lacnic csirt

Centro de Respuesta a Incidentes de Seguridad

@lacnic_csirt

Introducción a la creación de un CSIRT

Graciela Martínez

Líder CSIRT LACNIC

amparo

Reserva de derechos

lacnic Csirt

pa proyecto amparo

Taller AMPARO

- Promover la creación de CSIRT`s, los cuales contribuyen a resolver los incidentes de seguridad informática de forma sistematizada.
- Contribuir al análisis sobre los posibles modelos e impactos de la constitución de un CSIRT
- Contribuir al desarrollo de mejores prácticas
- Generar una red de confianza para el intercambio de información, frente a la ocurrencia de incidentes

lacnic Csirt

pa proyecto amparo

Tutorial AMPARO

Objetivo:

- Abordar los conceptos básicos para la creación de un Centro de respuesta a Incidentes de Seguridad

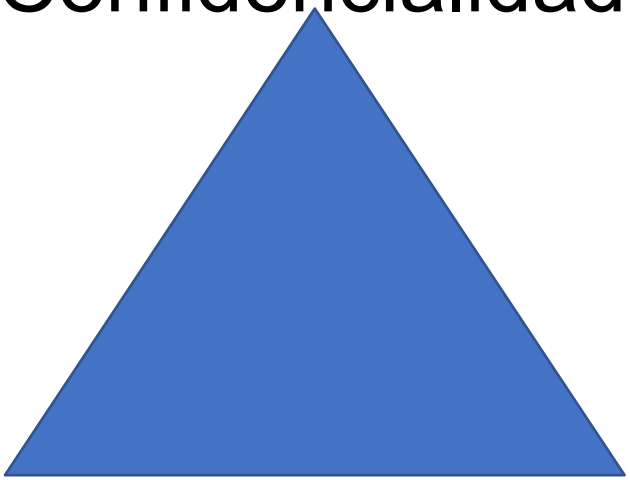
lacnic Csirt

pa proyecto amparo

Incidente de Seguridad Informática

Cualquier acto que viole una política de seguridad de la información y que afecte:

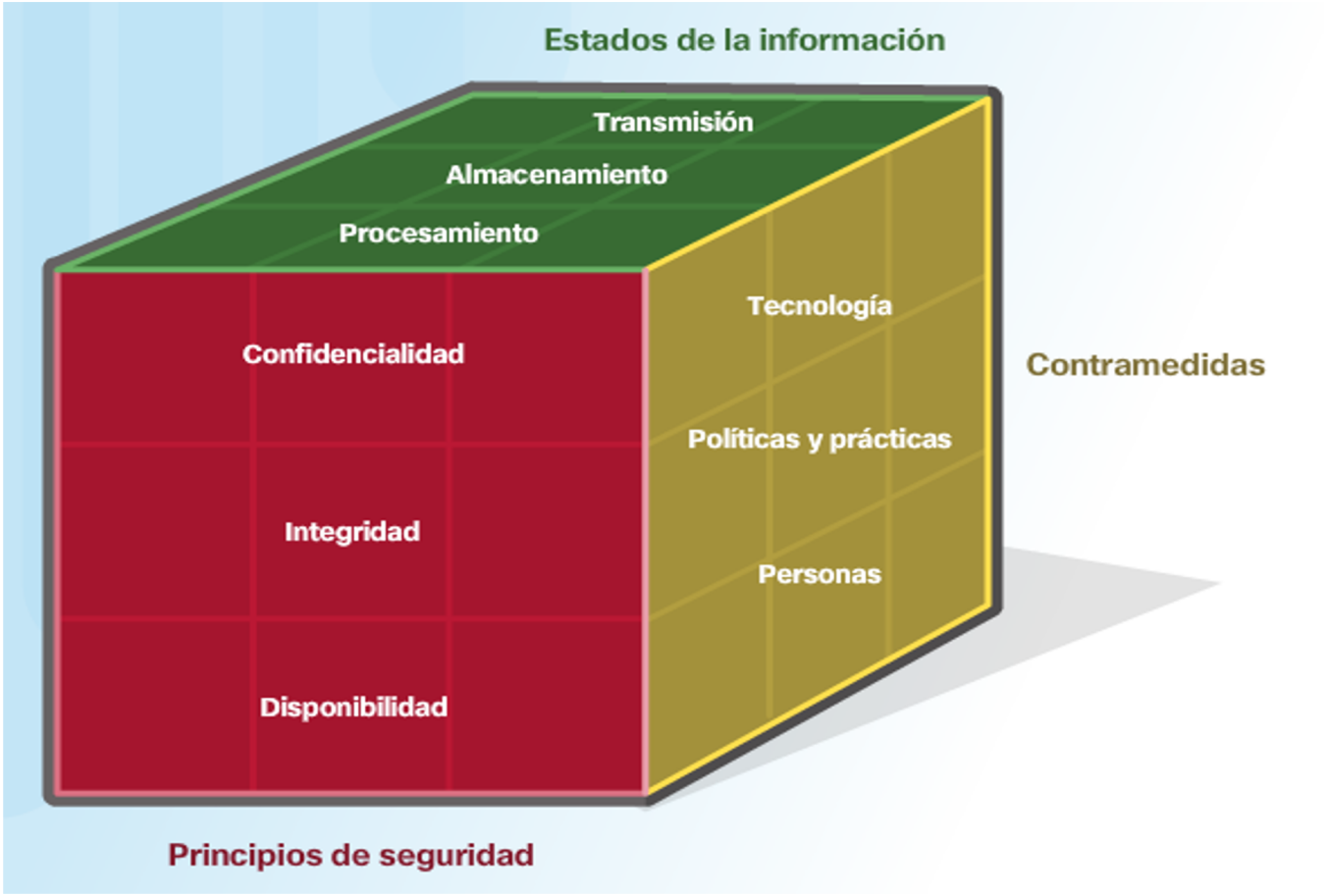
Confidencialidad



Disponibilidad

Integridad

Cubo Mc. Cumber



Incidente de Seguridad Informática

Evento vs. Incidente de Seguridad

Un **evento de seguridad** cualquier suceso que pueda afectar potencialmente la seguridad de un sistema

Un **incidente de seguridad** es un **evento de seguridad** que causa un determinado daño en un sistema

Motivaciones para el establecimiento de un CSIRT

- Incremento de reportes de eventos de seguridad
- La cantidad de organizaciones que han sido afectadas ha aumentado
- El tipo de organización se ha diversificado
- Los administradores de sistemas de información y redes ocupados en operaciones
- Estrategias de gestión de riesgos incrementaron la consciencia de la importancia de la seguridad de la información y la infraestructura que la sostiene
- Nuevas leyes y regulaciones para el manejo de información

¿Qué significa CSIRT?

Computer Security Incident Response Team

- Equipo de respuesta a incidentes de seguridad informática -

lacnic Csirt

pa proyecto amparo

Abreviaturas utilizadas

- CERT o CERT/CC (Computer Emergency Response Team / Coordination Center, equipo de respuesta a emergencias informáticas / Centro de coordinación).
- CSIRT (Computer Security Incident Response Team, equipo de respuesta a incidentes de seguridad informática).
- IRT (Incident Response Team, equipo de respuesta a incidentes)
- CIRT (Computer Incident Response Team, equipo de respuesta a incidentes informáticos)
- SERT (Security Emergency Response Team, equipo de respuesta a emergencias de seguridad)

¿Quién inventó el término?

- La primera vez que apareció un gusano importante en la infraestructura global de TI fue a finales de los años ochenta. El gusano llamado Morris.
- Así, unos días después del «incidente Morris», la DARPA (Defence Advanced Research Projects Agency, Agencia de Investigación de Proyectos Avanzados de Defensa) creó el primer CSIRT: el CERT Coordination Center (CERT/CC3), ubicado en la Universidad Carnegie Mellon, en Pittsburgh (Pensilvania).

¿Qué es un CSIRT?

Un CSIRT es un **equipo** de especialistas de seguridad informática que ejecuta, coordina y apoya la respuesta a incidentes de seguridad ocurridos en su comunidad objetivo

lacnic Csirt

pa proyecto amparo

¿ Qué nos provee un CSIRT ?

- Servicios necesarios para el manejo de incidentes
- Colabora con su Comunidad Objetivo para que se recupere de ataques.
- Ayuda a minimizar y controlar el daño resultante de un incidente de seguridad informático
- Trabaja para prevenir futuros incidentes

Beneficios de contar con un CSIRT

- Brindar a su comunidad un servicio de gestión de incidentes de seguridad centralizada y especializada
- Dar una respuesta *rápida* y *planificada* que permita contener un incidente de seguridad informática
- Punto de contacto confiable para el reporte y manejo de incidentes de seguridad
- Punto de contacto efectivo con otros CSIRTs y comunidades

Beneficios de contar con un CSIRT

- Contar con expertos a mano para apoyar a los usuarios en la recuperación de incidentes de seguridad
- Trabajar de forma adecuada aspectos legales y preservación de evidencia en caso de necesidad.
- Proveer servicios de publicación de información útil para socializar la cultura de seguridad informática.
- Estimular la cooperación dentro de su membresía sobre seguridad de TI (awareness building).

Acciones iniciales

Acciones iniciales para la creación de un CSIRT

- Contar con la aprobación de la Dirección de la organización
  - Justificación
- Dar enfoque de Gestión de Proyectos
- Definir líder y equipo inicial
  - Capacitación
  - Consultoría de apoyo

lacnic Csirt

pa proyecto amparo

Definiciones iniciales para un CSIRT

- ***Nombre***
- Tipo de CSIRT
- Comunidad objetivo que atenderá
- Misión del CSIRT
- Autoridad
- Servicios que brindará el CSIRT
- Políticas y procedimientos
- Canales de comunicación
- Estructura organizacional

lacnic Csirt

pa proyecto amparo

Tipos de CSIRT

- CSIRT del sector académico
- CSIRT comercial
- CSIRT del sector público
- CSIRT interno
- CSIRT del sector militar
- CSIRT nacional
- CSIRT de soporte - PSIRT

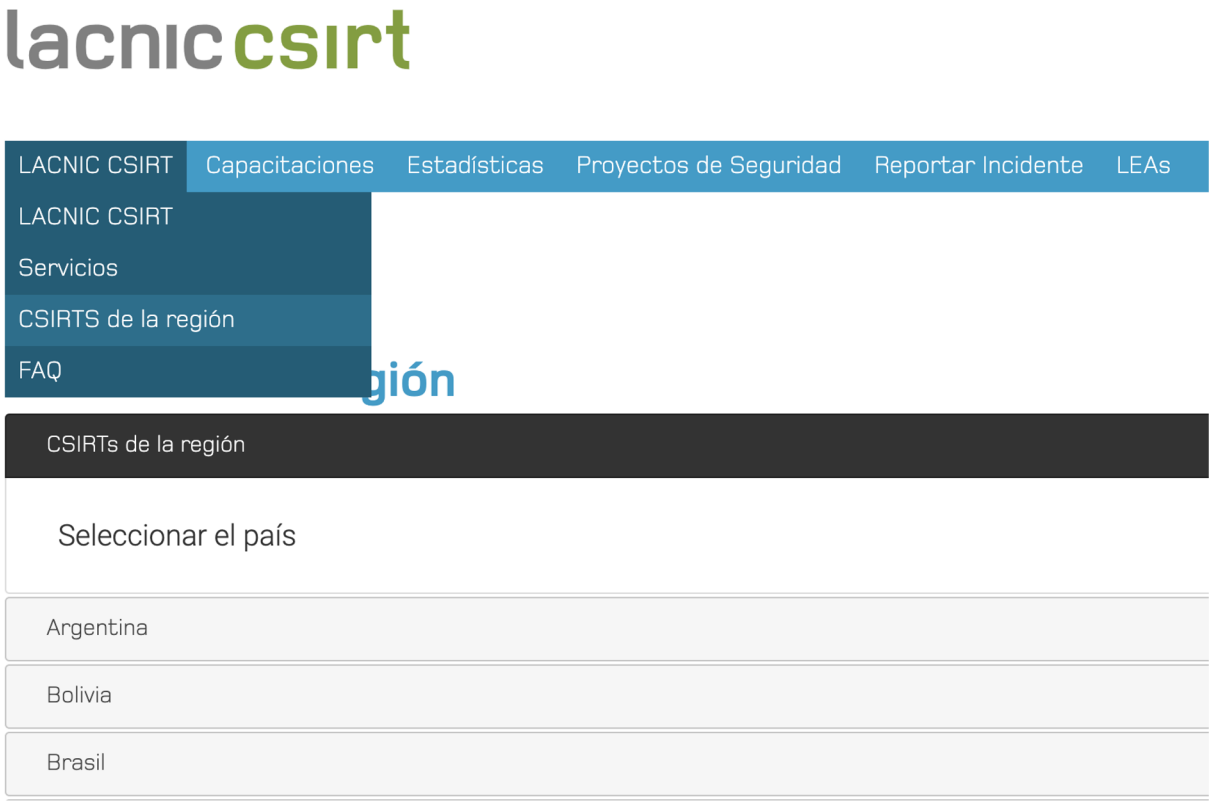
lacnic Csirt

pa proyecto amparo

Comunidad objetivo

La comunidad objetivo o “constituency” define a quién le brindará servicios el centro de respuesta

Ejemplos de Comunidad Objetivo



https://csirt.lacnic.net/nuevo-csirt-de-la-region

Misión

- Describe la función básica del CSIRT en términos de productos y servicios que brinda a su comunidad objetivo
- Comunica claramente la existencia y la función del mismo
- Debe ser compacta y precisa y de largo alcance

Ejemplo de MISIÓN

Misión del CSIRT de LACNIC

“Llevar a cabo las funciones de coordinación necesarias para el fortalecimiento de las capacidades de respuesta a incidentes vinculados a los recursos de numeración de Internet (IPv4, IPv6), Números Autónomos y Resolución Inversa de América Latina y el Caribe, en el marco de las metas específicas establecidas por la misión de LACNIC tendientes a lograr el fortalecimiento constante de una Internet segura, estable, abierta y en continuo crecimiento.”

Autoridad

– Autoridad
  - Total – puede decidir que se tomen medidas durante la gestión. Ej: apagar un equipo
  - Compartida – participa en la decisión pero no decide solo
  - Nula o sin autoridad – sugiere acciones

Diferencia: Toma de decisiones en el manejo de incidentes

Servicios de un CSIRT

PROACTIVOS	*REACTIVOS*	*CALIDAD de SERVICIOS de GESTIÓN de la Seguridad*
Publicaciones	**Gestión de Incidentes**	Análisis de Riesgos
Observatorio Tecnológico	Alertas	Plan de Continuidad del Negocio
Audiotorías de Seguridad/Tests de Penetración	Manejo de Vulnerabilidades	Plan de Recuperación de Desastre
Desarrollo de herramientas	Análisis de Artefactos	Entrenamiento
Detección de Intrusos		Educación sobre seguridad
Compartir Información de Inteligencia de Amenazas		

lacnic Csirt

pa proyecto amparo

Políticas y procedimientos

- Políticas básicas recomendadas:
  - Política de manejo e intercambio de información
  - Política de gestión de incidentes
    - Procedimiento de gestión de incidentes
  - Política de uso aceptable de recursos
  - Procedimientos de vinculación y desvinculación del personal
  - Contrato de confidencialidad

Políticas y procedimientos

Debe quedar definido:

- **Tipos de incidentes y nivel de apoyo**

  Tipos de incidentes que el equipo sea capaz de atender y nivel de apoyo que se ofrecerá
- **Cooperación, interacción y divulgación**
  - Qué tipos de interacciones se han establecido y sus propósitos.
  - Quiénes son los destinatarios de los informes
  - Identificar los grupos que van a interactuar con mi Centro

- Descripción de histórico de actualización de documentos
  - Cambios de versión de documentos (fecha última act., lista de distribución)

Traffic Light Protocol (TLP)

https://www.us-cert.gov/tlp

Color	When should it be used?	How may it be shared?
TLP:RED  Not for disclosure, restricted to participants only.	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER  Limited disclosure, restricted to participants' organizations.	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**
TLP:GREEN  Limited disclosure, restricted to the community.	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
TLP:WHITE  Disclosure is not limited.	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Canales de Comunicación

¿ Cómo nos comunicamos con nuestra C.O. ?

- Información de contacto
  - Detalles completos de cómo ponerse en contacto con el CSIRT (nombre, dirección, teléfono, GMT, claves públicas, horario de atención)
  - Información de miembros del equipo: el nivel de detalle de esta información queda a criterio de cada grupo

lacnic Csirt

pa proyecto amparo

Canales de Comunicación

✓ Sitio web público
https://csirt.lacnic.net/

✓ Formularios web para comunicar incidentes
https://csirt.lacnic.net/reportar-incidente

✓ Correo electrónico personalizado
csirt@lacnic.net

✓ Teléfono / fax

lacnic Csirt

pa proyecto amparo

Servicios básicos para la operación

- Aplicaciones que apoyan la implementación de los servicios informáticos de un CSIRT
  - Sistema de seguimiento de incidentes
  - Correo electrónico seguro PGP
  - Sistemas de comunicación segura (SSH, SSL, cifrado de datos)
  - Sistema de correlación de reportes
  - Sistema de análisis de datos

Estructura organizacional

- Independiente – Ejemplo: CSIRT comercial
- Distribuído – Ejemplo: campus
- Embebido en la organización
  - Para su ubicación se recomienda tener en cuenta su misión y comunidad objetivo

Algunos COSTOS

- ✓ RRHH
  - ✓ Contratación - *expertise*
  - ✓ Staff - *cantidad*
  - ✓ Capacitación
- ✓ Seguridad física del área de trabajo del centro de respuesta
- ✓ Medios y dispositivos de comunicación
- ✓ Resguardo de la información

lacnic Csirt

pa proyecto amparo

Modelos de ingresos

- ✓ Uso de los recursos existentes
- ✓ Cuotas – venta de servicios
- ✓ Subvenciones – Estado, organismos públicos

lacnic Csirt

pa proyecto amparo

Gestión de Incidentes

La gestión de un incidente de seguridad abarca todo el proceso desde su detección inicial, respuesta y cierre.

- Detección: proactiva o reactiva

Gestión de Incidentes - Beneficios

Beneficios de una correcta gestión de incidentes:

- Cumplimiento de los niveles de servicios acordados
- Optimiza los recursos disponibles
- Mejora la satisfacción general de clientes y usuarios
- Genera una base de conocimiento

Gestión de Incidentes – Efectos adversos

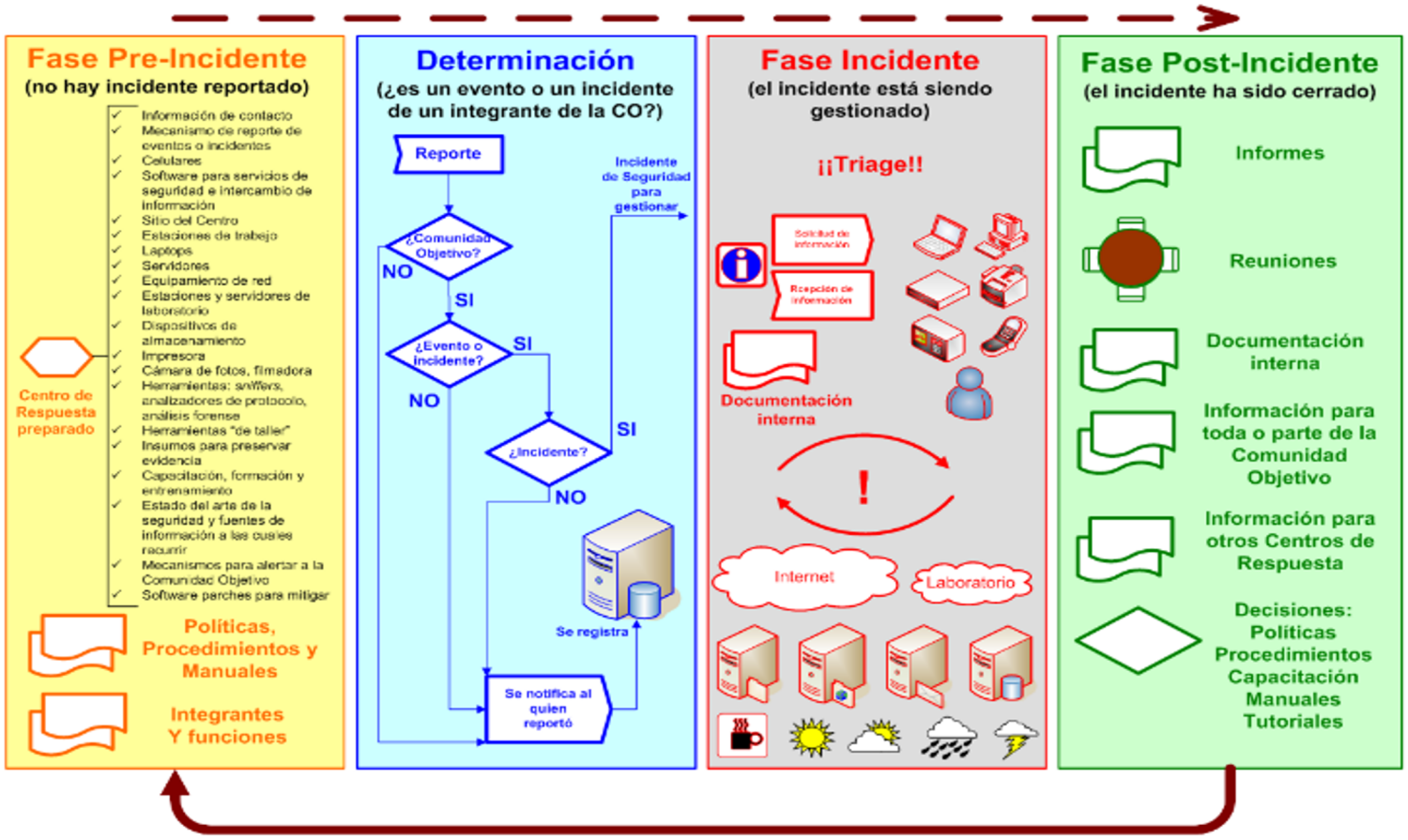
Una incorrecta gestión de incidentes puede ocasionar efectos adversos tales como:

- Reducción de los niveles de servicios
- Pérdida de información valiosa sobre las causas de un incidente para responder de forma efectiva ante posibles eventos futuros
- Pérdida de imagen y confianza

Gestión de Incidentes - Triage

- Clasificación
  - Definir taxonomía: asignar una categoría dependiendo del tipo de incidente
  - Establecer prioridad: depende del impacto y la severidad
  - Asignación de recursos: personal que dará el soporte
  - Estimar tiempo de resolución del incidente.

Ciclo de vida de un incidente de seguridad

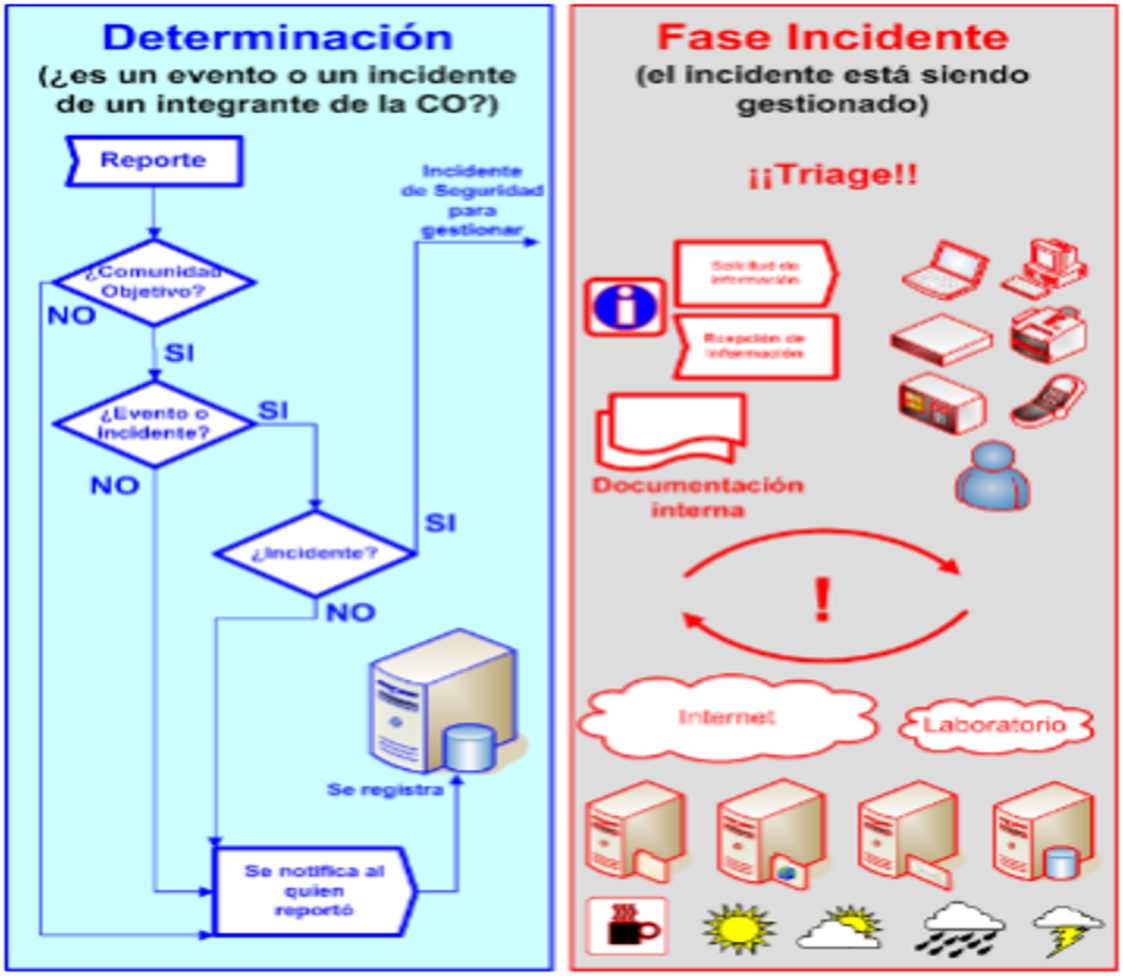


lacnic Csirt

pa proyecto amparo

Ciclo de vida de un incidente de seguridad

Ciclo de vida de un incidente de seguridad



lacnic Csirt

pa proyecto amparo

Ciclo de vida de un incidente de seguridad

Después de la tormenta...

lacnic Csirt

pa proyecto amparo

Muchas gracias

Contactos:

Graciela Martínez
gmartinez@lacnic.net
o
csirt@lacnic.net

lacnic Csirt

pa proyecto amparo

Referencias

- **Manual AMPARO**

https://csirt.lacnic.net/taller-amparo

- **RFC 2350 - Expectations for Computer Security Incident Response –**

https://tools.ietf.org/html/rfc2350

- **FIRST**

https://www.first.org/

lacnic Csirt

pa proyecto amparo