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: José Luis Pacheco González

Fecha: 4 de septiembre de 2024

Índice

Introducción

El análisis de vulnerabilidades y amenazas es un proceso crucial en la gestión de la seguridad de la información, especialmente en instituciones educativas como un colegio de educación superior. En un entorno donde se manejan grandes volúmenes de datos personales, académicos y financieros, es fundamental identificar las posibles brechas de seguridad que podrían ser explotadas por actores malintencionados. Este análisis permite evaluar los riesgos asociados a la infraestructura tecnológica, los sistemas de información y los procesos administrativos de la institución. Al entender mejor las amenazas potenciales, como el acceso no autorizado, el robo de información, o los ciberataques, el colegio puede implementar medidas de seguridad más efectivas para proteger su información y garantizar un entorno seguro tanto para los estudiantes como para el personal. Además, el análisis de vulnerabilidades proporciona una base sólida para desarrollar políticas de seguridad, capacitaciones y planes de respuesta ante incidentes, fortaleciendo así la resiliencia de la institución frente a posibles ataques cibernéticos. Esta actividad se enfoca en identificar y mitigar dichas vulnerabilidades, con el objetivo de garantizar la integridad, confidencialidad y disponibilidad de la información en un entorno educativo cada vez más digitalizado.

Descripción

En esta actividad se llevará a cabo un análisis exhaustivo de las vulnerabilidades y amenazas que enfrenta un colegio de educación superior ubicado en Veracruz, cerca de la costa. La institución cuenta con una infraestructura que incluye 18 salones distribuidos en dos pisos, tres departamentos clave (Contabilidad y Finanzas, Dirección, y Desarrollo Académico), un centro de cómputo, y una biblioteca. A pesar de tener un sistema básico de seguridad física, como extintores y una salida de emergencia, se identifican múltiples áreas de mejora en términos de seguridad informática y protección de datos.

En particular, el área administrativa carece de alarmas de seguridad, mientras que el centro de cómputo, que alberga equipos esenciales, como 10 computadoras de escritorio, 5 laptops, y un servidor espejo, se conecta a internet mediante un servicio comercial de 20GB. La infraestructura tecnológica presenta serias deficiencias, como la falta de firewall habilitado, el uso de un antivirus gratuito y desactualizado (NOD32), y credenciales de acceso extremadamente débiles. Además, los equipos se encuentran lentos y con poco espacio de almacenamiento. El servidor principal, que maneja la base de datos general, utiliza Oracle Database en un sistema operativo Linux, mientras que un segundo servidor aloja un software de origen desconocido para la gestión de registros estudiantiles. Esta actividad se centrará en identificar y clasificar las amenazas y vulnerabilidades presentes, abordando tanto aspectos humanos, lógicos, como físicos.

Justificación

Este proyecto surge de la necesidad de proteger la integridad, confidencialidad y disponibilidad de la información en un colegio de educación superior, ubicado en una zona costera de Veracruz, con infraestructura y sistemas tecnológicos vulnerables. En un entorno donde la tecnología juega un papel crucial en la gestión educativa, es fundamental identificar y mitigar las amenazas y vulnerabilidades que podrían comprometer tanto la seguridad física como la lógica de la institución.

Las deficiencias observadas, como la falta de un sistema de alarma en el área financiera, la ausencia de un firewall habilitado, el uso de credenciales débiles y un antivirus gratuito, exponen a la institución a riesgos significativos, incluyendo accesos no autorizados, pérdida de datos y ataques cibernéticos. Además, la lentitud y falta de espacio en los equipos indican problemas en la gestión de recursos tecnológicos, lo que podría afectar la operatividad diaria y la calidad educativa.

El análisis propuesto permitirá a la institución identificar las áreas críticas que requieren intervención inmediata, así como establecer un marco para la implementación de medidas correctivas y preventivas. Este enfoque proactivo no solo contribuirá a proteger los activos informáticos y físicos de la institución, sino que también garantizará un entorno seguro y eficiente para los estudiantes, docentes y personal administrativo.

Desarrollo

Tabla de Análisis

Amenazas humanas	Amenazas Lógicas	Amenazas Físicas	Vulnerabilidades de almacenamiento	Vulnerabilidades de Comunicación
Uso de contraseñas débiles y fáciles de adivinar como "1234abc".	Falta de firewall habilitado,la red interna está expuesta a posibles accesos no autorizados o ataques externos.	Acceso físico no autorizado, entradas y salidas no controladas permiten el acceso no autorizado a la institución	Uso de software de fuentes desconocidas descargado sin verificar puede contener malware o backdoors.	Acceso a internet sin restriccione, Uso de la red para actividades no relacionadas con el trabajo, exponiéndose a phishing y malware.
Acceso no autorizado a equipos para actividades personales,como el uso de redes sociales.	Antivirus gratuito puede no ser efectivo contra nuevas amenazas.	Falta de alarma de seguridad en área financiera, corre peligro de robo físico de información sensible o equipo.	Equipos con falta de espacio de almacenamiento, aumenta el riesgo de pérdida de datos o corrupción de archivos debido a un manejo inadecuado del almacenamiento.	Falta de protección de red en equipos conectados vía Wi-Fi y posible intercepción de datos.
Falta de concientización entre los empleados sobre buenas prácticas de seguridad.	Servidor espejo vulnerable en la misma red, se expone a ataques de red que pueden comprometer ambos servidores.	Ausencia de dispositivos de detección de sismos y otros desastres naturales que podrían dañar físicamente la infraestructura.	Contraseñas débiles almacenadas en equipos, fácilmente accesibles o predecibles, comprometen la seguridad de los datos almacenados.	Exposición a ataques de red por no tener firewall habilitado, debido a la falta de control de tráfico y filtrado de paquetes
Uso inadecuado de recursos institucionales software y hardware. Provoca riesgo de introducir malware.	Sin restricciones en el uso de internet, genera riesgo de infecciones por malware debido a la navegación en sitios no seguros.	Extintores insuficientes en caso de incendio,riesgo de daño físico a equipos y pérdida de datos por fuego.	Lentitud en equipos debido a software no optimizado,afectación al rendimiento y aumento de la exposición a fallos de seguridad.	Riesgo de interceptación de comunicaciones por falta de cifrado,posibilidad de que datos sensibles sean interceptados y robados durante la transmisión.

Conclusión

El análisis de vulnerabilidades y amenazas realizado en el colegio de educación superior, resalta la urgente necesidad de fortalecer su infraestructura de seguridad tanto física como informática. La institución enfrenta desafíos significativos debido a la falta de medidas de protección adecuadas. La ausencia de un sistema de alarma en el área financiera, el uso de credenciales débiles, la falta de un firewall habilitado y la utilización de un antivirus gratuito son factores que incrementan la exposición a riesgos, comprometiendo la integridad de los datos y la operatividad de los sistemas.

Además, la infraestructura tecnológica del colegio muestra señales de deterioro, como la lentitud de los equipos y la falta de espacio de almacenamiento, lo que podría afectar negativamente la gestión educativa y administrativa. La dependencia de un software de origen desconocido para la gestión de registros estudiantiles también representa un riesgo considerable para la seguridad de los datos sensibles.

Este análisis denota la importancia de implementar medidas de seguridad robustas y actualizadas para proteger los activos tecnológicos de la institución. Al abordar las vulnerabilidades identificadas y mitigar las amenazas potenciales, el colegio podrá garantizar un entorno más seguro y eficiente para su comunidad educativa, fortaleciendo así su capacidad para enfrentar desafíos futuros en un mundo cada vez más digitalizado.

Referencias

3., E. (2023, July 25). *Así pueden protegerse los centros educativos de las amenazas informáticas*. EDUCACIÓN 3.0. https://www.educaciontrespuntocero.com/tecnologia/ciberseguridad-en-los-centros/

EEE. (2019, November 13). *Listado de amenazas y vulnerabilidades en ISO 27001*. Escuela Europea de Excelencia. https://www.escuelaeuropeaexcelencia.com/2019/11/listado-de-amenazas-y-vulnerabilidades-en-iso-27001/

Enlace Github