



## 1. Información del documento

### 1.1 Fecha de la última actualización

Esta es la versión 1.0 del 10 de noviembre de 2023

### 1.2 Lista de distribución para notificaciones

Los cambios a este documento no se distribuyen por una lista de correo. Cualquier pregunta o comentario específico, por favor diríjase a la dirección de correo [csirt@micitt.go.cr](mailto:csirt@micitt.go.cr)

## 2. Información de contacto

### 2.1 Nombre del equipo

Centro de Respuesta a Incidentes de Seguridad Informática  
(CSIRT-CR)

### 2.2 Zona horaria

UTC / GMT -6 horas

### 2.3 Otras telecomunicaciones

Ninguna

### 2.4 Correo electrónico

Reporte de incidentes: [csirt@micitt.go.cr](mailto:csirt@micitt.go.cr)

Llave pública: Descarga en este [enlace](#)

Huella digital: FF7A 4868 967E 0C46 3835 B1F5 DC3C 835A AF08 90FD

Información de carácter general: [csirt@micitt.go.cr](mailto:csirt@micitt.go.cr)

### 2.5 Miembros del equipo

Una lista completa de los miembros del equipo CSIRT-CR no está disponible públicamente. Los miembros del equipo se identificarán ante la parte informante con su nombre completo en una comunicación oficial sobre un incidente.



## 2.6 Otra información

La información relacionada con temas de ciberseguridad y por el CSIRT-CR y sobre el propio organismo se encuentran publicadas en el portal web [www.micitt.go.cr](http://www.micitt.go.cr)

## 2.7 Puntos de contactos con el cliente

En cualquier caso, utilice la dirección de correo [csirt@micitt.go.cr](mailto:csirt@micitt.go.cr). Nuestro horario de respuesta regular es con un horario de 24 horas los 7 días de la semana.

## 3. Carta

### 3.1 Misión

El CSIRT-CR es el Centro de Respuesta a Incidentes de Seguridad Informática, creado mediante el decreto N° 37052-MICIT el 9 de marzo del 2012. Su misión es impulsar la ciencia, tecnología, innovación y telecomunicaciones a través de políticas públicas para el beneficio de la sociedad costarricense.

["https://www.micitt.go.cr/micitt/mision-y-vision#:~:text=Impulsar%20la%20ciencia%2C%20tecnolog%C3%A9a%20innovaci%C3%B3n,beneficio%20de%20la%20sociedad%20costarricense."](https://www.micitt.go.cr/micitt/mision-y-vision#:~:text=Impulsar%20la%20ciencia%2C%20tecnolog%C3%A9a%20innovaci%C3%B3n,beneficio%20de%20la%20sociedad%20costarricense.)

### 3.2 Comunidad atendida

Los incidentes atendidos por el CSIRT-CR serán aquellos que afecten a sistemas de Sector Público o Empresas de interés estratégico, así como cualquier otro sistema en el que se procese información clasificada.

### 3.3 Patrocinio y/o afiliación

CSIRT-CR es el Centro de Respuesta a Incidentes de Seguridad Informática del gobierno costarricense. Dirigido a prevenir incidentes relacionados con las TIC y la internet. Es parte del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, está formado por el director de ciberseguridad y analistas de ciberseguridad.



### **3.4 Autoridad**

El objetivo principal es la coordinación de la respuesta a incidentes y el manejo adecuado que deben tener los constituyentes como tal asesoramos.

## **4. Políticas**

### **4.1 Tipos de incidentes y nivel de soporte**

El CSIRT-CR maneja diferentes tipos de incidentes y sus criterios de determinación de peligrosidad, el nivel de apoyo dependerá de ambos factores y de la gravedad que determine el personal del CSIRT-CR.

### **4.2 Cooperación, interacción y divulgación de información**

CSIRT-CR maneja de manera confidencial toda la información sin importar su prioridad. Aquella información de naturaleza muy sensible solo se comunica y almacena en un entorno seguro y en caso de ser necesario utilizando tecnologías de cifrado. Toda la información suministrada al CSIRT-CR será utilizada para ayudar a resolver incidentes de seguridad. La información solo se distribuirá a otros equipos y miembros según la necesidad de saber y preferiblemente de forma anónima. El CSIRT-CR utiliza el TLP para el intercambio de información.

### **4.3 Comunicación y autenticación**

El método preferido de comunicación es por correo electrónico.

## **5. Servicios**

**5.1** La respuesta a incidentes proporciona disponibilidad 24/7 para coordinar la recuperación de todo tipo de incidentes relacionados con las TIC y consiste en experiencia, herramientas y otras capacidades para actuar, analizar y comunicarse con las partes interesadas y los medios de comunicación.

### **5.1.1 Clasificación del incidente**

- Investigar si efectivamente ocurrió un incidente.
- Determinación de la extensión del incidente.
- Evaluación y comparación del incidente con históricos.

### **5.1.2 Coordinación de incidentes**



- Determinar la causa inicial del incidente.
- Facilitar el contacto con otros sitios que puedan estar involucrados.
- Comunicarse con las partes interesadas y los medios

### **5.1.3 Resolución de incidentes**

- Brindar asesoramiento a la parte informante que ayudará a eliminar las vulnerabilidades que causaron el incidente y proteger los sistemas de los efectos de los incidentes.
- Evaluar qué acciones son más adecuadas para proporcionar los resultados deseados con respecto a la resolución del incidente.
- Proporcionar asistencia en la recopilación de pruebas y la interpretación de datos cuando sea necesario.

## **5.2. Actividades proactivas**

**5.2.1** La prevención y la preparación consisten en todas las actividades destinadas a reducir la probabilidad o el impacto de un incidente para los constituyentes. CSIRT-CR proporciona a los constituyentes información actual y asesoramiento sobre nuevas amenazas y ataques que pueden tener un impacto en sus operaciones y busca crear conciencia y habilidades en los empleados. CSIRT-CR proporciona alertas y consejos prácticos al público y a las pequeñas empresas a través del servicio de alertas técnicas.

## **6. Formularios de notificación de incidentes**

Para informar incidentes enviar comunicación: [csirt@micitt.go.cr](mailto:csirt@micitt.go.cr).

## **7. Descargo de responsabilidad**

EL CSIRT-CR toma todas las precauciones en la preparación de información, notificaciones, alertas e informes, pero no asume ninguna responsabilidad por errores u omisiones, ni por daños resultantes del uso de la información suministrada.