Universidad Corporativa Coppel | Programas Académicos

Ingeniería en Desarrollo de Software

# Actividad |1| Análisis de vulnerabilidades y Amenazas.

## Seguridad Informática 1.

Ingeniería en Desarrollo de Sofwtare.

academia global

TUTOR: Jessica Hernández Romero.

ALUMNO: Carlos Ariel Nicolini

FECHA: 30/12/2024

# Índice

# Introducción

Un análisis de riesgos y vulnerabilidades es un método de definir, identificar, clasificar y priorizar las debilidades de una aplicación, servicio, organización, etc. Realizar un análisis de riesgos y vulnerabilidades puede ayudar a proteger su organización, sistema o proceso de posibles amenazas. Al aplicarlo, se pueden identificar los riesgos más críticos y desarrollar un plan de mitigación de riesgos efectivo para proteger sus activos críticos. Sus pasos son los siguientes:

- Identificar los activos críticos: Identifique los activos críticos que deben protegerse (información confidencial, recursos físicos, sistemas de tecnología, edificios, etc.)
- Identificar las amenazas potenciales: Esto podría incluir amenazas físicas como incendios o inundaciones, amenazas cibernéticas (ataques de hackers) y amenazas internas como el robo por parte de empleados.
- Evalué la vulnerabilidad de cada activo crítico a cada amenaza identificada: que tan vulnerables es cada activo a cada amenaza.
- Evaluar el impacto potencial: Evaluar el impacto potencial de casa amenaza en cada activo y que tan grave seria el daño si se explota una vulnerabilidad.
- Calcular el riesgo: El riesgo se calcula multiplicando la probabilidad de que ocurra una amenaza por el impacto potencial de esa amenaza.
- Priorizar los riesgos: Identificarlos por su nivel de riesgo. Los riesgos más críticos deben abordarse primero.
- Desarrollar un plan de mitigación de riesgos: Desarrollar un plan para abordar los riesgos más críticos. Esto podría incluir la implementación de medidas de seguridad físicas o cibernéticas, la creación de políticas y procedimientos, y la capacitación del personal.
- Monitorear y actualizar: Monitoree el plan de mitigación de riesgos y actualícelo regularmente para asegurarse de que se mantenga actualizado y efectivo.

# Descripción

**Contextualización:**

Se pretende aplicar mecanismos de seguridad informática a un colegio de educación superior, realizando un análisis de los factores que se describen a continuación tipificando vulnerabilidades y amenazas.

**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.

Respecto al centro de cómputo presenta la siguiente infraestructura:

- 1 Servicio de internet de 20 GB 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 modem. 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 contraseñas 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 descargan de internet, y que les ayuda para mantener los registros de los alumnos (se desconoce la fuente del software).

Actividad:

De acuerdo al escenario presentado en la contextualización analizar y realizar una tabla de posibles fuentes de amenazas y vulnerabilidades (Amenazas: Humanas, lógicas y físicas, Vulnerabilidades: Almacenamiento y comunicación).

# Justificación

En esta actividad de la materia de seguridad informática aprenderemos los métodos que deben aplicarse para poder tener un ambiente seguro, por tal motivo realizaremos análisis de vulnerabilidades y amenazas de una institución educativa de Veracruz. Para dicha institución realizaremos el análisis de acuerdo al contexto proporcionado y ayudaremos realizando un análisis tras el cual realizaremos una tabla de las posibles fallas que nosotros detectamos en ella.

Este ejercicio nos enseñara que la seguridad es muy importante y realizar revisiones periódicas sobre todo el ambiente es muy necesario para poder detectar cualquier clase de debilidades que puedan ser causas de afectación a los servicios ofrecidos por dicha organización.

En mi trabajo es muy común las evaluaciones de procesos, herramientas, medidas de seguridad, etc. y todas llevan revisiones de vulnerabilidades y amenazas, las cuales si uno no comprende lo importante de su realización y su finalidad, eso puede ocasionar una afectación importante, lo cual puede significar perdida de información, interrupción de servicios (que ocasionan perdidas de dinero), accidentes mortales por no respetar normas de evacuación. Por eso es muy importante entenderlas, aplicarlas y hacer que se cumplan.

Este trabajo fue subido al siguiente enlace de GitHub

https://github.com/CarlosNico/Seguridad-Inform-tica-1

# Desarrollo

# Tabla de análisis

En el trabajo se nos pide realizar de acuerdo al escenario presentado en la contextualización, realizar un análisis y realizar una tabla de posibles fuentes de amenazas y vulnerabilidades.

De acuerdo a nuestro análisis y clasificando las amenazas en humanas, lógicas y físicas se realizó la siguiente tabla (la puse en partes por que no entraba completa una al lado de la otra) con los hallazgos que detecte.

| Amenazas Humanas |
|---|
| Contraseñas débiles y genéricas para los equipos y servidores |
| Ausencia de controles de acceso en el área administrativa y financiera |
| Uso de los equipos para actividades personales, aumentando la exposición a malware. |
| Usuarios o empleados malintencionados que podrían robar información o manipular datos |
| Visitantes o personas no autorizadas tienen acceso potencial a las instalaciones y equipos debido a la falta de controles estrictos. |

Las amenazas humanas, las cuales pueden ser por error humano, por amenazas internas intencionales o por amenazas externas se deben por la falta de aplicación de medidas de seguridad en contraseñas, falta de control de acceso a las instalaciones y departamentos además de la utilización de equipos de trabajo para actividades que no corresponden a la operación.

| Amenazas Lógicas |
| --- |
| Uso de software descargado de internet sin verificar la fuente en el servidor 2 |
| Antivirus gratuito, posiblemente desactualizado y sin soporte |
| Firewall deshabilitado, dejando vulnerable la red |
| Equipos del piso superior conectados a través de Wifi sin medidas de seguridad avanzadas. |
| Acceso no restringido a redes sociales, correos personales y aplicaciones de mensajería. |

Las amenazas lógicas detectadas se deben a la utilización de software sin verificar y sin licenciamiento, fallas en la seguridad de firewall y de la red, además de acceso a aplicaciones no afines para trabajo laboral lo cual aumenta la exposición a ataques.

| Amenazas Físicas |
| --- |
| Proximidad a la costa, lo que aumenta el riesgo de fenómenos naturales, como tormentas, huracanes y problemas derivados por la humedad. |
| Entradas múltiples sin controles estrictos ni alarmas de seguridad en áreas importantes y sensibles. |
| Falta de detectores de sismos o alarmas contra fenómenos naturales |
| Extintores clase A y B, no aptos para incendios eléctricos. |
| Salidas de emergencias insuficientes |

Las amenazas físicas son debido a la ubicación geográfica de la institución sin contar con las medidas necesarias de seguridad, falta de sistema de vigilancia, alarmas y detectores de sismos, no se cuenta con extintores de clase C (contra incendios eléctricos) y salida de emergencias insuficientes.

| Vulnerabilidades de almacenamiento |
| --- |
| Equipos sin almacenamiento suficiente. |
| No se cuenta con plan de monitoreo y ampliación de almacenamiento |
| Contraseñas débiles y genéricas, fáciles de adivinar |
| Dependencia de un servidor principal y uno espejo sin mención de Backups de seguridad regulares |
| Base de datos general en un servidor vulnerable, expuesto a ataques debido a la falta de seguridad perimetral. |

Las vulnerabilidades de almacenamiento detectadas se deben a falta de mantenimiento y dimensionamiento de los equipos de cómputo, falta de medidas de seguridad y buenas prácticas en contraseñas de los equipos y seguramente en los servidores, no está implementado un plan de respaldos periódicos y bases de datos inseguras.

| Vulnerabilidades de comunicación |
| --- |
| Ancho de banda de 20 Gb comercial, insuficiente para las operaciones de una institución. |
| Red Wifi con configuraciones básicas y falta de cifrado seguro. |
| Firewall deshabilitado lo cual permite el acceso no autorizado y aumenta la exposición a ataques externos. |
| Falta de segmentación de la red, lo cual facilita los ataques laterales. |

Las vulnerabilidades de comunicación se deben a un servicio de ancho de banda mal dimensionado para la operación, redes inalámbricas inseguras, falta de segmentación de seguridad en la red y firewall deshabilitado lo cual deja expuesto a ataques.

# Conclusión

En el mundo de los negocios es muy importante realizar un muy buen análisis de vulnerabilidades y amenazas, ya que nos va a permitir identificar, evaluar y priorizar los riesgos potenciales que podrían afectar de manera muy drástica la infraestructura tanto física como tecnológica, los datos y las operaciones de una empresa u organización.

El análisis nos permitirá descubrir debilidades, identificar configuraciones incorrectas, software desactualizado o vulnerable, contraseñas débiles, practicas o comportamientos inseguros lo cual nos ayudara para poder realizar modificaciones que nos permitan reducir la posibilidad de ataques exitosos y también mitigar el impacto de amenazas.

Como nos dijeron en un curso de seguridad, no existe empresa que no haya recibido hackeada sino cuándo será hackeada, en ese momento sonó como una frase muy buena pero no fui consciente de lo que sería hasta que paso, lo cual me demostró de lo importante que es prestar mucha importancia a cada detalle de la seguridad, lo cual no es solo aplicarse a los estándares de seguridad y cumplirlos, sino que los demás sean conscientes y entiendan la razón de por qué se deben cumplir y la responsabilidad que uno tiene con solo tener un correo corporativo o una maquina asignada.

Este trabajo fue subido al siguiente enlace de GitHub

https://github.com/CarlosNico/Seguridad-Inform-tica-1

# Referencias

Gutierrez, E. (2023, March 13). Descubre Cómo Hacer Un Análisis De Riesgos En Tus Apps. *Codster*. https://codster.io/blog/seguridad-en-aplicaciones/aplication-vulnerability/como-realizar-analisis-de-riesgos-vulnerabilidades/

Análisis de vulnerabilidades para empresas: ¿Cómo se realiza? (2024, July 18). IT Masters Mag. https://www.itmastersmag.com/transformacion-digital/analisis-de-vulnerabilidades-cual-es-su-importancia/