



**Primera respuesta: antes de
que llegue la policía**

Luis A. Gorgona S.
Csirt-CR



Contenidos

- Conceptos básicos
- Los objetivos de la respuesta a Incidentes
- Funciones de un CSIRT
- El Rol de los CSIRTS
- El rol del administrador de sistemas en la respuesta a incidentes
- Asistiendo a las fuerzas del orden



Conceptos Básicos



Definición de CSIRT

Un Equipo de Respuesta a Incidentes de Seguridad (CSIRT) es una organización que es responsable de recibir, revisar y responder a informes y actividad sobre incidentes de seguridad. Sus servicios son generalmente prestados para un área de cobertura definida que podría ser una entidad relacionada u organización de la cual dependen, una corporación, una organización de gobierno o educativa; una región o país, una red de investigación; o un servicio pago para un cliente.



Tipos de CSIRTS

- **CSIRTS Internos**
- **CSIRTS Nacionales**
- **Centros de Coordinación**
- **Centros de Análisis**
- **Equipos de Vendedores**
- **Proveedores de Respuesta a Incidentes**

Fuente: CERT/CC traducido por ArCert

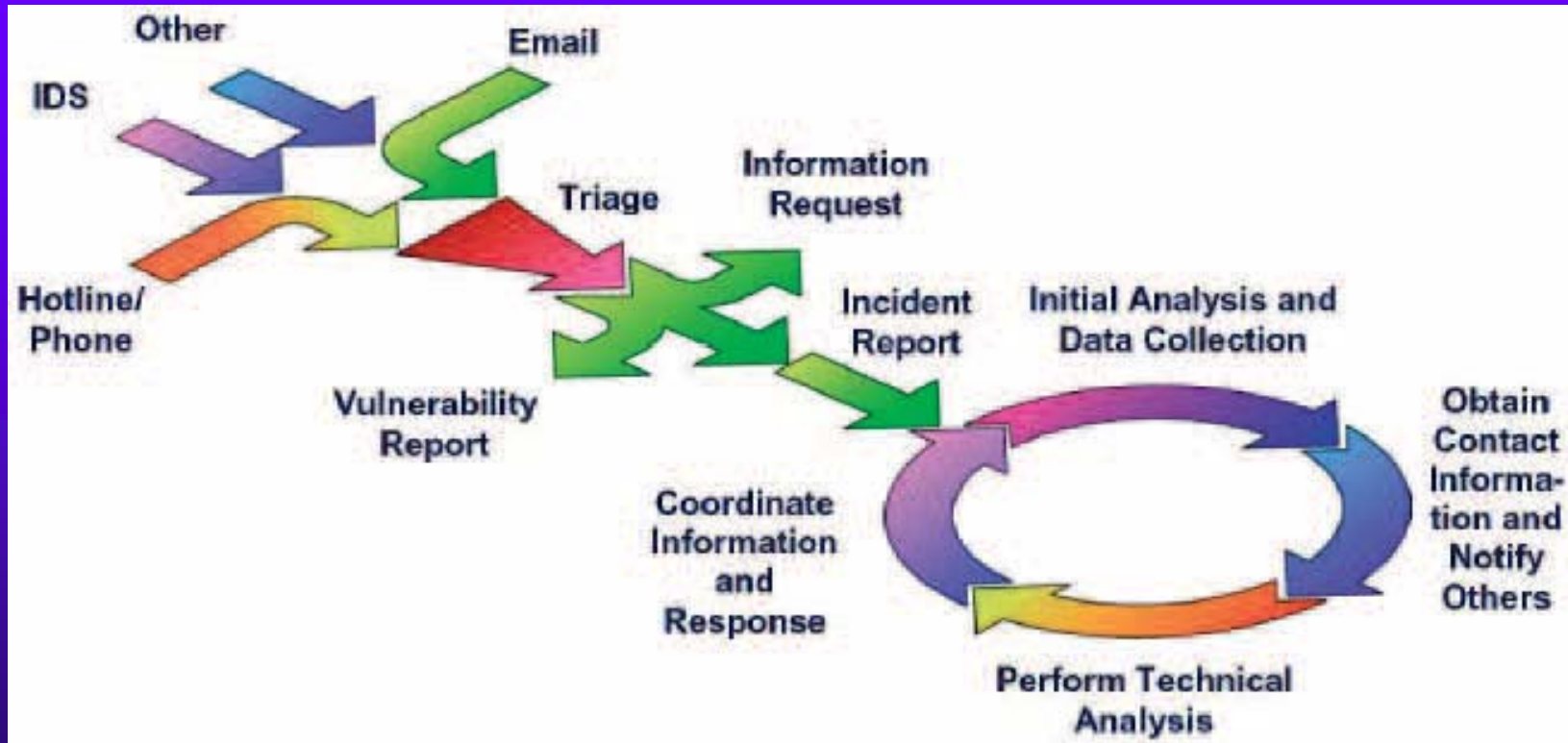


Manejo de incidentes

- La función de información sobre el incidente le permite al CSIRT servir como el punto de contacto central para informar los problemas locales. Esto es reunir todos los informes y actividad sobre incidentes en un lugar donde la información puede ser revisada y correlacionada a través de la organización de la que depende o del área de cobertura.

Fuente: CERT/CC traducido por ArCert

Ciclo de vida de un Incidente






Objetivos de la Respuesta a Incidentes



El manejo de incidentes es un trabajo de equipo. Todos debemos hacer nuestra parte



Los objetivos de la respuesta a Incidentes

- 1. Verificar que un incidente se ha producido.
- 2. Mantener o restaurar la continuidad del negocio.
- 3. Reducir el impacto del incidente.
- 4. Determinar la forma en que el ataque se convirtió en incidente.
- 5. Prevenir futuros ataques o incidentes.
- 6. Mejorar la seguridad y respuesta a incidentes.
- 7. Perseguir las actividades ilegales.
- 8. Mantenerse informado de la gestión de la situación y la respuesta.

Fuente: seguridad.ongei.gov.pe

La visión de cada jugador

	Adm. TI	CSIRT	Autoridades
Recuperación	Primordial	Primordial	Secundario
Prevención	Primordial	Primordial	Secundario
Pruebas y Evidencias	Secundario	Primordial	Primordial
Análisis Forense	Secundario	Primordial	Primordial
Divulgación y Coordinación	Secundario	Primordial	Secundario





Funciones de un CSIRT



Funciones de un CSIRT

- **Servicios reactivos**

Estos servicios se inician ante un evento o pedido, tal como un informe de un computador comprometido, código malicioso ampliamente diseminado, vulnerabilidad de software, o algo que fue identificado por un sistema de detección de intruso o un sistema de registro de eventos. Los servicios reactivos son el componente central del trabajo de un CSIRT.

Funciones de un CSIRT

- **Servicios proactivos**

Estos servicios ofrecen asistencia e información para ayudar a preparar, proteger y asegurar los sistemas de los miembros del área de cobertura anticipando ataques, problemas o eventos. Estos servicios reducirán directamente la cantidad de incidentes en el futuro.



Funciones de un CSIRT

- **Servicios de gestión de calidad de la seguridad**

Estos servicios aumentan los servicios existentes y bien establecidos que son independientes del manejo de incidentes y tradicionalmente llevados a cabo por otras áreas de una organización tales como Tecnología de la Información (IT), auditoría o departamentos de capacitación.





El Rol de los CSIRTS

Reporte de Incidentes

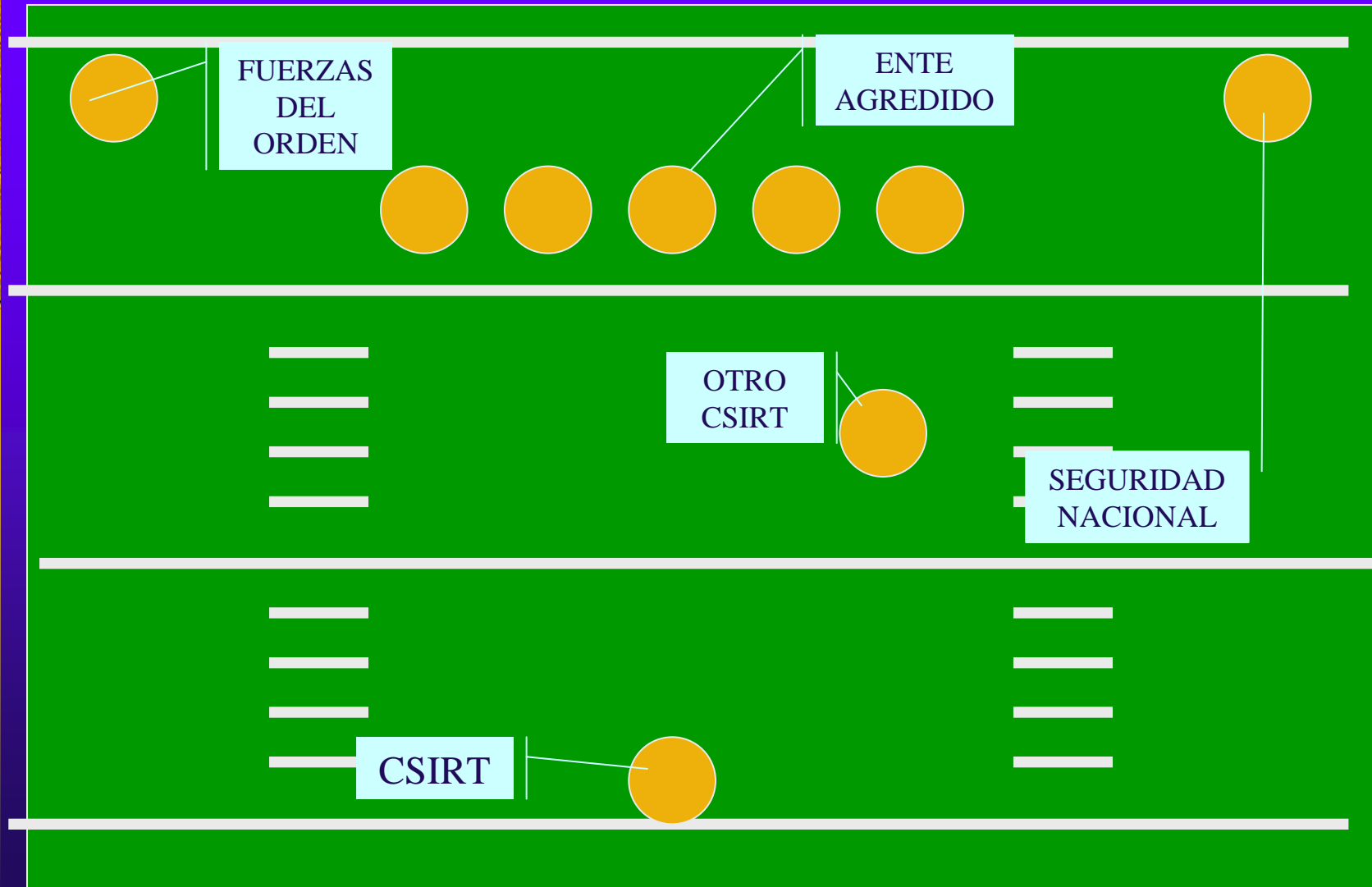


- Clientes
 - Declaratoria de servicios
- Correos Electrónicos
- Denuncias

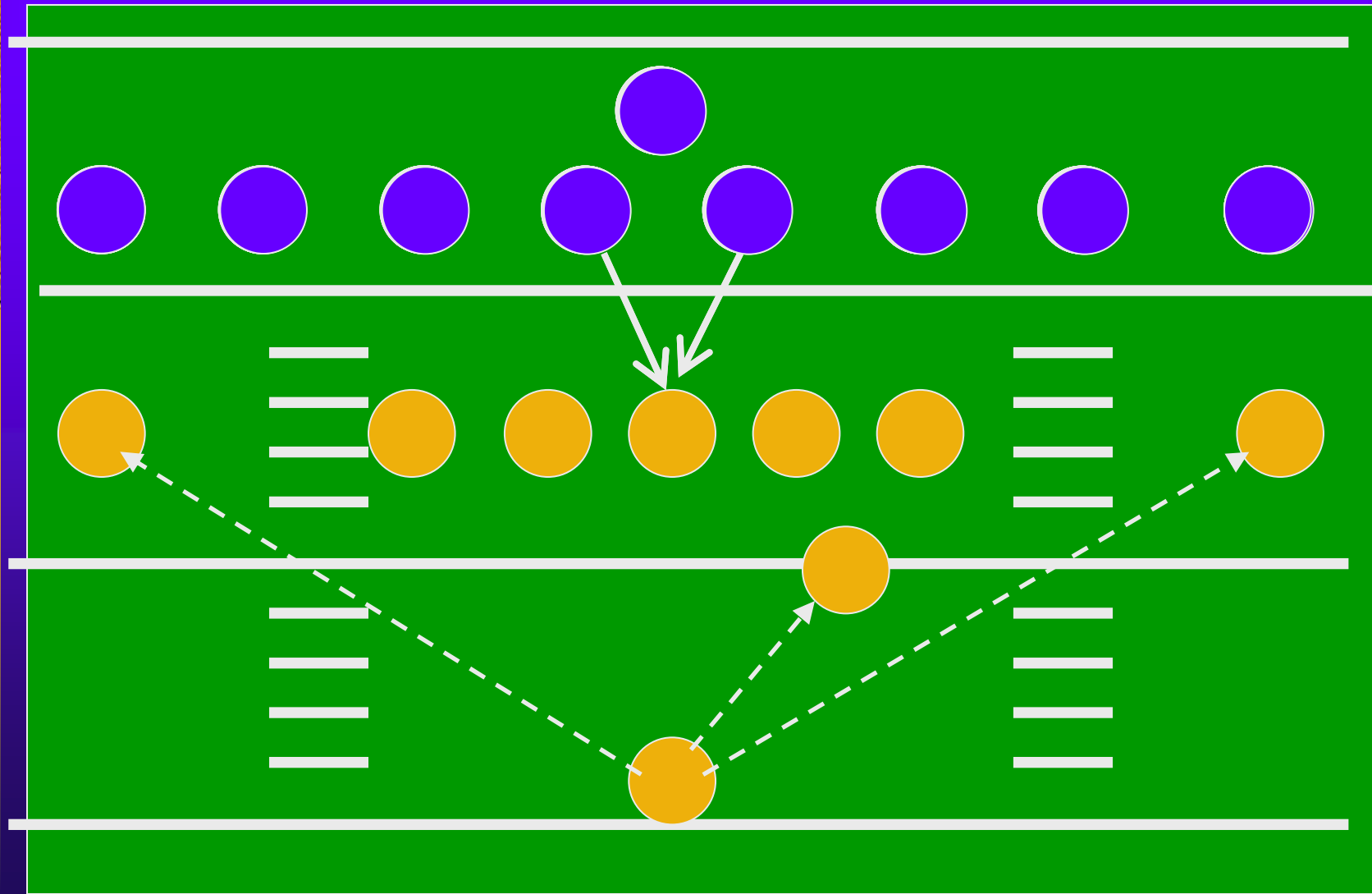
El proceso de Triage



La formación



La Jugada





El rol del administrador de sistemas en la respuesta a incidentes

- Proveer información de fuente primaria
- Elevar la alerta al CSIRT correspondiente
- Recopilar información para ser usada por los siguientes niveles.
- Iniciar el proceso de recuperación y prevención de nuevos incidentes.



Apectos clave

- El Csirt hace pases, rara vez anota.
- Las autoridades competentes deben de recibir toda la información.
- El proceso de triage es la base de un buen manejo de incidentes.
- Las autoridades anotan si todo el proceso funciona.



Asistiendo a las fuerzas del orden

Asistiendo a las fuerzas del orden

- **Análisis de incidentes**

Hay varios niveles de análisis de incidentes y muchos sub-servicios. Esencialmente, el análisis de un incidente es un exámen de la información disponible y la evidencia que la sustenta o de los “artifacts” relacionados con un incidente o evento.



Análisis

- Valoración
 - Uso inapropiado
 - Acceso no autorizado
 - Código malicioso
 - Denegación de servicio
 - Ambiental
 - Comportamiento
- Calificación
 - Amenaza Seguridad nacional
 - Es delito
 - Incidente local
- Análisis del Caso
 - Clasificación
 - Evaluación de riesgos
 - Análisis de impacto





Asistiendo a las fuerzas del orden


- **Recolección de evidencia forense** : la recolección, preservación, documentación, y análisis de evidencia de un sistema de computación comprometido para determinar los cambios al sistema y para asistir en la reconstrucción de los eventos que condujeron al compromiso.
- **Seguimiento o Rastreo** : rastreo de los orígenes de un intruso o del sistema de identificación al cual el intruso tuvo acceso.



Asistiendo a las fuerzas del orden

- **Coordinación de respuesta a incidentes**

El CSIRT coordina la tarea de respuesta entre las partes involucradas en el incidente. Esto generalmente incluye a la víctima del ataque, a otros sitios involucrados en el ataque, y a cualquier sitio que requiera asistencia en el análisis del ataque. Esto también puede incluir las partes involucradas que proveen soporte IT a la víctima, tal como proveedores de servicio de Internet, otros CSIRTs, y administradores de red y sistemas en el lugar.



Requisitos para una adecuada colaboración

- Capacidad de análisis técnico-jurídico
- Protocolos adecuados de:
 - Análisis forense
 - Preservación de la prueba
 - Cadena de custodia
- Elementos de discrecionalidad y confidencialidad

Coordinación





Preguntas?



Muchas Gracias!

Luis A. Gorgona S.

lgorgona@casapres.go.cr

506 2207-9297