ESTUDIO DE CASO Nº1

Evaluación del módulo

Profesor: Lautaro Castillo

UNIDAD 1: Principios y conceptos fundamentales de la gestión de incidentes

Contexto:

La Unidad de Inteligencia de Carabineros de Chile, encargada de labores criticas vinculadas a la seguridad publica, detecta actividades inusuales en su red interna. En las últimas 48 horas, varios sistemas han presentado lentitud, accesos no autorizados y archivos cifrados con una extensión desconocida. Además, se recibió un mensaje anónimo solicitando un rescate en criptomonedas a cambio de la restauración de la información.

El análisis preliminar sugiere un ataque de tipo ransomware, posiblemente vinculado a una amenaza persistente avanzada (APT). La situación afecta el acceso a información clave sobre investigaciones activas.

Se pide:

1. Identificar tres posibles indicadores de compromiso (IoC) que se pueden detectar en este incidente.

2. Enumerar los pasos que debe seguir la unidad siguiendo el marco NIST para responder al incidente.

3. ¿Qué medidas de recuperación propondrías para restaurar el funcionamiento de los sistemas afectados?

4. ¿Qué roles dentro de la institución deberían participar en la gestión de este incidente? Justifique.

5. ¿Cómo comunicarías este incidente a la ciudadanía sin afectar la confianza pública ni la seguridad del caso?

6. ¿Consideras que tu unidad cuenta con protocolos y capacidades adecuadas para enfrentar un ciberincidente? ¿Qué aspectos mejorarías?

7. ¿Qué recomendaciones darías para fortalecer los protocolos de respuesta a incidentes en una unidad policial?

Estructura del trabajo

Portada: La portada incluye el título del trabajo, los nombres del autor o de los autores, la afiliación del autor (nombre de la institución), el nombre del curso y profesor/orientador para el cual se presenta el trabajo. También se debe agregar la fecha y el número de página.

Introducción: Presenta el tema, su relevancia e importancia, y proporciona una visión general de lo que se discutirá en el trabajo. También establece el propósito y el alcance del mismo, y presenta la idea principal.

Desarrollo del tema: Expande los puntos clave del trabajo, proporciona evidencia, ejemplos y argumentos que respalden tu tesis. Organiza esta sección de manera lógica y coherente, utilizando párrafos bien estructurados.

Conclusión: Resume los puntos principales discutidos en el trabajo. Puedes ofrecer también reflexiones finales o implicaciones prácticas del tema tratado.

Formato: Documento Word, fuente legible y profesional, Arial 11. Márgenes Superior 2.5 inferior 2.5; Izquierdo 3, derecho 3.

Numeración de páginas: Numerar todas las páginas del documento, generalmente en la esquina superior derecha, excepto en la página de título.

Extensión: máximo 4 páginas, incluida la portada.

Grupos: Los grupos deben estar conformados por 3 integrantes.

Fecha de Entrega: A más tardar el día **jueves 31 de julio, 23:59 horas**.