

Plantilla Base para la Sesión de Lecciones Aprendidas

Objetivo de la Sesión

- Describa aquí el propósito general de la sesión de lecciones aprendidas.

Detalles del Incidente

Número o código del incidente:

Impacto del Incidente

- Enumere y describa los impactos directos e indirectos del incidente en la organización.

Cronología del Incidente

- Describa la secuencia de eventos del incidente, con tiempos y fechas clave.

Participantes

Nombre	Rol
Nombre Apellido	Rol1
Nombre Apellido	Rol2
Nombre Apellido	Rol3

Puntos de Discusión

Preparación

- ¿Cómo podríamos haber evitado el incidente por completo?
- ¿Qué prácticas o herramientas podrían haber mejorado todo el proceso?

Identificación

- ¿Qué herramientas podrían haber facilitado la identificación de la amenaza?
- ¿Qué investigación sobre la amenaza hubiesen ayudado?

Contención

- ¿Qué medidas de contención fueron efectivas? ¿Cuáles no?
- ¿Habrían sido útiles otras medidas de contención si hubieran sido más fáciles de implementar?

Erradicación

- ¿Qué mecanismos de erradicación salieron bien?
- ¿Qué se hubiese podido hacer mejor?

Recuperación

- ¿Qué demoró la recuperación? (Sugerencia: concéntrese en la comunicación, ya que es una de las partes más difíciles de la recuperación).

Preguntas Adicionales

Reflexiones Generales

- ¿Cuál fue el aspecto más desafiante de la respuesta a este incidente?
- ¿De qué aspectos de nuestra respuesta nos sentimos más orgullosos?

Mejoras Futuras

- ¿Qué acciones inmediatas deberíamos tomar para mejorar nuestras capacidades de respuesta a incidentes?
- ¿Hay algún proyecto a largo plazo que deberíamos iniciar basado en lo que hemos aprendido?

Desempeño del Equipo

- ¿Qué tan bien colaboró y comunicó el equipo durante el incidente?
- ¿Hay áreas donde la coordinación del equipo podría mejorarse?

Documentación y Reportes

- ¿Fue efectivo nuestro proceso de documentación del incidente?
- ¿Cómo podemos mejorar nuestra documentación y reportes para futuros incidentes?

Plan de Implementación

Actividad	Responsable	Fecha de validación
Ejemplo de actividad 1	Nombre y Rol	Fecha Ejemplo
Ejemplo de actividad 2	Nombre y Rol	Fecha Ejemplo
Ejemplo de actividad 3	Nombre y Rol	Fecha Ejemplo