Tarea Entregable Tema 4

ANDRES FELIPE ARIAS

CIBERSEGURIDAD

Sesión # 14: Vulnerabilidades, Amenazas y Riesgos

Título de la tarea: Análisis de Vulnerabilidades, Amenazas y Riesgos

Duración: 1 hora y media

Objetivos de la tarea

Aplicar los conocimientos adquiridos sobre análisis de riesgos, identificación de amenazas y vulnerabilidades, y propuesta de controles de mitigación en un entorno digital simulado o real.

Contexto: Eres responsable de seguridad en una empresa ficticia que maneja bases de datos de clientes, correo electrónico corporativo y servicios en la nube. El equipo directivo solicita un análisis de los riesgos más relevantes y propuestas de acción para prevenir incidentes.

Tu tarea es:

1. Describir brevemente el entorno tecnológico simulado o real (ej.: red doméstica, laboratorio virtual, red Wi-Fi pública, etc.).

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

3. Relacionar cada amenaza con una vulnerabilidad y justificar su impacto.

4. Proponer al menos 3 controles de mitigación (técnicos, administrativos o físicos).
5. Diseñar una tabla de riesgo utilizando criterios básicos de probabilidad e impacto (bajo, medio, alto).

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

Formato de Entrega

• Informe en PDF Máximo 4 páginas

• Archivo nombrado: Apellido_Nombre_Actividad4.pdf

DESARROLLO DEL LABORATORIO

Paso 1: Descripción del entorno tecnológico simulado

Entorno: Red corporativa híbrida (física y nube)

Se trabajará con una **red corporativa ficticia**, diseñada para simular un entorno empresarial moderno que maneja información sensible de clientes y procesos internos críticos. Esta red incluye:

- **Servidor de base de datos:** Contiene información confidencial de clientes, incluyendo datos personales, historial de transacciones y credenciales de acceso a sistemas internos. El servidor está conectado a la red corporativa con accesos controlados por firewall y políticas de seguridad.
- **Correo electrónico corporativo:** Sistema interno o en la nube utilizado para la comunicación empresarial. Es un vector crítico, ya que puede ser explotado mediante técnicas de phishing o malware para comprometer cuentas de usuario.
- **Servicios en la nube:** Incluyen almacenamiento de información, aplicaciones colaborativas y herramientas de productividad accesibles desde distintos dispositivos y ubicaciones. Estos servicios deben gestionarse con políticas de seguridad y control de accesos para evitar filtraciones o pérdida de datos.
- **Dispositivos de usuario y conectividad:** Los empleados acceden a la red mediante computadoras portátiles y dispositivos móviles conectados a través de Wi-Fi corporativo. Esto introduce riesgos adicionales, como la exposición a redes inseguras o el uso de dispositivos no actualizados.

Este entorno simulado permite **analizar riesgos, amenazas y vulnerabilidades en un escenario representativo de la realidad corporativa**, facilitando la implementación de controles y estrategias de mitigación efectivas.

Paso 2: Amenazas y vulnerabilidades

Amenazas:

1. **Phishing dirigido a empleados vía correo corporativo:** Correos electrónicos falsos que buscan engañar al personal para que revele información sensible o haga clic en enlaces maliciosos. Este tipo de

amenaza es frecuente y puede ser el punto de entrada para ataques más graves, como robo de credenciales o ransomware.
2. **Ataque de ransomware a servidores o estaciones de trabajo:** Software malicioso que encripta información crítica y solicita un rescate para recuperarla. Los ataques de ransomware pueden paralizar operaciones, generar pérdidas económicas y afectar la reputación de la empresa.
3. **Acceso no autorizado a las bases de datos:** Usuarios internos o externos que logran vulnerar los controles de acceso y obtienen información confidencial, ya sea por explotación de fallos de seguridad o credenciales comprometidas.

Vulnerabilidades:

1. **Contraseñas débiles o compartidas:** La utilización de contraseñas simples, repetidas o compartidas entre usuarios facilita que un atacante obtenga acceso no autorizado mediante técnicas como fuerza bruta o ingeniería social.
2. **Falta de actualizaciones en servidores y aplicaciones:** Sistemas sin parches recientes o con versiones obsoletas son altamente vulnerables a exploits conocidos. Esta vulnerabilidad aumenta el riesgo de infecciones por malware, ransomware y accesos indebidos.

Estas amenazas y vulnerabilidades están **estrechamente relacionadas**, y su análisis permite priorizar los riesgos más críticos, establecer controles efectivos y garantizar la seguridad de la infraestructura tecnológica corporativa.

Paso 3: Relación amenaza-vulnerabilidad e impacto

Amenaza	Vulnerabilidad	Relación y Justificación	Impacto
Phishing dirigido	Falta de doble autenticación	La ausencia de doble autenticación aumenta la probabilidad de que las credenciales robadas permitan el acceso directo a correos y sistemas críticos.	Alto
Ransomware	Parcheo incompleto	Los sistemas sin actualizaciones aprovechan vulnerabilidades conocidas, permitiendo que el ransomware encripte información esencial en servidores y estaciones de trabajo.	Muy alto
Acceso no autorizado	Falta de segmentación avanzada	Sin segmentación de la red, un atacante que consigue acceso inicial puede moverse lateralmente y comprometer otros sistemas y datos sensibles.	Alto

Controles de mitigación

Técnicos:

- **Implementación de autenticación multifactor (2FA/MFA)** en todos los accesos a sistemas críticos, incluyendo correo electrónico corporativo, VPN y plataformas en la nube. Esto garantiza que incluso si una contraseña es comprometida, un atacante no pueda acceder sin la segunda capa de verificación.
- **Actualización y parcheo automatizado** de sistemas operativos, servidores y aplicaciones mediante herramientas de gestión remota como WSUS, SCCM o soluciones equivalentes, asegurando que todas las vulnerabilidades conocidas sean corregidas de manera oportuna.
- **Monitoreo y registro de actividades críticas** con sistemas de detección de intrusos (IDS/IPS) para identificar patrones sospechosos en tiempo real y prevenir accesos no autorizados.

Administrativos:

- **Capacitación periódica en ciberseguridad** para todos los empleados, abordando temas como phishing, creación de contraseñas seguras, manejo adecuado de información sensible y uso seguro de servicios en la nube.
- **Políticas de seguridad internas claras y obligatorias**, que incluyan protocolos de uso de dispositivos, gestión de contraseñas, acceso a información confidencial y procedimientos ante incidentes de seguridad.

- **Simulaciones y pruebas de conciencia de seguridad**, como ejercicios de phishing controlados, para evaluar la preparación del personal y reforzar hábitos seguros.

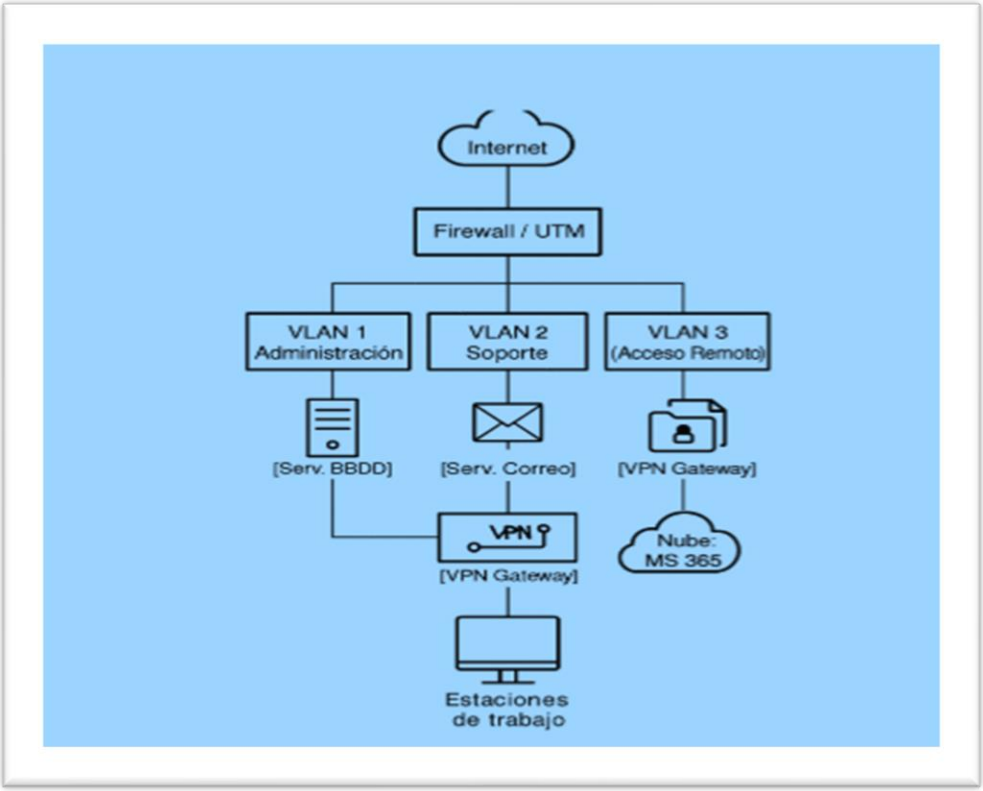
Físicos:

- **Control de acceso físico a salas de servidores y dispositivos críticos** mediante sistemas biométricos, tarjetas RFID o códigos de acceso únicos, restringiendo el ingreso solo al personal autorizado.
- **Monitoreo mediante cámaras de seguridad y alarmas** en áreas sensibles, para detectar cualquier intento de intrusión o manipulación no autorizada de los equipos.
- **Almacenamiento seguro de equipos y medios de respaldo** en cajas fuertes o ubicaciones físicas protegidas, evitando pérdidas o robo de información crítica.

Paso 5: Tabla de análisis de riesgos

Riesgo	Probabilidad	Impacto	Nivel de Riesgo
Robo de credenciales (phishing)	Alta	Alto	**Alto**
Infección por ransomware	Media	Muy alto	**Alto**
Acceso lateral desde externo	Media	Alto	**Alto**
Fuga de datos por pérdida de dispositivos	Media	Medio	**Medio**

Paso 6: Diagrama de red simplificado



Paso 7: Conclusiones

- **La identificación proactiva de amenazas y vulnerabilidades es clave para proteger los activos digitales:** En cualquier entorno corporativo que maneje información sensible, como bases de datos de clientes, correos electrónicos o servicios en la nube, amenazas como el phishing, el ransomware y los accesos no autorizados representan riesgos críticos que pueden comprometer la continuidad del negocio. Detectar y analizar estas amenazas de manera temprana permite implementar estrategias de mitigación más efectivas y reduce la probabilidad de incidentes que afecten la confidencialidad, integridad y disponibilidad de la información.
- **La correlación entre amenazas y vulnerabilidades facilita la evaluación del impacto real sobre la infraestructura tecnológica:** Relacionar amenazas específicas con vulnerabilidades técnicas, administrativas o físicas (por ejemplo, contraseñas débiles, falta de actualización de sistemas o accesos físicos no controlados) permite priorizar los riesgos que requieren atención inmediata. Este enfoque estructurado fundamenta decisiones informadas y orientadas a fortalecer la resiliencia digital de la organización, garantizando que los recursos se asignen de manera eficiente y que los controles de mitigación sean más efectivos.
- **La implementación de controles de mitigación integrales refuerza la seguridad organizacional:** La combinación de medidas técnicas (autenticación multifactor, actualización de sistemas, monitoreo),

administrativas (capacitaciones, políticas y simulaciones) y físicas (control de accesos, almacenamiento seguro y monitoreo de instalaciones) proporciona un enfoque integral que reduce significativamente la probabilidad y el impacto de los riesgos identificados.