicios para disminuir la probabilidad de que suceda un incidente de seguridad informática y aumentar la posibilidad de su detección, mediante actividades que permitan prepararse ante posibles amenazas, mejorando controles y las líneas base de seguridad existentes.

- ✓ Concienciación y formación.
- ✓ Evaluaciones de seguridad (auditorias de hacking ético).
- ✓ Descubrimiento de vulnerabilidades (análisis y gestión de vulnerabilidades).
- ✓ Avisos y alertas de ciberseguridad.

6. Formas para la notificación de incidentes

Para informar un incidente de seguridad cibernética utilice correo electrónico con cifrado PGP.

7. Descargo de responsabilidad

El presente documento establece las pautas para la gestión apropiada de la información sensible en las notificaciones, reportes, alertas e información en general remitida al CSIRT-ICE, así como los canales y formatos definidos para su adecuada transferencia, con el fin de procurar la protección de la información; por lo tanto, eximen al CSIRT-ICE por errores u omisiones contenidos en ellos.