

# **Actividad 1 - Análisis de Vulnerabilidades y Amenazas.**


## **Seguridad Informática 1.**

## **Ingeniería en Desarrollo de Software.**

**Tutor: Jessica Hernández Romero**

**Alumno: Homero Ramirez Hurtado**

**Fecha: 20 de Diciembre del 2023**



Índice.

. Introducción.

. Descripción.

. Justificación.

. Desarrollo.

- Tabla de Análisis.

. Conclusión.

. Referencias.



## Introducción.

El análisis de vulnerabilidades y amenazas es un proceso que tiene como objetivo evaluar el nivel de seguridad de un sistema informático frente a posibles ataques cibernéticos. Consiste en identificar las debilidades que pueden ser explotadas por los atacantes, así como las amenazas que representan para los activos de información de una organización. El propósito de este análisis es determinar el grado de riesgo al que está expuesto el sistema y establecer las medidas de protección adecuadas para prevenir o mitigar los posibles daños. El análisis de vulnerabilidades y amenazas se basa en la recolección de información sobre el sistema, la detección de las amenazas, la priorización de las vulnerabilidades y la remediación de las brechas de seguridad. Este proceso es fundamental para garantizar la confidencialidad, integridad y disponibilidad de los datos, así como para cumplir con las normas y regulaciones vigentes en materia de ciberseguridad.

## Descripción.

El análisis de vulnerabilidades y amenazas es un proceso que busca identificar y evaluar los riesgos que pueden afectar la seguridad de la información de una organización. El objetivo es determinar el nivel de exposición de los activos informáticos ante posibles ataques cibernéticos y establecer las medidas de protección adecuadas.

Un análisis de vulnerabilidades y amenazas consta de los siguientes pasos:

- Reunir información de los sistemas y datos de la organización, para crear una base de referencia.
- Identificar el objetivo del análisis, es decir, lo que se quiere lograr con él.
- Detectar las amenazas, señalando qué tipo de riesgos existen en el sistema.
- Evaluar las vulnerabilidades, indicando qué debilidades o fallas pueden ser aprovechadas por las amenazas.
- Estimar el impacto y la probabilidad de cada riesgo, para calcular el nivel de exposición.
- Priorizar las amenazas de mayor riesgo y trazar mecanismos de respuesta.
- Remediar el resto de brechas y problemas de seguridad.

El análisis de vulnerabilidades y amenazas es una herramienta fundamental para la gestión de riesgos y la prevención de desastres informáticos. Permite fortalecer la seguridad de la información y evitar costos y daños asociados a su pérdida o vulneración.

## Justificación.

El análisis de vulnerabilidades y amenazas es un proceso que permite evaluar el nivel de seguridad de un sistema informático frente a posibles ataques cibernéticos. El objetivo de este proceso es identificar las debilidades que pueden ser explotadas por los atacantes, así como las amenazas que representan para los activos de información de una organización. El análisis de vulnerabilidades y amenazas es importante porque ayuda a tomar decisiones sobre las medidas de protección que se deben implementar para reducir el riesgo de sufrir un incidente de seguridad que afecte la continuidad operativa, la reputación y la rentabilidad de la organización. Además, el análisis de vulnerabilidades y amenazas contribuye a cumplir con las normativas legales y regulatorias que exigen a las organizaciones garantizar la confidencialidad, integridad y disponibilidad de sus datos.

## Desarrollo.

A continuación, realizaremos una tabla en la cual tenemos un escenario con la siguiente información:

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 cómputo).

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).

Amenazas Humanas	Amenazas Lógicas	Amenazas Físicas	Vulnerabilidades de Almacenamiento	Vulnerabilidades de Comunicación
Docentes registran su entrada en una libreta, lo que podría ser manipulado o falsificado. Departamentos utilizan tarjetas de registro, pero estas también pueden ser vulnerables a pérdida o robo.	Falta de habilitación del firewall, lo que podría permitir ataques informáticos o intrusiones no autorizadas. Contraseñas básicas (por ejemplo, "1234abc") en los equipos pueden ser fácilmente adivinadas o comprometidas.	Falta de alarma de seguridad en el área administrativa financiera. Escasez de extintores en caso de incendio. Ausencia de dispositivos de detección de sismos o fenómenos naturales.	Equipos lentos y falta de espacio de almacenamiento pueden afectar la productividad y la seguridad de los datos. Servidor espejo no se menciona si está respaldado o protegido adecuadamente.	Conexiones inalámbricas (Wi-Fi) en los equipos portátiles pueden ser vulnerables a ataques de interceptación o acceso no autorizado. Servicio de internet de 20GB comercial podría ser blanco de ataques o sobrecarga.

## Conclusión.

Una conclusión personal sobre este análisis es que se trata de una herramienta fundamental para la gestión de la seguridad de la información, ya que permite tener una visión global y actualizada de la situación de riesgo, así como establecer las prioridades y los recursos necesarios para proteger los activos más críticos. Sin embargo, este análisis también implica algunos desafíos, como la necesidad de mantenerlo actualizado ante los cambios constantes en el entorno, la dificultad de cuantificar el impacto de algunos riesgos, y la posibilidad de que existan vulnerabilidades y amenazas desconocidas o emergentes.

## Referencias.

Video de la Tutoría 1.

Bing.