Ciberseguridad, conciencia y retos para el Gobierno de Costa Rica

Edgar Mora R.
CSIRT-CR

2018.04.30

Agenda

- CSIRT-CR
- ¿Qué estamos haciendo?
- Retos para el Gobierno

¿Qué es Ciberseguridad?

La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas y tecnologías que pueden utilizarse para proteger los activos de la organización y a los usuarios en el ciberespacio.

¿Qué es un CSIRT?

CSIRT = Computer Security Incident Response Team

Tradicionalmente se define un CSIRT como un equipo o una entidad dentro de un organismo o de forma independiente que ofrece servicios y soporte a un grupo en particular o comunidad objetivo, con la finalidad de prevenir, gestionar y responder a incidentes de seguridad de la información.

Conceptos importantes

Ámbitos de los CSIRT

Existen centenas de CSIRT en el mundo que varían en su misión y en su alcance. Una de las maneras más importantes de clasificar a los CSIRT es agruparlos por la comunidad o por el sector al que le prestan servicios.

CSIRT Nacionales	CSIRT Académicos	CSIRT Comerciales	CSIRT Militar
CSIRT Financieros	CSIRT Proveedores	CSIRT PYMES	CSIRT Infra. Críticas

Servicios proactivos

Servicios de monitoreo y alertas

- Monitoreo externo
- Monitoreo interno
- Desarrollo de herramientas de seguridad
- Reportes y alertas de seguridad

Servicios de investigación y desarrollo

- Auditorías de seguridad
- Escaneo de vulnerabilidades
- Escaneo de artefactos maliciosos
- Monitoreo de tecnología
- Análisis de artefactos
- Análisis forense

OWASP
Open Web Application Security Project

Servicios reactivos

Gestión de incidentes

- Análisis post mortem
- Asistencia en el sitio

Respuesta a vulnerabilidades

Respuesta a artefactos maliciosos

Servicios de valor agregado

- Capacitación y educación
- Concienciación
- Análisis de riesgos y continuidad de negocio
- Apoyo a emprendimientos de seguridad

CSIRT-CR

Decreto ejecutivo N° 37052-MICIT publicado en La Gaceta N° 72 del 13 de Abril 2012

"Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT-CR)", con sede en el Ministerio de Ciencia y Tecnología, "con facultades suficientes para coordinar con los poderes del Estado, instituciones autónomas, empresas y bancos del Estado todo lo relacionado con la materia de seguridad informática y cibernética y concretar el equipo de expertos en seguridad de las Tecnologías de la Información que trabajará para prevenir y responder ante los incidentes de seguridad cibernética e informática que afecten a las instituciones gubernamentales."

Dos proyectos, un objetivo

CSIRT ≠ Estrategia Nacional de Ciberseguridad

Modelo coordinador

- Instituciones de Gobierno, DIS, Poder Judicial
- Universidades
- Bancos
- Municipalidades
- NIC.CR
- ISP
- CSIRTs Nacionales
- CSIRTs Internacionales

Servicios básicos

Los servicios iniciales recomendados para un CSIRT Nacional según la Organización de Estados Americanos son:

- La gestión de incidentes
- La gestión de vulnerabilidades
- La publicación de alertas y la formación
- El monitoreo del sistema

OWASP
Open Web Application Security Project

Qué estamos haciendo?

- Estrategia Nacional de Ciberseguridad
- Proyecto: Creación de una Trayectoria Profesional en Seguridad Digital
- Proyecto: Análisis de vulnerabilidades en sitios web del Gobierno
- CSIRTamericas.org
- Identificación de contactos
- Fortalecimiento de colaboración con otras entidades
- Identificación de infraestructuras
- Desarrollo de protocolo de atención de incidentes de ciberseguridad

OWASP
Open Web Application Security Project

Retos del Gobierno

- Sensibilización, educación y capacitación
- Desarrollar respuestas colaborativas
- Compartir información
- Revisar el marco legal
- Alianzas público-privadas
- Implementación de la Estrategia Nacional de Ciberseguridad

Muchas gracias…

Edgar Mora R.
edgar.mora@micitt.go.cr
csirt@micitt.go.cr