CARABINEROS DE CHILE

ORDEN Y PATRIA

CURSO

RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Profesor: Lautaro Cabezas

UNIDAD 4

IMPLEMENTACIÓN DEL PROCESO DE GESTIÓN DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Objetivos de Aprendizaje

- Comprender los elementos clave para implementar un proceso de gestión de incidentes.
- Desarrollar políticas y procedimientos alineados a ISO 27035.
- Diseñar y operar un Playbook de respuesta a incidentes.
- Aplicar actividades prácticas para reforzar conocimientos.

Introducción a la Implementación del Proceso

- Recordatorio de las fases ISO 27035.
  - Planificar y Preparar
  - Detección y Notificación
  - Evaluación y decisión
  - Respuesta
  - Lecciones aprendidas
- Importancia de pasar de la teoría a la práctica.
- Integración con SGSI (ISO 27001).

Diseño del Proceso – Concepto General

- Definición de objetivos del proceso.
- Alcance (tipos de incidentes incluidos).
- Roles y responsabilidades.

Diseño del Proceso – Flujo General

Etapas del proceso:

1. Detección
2. Evaluación
3. Contención
4. Erradicación
5. Recuperación
6. Lecciones aprendidas

Componentes del Diseño

- Procedimientos asociados.
- Herramientas necesarias (SIEM, IDS/IPS, sistemas de tickets).
- Comunicación interna y externa.

Integración con Otros Procesos

- Gestión de riesgos.
- Gestión de continuidad de negocio (ISO 22301).
- Gestión de cambios (ITIL).

Política de Gestión de Incidentes – Introducción

- Definición de política.
- Objetivos de la política.
- Alineación con la dirección y cumplimiento legal.

Elementos Clave de la Política

- Declaración de propósito.
- Alcance y aplicación.
- Obligaciones del personal.
- Clasificación de incidentes.

Ejemplo de Política

- Texto modelo de política).
- Formato y estilo recomendado.

Procedimiento de Gestión de Incidentes – Introducción

- Diferencia entre política y procedimiento.
- Importancia de la estandarización.

Procedimiento – Etapas Detalladas

- Recepción y registro del incidente.
- Clasificación y priorización.
- Asignación de responsables.
- Acciones de respuesta.
- Documentación y cierre.

Ejemplo de Procedimiento

- Tabla con pasos
- Responsable
- Tiempo estimado
- Herramientas

Playbook de Respuesta a Incidentes – Concepto

- Definición y utilidad.
- Diferencia entre plan y playbook.
- Automatización y orquestación.

Componentes del Playbook

- Escenario de amenaza.
- Acciones paso a paso.
- Condiciones de decisión (if/then).
- Comunicación.

Ejemplo de Playbook

- Playbook de respuesta a un ransomware.
- Formato visual (cuadro de acciones secuenciales).

Herramientas para Operar un Playbook

- SOAR (Security Orchestration, Automation and Response).
- Integración con SIEM.

Factores de Éxito en la Implementación

- Apoyo de la alta dirección.
- Capacitación del personal.
- Actualización continua.

Métricas y KPIs del Proceso

- Tiempo medio de detección (MTTD).
- Tiempo medio de respuesta (MTTR).
- Número de incidentes gestionados.

Desafíos Comunes

- Resistencia al cambio.
- Falta de recursos.
- Desactualización de procedimientos.

Mejores Prácticas ISO 27035

- Enfoque basado en riesgos.
- Comunicación clara.
- Simulacros y ejercicios.

Actividad Práctica 1 – Análisis de un Caso Real

- Presentar un incidente real.
- Diseñar un procedimiento de respuesta.

Actividad Práctica 2 – Crear un Playbook

- Escenario: Ataque de DDos.
- Definir pasos de respuesta, roles y comunicación.

Actividad Práctica 3 – Simulación de Respuesta

- Dividir en equipos.
- Simular detección, contención y comunicación de un incidente.

Cierre y Conclusiones

- Resumen de lo aprendido.
- Importancia de la mejora continua.
- Aplicar lo aprendido en las organizaciones.