THE BRIDGE

Gestión de Ciber incidentes

Conceptos

Alerta	Incidente	Crisis
• **Evento** de especial **interés** generado por un sistema de monitorización, mediante la **correlación de diferentes eventos o patrones**, que requiere de un análisis. • Las alertas no necesariamente se convierten en un ciber incidente.	• **Evento** o conjunto de eventos **no deseados** o esperados que **suponen un impacto** comprometiendo las operaciones de negocio y poniendo en riesgo la seguridad de la información	• **Condición inestable** que implica un cambio abrupto o significativo repentino o inminente que requiere **atención y acción urgentes** para proteger personas, activos, propiedades y sistemas que puedan **afectar a los objetivos estratégicos** de una organización.

Resiliencia	**Capacidad de adaptación** de una organización en un entorno complejo y cambiante, así como la protección de los activos críticos

Ejemplos de Incidentes y Crisis

Incidente

"Cualquier pérdida, alteración, divulgación, mal uso, **acceso no autorizado o interrupción de los recursos de información** de la compañía relacionados con la seguridad que puedan ser perjudiciales para los clientes, la marca y/o reputación".

- **Malware**
- **Destrucción no autorizada de datos**
- **Intrusión**
- **Ataques DDOS**
- **Brecha de Información**
- **Ransomware**

Crisis

"Una situación anormal, inestable y compleja que supone una **amenaza significativa** para los objetivos estratégicos, la reputación o la existencia de la **organización**".

- A través de un DDoS, un atacante causa una **interrupción significativa en los procesos de negocio**.
- Un ransomware dentro de la organización que causa la **pérdida de datos confidenciales** y su posible divulgación pública.
- La escalada de intrusión de privilegios y el robo de credenciales que resulta en el **acceso no autorizado a los sistemas críticos**.

Toda emergencia se puede calificar como incidente, sin embargo, no todos los incidentes son emergencias

Resiliencia

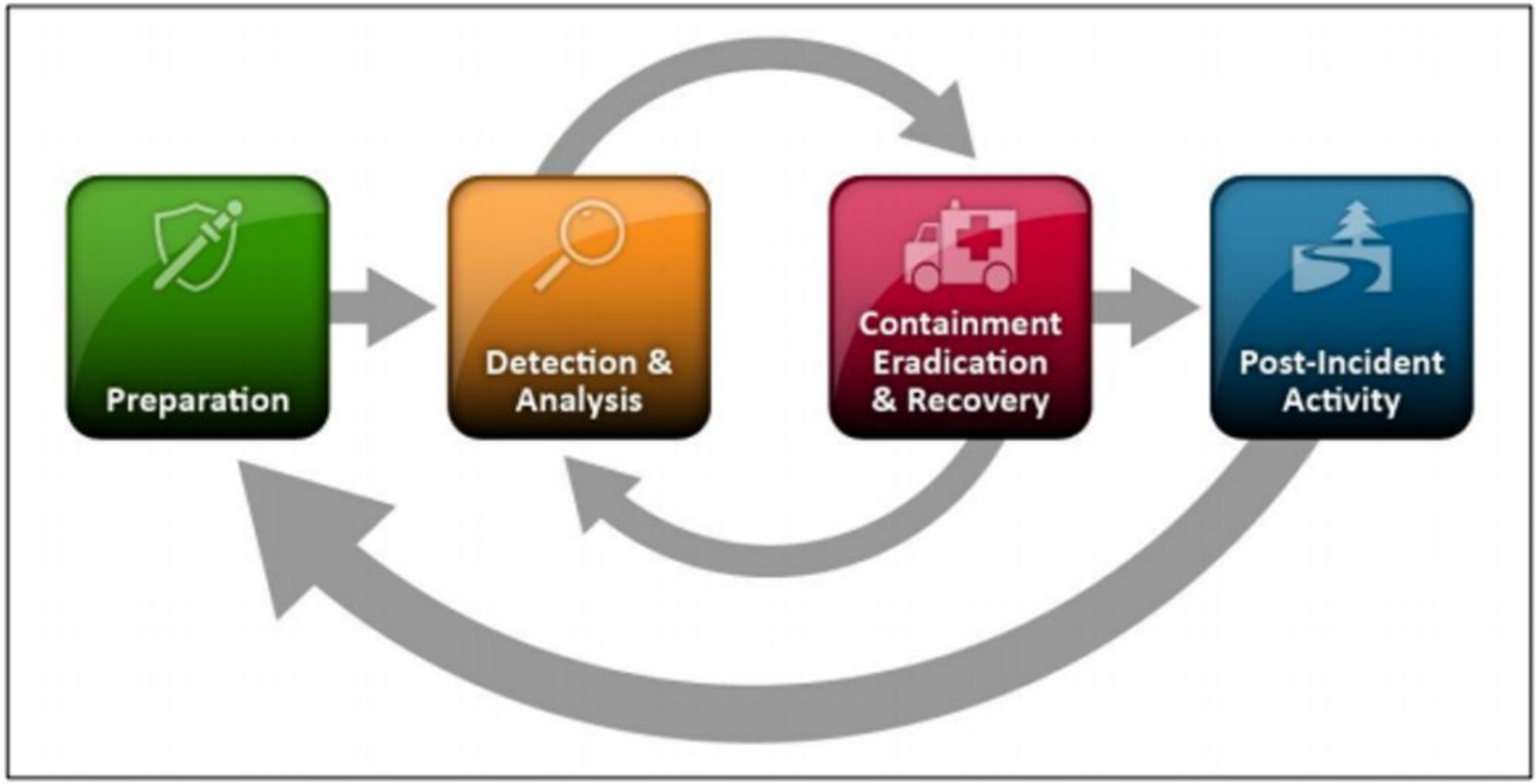
- Se requiere una estrategia integral que combine protección, preparación, respuesta rápida y recuperación.
- La ciber resiliencia permite reducir el impacto y mejorar la capacidad de recuperación y adaptación.
- Algunos puntos clave son:
  - **Evaluación y gestión de riesgos**
  - **Protección proactiva de la infraestructura**
  - **Capacitación y concientización de los empleados**
  - **Plan de respuesta y recuperación ante incidentes**
  - **Monitoreo y detección continua**
  - **Evaluación y mejora continua**
  - **Fomento de una cultura de ciberseguridad**

Gestión de Incidente

- Proceso estructurado que tiene como objetivo identificar, responder, contener y resolver eventos que comprometan la seguridad de la información y los sistemas de una organización.

- Para minimizar el impacto de los incidentes, restaurar operaciones normales de manera rápida y fortalecer las defensas.

- Las fases son:
  - **Preparación.**
  - **Detección e Identificación**
  - **Contención**
  - **Erradicación**
  - **Recuperación**
  - **Lecciones aprendidas**



https://www.avsoftware.com.mx/respuesta-a-incidentes-de-ciberseguridad-guia-de-nist/

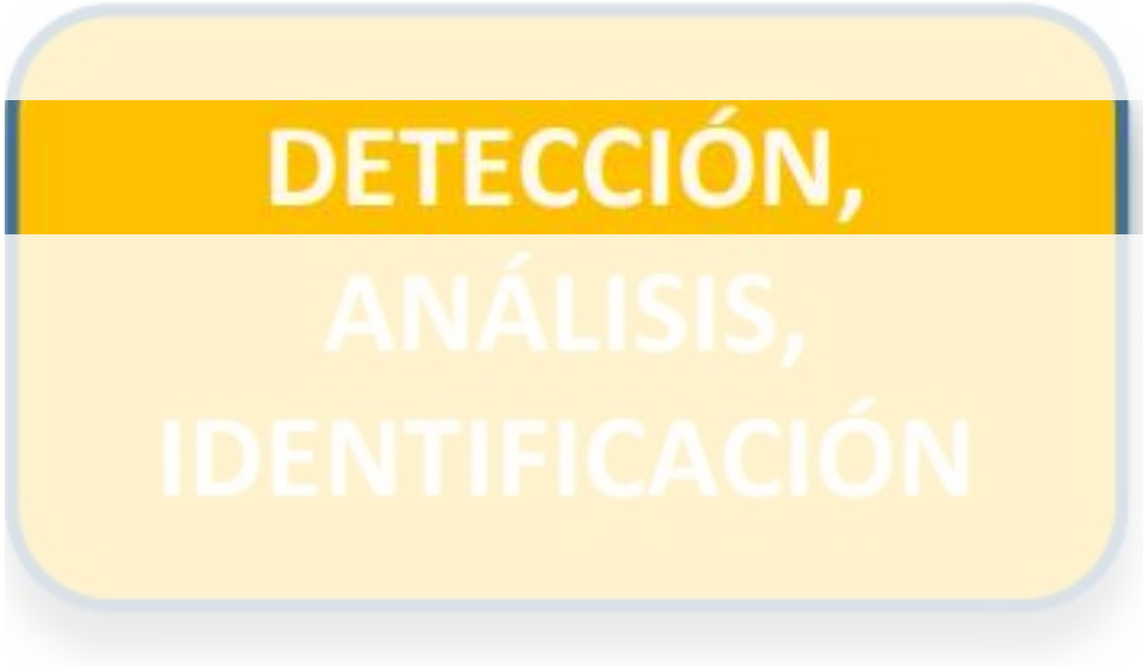
Introducción a la gestión de ciber incidentes

- **Preparación**:
  - Establecer las bases para una respuesta eficaz ante un incidente de ciberseguridad.
  - Desarrollar procedimientos, capacitar al personal y dotar a la organización de las herramientas necesarias para identificar, contener y mitigar incidentes rápidamente y con el menor impacto posible.
  - Componentes clave en la fase de preparación
    - **Creación de un plan de respuesta a incidentes.**
    - **Definición de roles y responsabilidades.**
    - **Capacitación y simulacros.**
    - **Herramientas y tecnologías.**
    - **Definir procedimientos de comunicación.**
    - **Identificación y clasificación de activos críticos.**

https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file.html

Introducción a la gestión de ciber incidentes

- **Detección**
  - Identificar la presencia de un incidente en sus primeras etapas.
  - Combinación de herramientas, métodos y procesos que trabajan en conjunto para identificar las actividades.
  - Las características principales de esta fase son:
    - **Monitoreo Continuo**
    - **Detección de Anomalías**
    - **Uso de Indicadores de Compromiso (IOC)**
    - **Correlación de Eventos**
    - **Alertas y Notificaciones Automáticas**
    - **Análisis de Logs y Registros**
    - **Inteligencia de Amenazas**
    - **Detección Proactiva**



https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file.html

Introducción a la gestión de ciber incidentes

- **Análisis**
  - Es para entender la naturaleza, el alcance y el impacto de un incidente.
  - Toma de decisiones informadas y aplicar contramedidas eficaces.
  - Las características principales de esta fase incluyen:
    - **Identificación de la naturaleza del ataque**
    - **Determinación del alcance**
    - **Evaluación del impacto**
    - **Recopilación de evidencia**
    - **Análisis de la causa raíz**
    - **Identificación de tácticas, técnicas y procedimientos (TTP)**
    - **Generación de inteligencia sobre amenazas**
    - **Evaluación de la respuesta inicial.**

https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file.html

Introducción a la gestión de ciber incidentes

- **Identificación**
  - Detectar un incidente en sus primeras etapas.
  - Aquí están las características principales de esta fase:
    - **Monitoreo continuo**
    - **Análisis de alertas y logs**
    - **Identificación de indicadores de compromiso (IOC)**
    - **Clasificación del incidente**
    - **Notificación interna y escalamiento**
    - **Documentación inicial**
    - **Trazar la fuente del ataque.**
    - **Analizar patrones**
    - **Identificación de posibles fallos.**

https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file.html

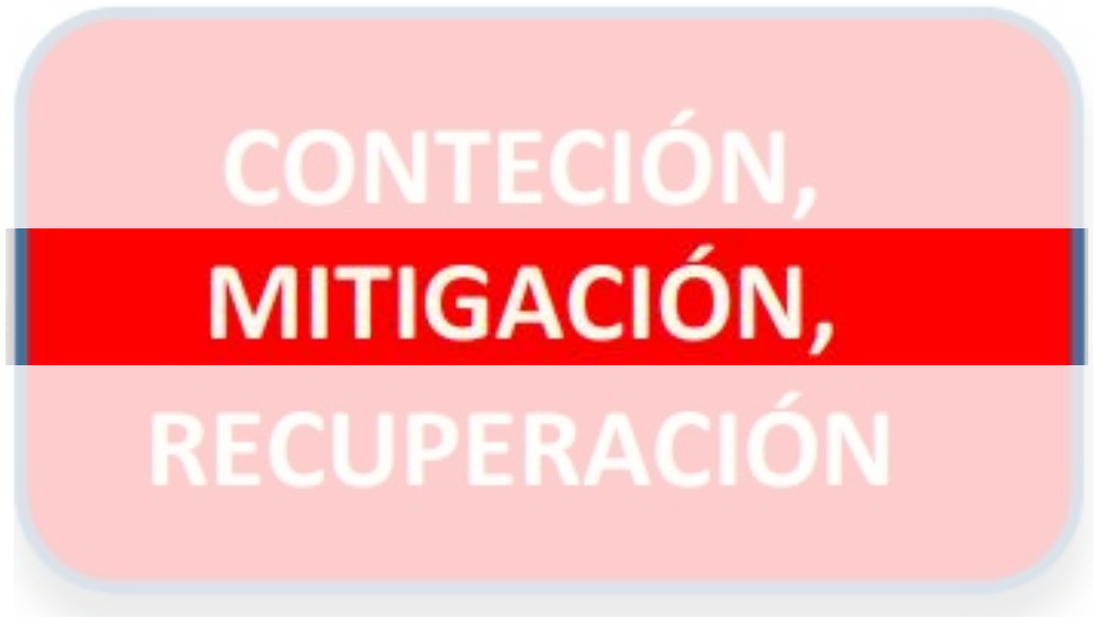
Introducción a la gestión de ciber incidentes

- **Contención**
  - Si un atacante comprometer un dispositivo, debe evitar el movimiento lateral y que salga más información al exterior.
  - La formación y experiencia del personal implicado en la gestión de incidentes.
  - La toman las decisiones de forma más rápida ya que el tiempo es un factor determinante y la reputación o la continuidad del negocio.
  - Documentación de cada paso que se tome o cada actividad.
  - La clasificación de los ciber incidentes para asignar la prioridad.
  - Conocida la extensión del problema a través de la documentación obtenida.
  - Ejecutar los procedimientos de toma y preservación de evidencias.
  - Las acciones típicas en esta fase incluyen:
    - **Aislamiento.**
    - **Desactivación de servicios.**
    - **Implementación de controles temporales.**

https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file.html

Introducción a la gestión de ciber incidentes

- **Mitigación**
  - Reducir el impacto y la gravedad del incidente.
  - Eliminar las amenazas y corregir vulnerabilidades
  - Principales características de esta fase:
    - **Identificación de la Causa Raíz**
    - **Remediación de Vulnerabilidades**
    - **Implementación de Medidas Adicionales de Seguridad**
    - **Revisión de Políticas y Procedimientos de Seguridad**
    - **Fortalecimiento de la Concienciación y Capacitación del Personal.**



https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file.html

Introducción a la gestión de ciber incidentes

- **Recuperación**
  - Se centra en restaurar los sistemas y servicios a su estado normal.
  - Algunas de las características de esta fase son:
    - **Restauración de sistemas**
    - **Validación de la seguridad**
    - **Monitoreo post-incidente.**
    - **Mejora de la seguridad**
    - **Comunicación y reportes**
    - **Evaluación post-incidente**
    - **Pruebas y simulaciones**

https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file.html

Introducción a la gestión de ciber incidentes

- **Post- incidente**
  - Aprender de la experiencia para mejorar la respuesta a futuros incidentes.
  - Las principales características son:
    - **Análisis y documentación del incidente**
    - **Evaluación de la respuesta al incidente**
    - **Lecciones aprendidas**
    - **Actualización de políticas y procedimientos de seguridad**
    - **Capacitación y sensibilización continua**

https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file.html


THE
BRIDGE