



Retroalimentación del modelo



GOBIERNO DE LA GESTIÓN DE CIBERCRISIS

(Elementos tales como: Política CCM, Plan General de Respuesta, Procedimientos Operativos, Criterios de Comunicación y Compartición de información ante Incidentes, etc.) A. INCIDENT C. INCIDENT RECOVER **B. INCIDENT HANDLING READINESS** 1. Prevención y 7. Actividad post-6. Recuperación 2. Detección 3. Análisis 5. Erradicación 4. Contención Preparación incidente · Análisis del Restitución de los Vectores de Estrategia de Eliminar Recopilar · Preparación contención según información ataque incidente componentes que servicios/sistemas (mejora continua Señales de puedan suponer Retención de Documentar el a BAU amenaza de marco ocurrencia de un incidente Recolección y una amenaza de evidencias documental. Actividades Priorización en la manejo de Medir desempeño incidente rebrote campañas de la gestión Uso de toma de evidencias awareness, etc.) · Identificación de Generar listado de decisiones precursores e Prevención Notificación y recomendaciones indicadores Hosts atacantes (monitorización escalado del incidente Direccionar 24x7 de fuentes información. de información, TIA, etc.) Tiempo de Guerra Tiempo de Paz Epílogo

Logística en la Gestión de Ciber incidentes/Ciber crisis

(específicas y/o transversales a la propia gestión de incidentes, tales como herramientas comunicación, evaluación de vulnerabilidades, etc.)

Monitorización 24/7

Elementos





Detección

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

Precursores

Señales o indicios de que un incidente puede ocurrir en el futuro.

Indicadores

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.





Análisis

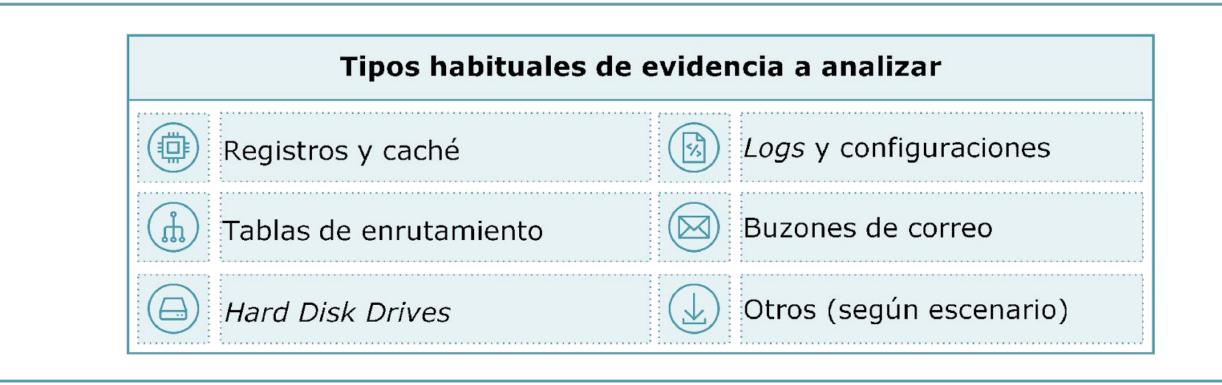
Obtención de información adicional sobre el incidente y sus impactos de forma que de soporte a las decisiones a tomar durante la gestión del incidente.

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







Contención

Limitación del alcance y los daños que pueda producir un incidente

Corto 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.

Largo Plazo

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.





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