ESTUDIO DE CASO Nº2

Evaluación del módulo

Profesor: Lautaro Castillo

UNIDAD 2: Mejores prácticas de gestión de incidentes basadas en la norma iso 27035

Contexto:

La Subsecretaría de Transporte Digital administra una plataforma nacional de control de tránsito y semáforos inteligentes en las principales ciudades del país. A inicios de semana, diversos sistemas comenzaron a presentar comportamientos inusuales, como reinicios repentinos de servidores, lentitud en la plataforma web y mensajes extraños en la consola de administración .

Luego de 24 horas, se detecta que una gran parte de los servidores de control han sido cifrados por un ransomware llamado "DarkSignal", que exige 100.000 USD en criptomonedas para liberar la información. Algunos controladores de tráfico comenzaron a operar en modo manual, afectando la fluidez del tránsito urbano.

Tu tarea como grupo de respuesta es aplicar cada una de las fases de la ISO 27035 para gestionar este incidente.

A partir del caso expuesto, responda lo siguiente:

1. Planificar y Preparar

a) ¿Qué controles, procedimientos y roles deberían haber existido antes del incidente?
b) ¿Qué recursos (humanos, técnicos, documentación) habrían ayudado a prevenir o mitigar este incidente?

2. Detección y Notificación

a) ¿Qué herramientas y señales podrían haber permitido una detección más temprana?
b) ¿Quién debería haber sido notificado, y cómo debe realizarse la notificación interna y externa?

3. Evaluación y Decisión

a) ¿Cómo clasificas este incidente? ¿Es un evento menor o crítico?
b) ¿Qué decisiones tomarías en cuanto a aislamiento, contención, y comunicación pública?

4. Respuesta

a) Describe las acciones inmediatas para detener el ataque y recuperar los sistemas afectados.
b) ¿Pagarías el rescate? ¿Por qué sí o por qué no?

5. Lecciones Aprendidas

a) ¿Qué falló y qué se aprendió del incidente?
b) ¿Qué acciones se deben implementar para que esto no vuelva a ocurrir?

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 7 de agosto, 23:59 horas**.