Universidad Corporativa | Programas Académicos

Ingeniería en Desarrollo de Software

Actividad |2| Prevención de Fuentes de Ataques e Intrusión.

Seguridad Informática I.

Ingeniería en Desarrollo de Software.

TUTOR: Jessica Hernández Romero.

ALUMNO: Ramón Ernesto Valdez Felix.

FECHA: 08/01/2025.

Introducción.

En esta actividad dos de la materia de Seguridad Informática I, realizaremos la documentación donde recomendaremos algunas de las soluciones para las vulnerabilidades presentadas en el análisis de la primera actividad, la contextualización de la actividad dos es la siguiente: se identificaron las diversas amenazas y vulnerabilidades del colegio de educación superior de la ciudad de veracruz y por tal el papel como analista de seguridad es realizar las recomendaciones para estos eventos, por tal es necesario planificar, mejorar o implementar las medidas necesarias para proteger tanto la parte física como la parte de la información, recordando que la información que no esta segura puede ser un factor de riesgo CRÍTICO para cualquier institución. Ya con el contexto de la actividad sin mas que decir realizaremos la documentación de la Prevención de Fuentes de Ataques e Intrusión para que se lleve a cabo un plan de mitigación en cualquier colegio o escuela pública de cualquier nivel que sufra de estos escenarios por no contar con ningún tipo de seguridad física o informática en el plantel.

Descripción.

En esta actividad dos de la materia de Seguridad Informática I, realizaremos la documentación de la Prevención de Fuentes de Ataques e Intrusión del análisis realizado al colegio de educación superior de la ciudad de Veracruz, el cual nos permitirá dar la recomendaciones de cada una de las vulnerabilidades y amenazas presentadas en dicho plantel ya que con esto daremos a conocer que afectaciones tiene el no tener ninguna tipo de seguridad física e informática implementada. Con el análisis de la información de las vulnerabilidades y amenazas que se presentan en el colegio de educación superior, realizaremos una tabla donde se anexara un campo de las recomendaciones de solución de cada uno de los riesgo o hallazgo detectado en el análisis de la actividad anterior, estos nos servirán para que cualquier plantel del pais de mexico que no cumpla con ningún tipo de acciones de seguridad físicas o informáticas puedan utilizar el material e implementar sus soluciones y así queden libres de amenazas y vulnerabilidades.

Justificación.

En esta actividad trabajaremos con la documentación de la Prevención de Fuentes de Ataques e Intrusión del colegio de educación superior donde utilizaremos el análisis de las vulnerabilidades y amenzas detectadas en la documentación de la actividad anterior el cual servirá para recomendar el como solucionar cada uno de los riegos o hallazgos obtenidos en el análisis creando una tabla identificando y plasmando la información del análisis y algunos puntos a tomar en cuenta para el llenado de la documentación de esta actividad de la materia de Seguridad Informática I que son los siguientes:

- PDF de está actividad en el portafolio GitHub.
- Anexar el archivo comprimida .zip en el portafolio de GitHub.
- Anexa link de GitHub en documento.
- Tabla de analisis amenzas y vulnerabilidades con sus recomendaciones.
- Con base en la Actividad 1 por cada amenaza o vulnerabilidad encontrada investigar, sustentar y redactar al menos tres recomendación para proteger, mejorar o monitorear dichos eventos y con ello evitar las fuentes de ataque e intrusión.

Desarrollo:

En este punto realizaremos la documentación de la actividad de Prevención de Fuentes de Ataques e Intrusión del colegio de educación superior de la ciudad de Veracruz, estas información nos servirá para la entrega de la actividad de la materia en curso de Seguridad Informática I, como información adicional se agregan dos recomendaciones por tipo de vulnerabilidad y amenazas dando a un total de 10 recomendaciones a las 3 requerida por la actividad de la materia en curso.

Link: GitHub

Tabla de Recomendaciones.

Se anexará la evidencia con el análisis de vulnerabilidades y amenazas detectadas en la actividad uno donde se analizó el colegio de educación superior de la ciudad de veracruz, crearemos una tabla de dichas detecciones con las recomendaciones para la solución o mitigación de cada vulnerabilidad o amenaza encontrada y así se apliquen las mejoras de la seguridad informática en el colegio.

Amenazas Humanas.		
	Numero 1	**Numero 2**
Factor de riesgo	Acciones involuntarias que comprometen la seguridad de los datos, como eliminar archivos importantes por error, compartir contraseñas o conectar dispositivos infectados a la red.	Empleados insatisfechos que pueden filtrar información confidencial o sabotear sistemas.
Recomendaciones.	**Concientización de los usuarios:** Realiza capacitaciones periódicas para que los empleados sean conscientes de las amenazas y las medidas de seguridad. **Políticas de seguridad:** Establece políticas claras y concisas sobre el uso de los sistemas informáticos y el manejo de la información.	**Concientización:** Implementar programas de concientización sobre seguridad para educar a los empleados sobre las consecuencias de sus acciones. **Canales de comunicación:** Establecer canales seguros y anónimos para que los empleados puedan expresar sus inquietudes de manera

	Respaldos regulares: Realiza copias de seguridad de forma regular y verifica que se puedan restaurar correctamente.	confidencial. **Auditoría de acceso:** Realizar auditorías periódicas de los permisos de acceso para identificar y eliminar privilegios innecesarios. **Sistemas de detección de intrusiones:** Implementar sistemas para detectar actividades sospechosas en la red y los sistemas.
Fuente de ataque e intrusión	**Ingeniería social:** Se aprovechan de la confianza de las personas para obtener que eliminen información confidencial de manera educada así realizando un ataque. **Error humano:** Personal no capacitado, confiado de lo que realiza elimina información por desconocimiento.	**Ingeniería social:** Se aprovechan de la situación del empleado insatisfecho para que se le proporcione información de la cual poder prescindir para dirigir un ataque. **Intencional humano:** El personal insatisfecho puede robar información confidencial o dañarla por no estar conforme de su situación con la institución..

Amenazas Logica.		
	Numero 1	**Numero 2**

Factor de riesgo	Denegación de servicio (DoS) para inhabilitar servicios.	Explotación de vulnerabilidades en software y sistemas operativos.
Recomendaciones.	**Implementa medidas de seguridad básicas:** Mantén tus sistemas operativos y aplicaciones actualizados, utiliza contraseñas fuertes, limita el acceso a puertos innecesarios y realiza copias de seguridad regularmente. **Monitorea constantemente tu red:** Utiliza herramientas de monitoreo para detectar anomalías en el tráfico de red que puedan indicar un ataque DDoS. **Colabora con un proveedor de servicios de Internet (ISP) confiable:** Un buen ISP puede ayudarte a identificar y mitigar ataques DDoS en tu red.	**Mantener software actualizado:** Aplicar parches de seguridad de forma regular. **Utilizar contraseñas fuertes:** Crear contraseñas únicas y complejas para cada cuenta. **Implementar firewalls y sistemas de detección de intrusiones:** Proteger la red y los sistemas de ataques externos. **Realizar copias de seguridad:** Permitir la recuperación de datos en caso de un ataque exitoso. **Concientizar a los usuarios:** Capacitar a los usuarios sobre las mejores prácticas de seguridad.
Fuente de ataque e intrusión	**Flood:** Inundar un sistema con un gran volumen de tráfico legítimo o	**Hackers individuales:** Personas con conocimientos técnicos que

	falso. **Amplificación:** Explotación de protocolos de red para amplificar el tráfico enviado, generando un mayor impacto en el objetivo. **Fragmentación:** Dividir los paquetes de datos en fragmentos más pequeños para dificultar su filtrado.	buscan explotar vulnerabilidades por diversos motivos (lucro, ideología, desafío). **Grupos de hackers organizados:** Grupos con objetivos específicos, como espionaje industrial, cibercrimen o activismo digital. **Estados-nación:** Gobiernos que utilizan ciberataques como herramienta de espionaje o sabotaje. **Criminales cibernéticos:** Individuos o grupos que buscan obtener ganancias financieras a través de actividades ilícitas en línea. **Script kiddies:** Individuos con pocos conocimientos técnicos que utilizan herramientas y exploits desarrollados por otros.

Amenazas Fisica		
	Numero 1	**Numero 2**
Factor de riesgo	Hurto de equipos, dispositivos de almacenamiento y documentación.	Incendios, inundaciones, terremotos que dañan equipos e

		nfraestructura.
Recomendaciones.	**Control de acceso:** ● Implementar sistemas de control de acceso físico, como tarjetas de identificación, biometría o cerraduras electrónicas, para restringir el acceso a áreas restringidas. ● Designar áreas específicas para el almacenamiento de equipos y documentos importantes. **Vigilancia:** ● Instalar sistemas de vigilancia por vídeo en áreas estratégicas, como entradas, salidas y zonas de almacenamiento. ● Considerar la contratación de personal de seguridad para realizar rondas periódicas.	**Incendios:** ● Instalar sistemas de detección y extinción de incendios. ● Almacenar sustancias inflamables en áreas seguras. ● Realizar inspecciones periódicas de la instalación eléctrica. **Inundaciones:** ● Elevar los equipos y sistemas eléctricos por encima del nivel de inundación. ● Instalar sistemas de drenaje y bombas de achique. ● Utilizar protectores contra sobretensiones. **Terremotos:** ● Asegurar equipos y muebles a las paredes o al suelo. ● Utilizar sistemas de amortiguación de

	Almacenamiento seguro: ● Utilizar armarios o cajas fuertes para guardar equipos y documentos confidenciales. ● Anclar equipos al mobiliario para dificultar su sustracción. **Identificación de equipos:** ● Marcar todos los equipos con un número de serie único y una etiqueta de identificación. ● Registrar los números de serie en una base de datos centralizada.	vibraciones. ● Instalar interruptores de circuito por falla a tierra (GFCI).
Fuente de ataque e intrusión	**Fuentes Internas** ● **Empleados descontentos:** Empleados que han sido despedidos o que tienen rencor hacia la empresa pueden robar equipos o documentos como acto de venganza.	**Aprovechamiento de la Vulnerabilidad:** ● **Ciberataques durante la recuperación:** Los ciberdelincuentes pueden aprovechar la vulnerabilidad de las organizaciones durante

	• **Empleados oportunistas:** Empleados que ven una oportunidad de robar equipos o documentos de bajo valor y que pueden venderlos fácilmente. • **Contratistas y visitantes:** Personas que tienen acceso a las instalaciones de la empresa y que pueden aprovechar una oportunidad para sustraer información confidencial. **Fuentes Externas** • **Ladrones comunes:** Personas que buscan oportunidades para robar cualquier tipo de propiedad, incluyendo equipos electrónicos y documentos. • **Hackers:** Ciberdelincuentes que pueden acceder a sistemas informáticos de forma remota para robar	los procesos de recuperación, cuando los sistemas de seguridad pueden estar debilitados o los empleados están ocupados con otras tareas. • **Ataques a proveedores de servicios:** Los proveedores de servicios que están involucrados en la recuperación, como empresas de telecomunicaciones o servicios en la nube, pueden ser objetivos de ataques para comprometer los sistemas de las organizaciones afectadas. **Ingeniería Social:** • **Phishing y estafas:** Los ciberdelincuentes pueden enviar correos electrónicos o mensajes de texto falsos que parecen provenir de organizaciones de ayuda o autoridades locales, con el

	datos sensibles o preparar el terreno para un robo físico.	objetivo de robar información personal o financiera de las víctimas. • **Llamadas fraudulentas:** Los delincuentes pueden llamar a las personas afectadas por el desastre, haciéndose pasar por empleados de compañías de seguros o agencias gubernamentales, para obtener información confidencial.

Vulnerabilidad de Almacenamiento.		
	Numero 1	**Numero 2**
Factor de riesgo	Dependencia de un solo servidor.	Falta de un sistema de respaldo centralizado
Recomendaciones.	**Alta Disponibilidad (HA)** • **Clustering:** Implementar clústeres de servidores para distribuir la carga de trabajo	**Implementar un Sistema de Respaldo Centralizado** • **Software de respaldo:** Utilizar un software de

	y proporcionar redundancia. ● **Balanceo de carga:** Utilizar balanceadores de carga para distribuir el tráfico entre múltiples servidores. ● **Failover automático:** Configurar sistemas de failover automático para que, en caso de fallo de un servidor, otro pueda asumir la carga de trabajo de forma transparente. **Copias de Seguridad** ● **Respaldos frecuentes:** Realizar copias de seguridad de los datos de forma regular y almacenarlas en un lugar seguro, preferiblemente fuera de las instalaciones. ● **Pruebas de restauración:** Realizar pruebas periódicas de restauración para verificar la integridad de las copias de seguridad.	respaldo especializado para automatizar el proceso de creación y almacenamiento de copias de seguridad. ● **Almacenamiento seguro:** Almacenar las copias de seguridad en un lugar seguro y físicamente separado del servidor principal, como en la nube o en un centro de datos externo. ● **Frecuencia de respaldos:** Establecer una frecuencia de respaldo adecuada según la criticidad de los datos, considerando opciones diarias, semanales o mensuales. ● **Rotulación y versión de respaldos:** Rotular y versionar las copias de seguridad para facilitar su identificación y recuperación. **Diversidad de Medios de Almacenamiento**

	• **Versionamiento de respaldos:** Mantener múltiples versiones de las copias de seguridad para permitir la recuperación de datos a un punto en el tiempo específico. **Redundancia de Componentes** • **Redundancia de hardware:** Utilizar componentes redundantes, como fuentes de alimentación, discos duros y tarjetas de red, para minimizar el riesgo de fallos. • **Redundancia de redes:** Implementar múltiples conexiones de red para garantizar la conectividad en caso de fallos en una de ellas. **Cloud Computing** • **Migración parcial o total a la nube:** Considerar la migración de aplicaciones y datos a la nube para	• **Combinación de medios:** Utilizar una combinación de medios de almacenamiento, como discos duros externos, cintas magnéticas y almacenamiento en la nube, para reducir el riesgo de pérdida de datos por falla de un solo medio. • **Copia de seguridad en la nube:** Almacenar una copia de seguridad en la nube para garantizar la disponibilidad de los datos en caso de desastres locales. **Pruebas de Restauración** • **Simulacros de recuperación:** Realizar pruebas periódicas de restauración para verificar la integridad de las copias de seguridad y validar los procedimientos de recuperación.

	aprovechar los beneficios de la escalabilidad y la alta disponibilidad que ofrecen los proveedores de servicios en la nube. ● **Nube híbrida:** Combina recursos locales y en la nube para obtener lo mejor de ambos mundos. **Virtualización** ● **Virtualización de servidores:** Consolidar múltiples servidores físicos en un único servidor físico mediante la virtualización, lo que facilita la gestión y la movilidad de las cargas de trabajo. **Monitoreo y Gestión** ● **Monitoreo proactivo:** Implementar herramientas de monitoreo para detectar y resolver problemas de forma proactiva.	**Políticas de Retención de Datos** ● **Definición de políticas:** Establecer políticas claras sobre el tiempo de retención de las copias de seguridad, considerando la legislación aplicable y los requisitos de la empresa. **Concientización del Personal** ● **Capacitación:** Capacitar al personal sobre la importancia de las copias de seguridad y los procedimientos a seguir en caso de pérdida de datos. **Seguridad de las Copias de Seguridad** ● **Encriptación:** Cifrar las copias de seguridad para proteger los datos en caso de robo o acceso no autorizado. ● **Control de acceso:**

	• **Gestión de configuración:** Utilizar herramientas de gestión de configuración para automatizar las tareas y garantizar la consistencia de los entornos. **Planes de Recuperación ante Desastres (DRP)** • **Desarrollo de un DRP:** Elaborar un plan detallado que describa los procedimientos a seguir en caso de un desastre. • **Pruebas del DRP:** Realizar pruebas periódicas del plan para verificar su eficacia. **Seguridad** • **Protección contra ciberataques:** Implementar medidas de seguridad robustas para proteger los sistemas y datos de ataques cibernéticos.	Restringir el acceso a las copias de seguridad a personal autorizado. **Consideraciones Adicionales** • **Sincronización en tiempo real:** Para aplicaciones críticas, considerar la sincronización en tiempo real de los datos con un servidor remoto. • **Replicación:** Implementar la replicación de datos a un sitio remoto para garantizar la alta disponibilidad. • **Archivos de registro:** Realizar copias de seguridad de los archivos de registro del sistema para facilitar la resolución de problemas.

	Conciencia del Personal ● **Capacitación:** Capacitar al personal sobre los procedimientos de recuperación y las medidas de seguridad.	
Fuente de ataque e intrusión	**Hackers y Cibercriminales:** ● **Ataques DDoS:** Estos ataques buscan saturar el servidor con un gran volumen de tráfico, impidiendo que los usuarios legítimos puedan acceder a los servicios. ● **Explotación de vulnerabilidades:** Los hackers buscan y explotan vulnerabilidades en el software del servidor o en las aplicaciones que se ejecutan en él. ● **Inyección de código:** Esta técnica permite a los atacantes inyectar código	**Ataques cibernéticos:** ● **Ransomware:** Este tipo de malware cifra los datos del sistema, haciendo imposible su acceso sin el pago de un rescate. Al no contar con copias de seguridad actualizadas, las organizaciones se ven obligadas a pagar a los ciberdelincuentes. ● **Malware:** Otros tipos de malware pueden dañar, borrar o robar los datos del sistema, causando pérdidas irreparables si no existen copias de seguridad.

	malicioso en las aplicaciones web, lo que puede darles acceso a la base de datos o a otros sistemas. • **Ransomware:** El ransomware cifra los datos del servidor, exigiendo un pago para restaurarlos. **Ataques internos:** • **Empleados descontentos:** Empleados con acceso al servidor pueden causar daño intencionalmente. • **Errores humanos:** Errores de configuración o manipulación accidental pueden comprometer la seguridad del servidor.	**Fallos del sistema:** • **Errores humanos:** Errores de configuración, eliminación accidental de datos o fallos en el hardware pueden causar la pérdida de información valiosa. **Desastres naturales:** • **Incendios, inundaciones, terremotos:** Estos eventos pueden dañar o destruir los equipos y los datos almacenados, causando pérdidas significativas.

Vulnerabilidad de Comunicación.		
	Numero 1	**Numero 2**
Factor de riesgo	Red local insegura:	Uso de contraseñas débiles.

Recomendaciones.	**Fortalecimiento de la Infraestructura de Red** ● **Contraseñas robustas:** Exige contraseñas fuertes y únicas para todos los dispositivos de la red, incluyendo routers, switches y servidores. Implementa políticas de rotación de contraseñas regularmente. ● **Cifrado:** Utiliza protocolos de cifrado como WPA2 o WPA3 para proteger la comunicación inalámbrica. ● **Segmentación de redes:** Divide la red en segmentos más pequeños para limitar el impacto de un posible ataque. ● **Actualizaciones constantes:** Mantén actualizado el firmware de	**Políticas de Contraseñas Robustas** ● **Complejidad:** Exige contraseñas que combinen mayúsculas, minúsculas, números y caracteres especiales. ● **Longitud:** Establece una longitud mínima de contraseña, idealmente de 12 caracteres o más. ● **Unicidad:** Prohíbe el uso de contraseñas comunes, fechas de nacimiento o nombres propios. ● **Rotación regular:** Implementa una política de rotación de contraseñas, obligando a los usuarios a cambiarlas cada cierto tiempo. ● **Prohibición de contraseñas compartidas:** Evita que los usuarios compartan

	todos los dispositivos de red y aplica parches de seguridad de manera oportuna. ● **Inventarios de dispositivos:** Lleva un registro detallado de todos los dispositivos conectados a la red para identificar y eliminar equipos no autorizados. **Consideraciones Adicionales** ● **VPN:** Si utilizas redes públicas, utiliza una VPN (Red Privada Virtual) para cifrar tu tráfico y proteger tus datos. ● **Autenticación de dos factores:** Implementa la autenticación de dos factores para agregar una capa adicional de seguridad a las cuentas de usuario. ● **Cifrado de disco completo:**	contraseñas entre diferentes cuentas. **Herramientas de Gestión de Contraseñas** ● **Gestores de contraseñas:** Utiliza gestores de contraseñas confiables para generar y almacenar contraseñas seguras de forma centralizada. ● **Autenticación de dos factores (2FA):** Implementa la 2FA para agregar una capa adicional de seguridad a las cuentas de usuario. **Concientización de los Usuarios** ● **Capacitación:** Ofrece capacitación regular a los empleados sobre la importancia de las contraseñas seguras y las mejores prácticas para

	Cifra el disco duro de los dispositivos para proteger los datos en caso de pérdida o robo.	crearlas y protegerlas. ● **Simulaciones de ataques:** Realiza simulaciones de ataques de phishing para evaluar la conciencia de los usuarios e identificar áreas de mejora. **Medidas Técnicas** ● **Bloqueo de cuentas:** Implementa políticas de bloqueo de cuentas después de un número determinado de intentos de inicio de sesión fallidos. ● **Auditoría de contraseñas:** Realiza auditorías periódicas de las contraseñas utilizadas en la organización para identificar contraseñas débiles o comprometidas. ● **Prevención de fuerza bruta:** Utiliza mecanismos de prevención de fuerza bruta para proteger contra ataques

		automatizados que intentan adivinar contraseñas.
Fuente de ataque e intrusión	• **Hackers y cibercriminales:** Estos actores buscan explotar vulnerabilidades para obtener acceso no autorizado, robar información confidencial, extorsionar a organizaciones o causar daños. • **Empleados malintencionados:** Los empleados con acceso a la red pueden aprovechar sus privilegios para cometer actos de sabotaje o robar información. • **Ataques internos:** Los ataques internos pueden ser intencionales.	**Hackers y cibercriminales:** Estos actores utilizan diversas técnicas para obtener contraseñas, como: • **Ataques de fuerza bruta:** Intentan adivinar contraseñas probando todas las combinaciones posibles. • **Ataques de diccionario:** Utilizan listas de palabras comunes y combinaciones para descifrar contraseñas. • **Phishing:** Engañan a los usuarios para que revelen sus contraseñas a través de correos electrónicos o sitios web falsos. • **Malware:** Instalan programas maliciosos en los dispositivos de los usuarios para robar información, incluyendo contraseñas.

Conclusion.

En conclusión: La seguridad de la información en la era digital es un desafío constante. Las amenazas evolucionan rápidamente y los individuos, tanto en el ámbito laboral como personal, son cada vez más vulnerables. Sin embargo, es posible minimizar los riesgos adoptando medidas preventivas adecuadas.

La prevención de ataques e intrusiones requiere un enfoque integral. Desde la implementación de tecnologías de seguridad robustas, como firewalls y sistemas de detección de intrusiones, hasta la concientización y capacitación de los usuarios, cada acción cuenta. Es fundamental que las organizaciones y los individuos comprendan que la seguridad es una responsabilidad compartida y que todos deben jugar un papel activo en la protección de sus datos.

En resumen, para protegerse de las amenazas cibernéticas, es esencial:

- Mantener software y sistemas actualizados.
- Utilizar contraseñas fuertes y únicas.
- Ser cauteloso con los correos electrónicos y enlaces sospechosos.
- Realizar copias de seguridad periódicas.
- Educar a los usuarios sobre las mejores prácticas de seguridad.

Al adoptar estas medidas, podemos reducir significativamente el riesgo de sufrir un ataque cibernético y proteger nuestra información confidencial. La seguridad cibernética es una inversión a largo plazo que protege tanto a las empresas como a los individuos.

Referencias.

Gemini - chat to supercharge your ideas. (n.d.). Gemini. Retrieved January 9, 2025, from https://gemini.google.com/

Ingeniería en desarrollo de software. (n.d.). Edu.Mx. Retrieved January 9, 2025, from https://umi.edu.mx/coppel/IDS/login/index.php