

Actividad 1 - Análisis de vulnerabilidades y amenazas

Seguridad Informática I

Ingeniería en Desarrollo de Software

Tutor: Jessica Hernández Romero

Alumno: José Domingo Reyes Arroyo

Fecha: 20 de diciembre de 2023

1 Índice

1	Índice	2
1	Introducción	3
2	Descripción	4
3	Justificación	7
4	Desarrollo	8
4.1	Tabla de análisis	8
5	Conclusión	9
6	Referencias	10

1 Introducción

Para comprender claramente la seguridad informática que actualmente se vive en las redes y sistemas, vamos a definir primeramente dos conceptos que son de suma importancia, estos son: vulnerabilidad, que se define como una debilidad existente en un sistema, red o aplicación que puede ser utilizada por una persona malintencionada a menudo llamados Hacker, con la intención de comprometer la seguridad de dicho sistema. A su vez una amenaza es propiamente la acción maliciosa encaminada a aprovechar esa vulnerabilidad para hacer daño a ese sistema o a una empresa en general.

Así pues desde el inicio de los sistemas informáticos y como todo aparato o sistema construido por el humano, tiene siempre vulnerabilidades, así mismo desde que hay personas que se dedican a crear, inventar o programar sistemas, existen a la par también personas que buscan dominar esa creación o invento para buscar alguna vulnerabilidad que permita poner en riesgo este y afecte a su creador, incluso hay ocasiones y sobre todo en el ámbito de la informática, se ha conocido que muchos que realizan el programa para una empresa en específico, posteriormente se encargan también de hackearlo afectando la seguridad de la empresa.

2 Descripción

Tomando en cuenta estas definiciones, las aplicaremos para diferenciar estas vulnerabilidades y amenazas dentro del caso contextualizado para la presente actividad, en la cual se nos pide aplicar mecanismos de seguridad informática a un colegio de educación superior, realizando un análisis de los factores que se describen a continuación tipificando las 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.

- 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.

Infraestructura por departamento:

- 4 equipos de cómputo.
- 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 Data base 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).

Con esta información presentada, realizaremos un análisis para detectar posibles vulnerabilidades y/o amenazas con la finalidad de definir posibles soluciones a futuro.

3 Justificación

El análisis de los factores que representan posibles vulnerabilidades y/o amenazas, además de representar grandes ventajas para el colegio ya que se van a considerar diferentes factores que a su vez pueden ser evitados o implementados para garantizar la seguridad de la información que se maneja dentro de la organización, información que dicho en otros términos puede ser muy sensible para la administración de dicha organización. El realizar este tipo de análisis permite a los programadores implementar herramientas que proveen seguridad informática a la organización y con ello asegurar que la información que a su vez esta organización maneja de sus estudiantes sea tratada con la seguridad adecuada y esta no llegue a manos ajenas que puedan poner en riesgo no solo la integridad del colegio, sino la de los mismos estudiantes, para los estudiantes el saber que su información pudiera estar en riesgo es algo que

podría afectar que estos sigan estudiando en este colegio, lo cual también puede traer pérdidas económicas para este.

4 Desarrollo

A continuación, se elabora una tabla de análisis con los puntos relevantes que se consideran con vulnerabilidades y/o amenazas, considerando cada uno de los factores que se presentan en la descripción, con la finalidad de enfocar cada factor en la amenaza o vulnerabilidad adecuada, no se detalla el porque se considera en cada una de las diferentes clasificaciones, pero se describe el factor con lo cual se puede identificar perfectamente cada amenaza o vulnerabilidad.

4.1 Tabla de análisis

A continuación, se presenta la tabla que se elaboró posteriormente al análisis desarrollado para cada uno de los puntos relevantes, esta tabla se inserta como imagen, pero se sube al repositorio de GitHub el archivo en Excel del cual se extrajo la imagen de la tabla:

Factores	Amenazas humana	Amenazas lógicas	Amenazas físicas	Vulnerabilidades de almacenamiento	Vulnerabilidades de comunicación
Ubicación			Se encuentra en la ciudad de Veracruz cerca de la costa		
Infraestructura	Tiene 3 departamentos, 1 centro de computo y 1 biblioteca		Cuenta con 2 pisos y 18 salones		
Movilidad			Tiene 2 escaleras y un ascensor		
Accesos al edificio	Presenta 1 entrada principal, 2 laterales y una salida posterior a la cancha principal				
Entrada/Salida de personal	Los docentes se registran en una libreta y los administrativos con tarjeta				
Seguridad en áreas financieras	El área administrativa y financiera no cuentan con alarma de seguridad				
seguridad ante contingencias			Cuenta con 2 extintores clase A y 1 clase B		
Salidas de emergencia			Cuenta con 1 salida de emergencia		
dispositivos de alarma			No se tiene detectores de humo, movimiento, impacto, etc.		
Servidores físicos		solo tiene 1 servidor			
Servicio de internet					1 servicio de internet de 20 GB comercial
Equipos de escritorio				Cuenta con 10 equipos de escritorio	
Laptops				cuenta con 5 laptop	
Servidor espejo				cuenta con 1 servidor espejo	
Infraestructura de los departamentos					
Conexión de los equipos					en planta baja es con conexión directa al modem por cable y en planta alta Wi-Fi
Condición de los equipos				Equipos lentos y sin espacio de almacenamiento	
Seguridad de los equipos		Usuario y contraseña básicos (Equipo-1, 1234abc)			

5 Conclusión

Después del análisis de los factores que representan amenazas y/o vulnerabilidades para la organización de la institución, como ingenieros en desarrollo de software adquirimos los conocimientos necesarios para realizar un análisis completo para cualquier organización que lo requiera, así mismo se adquieren los conocimientos necesarios en cuanto a l seguridad informática se refiere para aprender a identificar que factores nos pueden generar amenazas dentro de nuestra empresa, de la misma manera que cuando ingresamos a la empresa en la que laboramos, nos damos cuenta de las situaciones que se presentan dentro de

ella, comparándola con otras empresas en las que hayamos laborado con anterioridad, aprendemos a tener una visión mas amplia de lo que puede ocasionar tener vulnerabilidades dentro de las organización y con ello aprendemos a usar esta misma visión para detectar amenazas generadas a causa de las vulnerabilidades detectadas.

Esta es una ventaja competitiva dentro de cualquier ámbito laboral en el que nos desarrollemos ya que nos permite visualizar en cualquier organización o empresa y detectar posibles situaciones que pongan en riesgo nuestra propia integridad como la de la empresa en la cual laboramos, estos conocimientos pueden ser aplicados tanto para enfocar nuestro propio desarrollo hacia la seguridad informática, como para cuidar nuestra integridad en el día a día con nuestra propia información y estar al pendiente de cualquier situación que pudiera afectar nuestra integridad personal.

6 Referencias

De Seguridad Informática, S. (2023, 28 septiembre). *Vulnerabilidades y amenazas informáticas*. DragonJAR - Servicios de Seguridad Informática.

<https://www.dragonjar.org/vulnerabilidades-y-amenazas-informaticas.xhtml>

Santander, B. (s. f.). *Vulnerabilidad*. Banco Santander.

<https://www.bancosantander.es/glosario/vulnerabilidad-informatica>

Ortiz, A. E. (2020, 13 julio). ¿Qué es una amenaza informática? ¿Cómo contenerla? | Blog HostDime Latinoamérica, Servidores dedicados. *Blog HostDime Latinoamérica, servidores dedicados*. <https://www.hostdime.la/blog/que-es-una-amenaza-informatica-como-contenerla/>

Actividad subida al repositorio de GitHub: <https://github.com/drcksug/Seguridad-Informatica-I>