CARABINEROS DE CHILE

ORDEN Y PATRIA

CURSO

RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Profesor: Lautaro Cabezas

UNIDAD 5

SEGUIMIENTO, MEDICIÓN Y MEJORA DEL PROCESO DE GESTIÓN DE INCIDENTES

Introducción a la Unidad 5

- En esta unidad se aborda cómo realizar el seguimiento, medición y mejora continua del proceso de gestión de incidentes, con enfoque en métricas, indicadores, revisiones y planes de acción.

Contenidos de la Unidad

- Seguimiento, medición y mejora del proceso.
- Seguimiento y evaluación en operaciones.
- Desarrollo de métricas, indicadores y cuadros de mando.
- Revisiones de la gestión.
- Planes de acción correctivos y preventivos.
- Lecciones aprendidas.

Seguimiento del Proceso

- Implica recopilar información sobre incidentes detectados, tiempos de respuesta y efectividad de las acciones tomadas.

Medición del Proceso

- Cuantificar desempeño con métricas clave: tiempo de resolución, incidentes críticos, reincidencias.

Mejora Continua

- Identificación de debilidades, análisis de brechas y aplicación de mejores prácticas y controles.

Evaluación en las Operaciones

- Verificar eficacia del proceso en la operación diaria, mediante reportes y auditorías.

Actividades de Evaluación

- Revisar registros de incidentes.
- Analizar tiempos de respuesta.
- Comparar métricas con objetivos.
- Identificar áreas críticas.

Métricas de Gestión de Incidentes

- Tiempo medio de detección (MTTD).
- Tiempo medio de respuesta (MTTR).
- Número de incidentes por categoría.
- % incidentes resueltos en SLA.

Actividad 1

- Revisar un caso real y definir métricas para medir impacto y efectividad en la respuesta.

Indicadores Clave de Desempeño (KPI)

Ejemplos:

- % incidentes clasificados correctamente.
- % incidentes resueltos sin escalamiento.
- Reducción de incidentes repetitivos.

Cuadros de Mando

- Visualizar en tiempo real el estado de los incidentes y la eficiencia del proceso.

Actividad 2

- Diseñar un cuadro de mando simple con indicadores clave aplicables a su organización.

Revisiones de la Gestión

- Revisiones periódicas aseguran actualización y alineación con objetivos estratégicos.

Tipos de Revisiones

- Revisiones trimestrales.
- Auditorías internas.
- Retroalimentación de equipos de respuesta.

Planes de Acción Correctivos

- Eliminar causas de incidentes pasados para evitar recurrencia.

Planes de Acción Preventivos

- Anticiparse a incidentes fortaleciendo controles y procesos.

Ejemplos de Planes de Acción

- Parches de seguridad.
- Capacitación.
- Políticas de acceso.
- Simulacros de respuesta.

Actividad 3

- Proponer planes correctivos y preventivos para un incidente de fuga de información.

Lecciones Aprendidas

- Cada incidente debe generar conocimiento para mejorar la gestión futura.

Aplicación de Lecciones Aprendidas

- Documentar hallazgos.
- Compartir aprendizajes.
- Incorporar mejoras en procedimientos.

Actividad 4

- Elaborar un informe de lecciones aprendidas de un caso ficticio de ransomware.

Conclusión de la Unidad 5

- El seguimiento, medición y mejora de la gestión de incidentes fortalece la resiliencia organizacional y asegura una respuesta eficaz.