ANCI
AGENCIA NACIONAL
DE CIBERSEGURIDAD

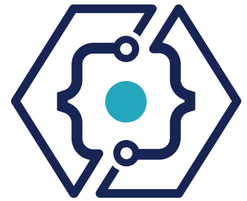
# Respuesta ante Incidentes y Plan de Crisis

Benjamín Iturra
Profesional ANCI

# Objetivo

*Brindar a los participantes los conocimientos y herramientas introductorios para identificar, corregir y recuperarse de un incidente de ciberseguridad de efecto significativo, permitiéndoles minimizar el impacto y fortalecer la resiliencia de sus sistemas ante futuras amenazas.*

# Temario



# Temario

1. Referencias
2. Incidente de efecto significativo
3. Etapas de la Respuesta ante Incidentes
4. Plan de Crisis
5. Aportes de los participantes

# Referencias

# Referencias, ¿por dónde empezar?

## Nacionales:

1. Ley N° 21.663, Marco de Ciberseguridad.
2. DS N° 295, de 2024, del Ministerio del Interior y Seguridad Pública, que aprueba el Reglamento de Reporte de Incidentes de Ciberseguridad.

## Internacionales:

1. CISA – Cybersecurity Incidents Response Playbooks.
2. NIST – Computer Security Incident Handling Guide.
3. MITRE ATT&CK.

# Incidentes de efecto significativo

# Incidente de Efecto Significativo

Ley Marco, Art 27


- Número de personas
- Duración
- Extensión geográfica

*Capaz de interrumpir la continuidad de un servicio Esencial o afectar la integridad física o la salud de las personas, así como en el caso de afectar sistemas informáticos que contengan datos personales.*

# Incidente de Efecto Significativo

Ley Marco, art 27.


- Número de personas
- Duración
- Extensión geográfica

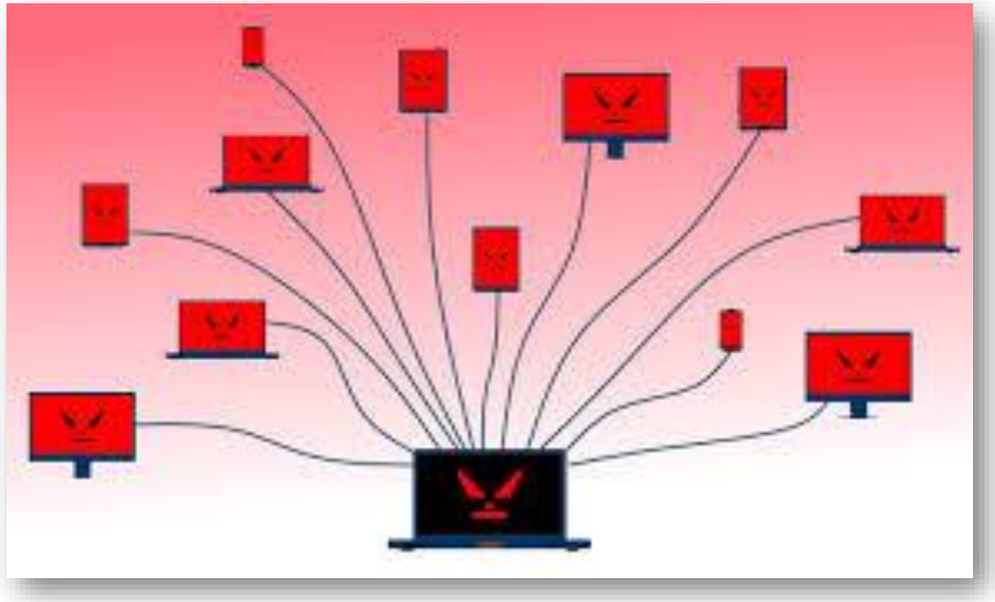
**Ejemplos:**

# Incidente de Efecto Significativo

Ley Marco, art 27.


- Número de personas
- Duración
- Extensión geográfica

**Ejemplos:**



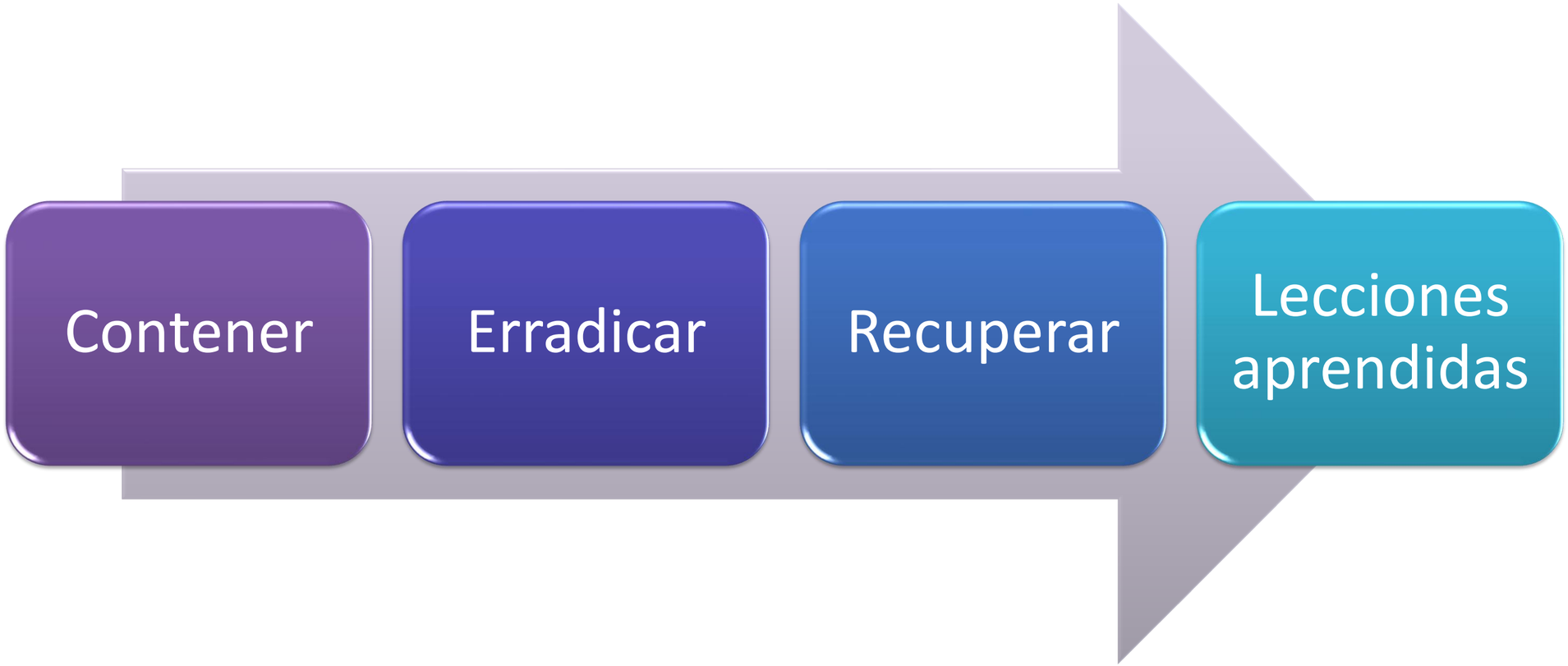
# Incidente de Efecto Significativo

Reglamento de Reporte de Incidentes de Ciberseguridad.
Publicado el 1 de marzo de 2025


- **Interrumpir la continuidad de un Servicio Esencial**
- **Afectar la integridad física o la salud de las personas**
- **Afectar la integridad o confidencialidad de activos informáticos**
- **Utilizar o ingresar sin autorización a redes o sistemas informáticos**
- **Afectar sistemas informáticos que contengan datos personales**

# Etapas de la Respuesta ante Incidentes

# Etapas de la Respuesta ante Incidentes



# Etapas de la Respuesta ante Incidentes

**Contener**

Objetivo: Limitar el impacto del incidente.

Se logra mediante la implementación de una medida reactiva temporal que permite aislar el sistema comprometido.

El éxito de una respuesta ante incidente es directamente proporcional con la velocidad de la contención.

# Etapas de la Respuesta ante Incidentes

**Erradicar**

Objetivo: Eliminar la causa raíz del incidente


**Ejemplos:**

- Eliminación del malware.
- Eliminación de cuentas creadas en el ataque.
- Cambio de credenciales.
- Eliminación de vulnerabilidades explotadas.

Para saber **todas las medidas de erradicación** que deben ser adoptadas en un incidente, es necesario realizar un **DFIR** *(Digital Forensics and Incident Response)*, servicio que ofrece el Equipo de Respuesta ante Incidentes de la ANCI.

# Etapas de la Respuesta ante Incidentes

## Recuperar

Objetivo: Restaurar los sistemas y operaciones afectadas a un estado seguro y funcional.

Se logra mediante la implementación de los respaldos con sus respectivas medidas de seguridad que hagan improbable un ataque de iguales características.


Esta es la etapa en que necesitará su **plan de recuperación ante desastres** y **continuidad operacional**.

# Etapas de la Respuesta ante Incidentes

**Lecciones aprendidas**

Objetivo: Analizar lo ocurrido para mejorar la capacidad de detección, respuesta y prevención de futuros incidentes.

**Ejemplos:**

1. ¿Qué oportunidades tuvimos para haber detectado antes de que ocurriera el incidente?
2. ¿Cuál fue el vector de entrada utilizado por el atacante?
3. ¿Nuestro plan de recuperación funcionó como esperábamos?
4. ¿Qué vamos a hacer si esto vuelve a ocurrir?

Esta es la etapa que le permite al CSIRT Nacional entregar recomendaciones para la comunidad que tiendan a evitar incidentes similares, mejorando la postura de ciberseguridad de todos.

# Plan de Crisis

# Plan de Crisis

## ¿Por qué debemos tener un plan?

- Todos los Ciber Ataques tienen un **propósito y un efecto**, prepararnos nos permitirá responder de forma rápida y coordinada, **reduciendo daños e impactos**.
- Lo anterior nos permitirá contar con una **continuidad operacional** aceptable ante un incidente de efectos significativos.
- Contar con una planificación en la respuesta ante incidentes, nos permitirá **entrenar**, lo que conducirá a perfeccionar aún más nuestros procesos e incluso exportar nuestra experiencia para otros organismos de características similares a este.
- Adicionalmente, una planificación nos permitirá diseñar un **plan de Comunicaciones ante Crisis**.

# Plan de Crisis

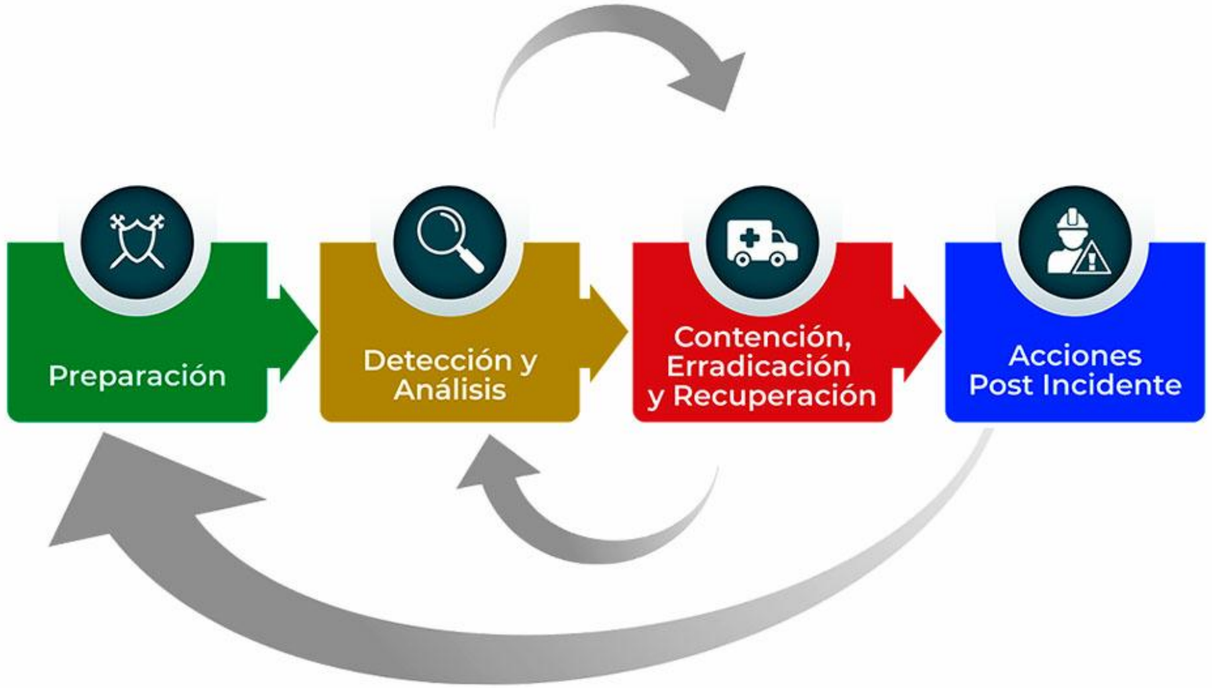
## ¿Qué pasa cuando no tenemos un plan?

La ausencia de plan nos lleva a la improvisación y a la dependencia excesiva de personas claves dentro de la organización, perdiendo la capacidad de gestión ante la ausencia de estos.

Efectos colaterales.


# Plan de Crisis

## Etapas del Manejo y Respuesta ante Ciber Incidentes

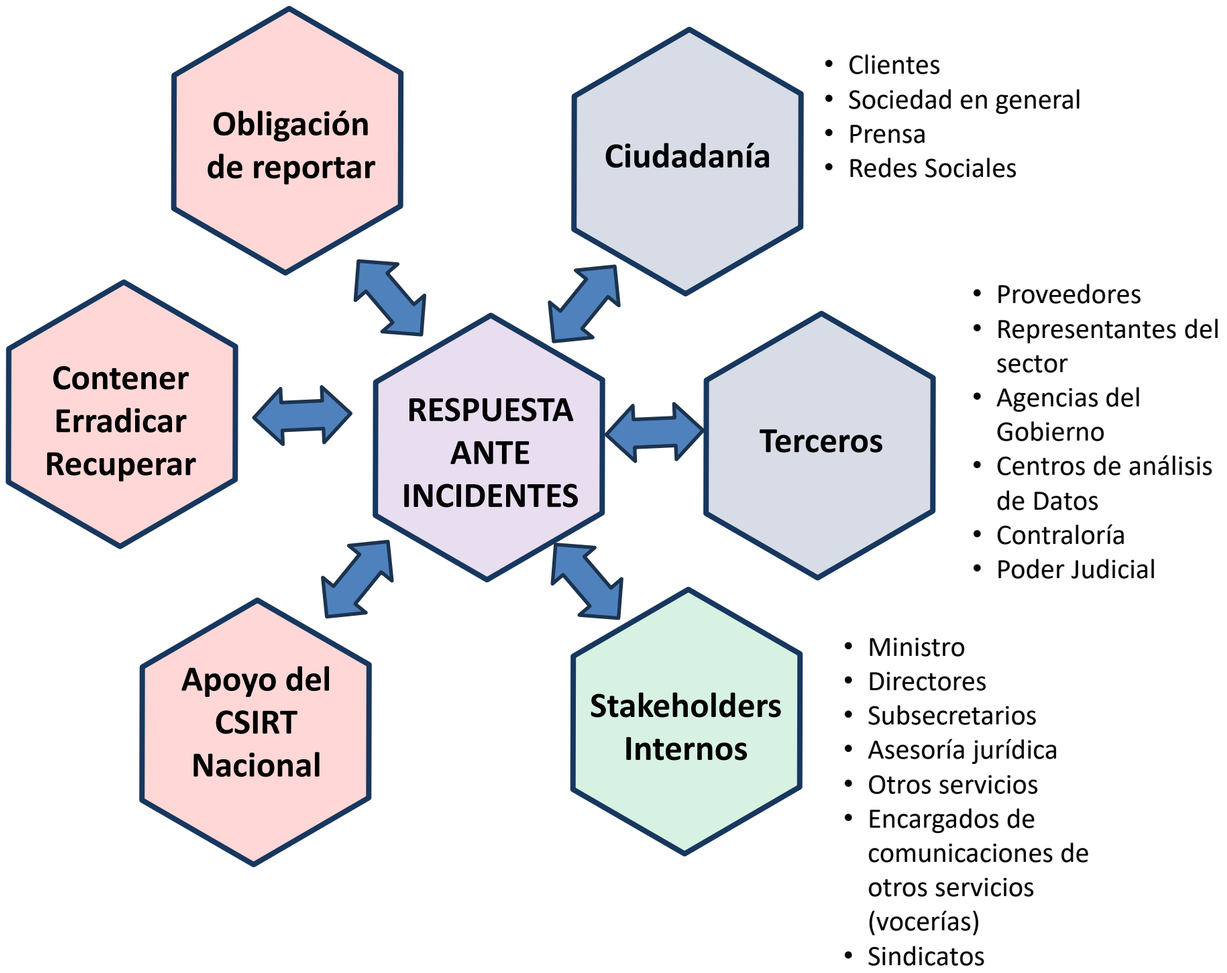



¿En qué etapa estamos?
¿Cuál es el impacto?
¿Cuáles son las implicancias?
¿Quiénes son los responsables?
¿Cuándo se resuelve el incidente?
¿Hay responsables?
¿Qué hay que hacer para que esto no vuelva a ocurrir, recursos, cambios organizacionales?

# Plan de Crisis

## Roles y responsabilidades de actores clave

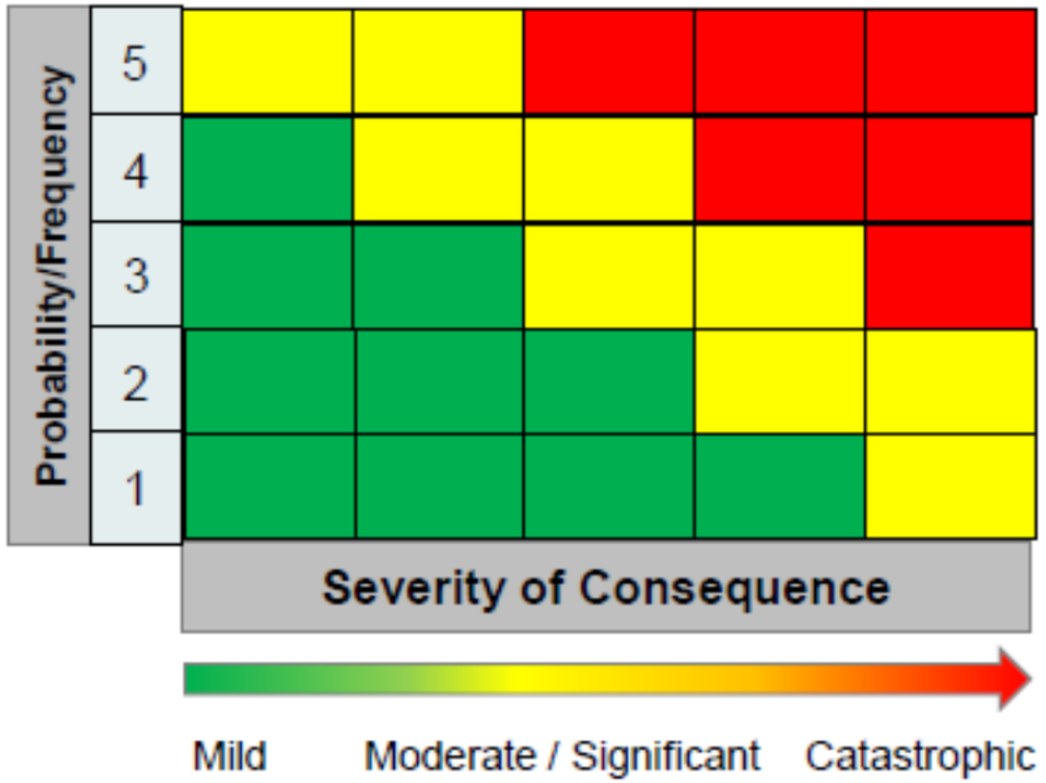
- Importancia de definir un **responsable de liderar** la respuesta ante incidentes.
- Definición de roles y responsabilidades en los distintos niveles.
- Definir severidad e impacto de los distintos tipos de incidentes.
- Desarrollar respuestas diferentes para los distintos tipos de incidentes.
- ¿Qué tiene que decirle el CSIRT a estos grupos?
- ¿Qué tienen que comunicar los distintos grupos al CSIRT?



# Plan de Crisis

## Evaluación de riesgo

*No todos los Ciberataques deben tener la misma respuesta, un incidente que ocurre todo el tiempo probablemente nunca va a requerir que activemos un plan de comunicaciones.*



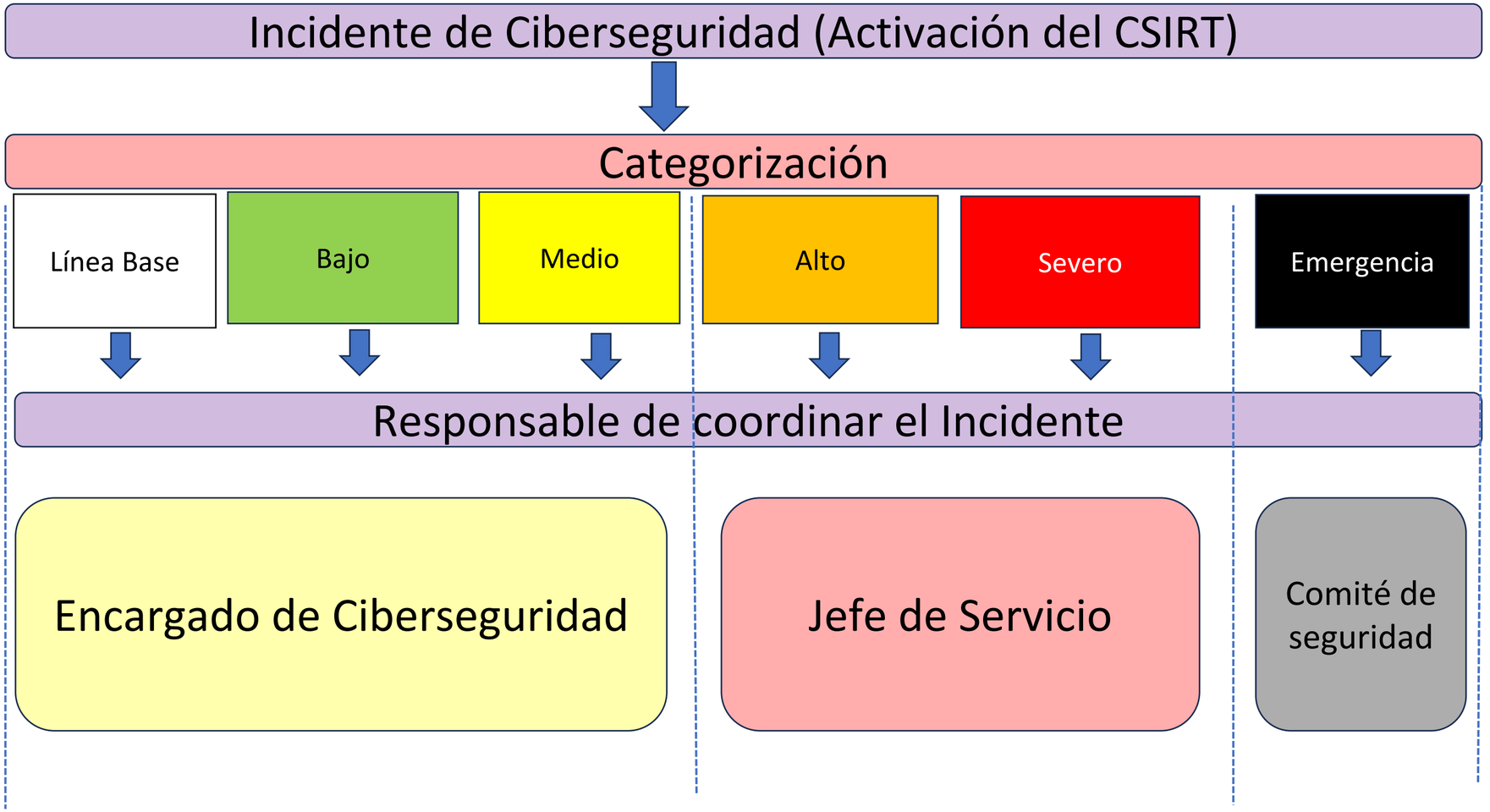
# Plan de Crisis

## Ejemplo de categorización de incidentes

| | Definición general | Ejemplo |
|---|---|---|
| Nivel 5<br>Emergencia (Negro) | Amenaza inminente a la infraestructura crítica | Daño a la infraestructura crítica, afectación a personas |
| Nivel 4<br>Severo (Rojo) | Impacto significativo a los servicios clave de la institución | Ransomware en la red interna. |
| Nivel 3<br>Alto (Naranjo) | Impacto evidente a los servicios clave de la institución | Ransomware en servidores expuestos. |
| Nivel 2<br>Medio (Amarillo) | Posible impacto a servicios clave para la institución | Robo de información, filtraciones u exposición de datos, defacement. |
| Nivel 1<br>Bajo (Verde) | Afectación de algún servicio sin consecuencias importantes | Detección de un malware en un PC por parte del AV |
| Nivel 0<br>Línea Base (Blanco) | Impacto bajo. | Denegaciones de servicio temporales o escaneos de puerto |

# Plan de Crisis

## Ejemplo de coordinación de incidentes



# Aportes de los participantes

# Aportes de los participantes

Seleccione 2 conceptos de los comentados en la charla y comente por qué considera que son relevantes

# ¡Muchas gracias!

anci.gob.cl