Taller - Ciberseguridad: Confidencialidad, Integridad, Disponibilidad y Malware

Sesión #2: Diferenciar entre Confidencialidad, Integridad y Disponibilidad

Duración: 60 minutos

Objetivos:

1. Comprender los principios de Confidencialidad, Integridad y Disponibilidad.

2. Aplicar estos conceptos en escenarios prácticos.

3. Analizar los impactos de brechas en estos tres pilares de la ciberseguridad.

Paso 1: Definir los Términos

Confidencialidad: Protección de la información, garantizando que solo personas autorizadas accedan a los datos.

Conceptos Relacionados:
- Cifrado
- Controles de acceso
- Autenticación

Integridad: Asegura que los datos no hayan sido alterados sin autorización.

Conceptos Relacionados:
- Suma de verificación (hashes)
- Controles de versiones

Disponibilidad: Garantiza que los datos y servicios estén accesibles cuando se necesiten.

Conceptos Relacionados:
- Redundancia
- Sistemas de respaldo
- Planificación ante desastres

Paso 2: Proporcionar y Analizar Ejemplos Prácticos (25 minutos)

Ejemplo de Confidencialidad: Empresa de salud protege los registros con cifrado y MFA.

Discusión: ¿Qué otros métodos mejorarían la confidencialidad?

Ejemplo de Integridad: Uso de hashes en descargas de software.

Discusión: ¿Qué pasa si la integridad se compromete?

Ejemplo de Disponibilidad: Banco usa servidores redundantes y backups.

Discusión: ¿Consecuencias si el banco no está disponible?

Paso 3: Reflexión y Comparación de Conceptos (15 minutos)

Actividad: Comparar los conceptos y cómo se complementan.

Preguntas de Reflexión:
- ¿Cuál es más crítico en salud vs comercio electrónico?
- ¿Cómo priorizar con recursos limitados?

Conclusión del Laboratorio:

Resumen de cómo los tres conceptos forman la base de la seguridad de la información.

Importancia de equilibrarlos según el tipo de organización.

Lista de Verificación:
- Revisar conceptos en Academia Cisco
- Subir PDF al GitHub

Laboratorio: Definir los Tipos de Malware

Duración: 60 minutos

Objetivos del Laboratorio:

1. Comprender y diferenciar los principales tipos de malware.

2. Identificar los efectos específicos de cada tipo de malware en los sistemas.

3. Asociar tipos de malware con situaciones reales.

Paso 1: Definir los Tipos de Malware (30 minutos)

Virus: Software malicioso que se adjunta a archivos legítimos.

Gusano: Se propaga automáticamente por redes.

Troyano: Se disfraza como software legítimo.

Ransomware: Cifra archivos y exige rescate.

Spyware: Monitorea actividades del usuario sin consentimiento.

Paso 2: Ejemplos de Impacto en los Sistemas (30 minutos)

Virus: Infecta correos, daña SO, se propaga.

Gusano: Saturación de red y caída de servicios.

Troyano: Acceso remoto, robo de datos.

Ransomware: Cifrado de datos, interrupción, pérdida financiera.

Spyware: Robo de datos personales, compromiso financiero.

Lista de Verificación:
- Revisar conceptos en Academia Cisco
- Subir PDF con definiciones y ejemplos a GitHub