CSIRTs

¿De qué se trata?, modelos posibles, servicios y herramientas

Lic. Einar Lanfranco

elanfranco @ cert.unlp.edu.ar

Ernesto Pérez Estévez

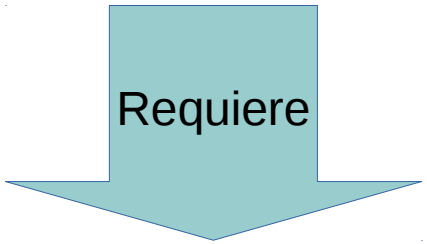
ernesto.perez@cedia.org.ec

CERT UNLP

Equipo de Respuesta a Incidentes de Seguridad

Motivación

Continuo incremento de incidentes de seguridad de la información que afecta a las organizaciones



Definir políticas de seguridad y prácticas asociadas como parte de la estrategias de manejo de riesgo

También es preciso definir responsables para:

- la recepción y revisión de incidentes de seguridad
- el tratamiento y la respuesta a los mismos

¿Que son los CSIRTs?

Un CSIRT o “Equipo de respuesta de incidentes de Seguridad Informática” es un equipo que ejecuta, coordina y apoya la respuesta a incidentes de seguridad que afectan a una comunidad objetivo

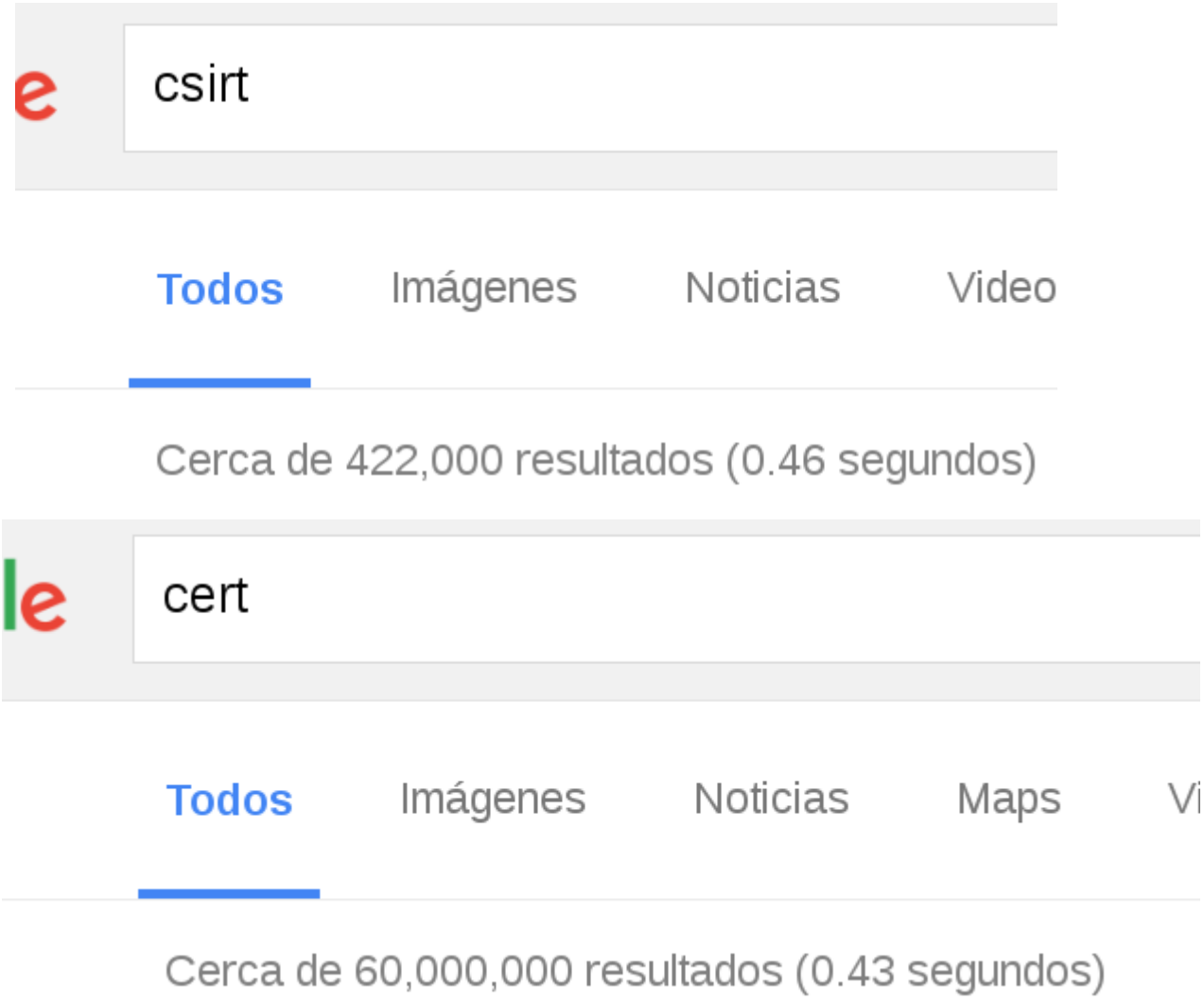
¿ CERT = CSIRT?

- CSIRT (Computer Security Incident Response Team) es el término genérico utilizado para equipos de tratamiento y respuesta a incidentes de seguridad.
- CERT (Computer Emergency Response Team) es el término originalmente utilizado.

  Se pueden usar ambos términos indistintamente. Aunque CERT es una marca registrada.

¿Que son los CSIRTs?

¿ CERT = CSIRT?



CERT UNLP
Equipo de Respuesta a Incidentes de Seguridad

Pasos en la formación de un CSIRT

Al momento de empezar a funcionar como un CSIRT, es importante saber:

- ¿Cuál es la misión? → Metas y Objetivos
- Posición en el organigrama
- ¿A quién se da servicio? → Comunidad Objetivo (Constituency)
- ¿Cuál es el modelo de funcionamiento?
- ¿Qué servicios se van a dar?

https://www.terena.org/activities/tf-csirt/starter-kit.html

Tipos de CSIRTs

Algunas categorías generales de CSIRTs pueden ser **(pueden haber otras):**

- **Centros de Coordinación:**

  Coordinan y facilitan el manejo de incidentes a través de diversos CSIRT. Un ejemplos de este tipo de CSIRT es el CERT Coordination Center (CERT/CC).

- **CSIRTs Nacionales:**

  Proporcionan servicios de manejo de incidentes a un país. Algunos ejemplos son: Japan CERT Coordination Center (JPCERT/CC) o Singapur Computer Emergency Response Team (SingCERT).

Tipos de CSIRTs (cont)

- **CSIRTs Internos:**

  Proporcionan servicios de manejo de incidentes a su organización. Esto podría ser un CSIRT para un banco, una empresa de fabricación, una universidad o una agencia federal.

- **Equipos de Proveedores (Vendor Teams):**

  Manejan informes de vulnerabilidades en sus productos de software o hardware. Pueden trabajar dentro de la organización y también ser un CSIRT interno dentro de la organización.

- **Proveedores de Manejo de Incidentes:**

  Ofrecen servicios de manejo de incidentes a terceros.

Aceptación del CSIRT en su comunidad

El éxito de un CSIRT está basado en:

- Que la comunidad conozca su CSIRT y los servicios que éste brinda.
- Que la comunidad entienda el compromiso del CSIRT en el manejo adecuado de la información de incidentes de seguridad.
- Que el equipo colabore e interactúe con otros CSIRTs en el manejo de incidentes
- La capacitación contínua

Modelos Posibles para las funciones de un CSIRT

Equipo de Seguridad:

No hay un CSIRT constituido. Las funciones

Modelo de CSIRT Centralizado:

Existe un único equipo de respuesta a incidentes que se encarga del manejo de todos los incidentes. Adecuado para organizaciones pequeñas y para organizaciones grandes cuya infraestructura tecnológica no esté en sitios geográficamente distantes.

El centro de respuesta centralizado es el único punto de contacto en toda la organización para la respuesta a incidentes y reportes de vulnerabilidades.

Modelos Posibles para las funciones de un CSIRT (cont)

CSIRT Distribuido

Se cuenta con varios equipos de respuesta a incidentes (según tipo de incidentes, áreas dentro de la organización o áreas geográficas). Todos los equipos conforman el CSIRT y es importante que estén coordinados para garantizar la consistencia del servicio de respuesta a incidentes.

CSIRT Combinado

Es una combinación entre el modelo Centralizado y el Distribuido.

Modelos Posibles para las funciones de un CSIRT (cont)

CSIRT Coordinador

Trabaja con otros CSIRTs. Proporciona asesoría e información a equipos de otras entidades sobre las que no necesariamente ejercen autoridad directa.

Su función principal es proporcionar análisis de incidentes y de vulnerabilidades, soporte y servicios de coordinación. También genera guías, boletines, mejores prácticas y alertas de ataques y vulnerabilidades.

Servicios de un CSIRT

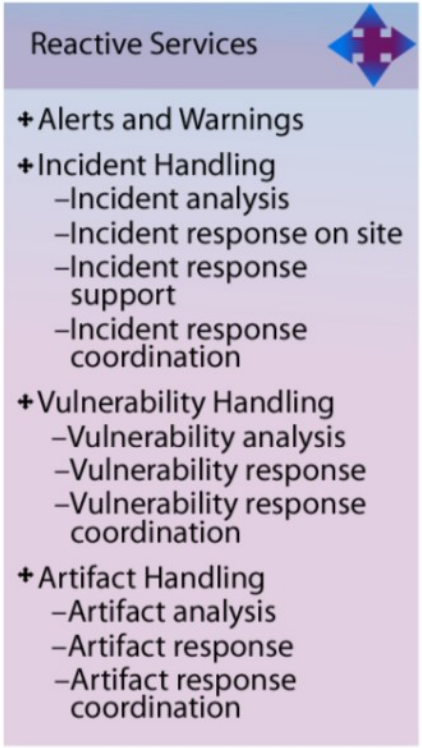
- **Servicios Reactivos**
  - Se activan como consecuencia de un evento o requerimiento.
  - Son el componente central en el trabajo de un CSIRT.
- **Servicios Proactivos**
  - Proveen información que ayuda a proteger su comunidad y su infraestructura anticipándose a los ataques.
  - El éxito de estos servicios reduce el número de incidentes futuros.
- **Servicios de Gestión de Calidad de Seguridad**
  - Mejoran servicios independientes del manejo de incidentes preexistentes (capacitaciones internas, auditoría, etc).
  - En general son servicios proactivos pero con una incidencia menor en la reducción de incidentes futuros.
  - Se valen de los conocimientos y la experiencia del personal del CSIRT.

Servicios Reactivos

La **Gestión de Incidentes de Seguridad** es el único servicio **reactivo** que cualquier CSIRT debe brindar.

Ejemplos de servicios **reactivos** que se pueden brindar:

- Avisos y Alertas
- Gestión de Incidentes:
  - Análisis de incidentes
    - Análisis Forense
  - Soporte es la Respuesta
  - Coordinación



Referencia: http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6305

Sobre la gestión de incidentes

El tratamiento de incidentes (único servicio obligatorio de un CSIRT) implica:

1. Recepción del incidente
2. Evaluación de incidentes (Analizar pertinencia y clasificación)
3. Tratamiento de incidentes

   [Opcional] Asistencia técnica en resolución de incidentes, erradicación de la causa y restablecimiento de servicios
4. Notificación

Gestión de Incidentes

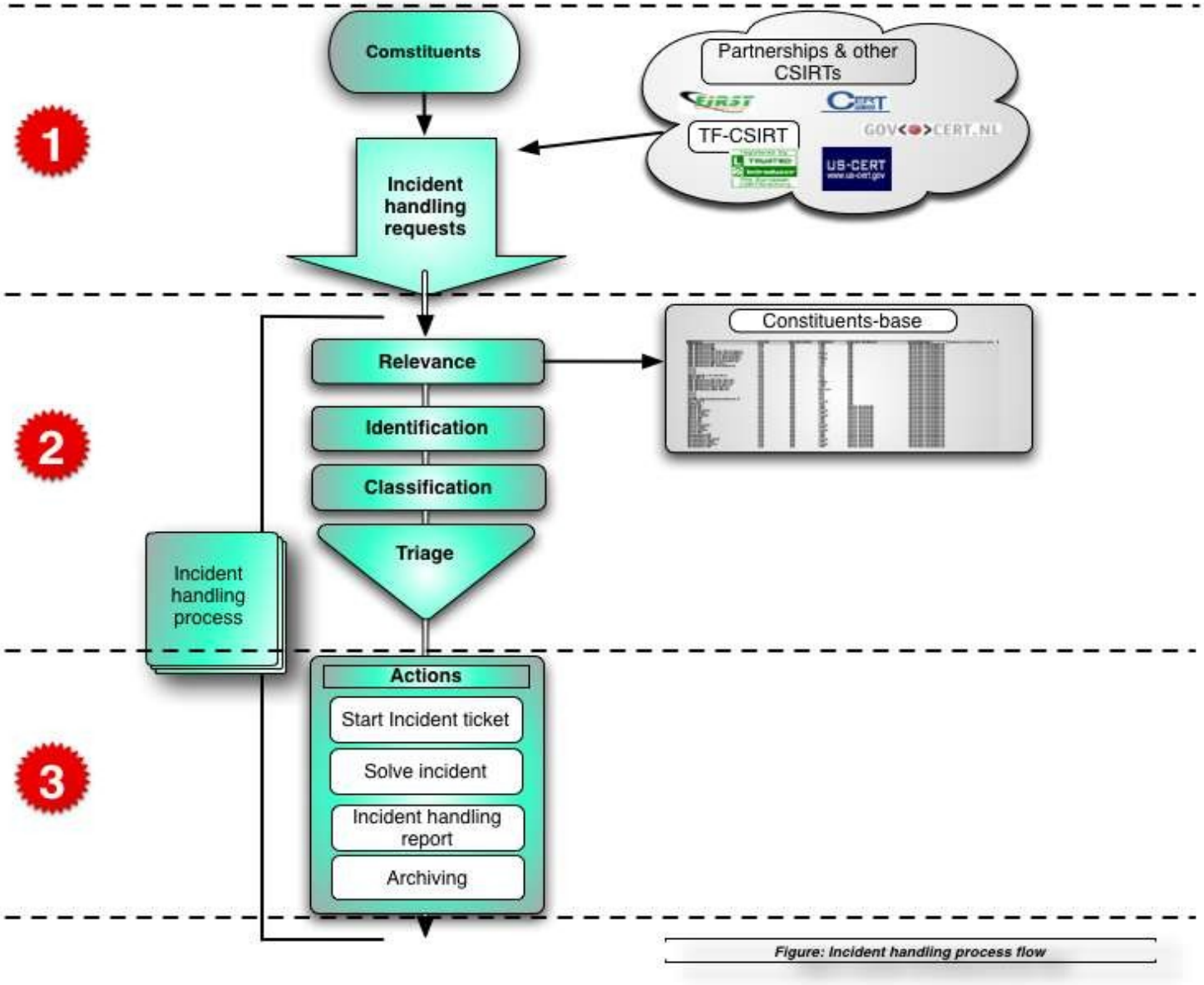


Figure: Incident handling process flow

Referencia: https://www.enisa.europa.eu/activities/cert/support/guide/workflows/incident-handling

CERT UNLP
Equipo de Respuesta a Incidentes de Seguridad

Servicios Proactivos

Ejemplos de servicios **proactivos**:

- Anuncios
- Auditorías de seguridad (Pentests)
- Desarrollo de herramientas de Seguridad
- Monitoreo, Detección y Prevención de intrusiones

Referencia: http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6305

Servicios de Gestión de Calidad la Seguridad

Ejemplos de servicios de **gestión de calidad de seguridad que se pueden brindar**:

- Consultoría
- Concientización
- Educación / Entrenamiento

Referencia: http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6305

Organismos de referencia

- **FIRST (Forum for Incident Response and Security Teams)**
  - Fomenta la cooperación y la coordinación en prevención de incidentes. Promueve el intercambio de información entre miembros y la comunidad en general. Desarrolla capacitaciones y talleres para la formación de nuevos CSIRTs
- **Iniciativas de LACNIC:**
  - **Proyecto AMPARO**
    - Su misión es el fortalecimiento de la capacidad de prevención y atención de incidentes de seguridad en América Latina y el Caribe, tanto en el ámbito privado como en organizaciones sociales.
    - Promover la difusión y capacitación de metodologías de trabajo de Centros de Respuesta a Incidentes de Seguridad Informática o CSIRTs (Computer Security Incident Response Teams).
  - **LACCSIRTs** – Espacio dentro de LACNIC para CSIRTs
  - **W.A.R.P. - Warning Advice and Reporting Point**

    Equipo Coordinador y Facilitador de manejo de incidentes de seguridad informática para la comunidad de miembros de LACNIC.
- **ENISA**, the European Union Agency for Network and Information Security

  Su objetivo es ser un punto de intercambio de información, mejores prácticas y conocimiento en el campo de la Seguridad Informática