

# 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/>

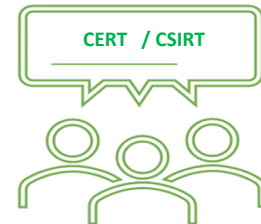
# ¿ Qué es un CSIRT ? (cont.)

## 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



# Importancia de un CSIRT

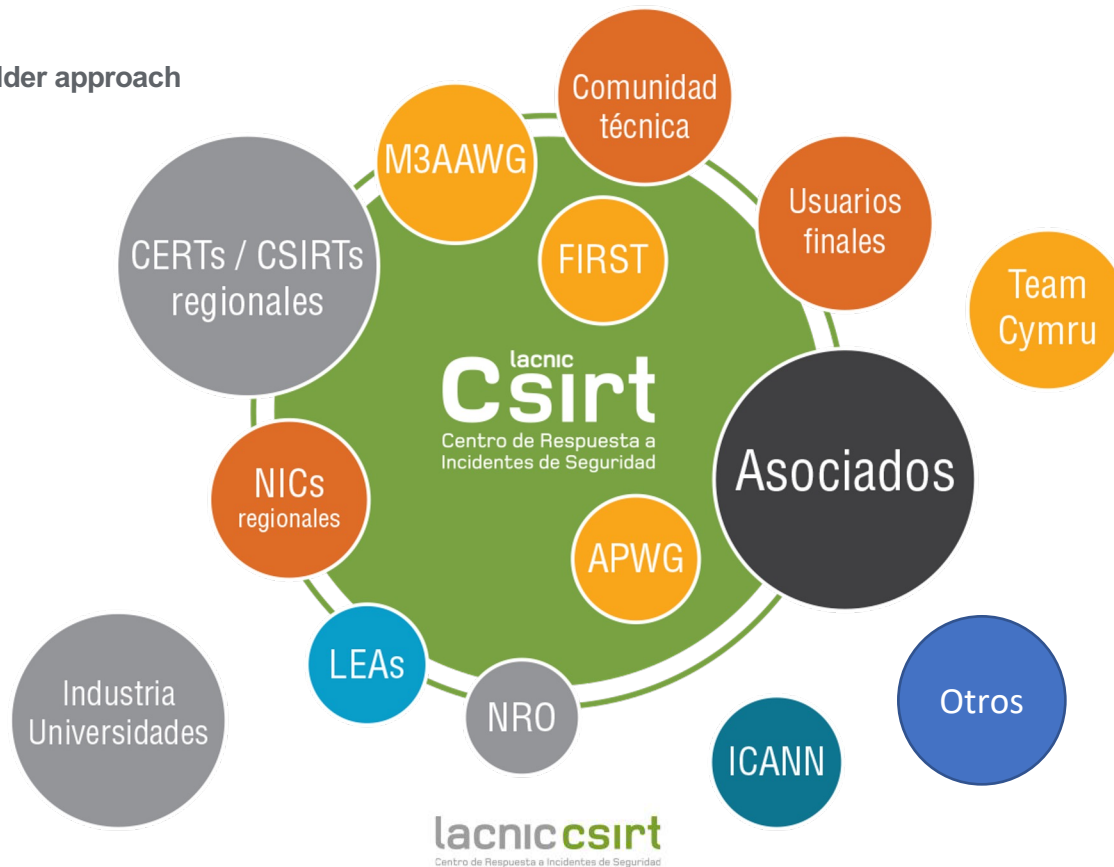
- Es fundamental responder de forma apropiada e inmediata ante la ocurrencia de un incidente de seguridad que pueda afectar a los recursos de una comunidad objetivo
- Permite coordinar acciones para limitar o minimizar los daños ante la ocurrencia de un incidente de seguridad
- A través del CSIRT, la 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

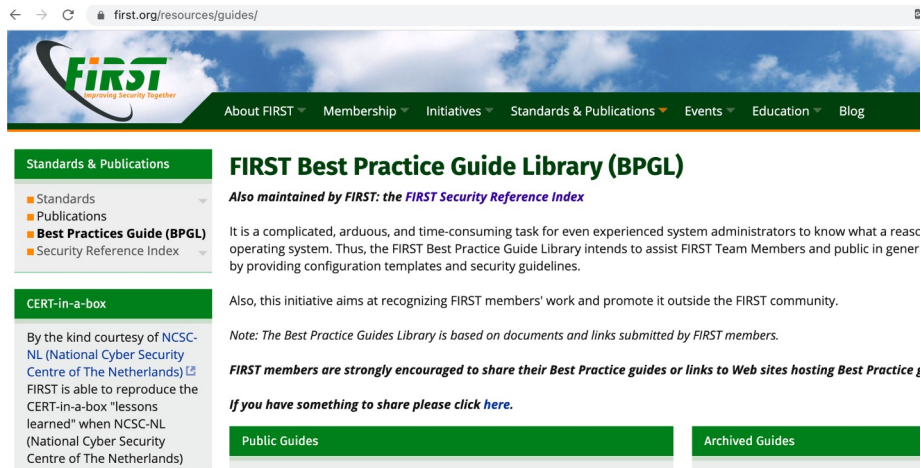
# ¿Existe una guía para establecer un CSIRT?

- 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

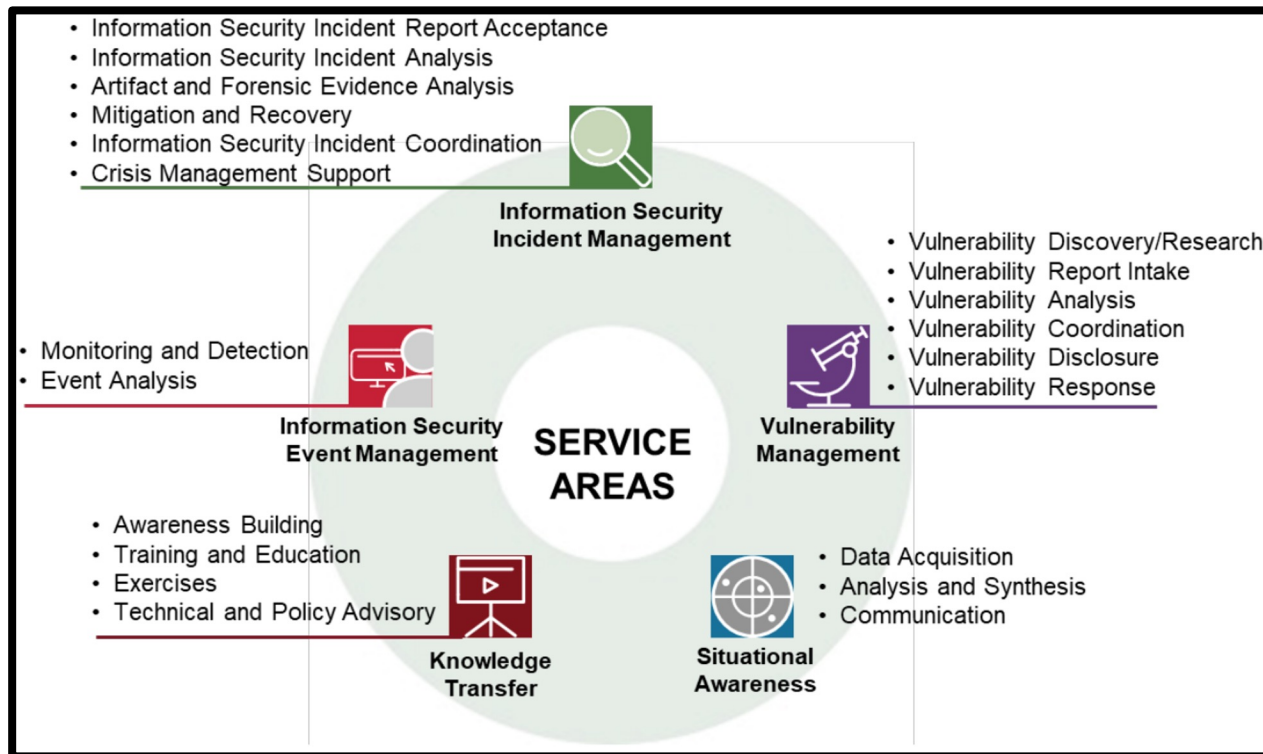
<https://www.first.org/>

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



The screenshot shows the website [first.org/resources/guides/](https://www.first.org/resources/guides/). The page features a navigation menu with options like 'About FIRST', 'Membership', 'Initiatives', 'Standards & Publications', 'Events', 'Education', and 'Blog'. The main content area is titled 'FIRST Best Practice Guide Library (BPGL)' and includes a sub-header 'Also maintained by FIRST: the FIRST Security Reference Index'. The text explains that the library is a complex task for system administrators and aims to assist members by providing configuration templates and security guidelines. It also mentions that the initiative recognizes members' work and promotes it outside the community. A note states that the library is based on documents and links submitted by members. A strong encouragement is given for members to share their best practice guides or links to web sites hosting best practices, with a link provided for sharing. At the bottom, there are two buttons: 'Public Guides' and 'Archived Guides'.

# 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



# 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

Open CSIRT Foundation SIM3 Self Assessment Tool

Open CSIRT Foundation License

Organisation Human Tools **Processes**

With **Processes** we refer to logically sequenced sets of actions which are carried out by humans (Human area) or automated tools (Tools area) in order to achieve a specific result (defined in the Organisation area). All processes can be characterised by a number of attributes. By applying such attributes we can also determine how successful a particular process is (in getting the job done) or how successful a particular organisation is in providing a service (as in getting this process right all the time). In mature organisations processes are documented, measurable and repeatable. To be able to grow and improve the effectiveness of an organisation it is also important to build processes that are adaptable. Here, we specifically talk about those processes that support the management of incidents and any other services the CSIRT offers - and we adopt the term 'processes' in the broadest meaning of the word, so that in this Processes area you will also find processes that might sometimes be labeled 'policy' or otherwise.

Expand all / Collapse all

**P-1: Escalation to Governance Level**

Each team must be able to escalate critical incidents to the appropriate management levels, including the highest level of governance (e.g. board of directors, minister) in case of potential crises or incidents that are at least a significant threat to the reputation of the organisation. In case the team is responsible for an external constituency, it also needs to be able to escalate to the appropriate management level of all constituents; the latter is not only required when the team's normal point of contact does not (timely) react, but also such

Choose your desired SIM3 Profile:

FIRST Membership Baseline ENISA/GCMF Basic

Spider-Chart/Show questions

If you click on a specific tile you will be taken to the corresponding page on this side.

Membership: Baseline not reached

powered by Open CSIRT Foundation

**Evaluación:**

**A cargo de terceros**

**Autoevaluación**

## [SIM3 Self Assessment Tool](https://sim3-check.opencsirt.org)

# 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

# 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](mailto:csirt@lacnic.net)

<https://csirt.lacnic.net/>