Universidad Corporativa | Programas Académicos

Ingeniería en Desarrollo de Software

Actividad |1| Análisis de Vulnerabilidades y Amenazas.

Seguridad Informática I.

Ingeniería en Desarrollo de Software.

TUTOR: Jessica Hernández Romero.

ALUMNO: Ramón Ernesto Valdez Felix.

FECHA: 06/01/2025.

Introducción.

En esta actividad uno de la materia de Seguridad Informática I, realizaremos el análisis y la documentación que plantea la actividad de la materia donde nos indica el analizar la contextualización de la actividad uno, analizando las vulnerabilidades y las amenazas que se encuentran en el colegio de educación superior en el cual aplicaremos el mecanismos de seguridad informática al realizar el análisis de los factores presentados en el punto de justificación, realizar una tabla de las posibles fuentes de amenazas y vulnerabilidades (Amenazas: humanas, lógicas y físicas; Vulnerabilidades: almacenamiento y comunicación) que se describe más adelante, como información adicional daremos una explicación breve y sencilla de que son las vulnerabilidades en el mundo digital: son fallas o debilidades en sistemas, aplicaciones o procesos que pueden ser explotadas por atacantes. Y las amenazas en el mundo digital: son las acciones o eventos que buscan aprovechar esas vulnerabilidades para causar daño.

Descripción.

En esta actividad uno de la materia de Seguridad Informática I, realizaremos el análisis de la información y documentación de las partes principales de la actividad donde realizaremos una tabla para describir las vulnerabilidades y amenazas que se presentan en el colegio de educación superior, donde se presentan una serie de situaciones a las cuales aplicaremos el mecanismos de seguridad informática analizando la documentación proporcionada por la materia en curso y agregamos como evidencia el análisis de la tabla de vulnerabilidades y amenazas encontradas en la contextualización de los escenarios presentados del colegio de educación superior de la ciudad de veracruz y cercano a la costa, el cual tiene muchas situaciones las analizaremos, documentamos para así llegar a tener visualizadas todos los puntos a que se tienen que mitigar para tener la solución de mejora del colegio educación superior de la ciudad de veracruz y así tener mejor seguridad en todos los puntos de los escenarios presentados.

Justificación.

En esta actividad trabajaremos con la documentación del colegio de educación superior donde se solicita el análisis de las vulnerabilidades y amenzas detectadas en la documentación presentados en los escenarios de la actividad donde crearemos una tabla identificando y plasmando la información de los puntos 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.
- Escenarios a analizar:
    - Escenario Uno.

Escenario principal.
● La institución educativa se encuentra en Veracruz , cerca de la costa. ● Su infraestructura es de 2 pisos con 18 salones , 3 departamentos (Contabilidad y finanzas / Dirección / Desarrollo Académico/ , así como un centro de cómputo y una biblioteca. ● Actualmente tiene 4 escaleras de acceso a planta superior y 1 ascensor principal. ● Presenta una entrada principal 2 laterales y posterior a la cancha principal una salida. ● Los docentes registran su entrada en una libreta y los departamentos utilizan tarjetas de registro . ● El área administrativa financiera no cuenta con una alarma de seguridad para su acceso.

● Se cuenta con 2 extintores Clase A y uno Clase B ubicados en el piso principal. ● Se cuenta con una salida de emergencia. ● No se identifica dispositivo de detección de sismos, u otros fenómenos naturales. ● Se cuenta con un servidor principal(diferente al del centro de computo).

- Escenario Dos.

Escenario infraestructura.
Respecto al centro de cómputo presenta la siguiente infraestructura: ● 1 Servicio de internet de 20GB comercial. ● 10 equipos de escritorio. ● 5 laptops. ● 1 servidor espejo. En los departamentos presenta la siguiente infraestructura: ● 4 equipos por departamento. ● Los equipos de la planta baja se encuentran conectados por cable de manera directa al módem. Los del piso de arriba son portátiles y se conectan vía wifi. ● Los equipos han estado lentos en el último mes y se están quedando sin espacio de almacenamiento. Otros detalles:

- Cada equipo cuenta con un usuario y contraseña básicos, por ejemplo:
  - Usuario: Equipo1
  - Password: 1234abc
- El firewall no se encuentra habilitado.
- El antivirus es nod32 versión gratuita en todos los equipos.
- No se tiene denegado el uso del equipo para actividades personales, por ejemplo, el acceso a redes sociales o el manejo del correo electrónico o whatsapp.
- El Servidor cuenta con la base de datos general. Este utiliza el software Oracle Database en un sistema operativo Linux. Por su parte, el Servidor 2 se destina para alojar un sistema de control que descargaron de Internet, y que les ayuda para mantener los registros de los alumnos (se desconoce la fuente de este software).

Desarrollo:

En este punto realizaremos la documentación de la actividad de análisis de vulnerabilidades y amenazas 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.

Link: GitHub

Tabla de Analisis.

Se anexará la evidencia con el análisis de vulnerabilidades y amenazas detectadas en el colegio de educación superior donde crearemos una tabla de dichas detecciones para que se realice la mitigación de los hallazgos y así se apliquen las mejoras de la seguridad informática en el colegio.

Escenario principal.	
Vulnerabilidades	
Almacenamiento	**Comunicacion.**
• **Falta de un sistema de respaldo centralizado:** La ausencia de un sistema de respaldo confiable para los datos almacenados en los equipos, servidores y departamentos expone a la institución a la pérdida permanente de información en caso de fallas del sistema, desastres naturales o ataques cibernéticos. • **Almacenamiento local en equipos:** El almacenamiento de datos de forma local en cada equipo (documentos, bases de datos pequeñas, etc.) puede dificultar la gestión y protección de la información, especialmente en caso de pérdida o daño del equipo. • **Falta de control de versiones:** No existe evidencia de un sistema para controlar las versiones de los documentos y archivos, lo que dificulta la recuperación de versiones anteriores en caso de errores o modificaciones no deseadas. • **Seguridad de los datos en los departamentos:** La forma en que se	• **Red local insegura:** La falta de un firewall y la conexión directa de algunos equipos al módem exponen la red a ataques externos y a la propagación de malware. • **Uso de contraseñas débiles:** El uso de contraseñas simples y fácilmente adivinables compromete la seguridad de los datos en tránsito y en reposo. • **Falta de encriptación de datos:** La comunicación de datos, especialmente a través de la red Wi-Fi, no parece estar encriptada, lo que permite la interceptación de información por parte de terceros. • **Ausencia de un sistema de detección de intrusiones:** No se menciona la existencia de herramientas para detectar y prevenir ataques a la red. • **Dependencia de un solo proveedor de internet:** La institución depende de un único proveedor de internet, lo que la vuelve vulnerable a interrupciones en el servicio.

almacenan y protegen los datos en cada departamento es desconocida, lo que podría exponer información confidencial a riesgos. • **Dependencia de un solo servidor:** La institución parece depender en gran medida de un solo servidor para almacenar datos críticos, lo que la vuelve vulnerable a fallas de hardware o software.	

Amenazas.		
Humanas.	**Lógicas.**	**Fisicas.**
Errores humanos: • Acciones involuntarias que comprometen la seguridad de los datos, como eliminar archivos importantes por error, compartir contraseñas o conectar dispositivos infectados a la red. • Configuración incorrecta de equipos o software.	**Malware:** • Virus, gusanos, troyanos, ransomware que infectan equipos y redes, cifrando datos o bloqueando el acceso a sistemas. • Ataques de phishing para obtener credenciales de acceso. **Ataques cibernéticos:**	**Desastres naturales:** • Incendios, inundaciones, terremotos que pueden dañar equipos, infraestructura y causar la pérdida de datos. **Robo:** • Hurto de equipos, dispositivos de almacenamiento y documentación que

Intención maliciosa: ● Empleados insatisfechos que pueden filtrar información confidencial o sabotear sistemas. ● Usuarios no autorizados que obtienen acceso a datos sensibles. ● Espionaje industrial por parte de competidores.	● Inyección de SQL para comprometer bases de datos. ● Denegación de servicio (DoS) para inhabilitar servicios. ● Explotación de vulnerabilidades en software y sistemas operativos. **Ingeniería social:** ● Tácticas para manipular a usuarios y obtener información confidencial, como correos electrónicos fraudulentos o llamadas telefónicas falsas.	contienen información confidencial. **Sabotage:** ● Daño intencional a equipos o infraestructura con el objetivo de interrumpir las operaciones o destruir datos.

Escenario de Infraestructura:	
Vulnerabilidades	
Almacenamiento	**Comunicacion.**

Servidor Principal (Oracle Database):

- Seguridad de la base de datos:
    - Credenciales débiles: El uso de credenciales predeterminadas o fácilmente adivinadas expone la base de datos a ataques de fuerza bruta.
    - Falta de parches: Si el software Oracle Database no se encuentra actualizado, podría ser vulnerable a exploits conocidos.
    - Permisos excesivos: Es posible que los usuarios tengan permisos excesivos sobre la base de datos, lo que podría permitirles realizar modificaciones no autorizadas.
- Respaldos:
    - Frecuencia y almacenamiento: La falta de una estrategia de respaldo regular y seguro puede resultar en la pérdida permanente de datos en caso de un incidente.
- Software de terceros:
    - Origen desconocido: El software de

Red:

- Firewall deshabilitado: La falta de un firewall deja la red expuesta a ataques externos.
- Conexiones directas: La conexión directa de los equipos al módem puede facilitar la propagación de malware.
- Wi-Fi sin encriptación: El uso de redes Wi-Fi sin encriptación permite que terceros interceptan el tráfico de datos.
- Datos en tránsito:
- Credenciales débiles: El uso de contraseñas débiles expone las comunicaciones a ataques de interceptación.
- Falta de VPN: La ausencia de una red privada virtual (VPN) para las conexiones remotas expone los datos a riesgos de seguridad.

control de alumnos descargado de Internet podría contener vulnerabilidades o puertas traseras. ○ Actualizaciones: Es probable que este software no reciba actualizaciones de seguridad, lo que lo convierte en un objetivo fácil para los atacantes.	
Equipos de escritorio y portátiles: ● Espacio de almacenamiento insuficiente**:** La falta de espacio disponible puede obligar a los usuarios a almacenar datos en dispositivos externos o en la nube, lo que aumenta el riesgo de pérdida o exposición de datos. ● Software desactualizado: La versión gratuita de Nod32 podría no ofrecer la protección más actualizada contra las últimas amenazas. ● Uso de equipos para actividades personales: El acceso a redes sociales y correo electrónico puede introducir malware en la red.	

Amenazas.		
Humanas.	**Lógicas.**	**Fisicas.**
Errores humanos: ● Configuración incorrecta de equipos o software. ● Descarga de software no confiable. ● Pérdida o robo de dispositivos. ● Uso de contraseñas débiles y compartidas. ● Clic en enlaces sospechosos en correos electrónicos o sitios web. ● Intención maliciosa: ● Empleados insatisfechos que sabotean sistemas. ● Usuarios que abusan de sus privilegios. ● Espionaje industrial por parte de competidores.	**Malware:** ● Virus, gusanos, troyanos, ransomware que infectan equipos y redes. ● Ataques de phishing para obtener credenciales de acceso. **Ataques cibernéticos:** ● Inyección de SQL para comprometer bases de datos. ● Denegación de servicio (DoS) para inhabilitar servicios. ● Explotación de vulnerabilidades en software y sistemas operativos. **Ingeniería social:**	**Desastres naturales:** ● Incendios, inundaciones, terremotos que dañan equipos e infraestructura. **Robo:** ● Hurto de equipos, dispositivos de almacenamiento y documentación. **Sabotage:** ● Daño intencional a equipos o infraestructura.

	• Tácticas para manipular a usuarios y obtener información confidencial.	

Conclusion.

En conclusión: El análisis de vulnerabilidades y amenazas revela un panorama complejo y en constante evolución, tanto en el entorno laboral como en nuestra vida diaria. La interconexión digital ha ampliado exponencialmente las superficies de ataque, haciendo que la protección de datos y sistemas sea un desafío crítico. En el ámbito laboral, las organizaciones deben implementar estrategias de seguridad proactivas, que incluyan la capacitación del personal, la adopción de tecnologías de seguridad robustas y la realización de evaluaciones de riesgo periódicas. En la vida cotidiana, es fundamental que cada individuo adopte hábitos de seguridad en línea, como el uso de contraseñas fuertes, la desconfianza ante correos electrónicos sospechosos y la actualización regular de software.

En definitiva, la ciberseguridad es un asunto que nos concierne a todos. Al comprender las amenazas y tomando las medidas adecuadas, podemos minimizar los riesgos y proteger nuestra información personal y profesional. La colaboración entre individuos, organizaciones y gobiernos es esencial para construir un entorno digital más seguro.

Referencias.

Gemini: Chatea para potenciar tus ideas. (n.d.). Gemini. Retrieved September 30, 2024, from https://gemini.google.com/app/3a3fbf6874cd5168?hl=es-MX

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