Tutorial de Seguridad LACNIC 38 - LACNOG 2022

Guillermo Pereyra - Analista de Seguridad del CSIRT de LACNIC

Graciela Martínez - Líder del CSIRT de LACNIC



lacnic Csirt

Centro de Respuesta a Incidentes de Seguridad



Agenda

- Incidente vs vulnerabilidad
- ¿ Qué es un CSIRT ?
- Framework de servicios del FIRST
- Modelo de Madurez - SIM3
- CSIRT de LACNIC

Incidentes y vulnerabilidades

- ***Vulnerabilidad***: debilidad o falla que está presente en un sistema informático, que puede ser aprovechada con fines maliciosos

- ***Incidente de seguridad***:
  - Vulnerabilidad que ha sido o está siendo explotada, causando algún tipo de daño o perjuicio a una organización o a terceros vinculados con ella.
  - Cualquier acto que viole una Política de Seguridad de la Información de una organización, afectando la confidencialidad, integridad o disponibilidad de uno o varios de sus servicios o activos.

¿Qué es un CSIRT?

¿ Qué es un CSIRT ?

Computer Security Incident Response Team

CSIRT (por sus siglas en inglés)

“ Es un *equipo de expertos en seguridad* de TI, responsable de gestionar la respuesta a incidentes y/o amenazas de seguridad que afecten sistemas informáticos dentro de una comunidad objetivo o *“constituency”* ”

Fuente:
https://www.first.org/resources/guides/

lacnic csirt
Centro de Respuesta a Incidentes de Seguridad

¿ Qué es un CSIRT ? (cont.)

Objetivos generales

- Minimizar y controlar el daño ocasionado por un incidente de seguridad
- Colaborar en las actividades de recuperación de un ataque
- Realizar actividades para prevenir futuros incidentes de seguridad

Otras denominaciones de CSIRTs

- **CERT**, "*Computer Emergency Response Team*" o Equipo de Respuestas a Emergencias informáticas. CERT marca registrada en Estados Unidos del Centro de Coordinación del Software Engineering Institute (SEI) de la Universidad de Carnegie Mellon (CMU)

- **CSIRT**, "*Computer Security Incident Response Team"* o Centro de Respuesta a Incidentes de Seguridad Informática.
  - Sin requerimientos previos para su uso.

Comunidad Objetivo

En la región de Latinoamérica y el Caribe también se utiliza la expresión en inglés “**constituency**” para identificar a la “**comunidad objetivo**”.

A quien el CSIRT prestará sus servicios.

lacnic csirt

- Comunidad objetivo
- Rol y Autoridad
- Punto de reporte - formulario web
  - https://csirt.lacnic.net/reportar-incidente
  - https://csirt.lacnic.net/solicitar-informacion-leas
- Cursos CAMPUS
  - Curso básico para creación de CSIRTS
  - Gestión de la información en investigaciones

TLP:WHITE

Importancia de un CSIRT

- Es fundamental responder de forma apropiada e inmediata ante la ocurrencia de un incidente de seguridad que pueda afectar a los recursos de una comunidad objetivo

- Permite coordinar acciones para limitar o minimizar los daños ante la ocurrencia de un incidente de seguridad

- A través del CSIRT, la organización se mantendrá actualizada sobre nuevos desafíos y avances en el campo de la seguridad

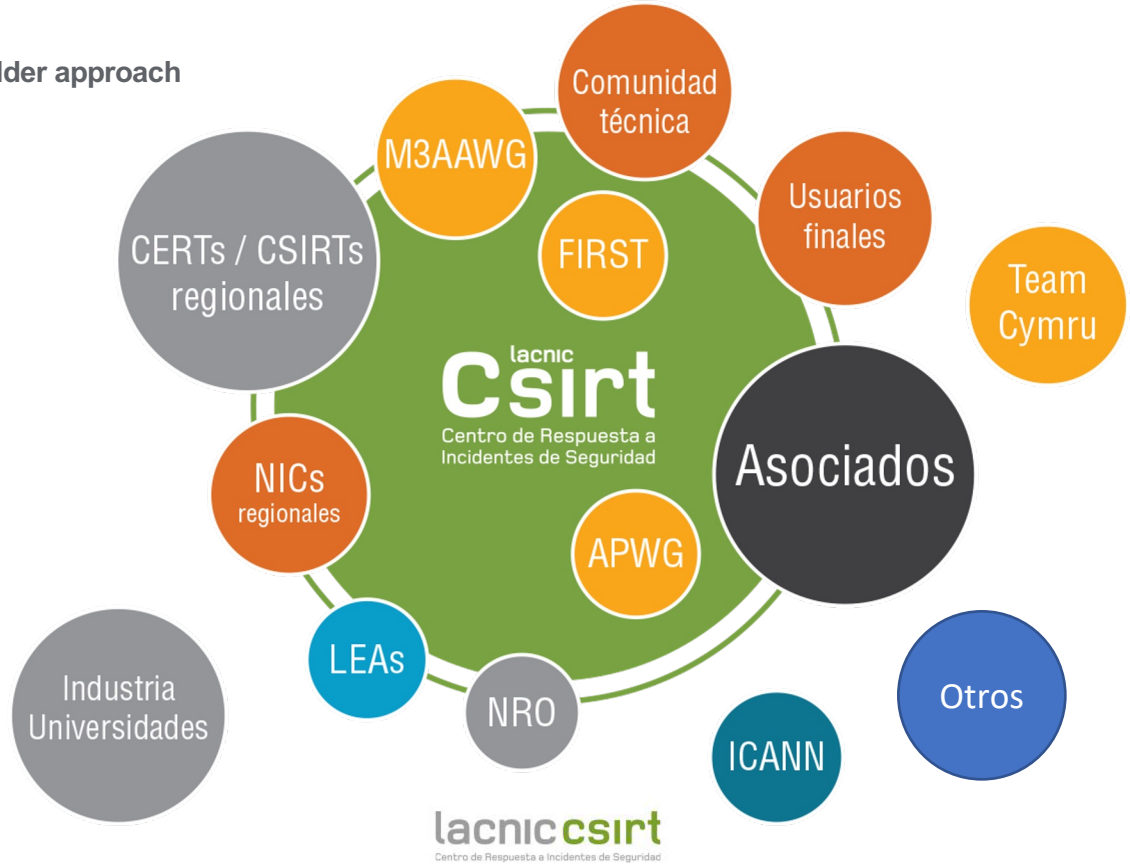
- Se mejora la percepción de seguridad de los usuarios, a través de la difusión de buenas prácticas y recomendaciones

Importancia de un CSIRT

- En suma:
  - Brinda un punto de contacto único
  - Colabora en la respuesta a tiempo (- impacto)
    - Respuesta predefinida - playbooks
    - Lenguaje común
    - TLP
  - Relación de confianza

¿ Cómo trabajamos ?

Multi Stakeholder approach

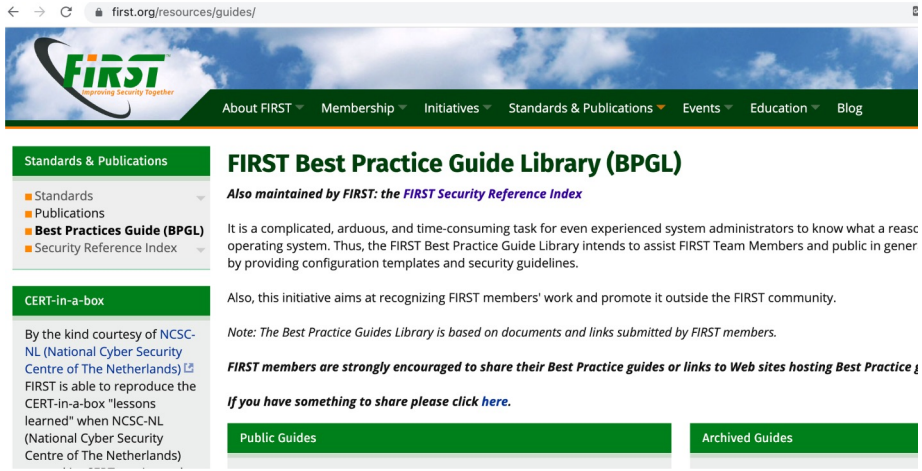


¿Es difícil establecer un CSIRT?

- Analizar si las condiciones están dadas
  - Fundamental: estar en condiciones de asumir formalmente la responsabilidad de gestionar la respuesta a incidentes de seguridad informática.
  - Madurez - Proceso de mejora continua

¿Existe una guía para establecer un CSIRT?

- FIRST - Forum of Incident Response and Security Team
  - Guía de cómo establecer un CSIRT
  - Marco de servicios
- RFC 2350 - Expectations for Computer Security Incident Response

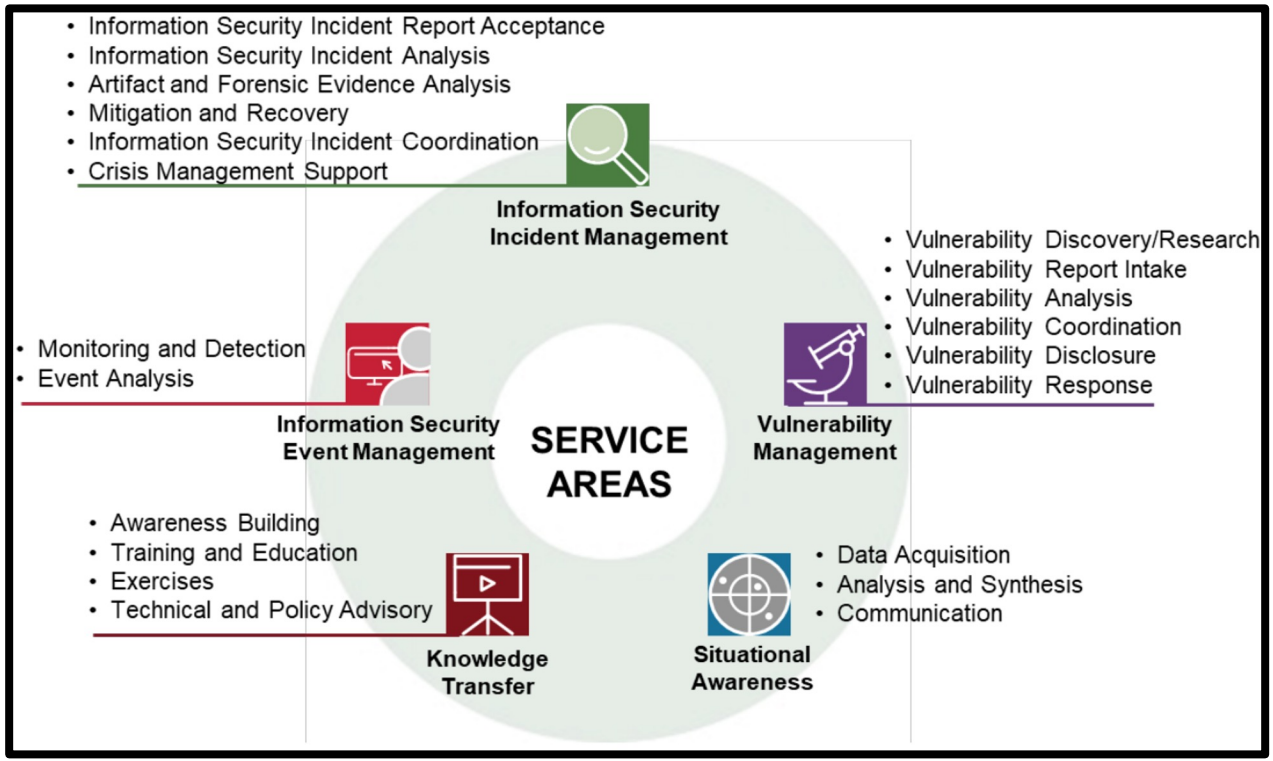


Referencias:

https://www.first.org/

https://www.rfc-editor.org/rfc/rfc2350

Framework de servicios de FIRST, v2.1



Áreas

Gestión de incidentes de seguridad informática

Gestión de eventos de seguridad informática

Gestión de vulnerabilidades

Conciencia situacional

Transferencia de conocimiento

Security Incident Management Maturity Model SIM3

lacnic csirt
Centro de Respuesta a Incidentes de Seguridad

Modelo de madurez - SIM3

- SIM 3 - acrónimo de las siglas en inglés de Security Incident Management Maturity Model, promovido por la Open CSIRT Foundation.
- Objetivo principal: incidentes de seguridad que involucran infraestructura IT y a la información que ésta soporta.
- Permite medir la madurez de la gestión de incidentes de seguridad de un CSIRT
  - Foco en: prevención, detección, resolución y control de calidad
- Es simple de realizar y genera un reporte que se puede compartir

Referencia: https://opencsirt.org/csirt-maturity/sim3-online-tool/

Parámetros y niveles de madurez de SIM3

Este modelo se compone 4 categorías, con un total de 44 parámetros y 5 niveles de madurez

Categoría	Número de parámetros	Niveles de madurez
Organizacional	10	0 = no disponible 1 = implícito 2 = explícito, interno 3 = explícito, formalizado por la autoridad del CSIRT 4 = explícito, evaluado regularmente por la alta gerencia, incluyendo un lazo de retroalimentación activa
Aspectos Humanos	7	
Herramientas	10	
Procesos	17	

Niveles de madurez de SIM3

Los niveles de madurez que se le pueden asignar a los parámetros:

0 = No disponible - *Not available / undefined / unaware*

1 = Implícito - *Implicit (known/considered but not written down, “between the ears”)*

2 = Explícito, interno - *Explicit, internal (written down but not formalised in any way)*

Niveles de madurez de SIM3 (cont.)

3 = Explícito, formalizado por la autoridad del CSIRT - *Explicit, formalised on authority of CSIRT head (rubberstamped or published)*

4 = Explícito, evaluado regularmente por la alta gerencia, sujeto a procesos de control/auditorías/mejoras - *Explicit, audited on authority of governance levels above the CSIRT head (subject to control process/audit/enforcement)*

Herramienta para la evaluación

Evaluación:

A cargo de terceros

Autoevaluación

SIM3 Self Assessment Tool

https://sim3-check.opencsirt.org

lacnic csirt
Centro de Respuesta a Incidentes de Seguridad

Acciones necesarias para escalar el nivel

0 = no disponible / indefinido / desconocido

1 = implícito: conocido / considerado pero no escrito

2 = explícito, interno: escrito pero no formalizado

3 = explícito, formalizado bajo la autoridad del jefe

4 = explícito, auditado con autoridad superior

0 a 1 - se considera - *"somos conscientes"*

1 a 2 - se agrega una descripción escrita - "lea, esta es la forma en la que lo hacemos"

2 a 3 - se agrega responsabilidad - "mire, esto es a lo que estamos comprometidos a hacer"

3 a 4 - se agrega forma de control - "y esto es como nos aseguramos de que se hace"

CSIRT de LACNIC

lacnic csirt
Centro de Respuesta a Incidentes de Seguridad

CSIRT de LACNIC

- Proyectos del CSIRT de LACNIC
- Reporte de incidentes
  - Comunicación con otros equipos de respuesta
- Honeynet del CSIRT de LACNIC
- Módulo de seguridad de MiLACNIC

¡Muchas gracias!

csirt@lacnic.net

https://csirt.lacnic.net/

lacnic csirt
Centro de Respuesta a Incidentes de Seguridad