LABORATORIO #1
Tema #1: Introducción a la Ciberseguridad
ANÁLISIS DE RIESGOS EN UN ENTORNO SIMULADO

PRESENTADO POR:

NAYIBE ESTHER ALTAMAR SERRANO

EJECUTOR TÉCNICO
JUAN SUÁREZ

MENTOR
ELISEO RODRÍGUEZ

CIBERSEGURIDAD – NIVEL BÁSICO

TALENTO TECH - UNIVERSIDAD LIBRE

JUNIO - 2025

OBJETIVOS DE LA TAREA

Aplicar los conceptos fundamentales aprendidos en el módulo "Introducción a la Ciberseguridad" para identificar activos, amenazas, vulnerabilidades y controles de seguridad en un escenario simulado.

ANÁLISIS DE RIESGOS EN UN ENTORNO SIMULADO

ESTRUCTURA DE LA TAREA.

Enunciado para el Estudiante

● **Situación:** Imagina que eres el responsable de seguridad de una pequeña empresa de comercio electrónico que maneja información sensible de clientes, incluyendo datos de tarjetas de crédito. La empresa ha detectado intentos sospechosos de acceso no autorizado.

Tu tarea es:

1. Identificar y clasificar al menos 3 activos críticos de la empresa.

2. Describir al menos 2 amenazas relevantes que podrían comprometer esos activos (una cibernética y otra física).

3. Identificar al menos 2 vulnerabilidades posibles en la infraestructura.

4. Proponer al menos 2 controles de seguridad aplicables a esas amenazas y vulnerabilidades (pueden ser técnicos o administrativos).

5. Relacionar los conceptos de confidencialidad, integridad y disponibilidad (CIA) con las amenazas y controles que describiste.

DESARROLLO DE ACTIVIDAD #1

Escenario: Empresa de comercio electrónico con datos sensibles de clientes

I. Identificar y clasificar al menos 3 activos críticos de la empresa.

1. Activos Críticos Identificados

Activo	Clasificación	Justificación
Base de datos de clientes	Crítico	Contiene información personal y tarjetas de crédito.
Servidor web de la tienda	Crítico	Plataforma principal de acceso y ventas en línea.
Cuentas administrativas (TI)	Muy crítico	Controlan configuraciones y accesos del sistema.

II. Describir al menos 2 amenazas relevantes que podrían comprometer esos activos (una cibernética y otra física).

2. Amenazas Relevantes

Tipo de amenaza	Descripción
Cibernética	Ataque de fuerza bruta para adivinar contraseñas de cuentas administrativas.
Física	Robo de un equipo con acceso a la base de datos sin cifrado.

III. Identificar al menos 2 vulnerabilidades posibles en la infraestructura.

3. Vulnerabilidades Detectadas

Vulnerabilidad	Riesgo asociado
Contraseñas débiles en cuentas administrativas	Facilita acceso no autorizado.
Falta de cifrado en datos sensibles almacenados	Datos expuestos si hay una fuga o robo físico del equipo.

IV. Proponer al menos 2 controles de seguridad aplicables a esas amenazas y vulnerabilidades (pueden ser técnicos o administrativos).

4. Controles de Seguridad Propuestos

Control	Tipo	Aplicación
Autenticación multifactor (MFA)	Técnico	Impide acceso incluso si se adivina la contraseña.
Cifrado de datos (AES-256)	Técnico	Protege la base de datos incluso si es robada o filtrada.
Políticas de contraseñas seguras	Administrativo	Exige uso de contraseñas robustas, renovación periódica y prohibición de duplicados.

V. Relacionar los conceptos de confidencialidad, integridad y disponibilidad (CIA) con las amenazas y controles que describiste.

5. Relación con el Modelo C-I-A

Pilar C-I-A	Relación con la amenaza/control
Confidencialidad	Se protege con cifrado y MFA para evitar accesos no autorizados.
Integridad	Se asegura mediante control de accesos y monitoreo de modificaciones.
Disponibilidad	Se garantiza manteniendo el servidor protegido y accesible.

Conclusión

En este análisis, se identificaron los activos más críticos y las amenazas más probables para una empresa de comercio electrónico. Se propusieron controles técnicos y administrativos que, al ser implementados correctamente, fortalecen los tres pilares esenciales de la ciberseguridad: confidencialidad, integridad y disponibilidad. Este ejercicio demuestra la importancia de tener un enfoque integral de protección, incluso en entornos pequeños o simulados.