LABORATORIO 3

Presentador por:

JESUS CANO

Ejecutor Técnico

Juan Suárez

Mentor

Eliseo Rodríguez

CIBERSEGURIDAD – NIVEL BÁSICO

Talento TECH

SEPTIEMBRE – 2025

Describir brevemente el entorno tecnológico simulado o real

El entorno simulado es un café que ofrece conectividad a clientes y personal mediante tecnologías de red. Dispone de una red Wi-Fi pública para que los usuarios se conecten desde sus dispositivos y de una red privada para el negocio, que enlaza equipos críticos como computadoras administrativas, POS, cámaras e impresoras. Esta separación garantiza la seguridad interna mientras se ofrece un servicio de Internet eficiente a los clientes.

Identificar al menos 3 amenazas y 2 vulnerabilidades en dicho entorno.

Amenaza	Vulnerabilidad
Acceso no autorizado a la red privada	Contraseñas débiles o repetidas en redes y dispositivos
Intercepción de comunicaciones en la Wi-Fi pública	Falta de segmentación o configuración deficiente en el router
Malware o ransomware	Dispositivos sin actualizaciones de seguridad

Relacionar cada amenaza con una vulnerabilidad y justificar su impacto.

Amenaza	Vulnerabilidad	Impacto

Acceso no autorizado a la red privada	Contraseñas débiles o repetidas en redes y dispositivos	Alto: riesgo de pérdida de datos sensibles
Intercepción de comunicaciones en la Wi-Fi pública	Falta de segmentación o configuración deficiente en el router	Medio: exposición de datos de clientes
Malware o ransomware	Dispositivos sin actualizaciones de seguridad	Alto: puede detener la operación del negocio

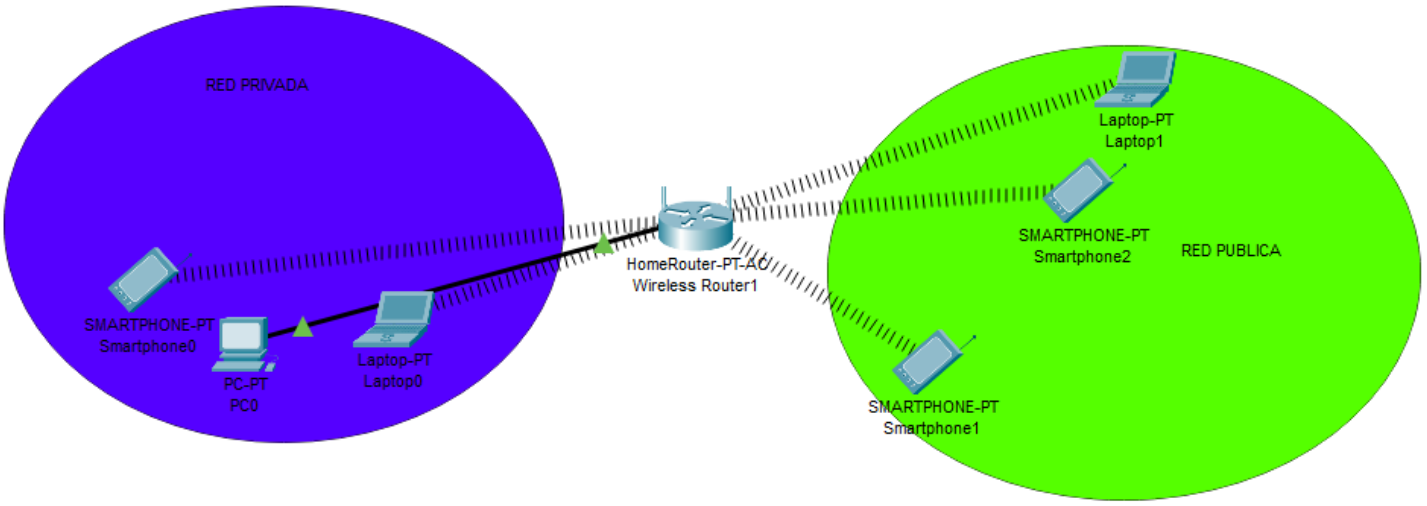
Proponer al menos 3 controles de mitigación (técnicos, administrativos o físicos).

Amenaza	Vulnerabilidad	Impacto	Control
Acceso no autorizado a la red privada	Contraseñas débiles o repetidas en redes y dispositivos	Alto: riesgo de pérdida de datos sensibles	Implementar contraseñas robustas, WPA3 en Wi-Fi y segmentación de redes (VLAN) para aislar la red privada de la pública
Intercepción de comunicaciones en la Wi-Fi pública	Falta de segmentación o configuración deficiente en el router	Medio: exposición de datos de clientes	Configurar correctamente el router, aplicar aislamiento de clientes en la Wi-Fi pública y monitorear el tráfico con firewall.
Malware o ransomware	Dispositivos sin actualizaciones de seguridad	Alto: puede detener la operación del negocio	Establecer políticas de actualizaciones periódicas, usar antivirus en equipos críticos y capacitar al personal en buenas prácticas.

Diseñar una tabla de riesgo utilizando criterios básicos de probabilidad e impacto (bajo, medio, alto).

Amenaza	Vulnerabilidad	Impacto	Probabilidad
Acceso no autorizado a la red privada	Contraseñas débiles o repetidas en redes y dispositivos	Alto	Alto
Intercepción de comunicaciones en la Wi-Fi pública	Falta de segmentación o configuración deficiente en el router	Medio	Medio
Malware o ransomware	Dispositivos sin actualizaciones de seguridad	Alto	Alto

Incluir un diagrama simple que muestre los componentes de la red o del sistema analizado.


RED PRIVADA
SMARTPHONE-PT
Smartphone0
PC-PT
PC0
Laptop-PT
Laptop0
HomeRouter-PT-AC
Wireless Router1
Laptop-PT
Laptop1
SMARTPHONE-PT
Smartphone2
RED PUBLICA
SMARTPHONE-PT
Smartphone1