



ESCUELA SUPERIOR  
DE GUERRA

"General Rafael Reyes Prieto"

Colombia

# DRP - BCP

# Gestión de Riesgos Continuidad del negocio

- Subtítulo diapositivas Calibri 24 pt



# PROBLEMÁTICA - Riesgos



## Riesgos Económicos

- \* Burbuja de Activos
- \* Crisis de Precios
- \* Falta mecanismos financieros
- \* Inflación inmanejable



## Riesgos Ambientales

- \* Catástrofes Naturales
- \* Falta adaptación al cambio climático
- \* Catástrofes Ambientales por el hombre



## Riesgos Tecnológicos

- \* Afectación de Infraestructura Crítica.
- \* Mal uso de la tecnología



## Riesgos Geopolíticos

- \* Ataques terroristas
- \* Armas de Destrucción masiva
- \* Conflictos de Estado



## Riesgos Sociales

- \* Inestabilidad Social
- \* Migración involuntaria
- \* Crisis de Agua



# PROBLEMÁTICA DE LAS ORGANIZACIONES

HERE'S OUR CURRENT  
DISASTER RECOVERY PLAN



# No es un Plan de Continuidad del Negocio

¿Era mejor salirse o quedarse?

¿Quién ordenó salir?

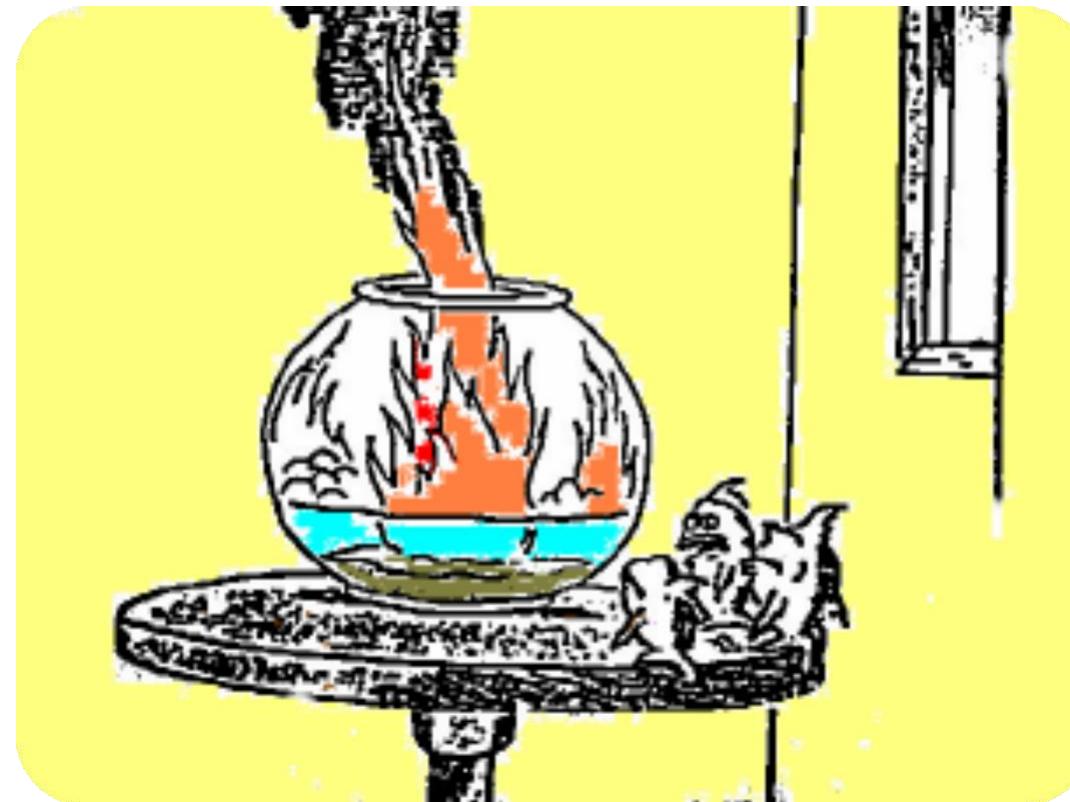
¿En este “sitio alterno” se cuenta con los recursos mínimos para sobrevivir?

¿Cuáles son estos recursos?

¿Cuánto tiempo podremos sobrevivir sin por ejemplo... agua?

Y una vez que se apague el fuego. ¿Cómo regresar?

Bueno gracias al cielo salimos a tiempo... ¿Y ahora qué?



¡Lograr salir sólo es el primer paso!

# Gestión de Continuidad del Negocio, definiciones

## Definición 1 (DRI): Continuidad de Negocio

Proceso de administración que identifica impactos potenciales que amenazan las organización y provee un marco para la construcción de **resilencia** con la capacidad para una respuesta eficaz que salvaguarde los intereses de sus stakeholders, reputación, marca y valor.

Fuente: Disaster Recovery Institute -DRI-.



## Gestión de Continuidad del Negocio, definiciones

### Definición 2 (BCM): Continuidad de Negocio

Todas las medidas preventivas y anticipadas que se puedan implementar para que cuando ocurra **algún evento que interrumpa** el normal desempeño de las actividades productivas del negocio, éste pueda seguir operando.

Fuente: Business Continuity Institute BCI, UK.



## Gestión de Continuidad del Negocio, definiciones

### Definición 3 (BCM): Continuidad de Negocio

La capacidad para dar una respuesta eficaz que salvaguarde los intereses de **sus grupos de interés clave, la reputación, la marca, y las actividades de creación de valor**, identificando las amenazas potenciales para la organización y el impacto en las operaciones que dichas amenazas, de realizarse, podrían causar.

Fuente: ISO 22301 Cláusula 3.4.

# **BCM (BCP) vs DRP**

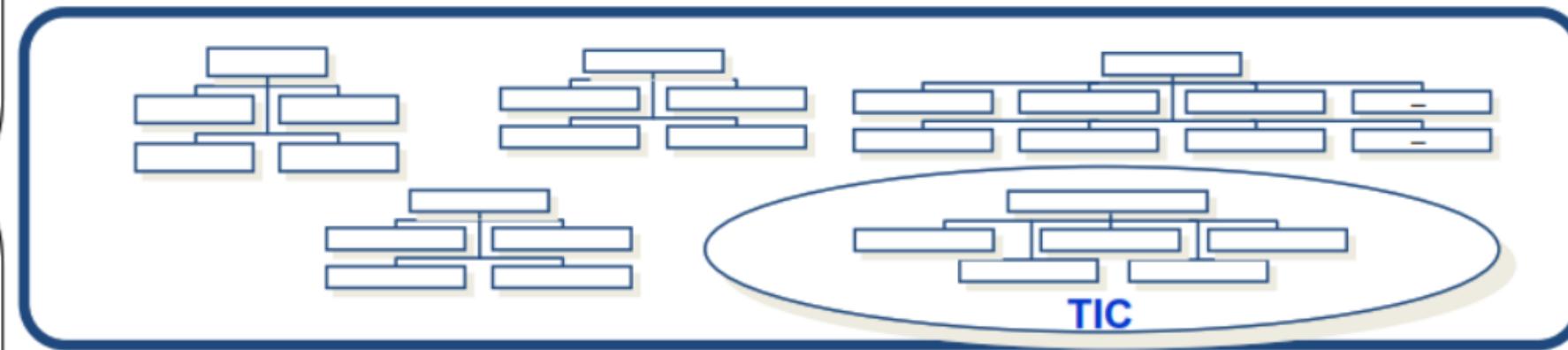
**PLAN DE CONTINUIDAD DEL NEGOCIO**  
**“Recuperación de los procesos de negocio y funciones críticas”**

**PLAN DE RECUPERACIÓN DE DESASTRES**  
**“Recuperación de los servicios de infraestructura TI”**

# BCM (BCP) vs DRP

***PLAN DE CONTINUIDAD DE  
NEGOCIOS – BCP***

B  
C  
M



***PLAN DE RECUPERACIÓN EN  
CASOS DE DESASTRE - DRP***

<b>Característica</b>	<b>Plan de continuidad del negocio</b>	<b>Plan de recuperación de desastres</b>
Objetivo	Mantener las operaciones del negocio en funcionamiento durante una interrupción	Recuperar las operaciones del negocio a su nivel anterior después de una interrupción
Enfoque	Preventivo	Reactivo
Duración	A largo plazo	A corto plazo
Ámbito	Todos los procesos y sistemas críticos	Sistemas y datos críticos
Etapas	Identificación, evaluación, planificación, implementación, prueba y mantenimiento	Identificación, respuesta, recuperación, restauración y lecciones aprendidas

PLAN DE

# RECUPERACIÓN ANTE DESASTRES

DRP

DISASTER  
RECOVERY  
PLAN

DRP

## Mantenimiento

- Plan de mantenimiento
  - Ejercicios
  - Pruebas
  - Capacitación
  - Auditoría Interna
  - Revisión Interna
  - Focalización
  - Hacer medición de cumplimiento
  - Hacer seguimiento
  - Rendir cuentas de resultados

## Pruebas

- Ejercicios
- Pruebas
- Pruebas de escritorio
- Operación en DRP



## Gestión del riesgo, Diseño Servicios Producción

- Alta disponibilidad / Redundancia
- Política y Plan de Backup
- Operación que cumplen con buenas prácticas
- Proveedores cumplen con buenas prácticas

## BIA - Producto del PCN

## Plan

- Estrategia del Plan de Continuidad de Servicios de Infraestructura Tecnológica
- Manual DRP
- Procedimientos

# ANTECEDENTES



Antes del año 2000

Planes de Emergencia  
Planes de Contingencia



Año 2000 Y2K

Plan de Recuperación de  
Desastres de TIC.

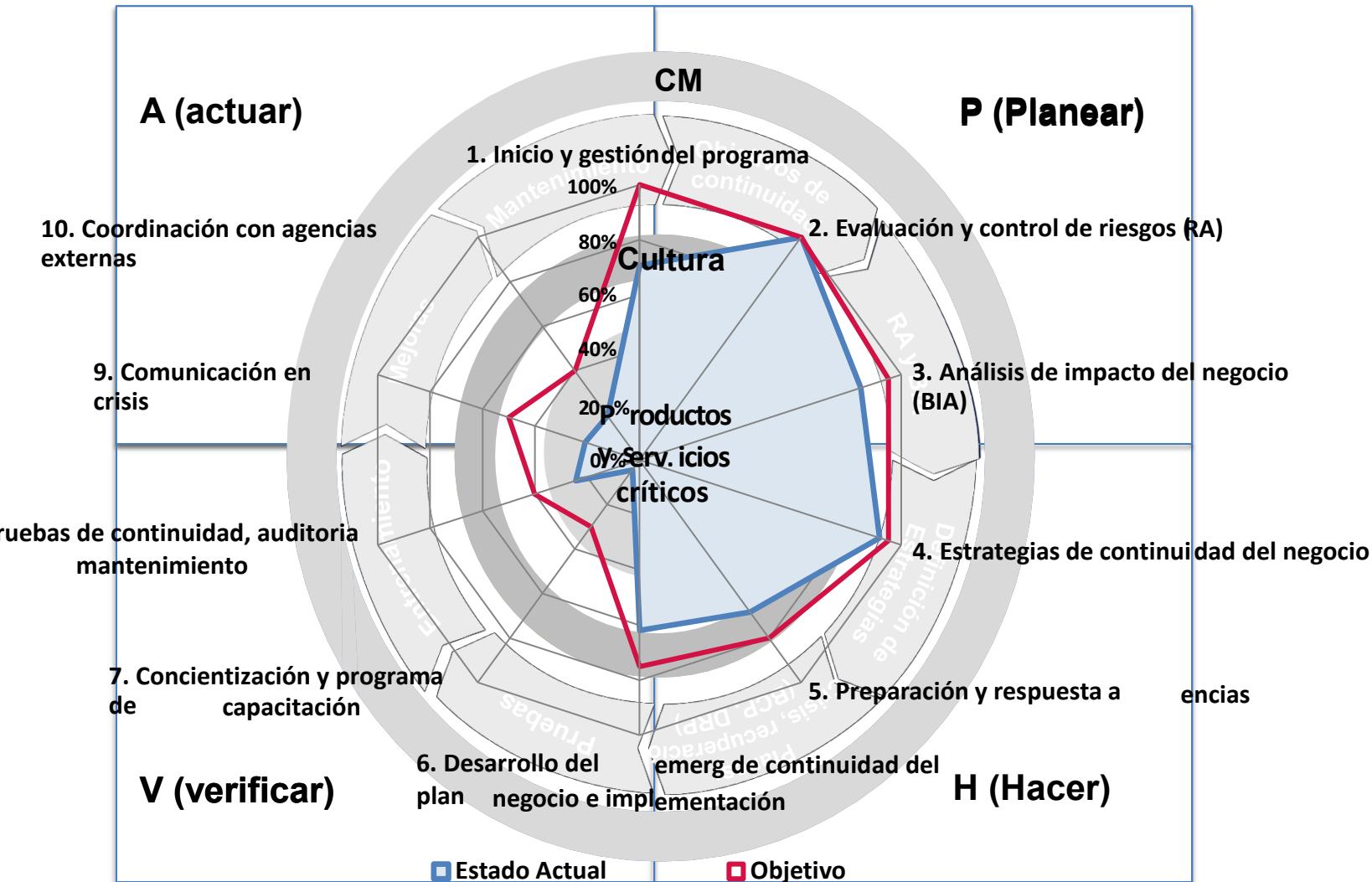


Después del 11 de  
Septiembre

Mejores prácticas y estándares  
Plan de Manejo de Crisis  
Plan de Continuidad del Negocio

# Sistema de Gestión de la Continuidad del Negocio

## IMPLEMENTACIÓN



# Análisis de Riesgos -- Continuidad del Negocio (TI)

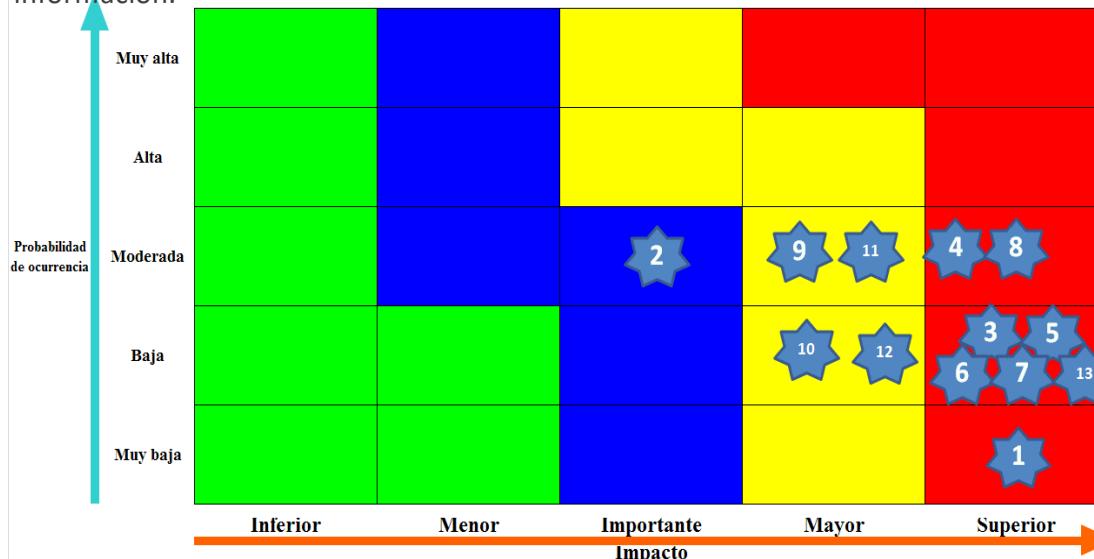
## Actividades

- Identificación de vulnerabilidades
- Identificación de Amenazas del negocio clasificadas en: "Humanas", "Tecnológicas" y "Naturales (Ambientales)".
- Identificación controles existentes.
- Análisis de riesgos de disponibilidad de recursos y funciones críticas del negocio.
- Identificación de roles de los miembros de la organización involucrados en estos servicios o aplicaciones críticas.

Incluirlos en el plan integral de manejo de riesgos  
(Seguimiento y presupuesto)

## Entregables

Informe análisis de riesgos de continuidad de negocio para los sistemas de información.



1. Indisponibilidad de Sede Principal
2. Indisponibilidad de Personal
3. Indisponibilidad de Plataforma de red
4. Indisponibilidad de Sistema 1
5. Indisponibilidad de Sistema 2
6. Indisponibilidad de Sistema 3
7. Indisponibilidad de Sistema 4
8. Indisponibilidad de Correo Externo
9. Indisponibilidad de Cajeros
10. Indisponibilidad de Internet
11. Alta dependencia de contratos de Outsourcing
12. Indisponibilidad de documentación física o electrónica
13. Indisponibilidad de Servicio Telefónico en Call Center

# Análisis de Impacto al Negocio (BIA)

## Actividades

Para cada proceso se establece:

- El impacto.
- Las criticidades.
- Identificación de tiempos objetivos:
  - El punto de recuperación objetivo (Recovery Point Objective – RPO)
  - El tiempo de recuperación objetivo (Recovery Time Objective - RTO)
- Identificación de servicios o aplicaciones críticas de los procesos.
- Estimación de recursos tecnológicos necesarios para el funcionamiento de las aplicaciones o servicios críticos detectados
- Identificación de interdependencias.

Priorización de procesos de Negocio – TOP Process

## Entregables

Informe BIA para los procesos seleccionados

Perfil del Proceso		
Procesos Estratégicos, misionales, apoyo, evaluación y control		
Proceso	Descripción	Criticidad
Dependencia de	Razón	Observaciones
Recurso o Registro Vital	Tipo	Observación
Sistemas	Razón	
Periodo Crítico	Razón	
Operación Normal	Operación en Contingencia	Observaciones
Procedimientos Manuales	Usuarios entrenados en su uso	Observaciones
RTO	RPO	Observaciones
Impacto	Nivel	Impacto Financiero
Económico		
Operacional		
Comercial		
Imagen		
Legal		

Para los que es posible su estimación

# Análisis de Impacto al Negocio (BIA)



# Definición de Estrategias de Continuidad

## Actividades

Se desarrollan **dos alternativas** definiendo los diferentes recursos que se deben adquirir o contratar para implementar la estrategia:

- La relación de recursos, insumos, elementos de hardware y software necesarios para lograr los tiempos objetivos requeridos por el negocio.
- Tipo de procesamiento: Virtualización o consolidación
- Formas de almacenamiento: NAS, SAN
- Sitio de contingencia: Propio, hosting, collocation, hot, warm o cold.
- Aspectos de conectividad: LAN y WAN
- Construcción de una matriz de ventajas y desventajas por alternativa en cada uno de los aspectos (procesamiento, almacenamiento, sitio y conectividad).
- Análisis de Costo / Beneficio por alternativa en cada uno de los aspectos (procesamiento, almacenamiento, sitio y conectividad).

## Entregables

- Análisis Costo/Beneficio para dos (2) estrategias de continuidad de negocio .

Estrategias Generales					
Personas	Type de riesgo	Personas			
	Riesgo	Indisponibilidad de personas claves en los procesos			
Locales	Estrategias de mitigación	Descripción	Beneficio	Requerimientos	Costo
Locales	Type de riesgo	Locales			
	Riesgo	Indisponibilidad de casa matriz			
Tecnología	Estrategias de mitigación	Descripción	Beneficio	Requerimientos	Costo
Tecnología	Type de riesgo	Tecnológico			
	Riesgo	Indisponibilidad de sistemas críticos			
Suministros	Estrategias de mitigación	Descripción	Beneficio	Requerimientos	Costo
Suministros	Type de riesgo	Suministros			
	Riesgo	Indisponibilidad de suministro			
Información	Estrategias de mitigación	Descripción	Beneficio	Requerimientos	Costo
Información	Type de riesgo	Información			
	Riesgo	Indisponibilidad de información física y electrónica necesaria para la operación del negocio			

## Actividades y Entregables

A partir de la estrategia seleccionada se documenta el plan que contiene:

- Desarrollar el cronograma de implementación de la estrategia definida.
- Realización del manual de respuesta a emergencia que describe:
  - Cómo
  - Con qué
  - Quienes
  - Ciclo
  - Notificación
  - Árbol de llamadas
  - Lista de proveedores
- Procedimientos de activación (Declaratoria de alerta) del plan.
- Definición de roles y responsabilidades en la participación de los planes de recuperación.



# **Estándares Well Known para IT DRP**

- NIST requires contingency and continuity plans and management.
- ISO 1799 has a section entitled Business Continuity Management that requires testing, maintaining, and reassessing a business continuity plan.
- COSO requires data center operation controls and transaction management controls in order to ensure data integrity and availability.
- ISACA's COBIT requires uninterruptible power supplies under its Manage Facilities section.



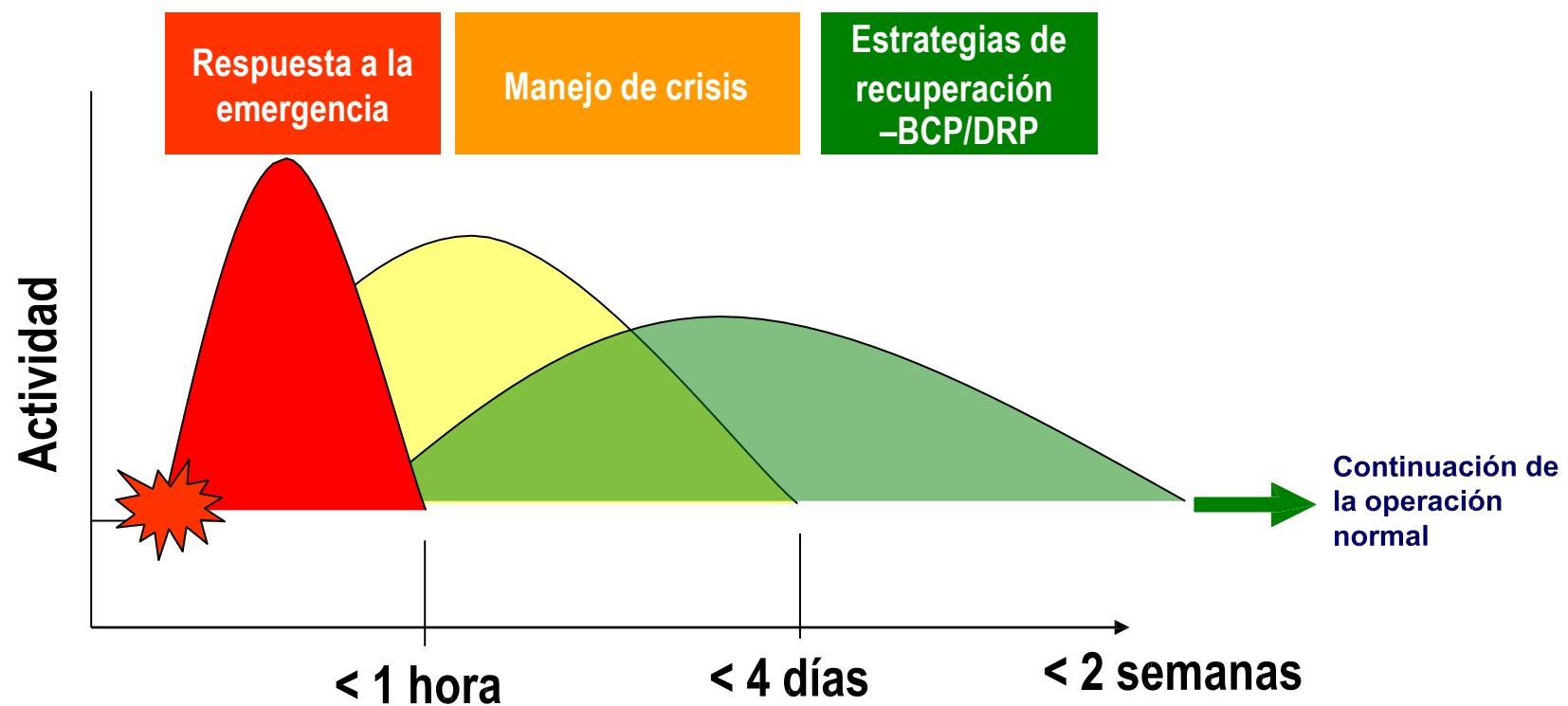
Escuela Superior de Guerra  
"General Rafael Reyes Prieto"  
Colombia



# Conceptos del Plan de Continuidad de Negocio RPO, RTO, WRT, MTD

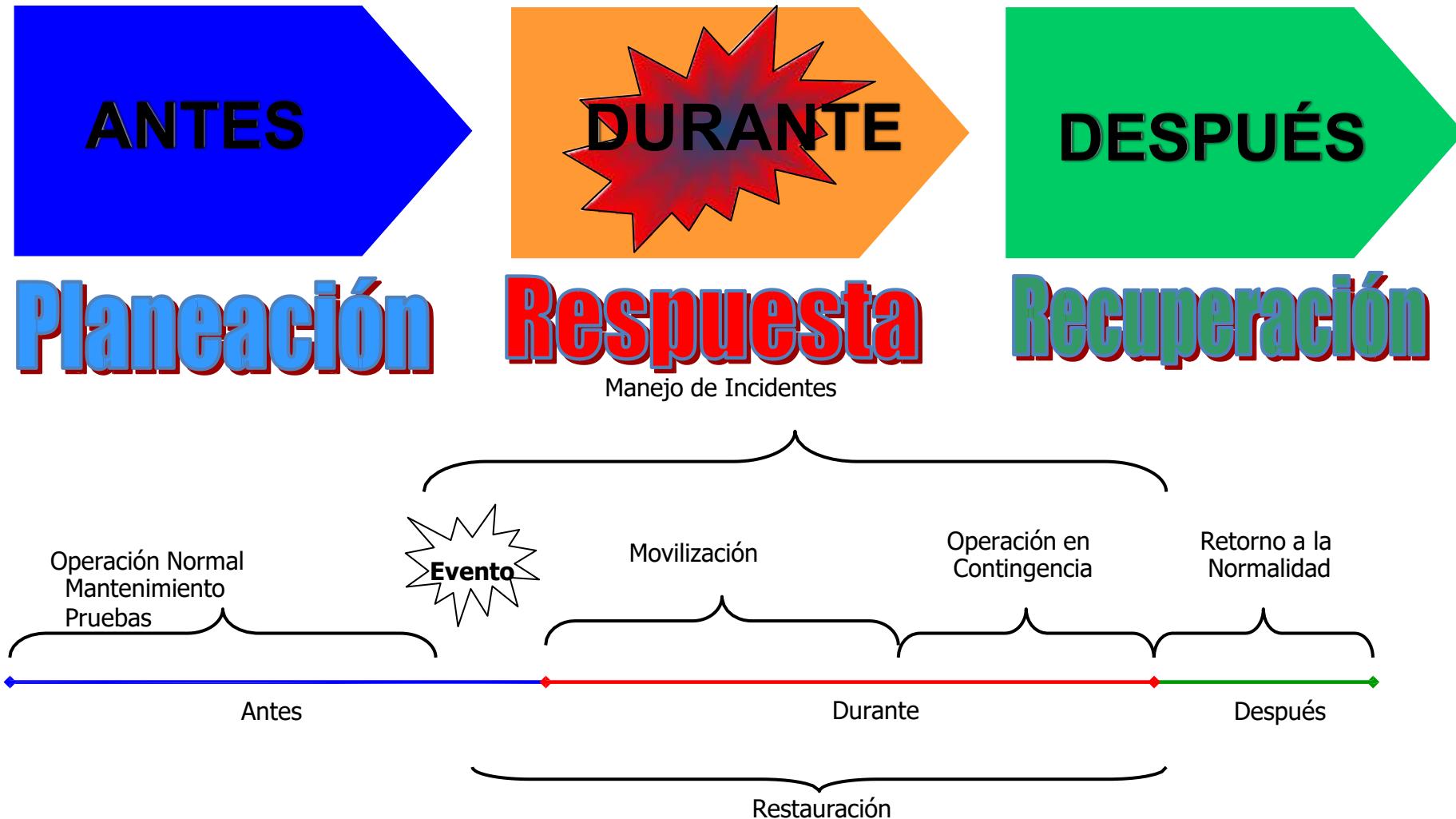
# Desarrollo del Plan del Continuidad del Negocio

## Tiempos



# Ciclo de Manejo de Interrupción

## Desarrollo del Plan de Continuidad del Negocio



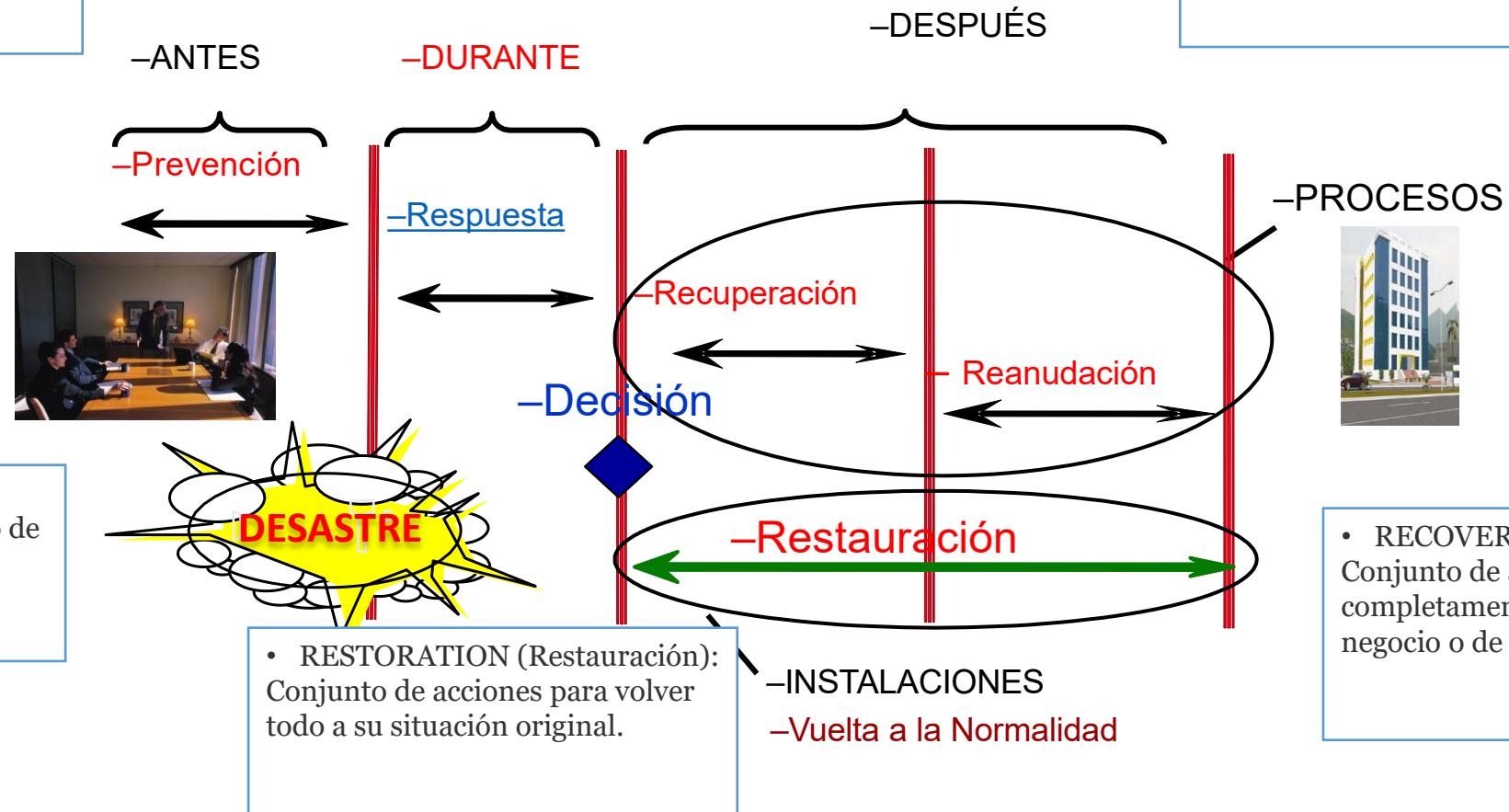
# Desarrollo del Plan de Continuidad

## Metodología PR4

(Prevention, Response, Resumption, Recovery, Restoration).

- PREVENTION  
(Prevención): Conjunto de acciones e iniciativas para prevenir situaciones de riesgo.

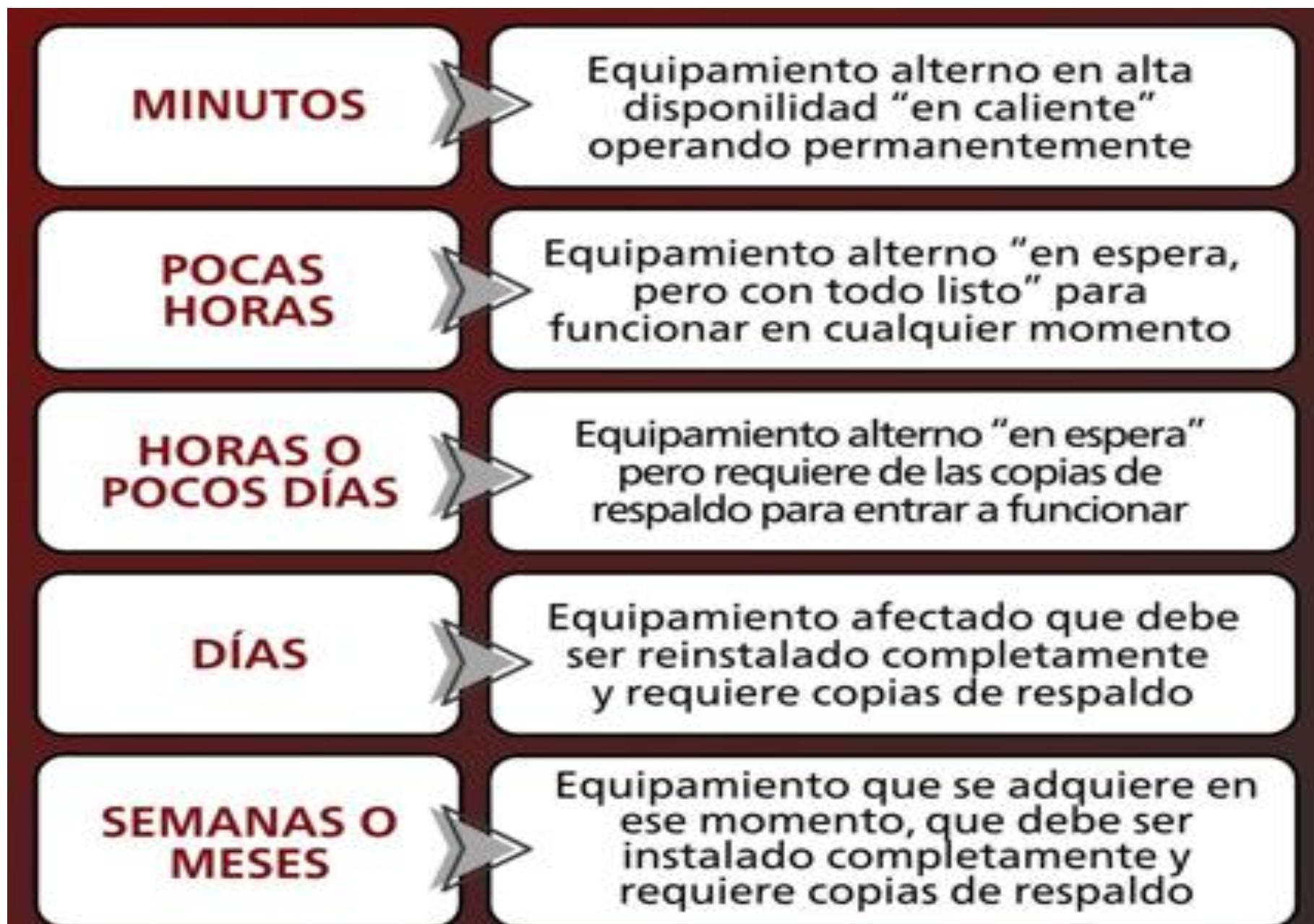
RESPONSE (Respuesta): Conjunto de acciones para evaluar la situación y establecer las acciones de comunicación (a clientes, a empleados, a ciudadanos, a los medios de comunicación, ...)



- RESUMPTION  
(Reanudación): Conjunto de acciones para dar continuidad mínima al negocio o situación.

- RECOVERY (Recuperación):  
Conjunto de acciones para recuperar completamente la funcionalidad del negocio o de la situación

# Soluciones DRP según RTO



# A que nos exponemos sin un DRP-BCP

## Baja de productividad

- Inabilidad para atender a los clientes
- Problemas con la cadena de suministros
- Problemas en la logística de suministros
- Proceso de ordenes

## Daños en la Reputación

- Clientes
- Proveedores
- Bancos
- Socios de Negocio
- Inversionistas
- Agencias Regulatorias

## Gastos Inesperados

Tiempo extra de personal o personal temporal extra, reemplazo o alquiler de equipos, compras de emergencia, costos extra de envíos, gastos de viaje, demandas legales potenciales, etc.



## Ingresos

- Perdidas Directas
- Pagos Compensatorios
- Retraso en Entrega de Servicios
- Perdidas por la Facturación
- Perdidas en las Inversiones

## Rendimiento Financiero

- Multas/Penalizaciones
- Flujo de Efectivo
- Reportes Financieros
- Evaluación Crediticia
- Precio de las Acciones
- Participación del Mercado

# REFERENTES

Guía para realizar el Análisis de Impacto de Negocios BIA



SEGURIDAD Y  
PRIVACIDAD DE  
LA INFORMACIÓN

[https://www.mintic.gov.co/gestonti/615/articles-5482\\_G11\\_Analisis\\_Impacto.pdf](https://www.mintic.gov.co/gestonti/615/articles-5482_G11_Analisis_Impacto.pdf)

Guía para la preparación de las TIC  
para la continuidad del negocio



SEGURIDAD Y  
PRIVACIDAD DE  
LA INFORMACIÓN

[https://www.mintic.gov.co/gestonti/615/articles-5482\\_G10\\_Continuidad\\_Negocio.pdf](https://www.mintic.gov.co/gestonti/615/articles-5482_G10_Continuidad_Negocio.pdf)



<https://www.esap.edu.co/portal/wp-content/uploads/2019/03/Plan-de-continuidad-del-negocio-v1.pdf>

# ACTIVIDAD EN CLASE



# Actividad 1

Relacione la columna 1 con la 2:

a. Riesgo

1. Origen de un riesgo.

b. Falla

2. Acción tomada para mitigar o administrar el riesgo e incrementar la probabilidad de que el negocio/proceso alcance sus metas y objetivos.

c. Factor de Riesgo

3. Procesos, personas, tecnología, infraestructura, externalidades.

d. Control

4. Hecho, falla o amenaza, materializado o no, que podría afectar negativamente la capacidad de la Universidad para lograr sus objetivos institucionales o de procesos, y ejecutar sus estrategias con éxito.

e. Evento de Riesgo

5. Hecho, acción u omisión que podría afectar adversamente la capacidad de la Universidad de lograr sus objetivos institucionales o de procesos, y ejecutar sus estrategias con éxito.

# Actividad N 2

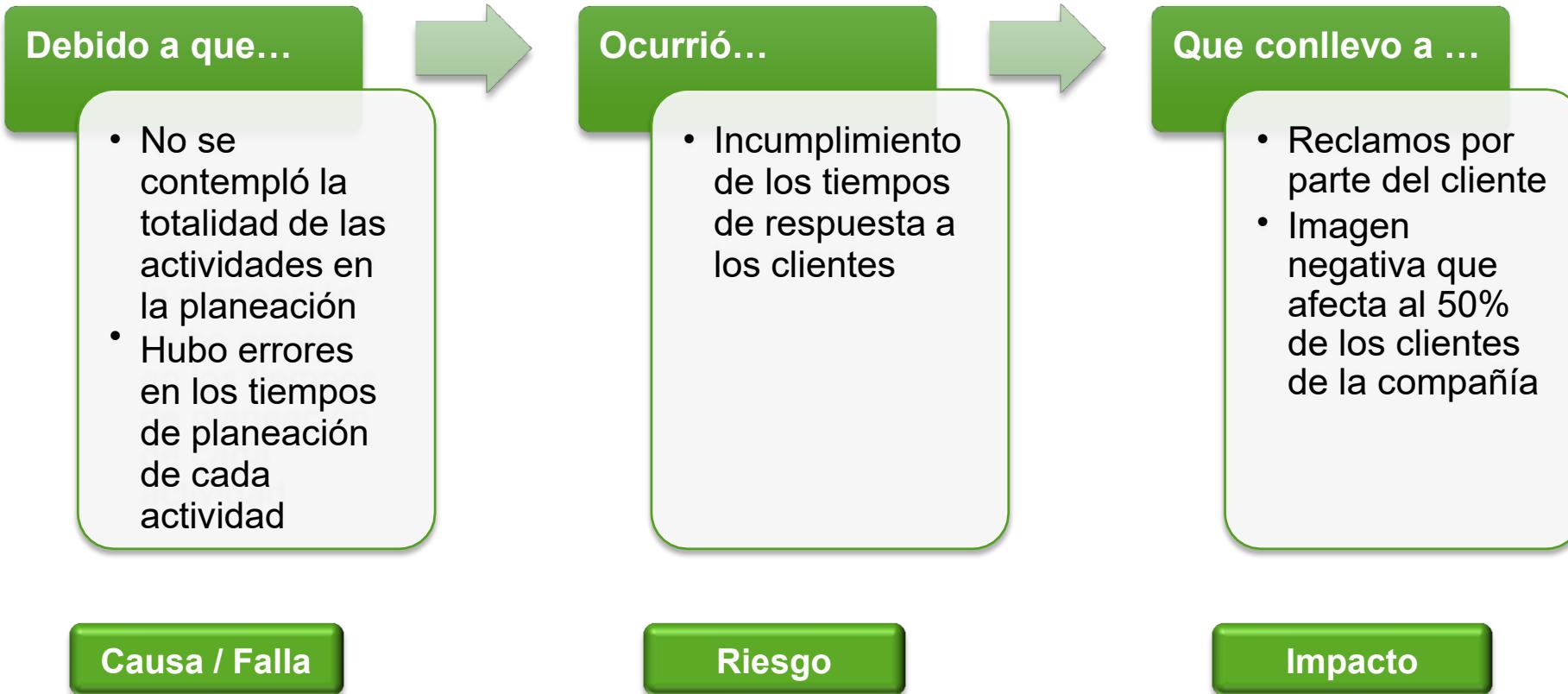
Defina la causa, riesgo y efecto:

## Caso 1

La empresa “Consulto S.A.” se dedica a la consultoría en diferentes temas. En cada uno de sus clientes se elabora un plan de trabajo y se acuerda la fecha de entrega del informe final. En los últimos 3 meses se ha entregado este informe en promedio 5 días después de la fecha inicialmente pactada con el cliente.

# Actividad N 2

Respuesta:



# Actividad N 3

Defina la causa, riesgo y efecto:

## Caso 2

El Auxiliar del Laboratorio de química, en su trabajo rutinario, desarrolló una práctica que incluía la mezcla de dos sustancias químicas altamente contaminantes, el día siguiente a la práctica, empezó a presentar una fuerte irritación en sus ojos que le provocó una incapacidad de 3 días.

# Actividad N 3

Respuesta:



# Actividad n<sup>a</sup>4

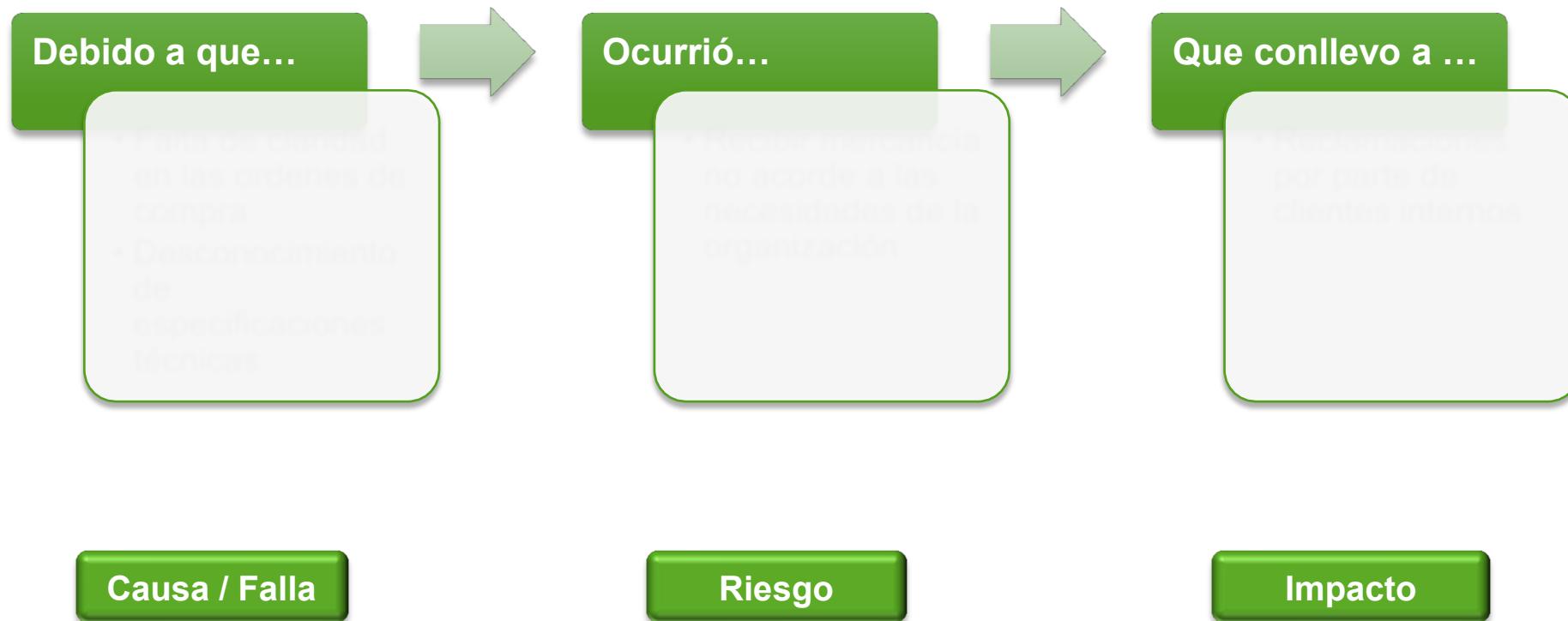
Defina la causa, riesgo y efecto:

## Caso 3:

La compañía “Partemovil S.A.”, dedicada a la importación y comercialización de partes especializadas para automóviles, ha tenido que realizar la devolución de pedidos realizados a sus proveedores, ya que con cumplen con los requisitos de los clientes.

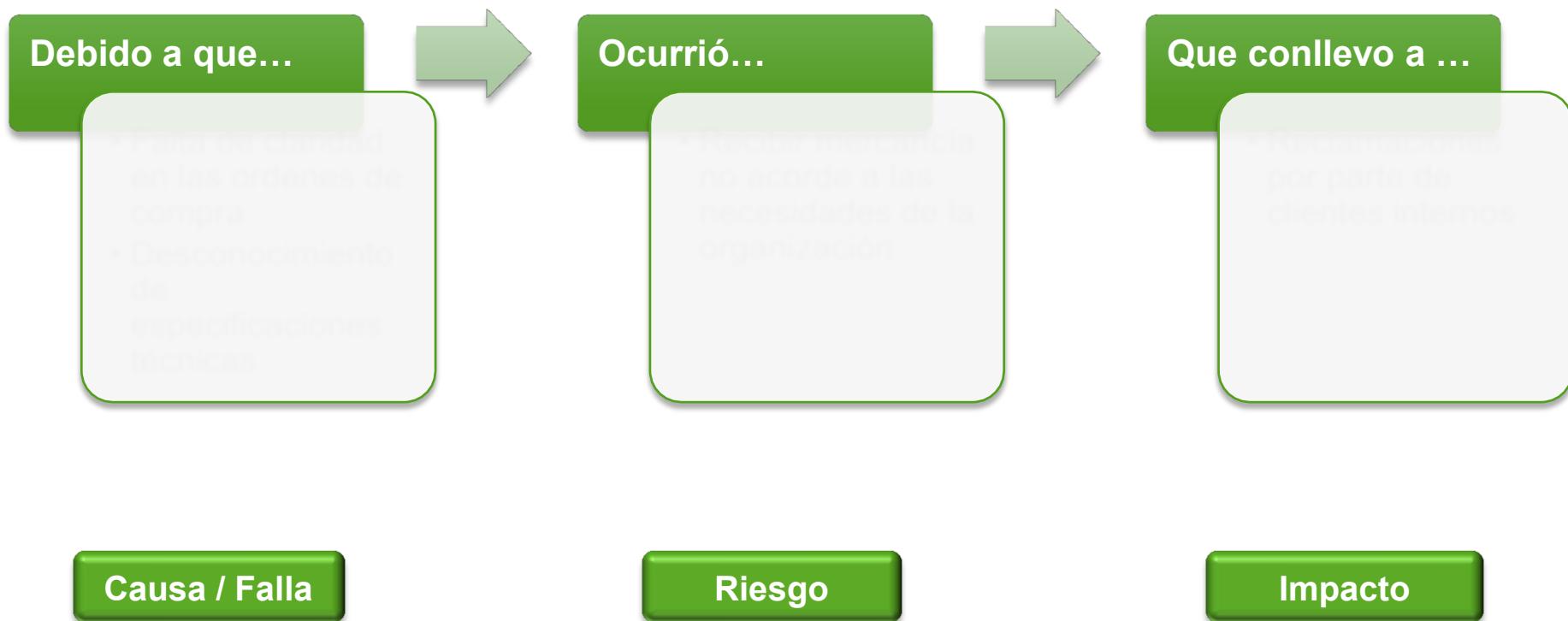
# Actividad N 4

Respuesta:



# Actividad N 5

Proponga 2 enunciados ( situaciones) similares a las anteriores que apliquen al campo de la ciberseguridad.





Escuela Superior de Guerra  
"General Rafael Reyes Prieto"  
Colombia



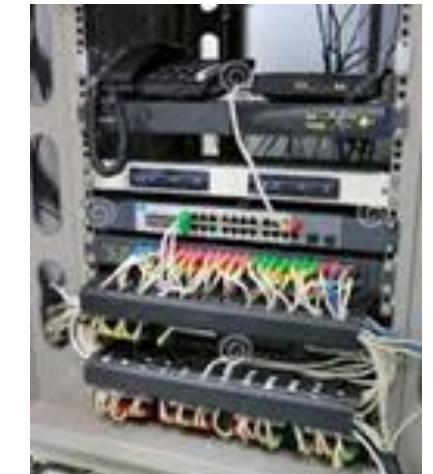
SOC - Security Operations Center  
CSIRT - Computer Security Information Response Team  
CERT - Computer Emergency Response Team

# NOC

Network Operations Center Network  
Centro de operaciones de Red



- Atención y Seguimiento de Fallas (Help Desk).
- Monitoreo de la red
- Operación/Soporte.
- Ingeniería de la Red.
- Administración de Software  
Análisis/Configuración



Interno/Externo/Mixto



# SOC

Security operations center Security  
Centro de operaciones de Seguridad

- Personas / Procesos / Tecnologías .
- Brindan conocimiento situacional a través de la detección / la contención / la reparación
- Se encarga incidentes  
Identificación, validación, priorización, análisis, notificación, investigación.



# Actividades del SOC

Realizar **seguimiento y analizar la actividad** en redes, servidores, puntos finales, bases de datos, aplicaciones, sitios web y otros sistemas, buscando actividades anómalas que puedan ser indicativas de un incidente o compromiso de seguridad.

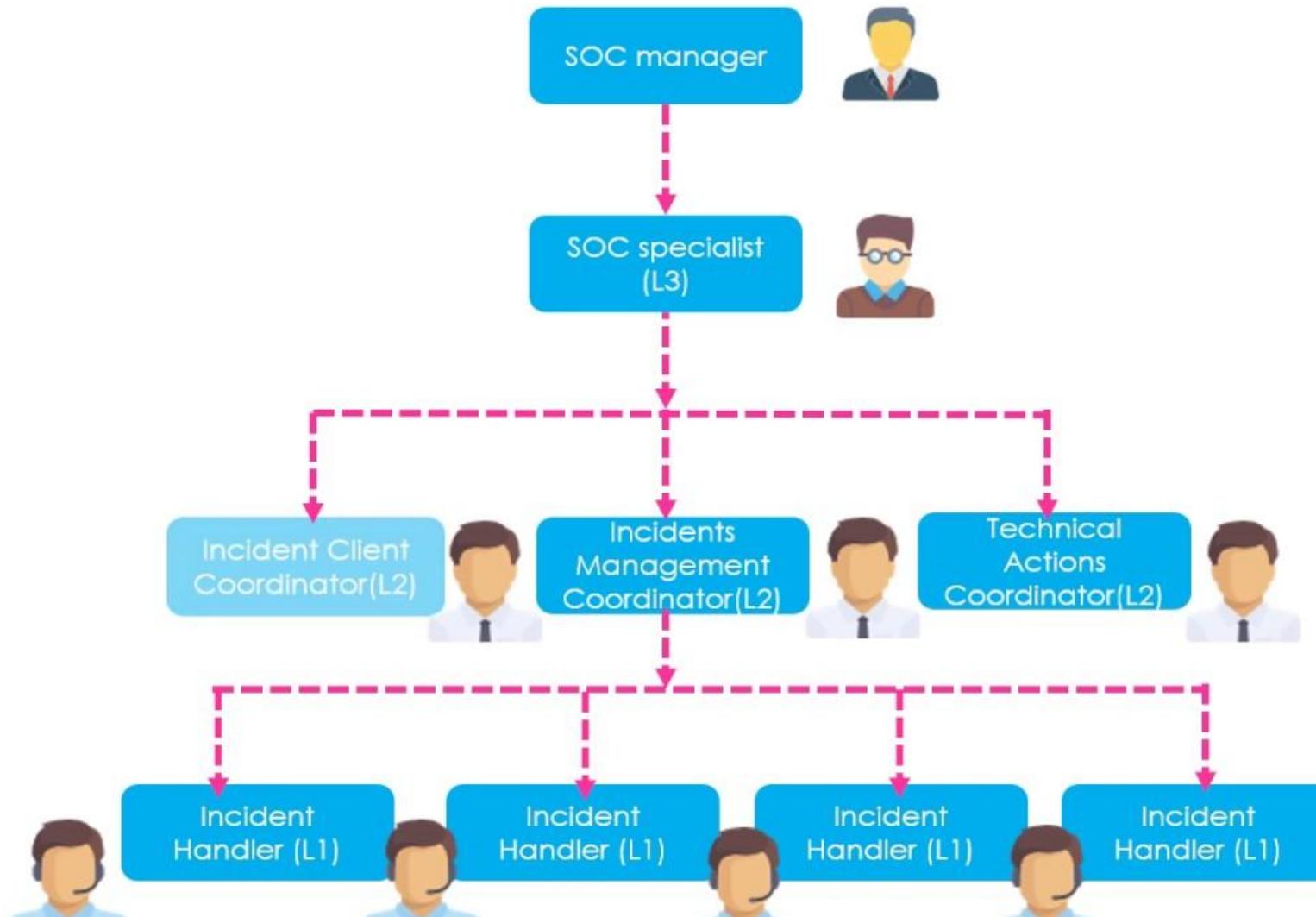
La finalidad de un **SOC** es prestar servicios horizontales en el ámbito de la **ciberseguridad**.

Garantizar que los posibles **incidentes** de seguridad se identifiquen, analicen, defiendan, investiguen e informen correctamente.

## Sus objetivos son:

- Incrementar la capacidad de vigilancia y detección de amenazas en las actividades diarias de los sistemas de información y comunicaciones de una empresa.
- Analizar los ataques o posibles amenazas.
- Recuperar información perdida o dañada que una empresa haya podido tener por consecuencia de dichos ataques.
- Mejorar la capacidad de respuesta ante cualquier ataque.

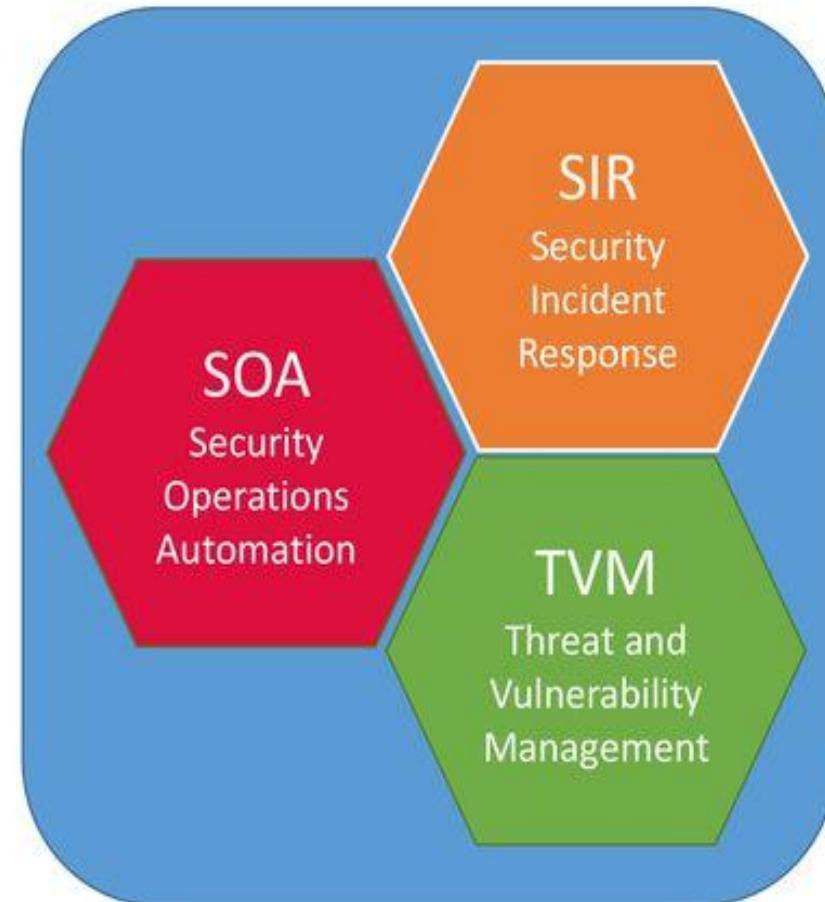
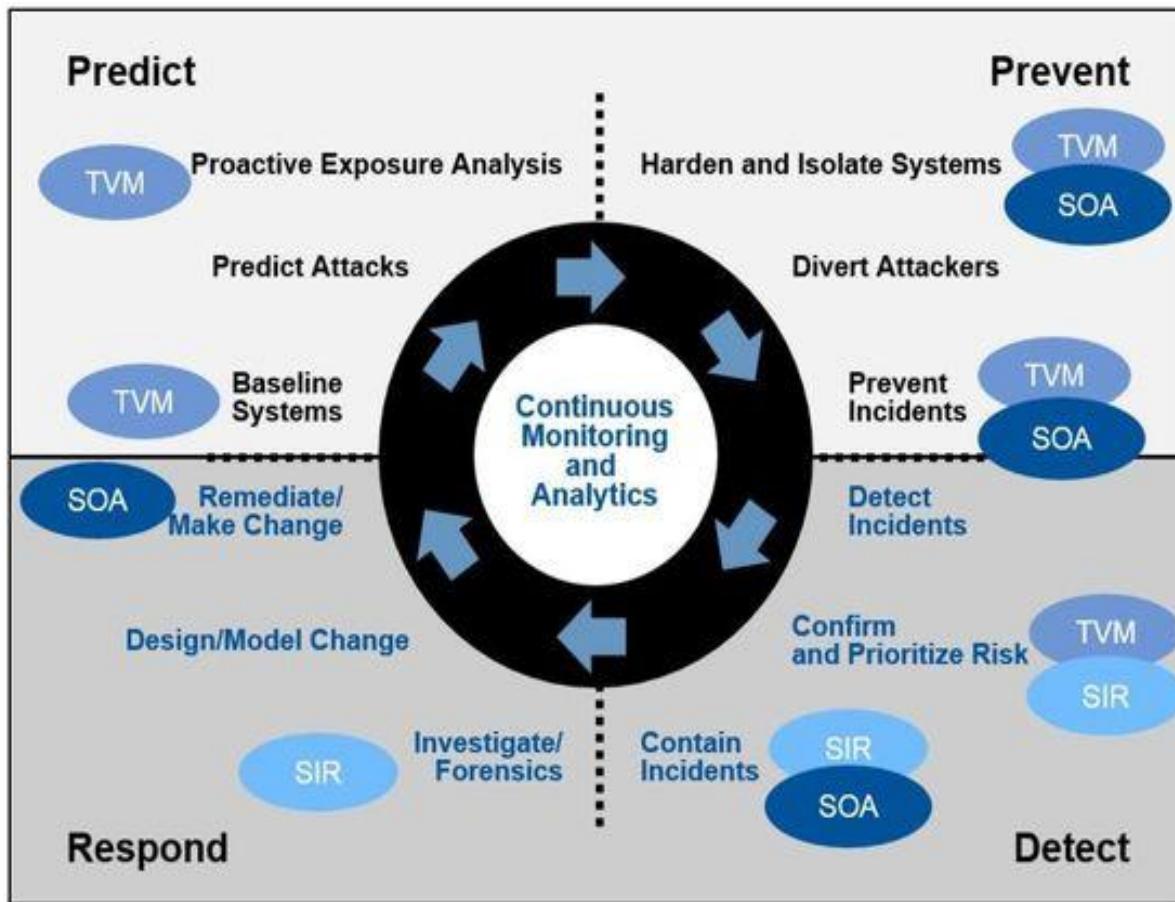
# ¿Cómo se organiza el SOC?



## ¿Qué actividades realiza el SOC?



# Intelligence-Driven SOC



More information: The Five Characteristics of an Intelligence-Driven Security Operations Center, Gartner 2015

# ¿Qué actividades realiza el SOC?

Vigilancia y análisis de activos, mediante **metodologías y procesos estratégicos**.

Estos procedimientos se desglosan en las siguientes tareas identificables:

## Establecimiento conciencia de los activos

Desde un primer momento los **SOC** cuentan con un amplio conocimiento y experiencia de las herramientas y tecnología a su disposición.

## Monitorización continua y proactiva

Los **SOC** toman medidas intencionales para detectar actividades maliciosas antes de que puedan causar un daño, en lugar de enfocarse en medidas reactivas una vez que tiene lugar una amenaza.

# ¿Qué actividades realiza el SOC?

## Clasificación de alertas

Una de las principales tareas de un **SOC** es clasificar las alertas conforme las van recibiendo.

- 1. Monitorización de seguridad.**
- 2. Gestión de incidentes de seguridad.**
- 3. Análisis forense digital y de seguridad.**
- 4. Inteligencia de amenazas.**
- 5. Gestión de vulnerabilidades.**
- 6. Gestión de Logs.**

## Ajuste de las defensas

Gestión de vulnerabilidades y el aumento de la concienciación sobre las amenazas son partes esenciales de la prevención de violaciones de seguridad.

Eso incluye la vigilancia constante del perímetro y las operaciones internas.

# A Working Definition of NOC-SOC

## NOC-SOC *perspective*

### PEOPLE

Network  
Engineer

**SECURITY  
ENGINEER**

Security  
Analyst

### TECHNOLOGY

network  
throughput

**SECURE  
THROUGHPUT**

detection  
rate

### PROCESSES

operational  
efficiency

**SECURITY AWARE  
OPERATIONS**

intelligence  
efficacy



# NOC vs SOC

Parameter	NOC	SOC
Full Form	Network Operations Center	Security Operations Center
Terminology	Used to handle challenges related to managing, monitoring, and controlling the networks in customer IT ecosystem	Tracks threats to infrastructure making attempts to use vulnerability and get inside of an network.
Key Role	To meet service level agreements and manage incidents to achieve maximum uptime.	To protect intellectual property and secure sensitive customer information
Objectives	To monitor performance	To monitor quality
Technology	Real-time data access	Real-time and historical data access
Tools	Fault, trouble and performance monitoring software.	Service quality, customer experience and marketing software.
Skills	<ul style="list-style-type: none"><li>• Network infrastructure</li><li>• Data analytics,</li><li>• troubleshooting and</li><li>• technology know- how.</li></ul>	<ul style="list-style-type: none"><li>• Security infrastructure</li><li>• Service modelling</li><li>• data interpretation</li><li>• communication.</li></ul>
Metrics	Reactive approach	Proactive approach
Business impact	Operational	Strategic
Size	80-500+ engineers	10-100 engineers

# Actividad

Realice una corta descripción de las diferencias entre un NOC y un SOC en:

1. Objetivos.
2. Tecnologías (tipo de acceso requerido a los datos).
3. Habilidades.
4. Métricas usadas (principales).
5. Rol jugado en el impacto al negocio.

- **Establecer mecanismos de comunicación:**

- **Intra-equipo:**

- **Lenguaje estándar**
      - Sin jergas rebuscadas.
      - Conociendo nomenclatura del sector.
        - IOC = Indicadores de compromiso.
        - RIG = Kit de exploits común.
        - IPS = Sistema de prevención de intrusos.

- **Identificadores únicos de:**

- Recursos / Locaciones / Servicios.

- **Software de comunicación.**

- **Todo el equipo conectado**

- **Establecer horarios de disponibilidad.**

- **Con pares:**

- **¿Quienes son? ¿Cómo me pueden ayudar?**  
¿cuándo acudir?
    - **¿Cómo puedo ayudarlos?**

- **Inventario / Identificación / clasificación activos TIC:**

- **Información**

- Metadatos / Bitácoras

- **Hardware**

- Portátiles
    - Móviles
    - IoT
    - Ciberfísicos

- **Software**

- Bases de datos
    - Web / Cloud
    - Apps

- **Servicios**

- **Redes**

- **Inventario / Identificación / clasificación activos TIC:**
  - Información
    - Metadatos / Bitácoras
  - Hardware
    - Portátiles
    - Móviles
    - IoT
    - Ciberfísicos
  - Software
    - Bases de datos
    - Web / Cloud
    - Apps
  - Servicios
  - Redes

- **Inventario/identificación de activos no TIC críticos.**
  - Fluido eléctrico.
  - Conectividad
    - Internet - servidores onLine/Cloud.
  - Infraestructura.
  - Buen nombre
  - Clima / plagas / polvo / sal marina...
  - Relaciones con:
    - Directivos, implicados, clientes, proveedores
    - Pares, entes de control.
  - Personal con condiciones especiales.
  - Secretos industriales.
  - Propiedad intelectual.

## Actividades del SOC

### Actividades preventivas

- **Definición de incidentes y prioridad**
- **Aseguramiento de plataformas**
  - Servidores.
  - Apps / WebApps.
  - Estaciones de trabajo.
    - Conectores red / periféricos
  - Análisis de bitácoras.
    - Centralizado.
    - Distribuido.
- **Auditorías periódicas.**
  - Aconsejar / Capacitar personal.
    - moodle
  - Prevenir.

- **Monitoreo de Infraestructura**
  - Comunicaciones / Almacenamiento.
  - Comparar con línea base
    - Periódicamente.
    - Homogénea a su establecimiento.
    - Identificar cambios:
      - Detectar posibles ataques.
      - Identificar falsos positivos.
    - Ajustar línea base.
    - Reaccionar oportuna y adecuadamente.
      - ¿desconectar equipo?
      - ¿interrumpir comunicaciones?
      - ¿establecer el tipo de ataque?
  - Monitorix.
  - Tripwire.

## Actividades del SOC

### Actividades preventivas

- **Plan y operación de backups.**
  - Simulacros de recuperación.
  - Cuantificar/valorar el tiempo de:
    - Generación.
    - Recuperación.
- **Plan de mejora continua del SOC.**
  - Adquisición de nuevas herramientas.
  - Capacitación permanente.
  - Canales de comunicación para:
    - Identificar nuevas amenazas.
    - Adoptar buenas prácticas y procedimientos.
- **Actualizar los inventarios.**

- **Detección de ataques**
  - Software especializado.
    - Antivirus.
    - NIDS - detección de intrusos.
  - Actualizado.
  - Honeypots.
- **Disposición final / Retención de la información.**
- **Plan de continuidad / recuperac.**
  - Simulacros.

## Actividades del SOC

### Actividades reactivas

#### ● **Triaje de incidentes**

##### – Verificación inicial.

- ¿Está sucediendo?
- ¿que tan peligroso es?
- Valor/identificación de los activos expuestos/afectados.
- Nivel jerárquico del personal afectado.

##### – Reducir falsos positivos.

##### – Priorización.

##### – Trabajo durante la operación de la infraestructura informática

#### ● **Priorización**

- Orden de los servicios a restablecer.
- Identificar el mínimo nivel obligatorio.

#### ● **Verificación**

- De la afectación.
- Sanidad de los backups

#### ● **Recuperación.**

- De los backups.
- Reinstalación de aplicativos.

#### ● **Estabilización.**

- De la prestación del servicio.
- Prevención de repeticiones.
- Capacitación / Divulgación.

# ¿CERT/CSIRT/CIRT o SOC?

SOC

CSIRT



IRT (Incident Response Team, equipo de respuesta a incidentes)

CIRT (Computer Incident Response Team, equipo de respuesta a incidentes informáticos)

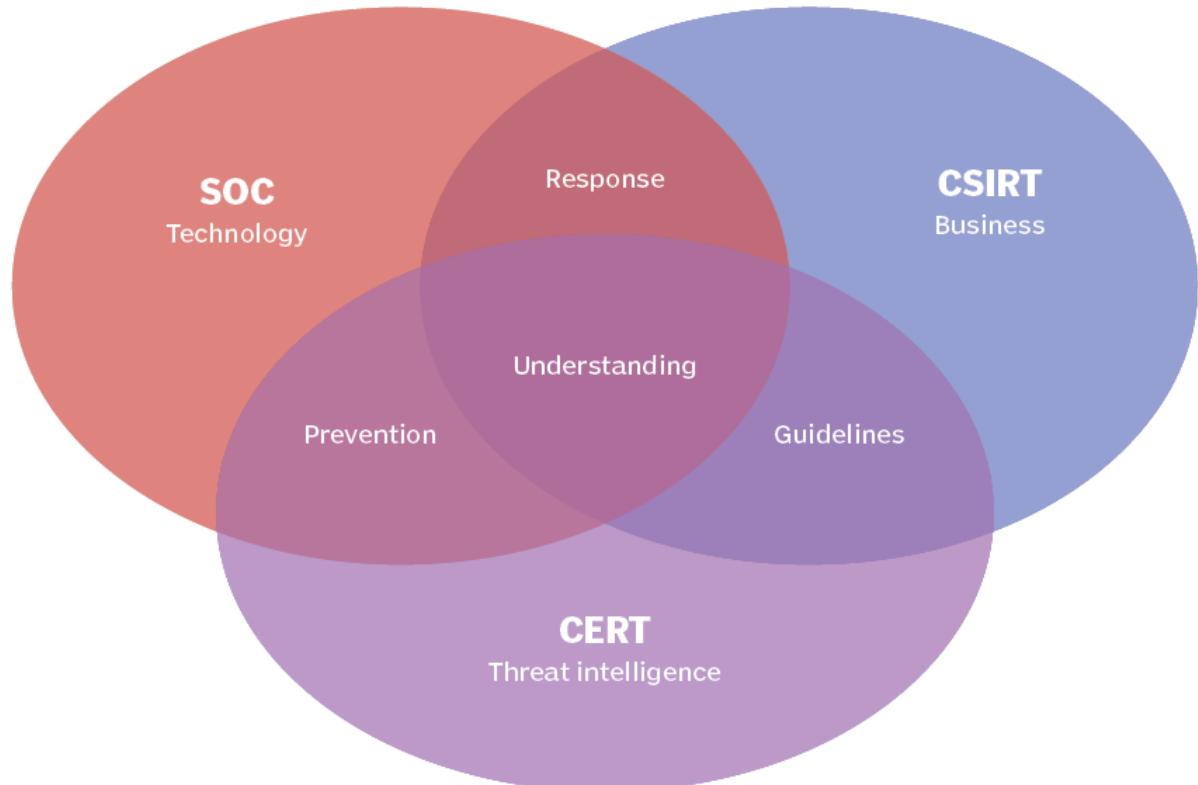
**SOC**  
Security operations center Security  
Centro de operaciones de Seguridad

CERT o CERT/CC (Computer Emergency Response Team / Coordination Center, equipo de respuesta a emergencias informáticas / Centro de coordinación)

SERT (Security Emergency Response Team, equipo de respuesta a emergencias de seguridad)

CSIRT (Computer Security Incident Response Team, equipo de respuesta a incidentes de seguridad informática)

# Comparing CSIRT, CERT and SOC



# Madurez CIRT según la OEA

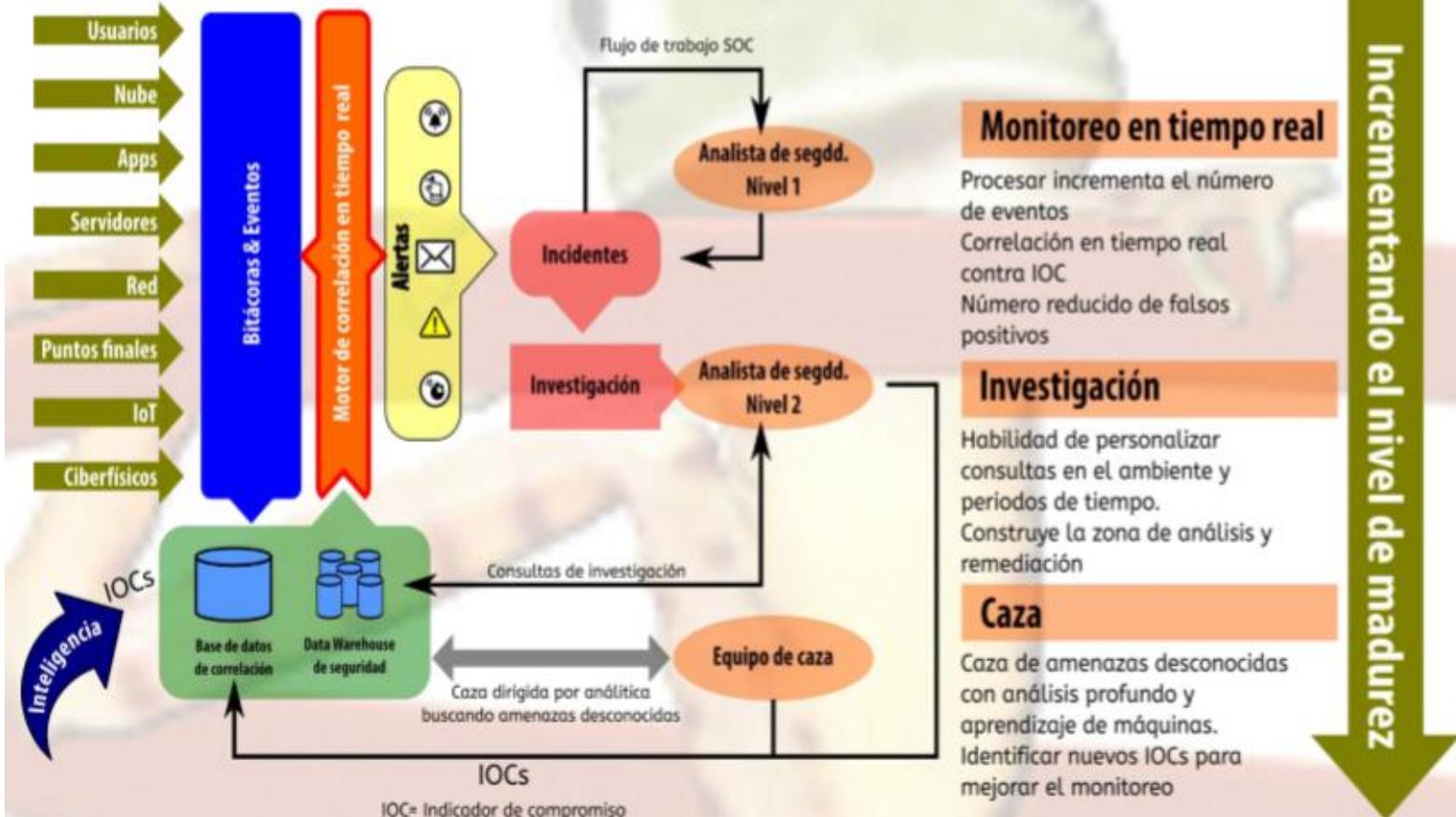


OEA - Documento "Buenas Prácticas para establecer un CSIRT nacional"

Fuente: <https://www.skinait.com/soc-csirt-Escritos-54/>

# Actividad

## Modelo HP



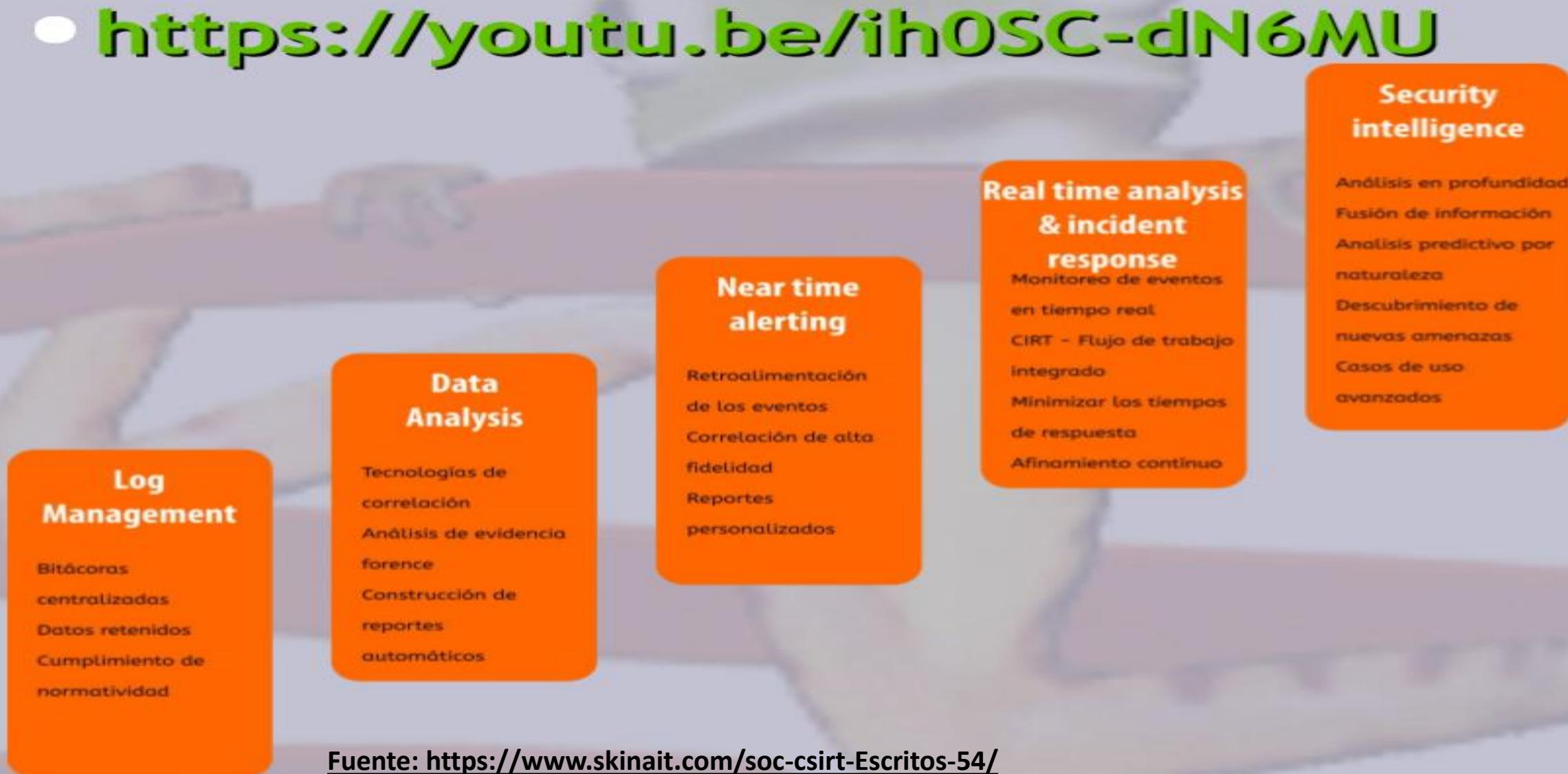
Fuente: Paul Brettle, Hewlett Packard

<https://www.youtube.com/watch?v=ih0SC-dN6MU>

Fuente: <https://www.skinait.com/soc-csirt-Escritos-54/>

# HP's: Security Intelligence Capability

- <https://youtu.be/ihOSC-dN6MU>



# Herramientas de soporte al SOC

- **Sistema de gestión del ciclo de vida de los incidentes.**
  - Visibilidad.
  - Trazabilidad.
  - Control.
  - Análisis.
  - Gobernabilidad.
  - Centralizada.
  - Ubiqua.
  - Punto único de reporte.

- **Inventario:**
  - Activos
    - TIC
    - No TIC - críticos
  - Personal
- **Base de datos de conocimientos.**
  - Alimentada desde diferentes fuentes.
  - Acceso abierto para todos.
  - Construcción colaborativa/moderada.
  - Interacción con pares.
- **GLPI** <https://glpi-project.org/>

# Herramientas de soporte al SOC

- **Monitoreo centralizado y automatizado de bitácoras.**

- Nagios
- Solarwinds

Zabbix  
Pandora

- **Monitoreo centralizado y automatizado de bitácoras.**
  - Nagios
  - Solarwinds
- **Alerta ante cambios críticos:**
  - Tripwire.

# Tripwire

Tripwire Log Center

File View Options Help

Views | Dashboard: Ev |

Events

Display data for: Events | Layout: Events overview

Status Overview

Overall Status

Total Events: 374584 Filtered Events: 374584

Unique Rules: 19 Filtered unique Rules: 19

Events last refreshed: 05/02 13:30:45 Last Event time: 05/02 13:29:44

Top 10 Priorities

Priority	Count
High	2254
Med	2800
Info	334001
Low	35522

Top 10 Vulnerable Hosts

Top 10 Host Names

Host Name	Percentage
Alderaan	26%
Coruscant	41%
Endor	31%
Empire galaxy ffa	0%
Degobeh galaxy ffa	0%
IP360	0%
IMPACT	0%
Hoth	0%
ETL	0%
DNS Timed out	2%

Top 10 Event Sensors

Sensor	Count
TLC galaxy ffa	228
Degobeh galaxy ffa	74174
Empire galaxy ffa	259059
Tatooine galaxy ffa	642
Coruscant	2243
Naboo	2218
Endor	764
192.168.97.52	35228
kamino galaxy ffa	28

Top 10 Src IP Addresses

IP Address	Count
127.0.0.1	3520
172.31.42.151	9
172.31.42.156	31321
192.168.97.52	234
192.168.97.59	185
192.168.97.102	259103
192.168.97.103	74174
192.168.97.103	642
192.168.97.151	2243

Top 10 Dst IP Addresses

IP Address	Count
127.0.0.1	3520
172.31.42.151	9
172.31.42.156	31321
192.168.97.52	234
192.168.97.59	185
192.168.97.102	259103
192.168.97.103	74174
192.168.97.103	642
192.168.97.151	2243

Destination IP Address Map

Resources

Fuente: <https://www.skinait.com/soc-csirt-Escritos-54/>

C pandorafms.com/es/descargar-pandora/  
iones Billing Management... CURSOS\_2020 RECURSOS\_C



Pandora FMS Community

<https://pandorafms.com/es/>

ZABBIX

of experience Free and Open Source Software installations worldwide

## Monitor anything

Solutions for any kind of IT infrastructure, services, applications, resources

Network monitoring

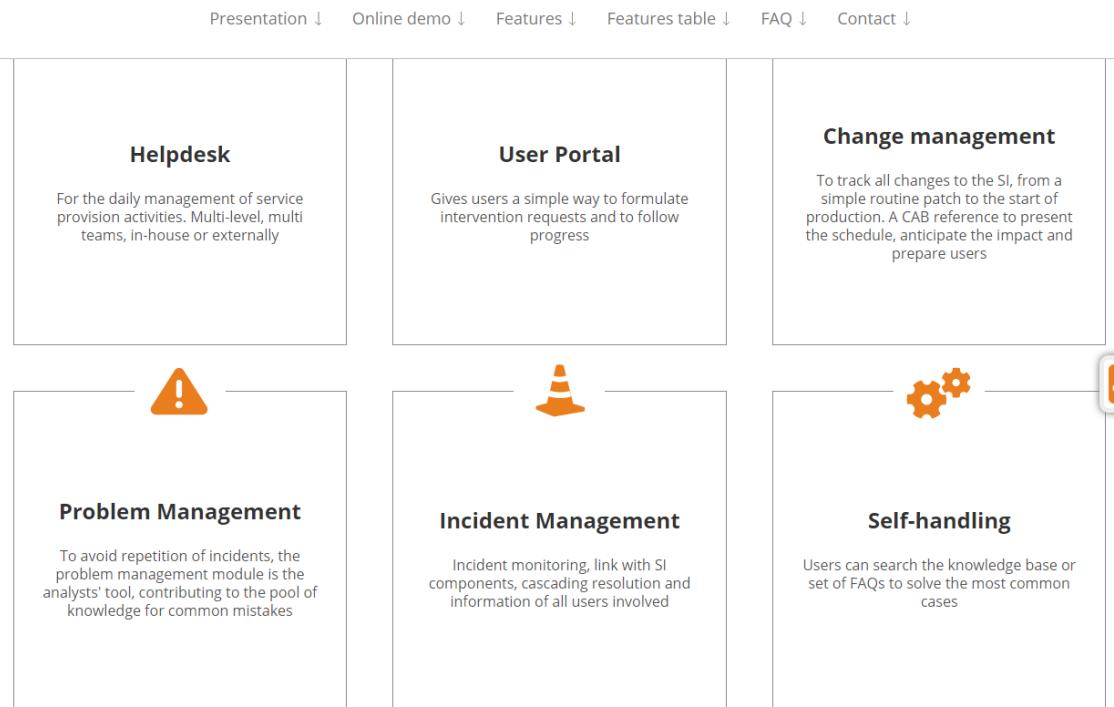
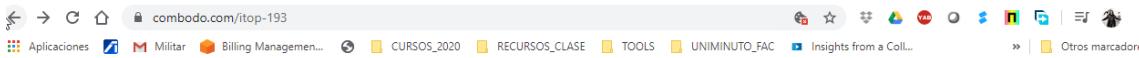
Server monitoring

Cloud monitoring

Application monitoring

<https://www.zabbix.com/>

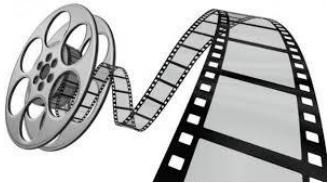
# itop

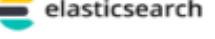


<https://www.combodo.com/>

# 10 Best Free and Open-Source SIEM Tools

## What You Need to Know



OSSIM	 ALIEN VAULT OSSIM	Offers both server-agent and serverless modes, with log analysis for mail servers, databases, and more.
Sagan	 QUADRANT INFORMATION SECURITY	Real-time log analysis and correlation tool that's compatible with graphic consoles like Snorby and EveBox.
Splunk Free	 splunk>	Free version of Splunk tool that lets you index up to 500 MB daily for real-time data indexing and alerts.
Snort	 SNORT	Analyzes network traffic in real time, but features make it best-suited for experienced IT professionals.
Elasticsearch	 elasticsearch	Combine log search types and easily scan through large volumes of logs with this basic tool.
MozDef	 moz://a	A microservices-based tool that can integrate with third-party platforms for straightforward security insights.
ELK Stack	 Stack	Combines Elasticsearch with tools like Kibana, Beats, and Logstash, for a fuller SIEM solution.
Wazuh	 WAZUH	An on-premises tool that offers threat detection, incident response, and compliance support.
Apache Metron	 APACHE METRON	Combines security operations center functions into one centralized, dynamic tool for catching threats.

<https://www.dnsstuff.com/free-siem-tools>

# Fuentes

1. ISO 31000 <https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es>
2. Magerit  
[https://administracionelectronica.gob.es/pae/Home/pae\\_Documentacion/pae\\_Metodolog/pae\\_Magerit.html.](https://administracionelectronica.gob.es/pae/Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html)
3. ISO 22301:2019 <https://www.iso.org/standard/75106.html>
4. [https://www.mintic.gov.co/gestionti/615/articles-5482\\_G11\\_Analisis\\_Impacto.pdf](https://www.mintic.gov.co/gestionti/615/articles-5482_G11_Analisis_Impacto.pdf)



# Gracias!!!

---



Escuela Superior  
de Guerra



@EsdegCol



Escuela Superior  
de Guerra



Escuela Superior  
de Guerra



@esdeguocol

