CARABINEROS DE CHILE

ORDEN Y PATRIA

CURSO

RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Profesor: Lautaro Cabezas

UNIDAD 3

DISEÑO Y DESARROLLO DE UN PROCESO DE GESTIÓN DE INCIDENTES ORGANIZATIVOS BASADO EN LA NORMA ISO 27035

Objetivos de la Unidad

- Comprender los componentes clave del diseño y desarrollo de un proceso de gestión de incidentes.

- Aplicar los lineamientos de la ISO 27035 en una organización.

Contenidos

- Estrategia y Cartera de proyectos.
- Creación de un plan de gestión de incidentes de seguridad de la información.
- Establecimiento de un equipo de respuesta a incidentes y de relaciones con otras organizaciones.
- Creación de una concienciación y formación sobre incidentes de seguridad de la información.
- Política de gestión de incidentes de Seguridad de la información.

Rol de la Estrategia en la Gestión de Incidentes

- Alineación con los objetivos del negocio.
- Gobierno de la seguridad de la información.

Cartera de Proyectos de Seguridad

- Priorización de iniciativas
- Gestión de recursos y riesgos.

Actividad Práctica N°1

- Ejercicio grupal: Identifica y redacta 3 iniciativas estratégicas para fortalecer la gestión de incidentes.

¿Qué es un Plan de Gestión de Incidentes?

- Documento formal con objetivos, alcance y procedimientos.
- Define la estructura de respuesta y los responsables.

Elementos del Plan según ISO 27035

- Alcance, roles, procesos, recursos, etc.
- Procedimientos de notificación y escalamiento.

Ciclo de Vida del Plan

- Diseño, implementación, mantenimiento y mejora continua.

Revisión y Actualización del Plan

- Revisión periódica.
- Inclusión de lecciones aprendidas y cambios organizacionales.

Actividad Práctica N°2

Caso práctico: Redacta un índice tentativo de un Plan de Gestión de Incidentes para una empresa tecnológica.

¿Qué es un CSIRT/IRT?

- Equipo de respuesta a incidentes.
- Funciones y tipos: centralizado, distribuido, virtual.

Composición del Equipo

- Roles técnicos, legales, comunicaciones y soporte.

Capacidades mínimas requeridas

- Herramientas, habilidades, tiempos de respuesta.

Actividad Práctica N°3

- Diseña un organigrama de un equipo de respuesta para una organización del sector salud.

Importancia de las Relaciones Externas

- Coordinación con CERTs, alianzas sectoriales, proveedores, etc.

Establecimiento de Acuerdos y Protocolos

- NDA, MOU, contratos con terceros.

Actividad Práctica N°4

- Estudio de caso: ¿Qué actores externos debería involucrar una universidad ante una fuga o filtración de datos?

Cultura de Seguridad de la Información

- Concientización constante.
- Implicancia en todos los niveles organizacionales.

Programas de Concienciación

- Campañas internas, simulacros de phishing, boletines informativos.

Formación y Entrenamiento Especializado

- Talleres, cursos, ejercicios prácticos y simulacros.

Actividad Práctica N°5

- Diseña una actividad de concienciación para empleados administrativos sobre gestión de incidentes.

Resumen de la Unidad

- Principales aprendizajes sobre estrategia, planificación, equipos, relaciones y cultura de seguridad.

Evaluación Final

Mini taller: Diseña un esquema de proceso de gestión de incidentes basado en ISO 27035.

Preguntas y Cierre

- Espacio de retroalimentación y dudas.