Laboratorio 4 realizado por Adrian Molano

En este trabajo se analizará el entorno tecnológico simulado que consiste en una **red corporativa ficticia** que incluye:

- Servidor de base de datos de clientes
- Servidor de correo electrónico interno
- Almacenamiento en la nube (Google Drive o similar)
- Red Wi-Fi para empleados y una VPN para trabajo remoto

Amenazas Identificadas (3)

1. **Acceso no autorizado** a la base de datos por parte de usuarios externos.
2. **Phishing** contra empleados para obtener credenciales.
3. **Malware** (ransomware) que afecte los servidores de almacenamiento.

🔸 **Vulnerabilidades Identificadas (2)**

1. Configuración débil en los permisos de usuarios en la base de datos.
2. Empleados sin capacitación en ciberseguridad.

Amenaza	Vulnerabilidad	Impacto
Acceso no autorizado	Configuración débil en permisos	Robo o alteración de datos críticos del cliente
Phishing	Empleados sin capacitación	Fuga de credenciales corporativas y acceso al sistema
Malware	Configuración débil en permisos	Cifrado o pérdida masiva de información y tiempos de inactividad

Controles de Mitigación

Tipo	Control Propuesto
Administrativo	Entrenamiento periódico a empleados en buenas prácticas de seguridad
Técnico	Configuración de roles y permisos en base de datos
Técnico	Implementación de antivirus y firewalls en servidores y endpoints

Tabla de Riesgos (probabilidad e impacto)

Riesgo	Probabilidad	Impacto	Nivel de Riesgo
Acceso no autorizado	**Media**	**Alto**	**Alto**
Phishing	**Alta**	**Medio**	**Alto**
Malware	**Baja**	**Alto**	**Medio**