CARABINEROS DE CHILE

ORDEN Y PATRIA

CURSO

RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Profesor: Lautaro Cabezas

UNIDAD 2

MEJORES PRÁCTICAS DE GESTIÓN DE INCIDENTES BASADAS EN LA NORMA ISO 27035

Contenidos

- Planificar y preparar
- Detección y notificación
- Evaluación y decisión
- Respuestas
- Lecciones aprendidas

Objetivos de la Unidad

- Conocer la estructura de la norma ISO/IEC 27035.
- Aplicar mejores prácticas en cada fase de la gestión de incidentes.
- Desarrollar competencias para evaluar, responder y aprender de los incidentes.

¿Qué es ISO/IEC 27035?

- Norma internacional para la gestión de incidentes de seguridad de la información.
- Aborda desde la planificación hasta las lecciones aprendidas.
- Parte 1: Principios; Parte 2: Preparación; Parte 3: Respuesta y Parte 4: Mejora.

Fases según ISO 27035

- Planificar y Preparar
- Detección y Notificación
- Evaluación y Decisión
- Respuesta
- Lecciones Aprendidas

Fase 1: Planificar y Preparar

- Definir políticas y procedimientos.
- Establecer el equipo de respuesta (CSIRT).
- Asignar roles y responsabilidades.
- Capacitación y herramientas disponibles.

Actividad: Plan de Preparación

- Diseña un plan de preparación para tu institución.
- Define responsables, recursos y comunicación.
- Utiliza herramientas como Word.

Fase 2: Detección y Notificación

- Identificación de incidentes mediante SIEM, IDS/IPS, antivirus.
- Clasificación de eventos vs. incidentes.
- Procedimiento de notificación y escalamiento.

Actividad: Caso Simulado

- Analiza un incidente ficticio y determina si debe ser reportado.
- Clasifica la severidad e identifica responsables.

Fase 3: Evaluación y Decisión

- Evaluación del impacto y alcance del incidente.
- Clasificación por criticidad: alta, media, baja.
- Decisión: escalar, contener, descartar.
- Matriz de impacto y probabilidad.

Actividad: Evaluación de Caso

- Analiza un caso real o ficticio y decide la acción a seguir.
- Aplica criterios de criticidad y afectación.
- Presenta tu decisión en grupos.

Fase 4: Respuesta

- Contención del incidente: inmediata y a largo plazo.
- Erradicación: eliminación de la causa raíz.
- Recuperación: restauración de sistemas afectados.
- Seguimiento continuo del incidente.

Actividad: Plan de Respuesta

- Desarrolla un plan de respuesta para un ataque DDoS.
- Incluye acciones técnicas, comunicacionales y legales.
- Evalúa tiempo de respuesta y recursos.

Fase 5: Lecciones Aprendidas

- Documentar el incidente y sus consecuencias.
- Analizar causas y brechas detectadas.
- Actualizar políticas y controles.
- Fomentar la mejora continua.

Actividad: Informe Post-Incidente

- Completa una plantilla de lecciones aprendidas.
- Evalúa los errores y aciertos del equipo.
- Propón acciones de mejora específicas.

Resumen del Ciclo de Incidentes

- Visualización de todas las fases.
- Entradas, procesos y salidas clave.
- Papel del CSIRT en cada fase.

Buenas Prácticas por Fase

- Preparar: capacitación, políticas claras.
- Detectar: monitoreo 24/7, alertas automáticas.
- Evaluar: decisiones ágiles y fundamentadas.
- Responder: documentación y control.
- Aprender: retroalimentación estructurada.

Taller Práctico: Caso Integrador

- Caso: ciberataque a hospital con datos cifrados.
- Identificar fases y acciones ejecutadas.
- Evaluar respuesta y redactar informe final.

Dinámica de Grupo

- División en equipos: análisis por fase.
- Discusión guiada: fortalezas y debilidades.
- Presentación de hallazgos y aprendizajes.

Conclusiones de la Unidad

- La gestión estructurada mejora la respuesta.
- ISO 27035 proporciona una guía clara y adaptable.
- La mejora continua es clave en ciberseguridad.

Recursos y Referencias

- ISO/IEC 27035:2023 (Partes 1, 2 y 3).
- NIST SP 800-61 Rev.2.
- Guías ENISA sobre respuesta a incidentes.
- CyberRange, MITRE ATT&CK simuladores.