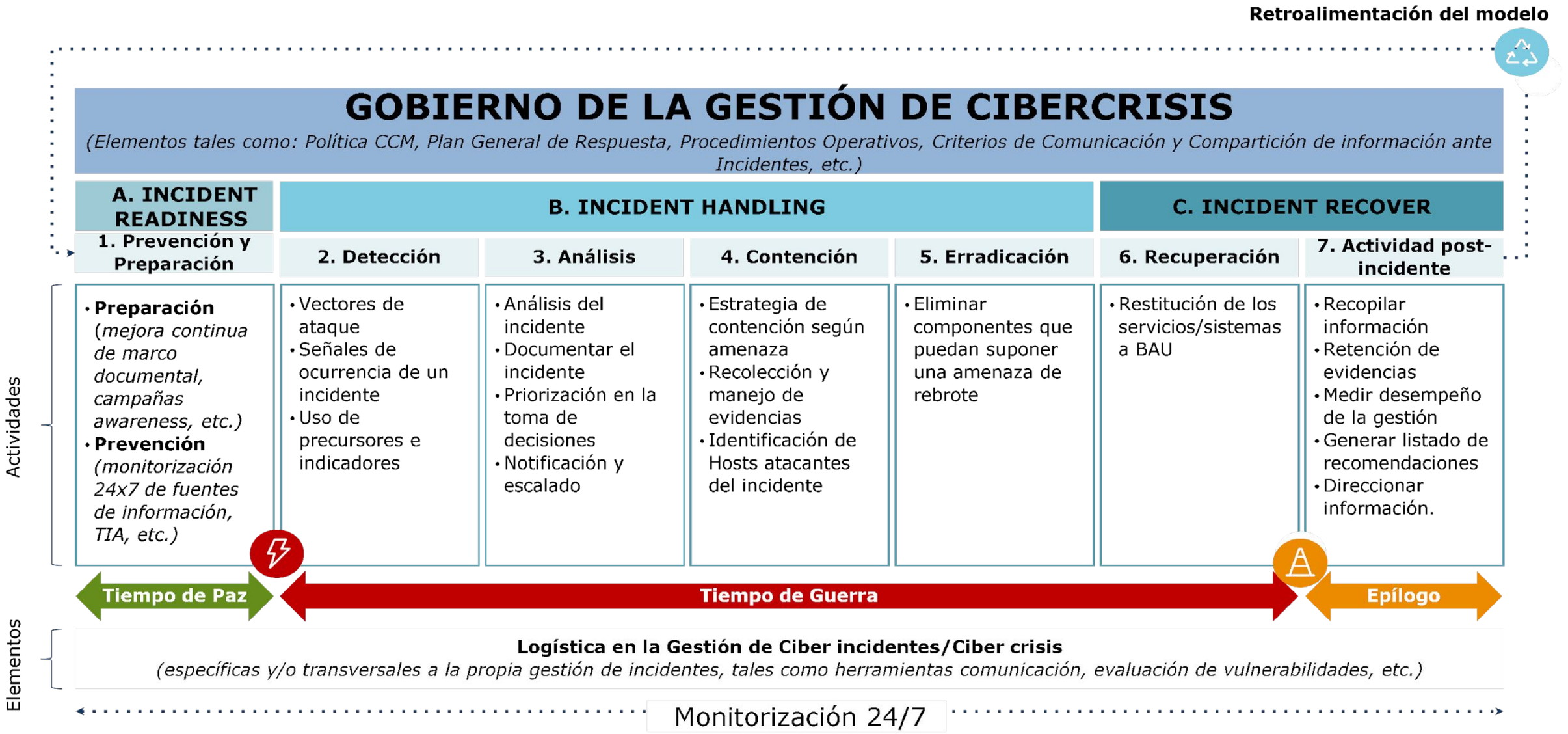
THE BRIDGE

# Ciclo de Vida del Incidente

# Ciclo de Vida del Incidente



# Ciclo de Vida del Incidente

**Detección**

Descubrimiento de posibles alertas, eventos y ciber incidentes confirmados a través de la monitorización de varias fuentes de información.

| Precursores | Indicadores |
| --- | --- |
| Señales o indicios de que un incidente puede ocurrir en el futuro. | Señales o indicios de que un incidente ya ha ocurrido o está ocurriendo actualmente. |

La identificación de estos precursores e indicadores para diferentes tipos de incidentes o escenarios es un elemento clave para facilitar las labores de detección.

## Fuentes de Detección

- **Detección humana**: como por ejemplo mediante el empleo de herramientas de ticketing.
- **Detección automatizada**: mediante el empleo de sistemas de monitorización, SIEM o el despliegue de sondas.

# Ciclo de Vida del Incidente

## Análisis

Obtención de información adicional sobre el incidente y sus impactos de forma que de soporte a las decisiones a tomar durante la gestión del incidente.

### Triaje inicial

Actividades de análisis preliminar que permiten identificar los impactos del incidente en primera instancia y priorizar las actividades a realizar

### Análisis en profundidad

Realización de investigaciones detalladas en los sistemas implicados que permitan obtener información suficiente para una toma de decisiones adecuada en función a los impactos observados

**Tipos habituales de evidencia a analizar**

| | | | |
|---|---|---|---|
| Registros y caché | | *Logs* y configuraciones | |
| Tablas de enrutamiento | | Buzones de correo | |
| *Hard Disk Drives* | | Otros (según escenario) | |

# Ciclo de Vida del Incidente

**Contención**

Limitación del alcance y los daños que pueda producir un incidente

| Corto Plazo | Largo Plazo |
| --- | --- |
| Evitar que el incidente alcance mayores dimensiones, aislándolo del resto de los elementos de la red si es posible o estableciendo medidas para limitar su libre evolución. | Actividades que puedan ser realizadas sin afectar a las operaciones de la organización, manteniendo los sistemas afectados activos. En muchos casos esta estrategia marca el comienzo de la fase de erradicación. |

**Erradicación**

Resolución del incidente, eliminando de forma definitiva su causa

- Cambios en políticas de seguridad a aplicar en los sistemas de la organización.
- Bloqueo total de aplicaciones, servicios o dominios.
- Cambios en reglas de navegación a nivel global en la compañía.
- Limpieza de equipos parcial o total.

# Ciclo de Vida del Incidente

**Recuperación y cierre**

Restauración de los sistemas a su funcionamiento habitual previo al incidente.

Una vez el incidente pueda **darse por controlado** y se aprecie una **reducción del impacto** del mismo pueden comenzar las labores de recuperación

Restaurar sistemas a su funcionamiento habitual, **revertiendo aquellas medidas aplicadas que ya no sean de utilidad** y, si corresponde, fortaleciendo la seguridad global para evitar ciber incidentes similares.

El cierre del incidente debe ser declarado por el **responsable del mismo**, teniendo en cuenta la reducción de los impactos y **asegurando una correcta notificación a todas las partes** involucradas

En caso de que existan **actividades de recuperación a medio o largo plazo por concluir**, se podrá dar por cerrado el incidente una vez finalizadas las tareas que garanticen que éste **ya no supone un impacto** para la organización


THE
BRIDGE