UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA.

PROCESO DE TITULACIÓN

DICIEMBRE 2022 – MAYO 2023

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERO EN SISTEMAS DE INFORMACIÓN

TEMA:

ANÁLISIS COMPARATIVOS DE LAS AMENAZAS INFORMÁTICAS SUSCITADAS A LOS SITIOS WEB DE LAS ENTIDADES DEL SISTEMA FINANCIERO.

ESTUDIANTE:

PAULINA EVELINA AVEGNO TENORIO

TUTOR:

ING. ENRIQUE DELGADO CUADRO

AÑO 2023

Contenido

PLANTEAMIENTO DEL PROBLEMA

En la actualidad, los sitios web de las entidades del sistema financiero están cada vez más avanzados en términos de seguridad y privacidad, lo que los hace más confiables y seguros para los clientes. En estas entidades han invertido en la tecnología avanzada para proteger la información de los clientes, como el uso de encriptación de datos, sistemas de autenticación de dos factores, monitoreo continuo de actividad sospechosa y pruebas regulares de seguridad.

Además, muchas entidades financieras también han mejorado la experiencia del usuario en sus sitios web, ofreciendo interfaces más intuitivas y personalizadas, lo que facilita a los clientes el acceso a información sobre sus cuentas y transacciones.

Sin embargo, a medida que la tecnología avanza, también lo hacen las amenazas informáticas, lo que significa que los sitios web de las entidades financieras sigue siendo vulnerables a los ataques maliciosos.

El problema que surge es de la creciente actividad financiera en línea que hay en todo el mundo. Con el aumento del uso de internet y las tecnologías digitales, cada vez más personas realizan transacciones bancarias y financieras a través de la web, lo que ha llevado a un aumento en los ataques informáticos dirigidos a las entidades del sistema financiero.

Es común que los delincuentes informáticos intenten robar información de los clientes de las entidades financieras, incluyendo sus datos personales, sus claves de acceso, sus cuentas bancarias y sus tarjetas de crédito. Esto puede llevar a la perdida de dinero y a la violación de la privacidad de los clientes. Además, los ataques informáticos también pueden afectar la reputación de estas agrupaciones y dañar su imagen frente a sus clientes.

Para una posible solución nos lleva a plantearnos la siguiente interrogante ¿Cómo un análisis comparativo de las amenazas informáticas a las que están expuestas los sitios web de las entidades financieras puede contribuir a la implementación de medidas de seguridad más efectivas y reducir la vulnerabilidad de sus sistemas en línea?

El problema central de este estudio es identificar las amenazas informáticas más comunes a las que se enfrentan estas empresas en sus sitios web y compararlas para entender su impacto y frecuencia. Así se desarrollará las medidas de seguridad adecuadas para proteger los sistemas financieros en línea y evitar posibles pérdidas de dinero y datos personales. Esto podría incluir la utilización de software antivirus, firewalls, autenticación de dos factores, encriptación de datos y otras herramientas de seguridad avanzadas.

Dentro de estas soluciones se puede tener en cuenta el fortalecimiento de la colaboración entre entidades financieras: Estas agrupaciones podrían colaborar entre sí para compartir información sobre amenazas informáticas y trabajar en la creación de soluciones conjuntas. Esto podría mejorar la seguridad en línea de todas las entidades financieras y reducir la cantidad de ataques informáticos que se producen.

JUSTIFICACIÓN

La seguridad informática es un tema de vital importancia en el mundo actual, especialmente en el contexto financiero donde los ataques cibernéticos pueden generar graves consecuencias tanto para las entidades financieras como para los usuarios de sus servicios. En este sentido, el análisis comparativo de las amenazas informáticas en los sitios web de las entidades financieras se vuelve cada vez más relevante y necesario.

Conocer las amenazas informáticas más comunes a las que se enfrentan las entidades financieras permitirá identificar las debilidades en sus sistemas y proponer soluciones específicas para cada caso. Además, realizar un análisis comparativo entre diferentes entidades financieras permitirá entender las similitudes y diferencias entre ellas, así como las medidas de seguridad más efectivas que pueden implementarse.

La realización de un estudio en este ámbito podría tener un impacto positivo tanto en las entidades financieras como en los usuarios de sus servicios. Podrían mejorar la seguridad de sus sistemas en línea y reducir el riesgo de posibles ataques informáticos, lo que a su vez podría mejorar su reputación y la confianza de los usuarios en sus servicios. Por otro lado, los usuarios de los servicios financieros en línea podrían tener una mayor conciencia de los riesgos que existen y tomar medidas de seguridad más efectiva para proteger su información y su dinero.

Además, se evaluarán las debilidades actuales de los sistemas de seguridad para entender por qué ciertas amenazas son más comunes que otras. Se establecerán medidas para mitigar dichas amenazas y se determinará su efectividad.

OBJETIVOS

OBJETIVO GENERAL:

- Analizar las amenazas informáticas a las que están expuestas los sitios web de las entidades financieras.

OBJETIVOS ESPECÍFICOS:

- Identificar teóricamente las principales amenazas informáticas a las que están expuestas los sitios web de las entidades financieras.
- Comparar los diferentes tipos de amenazas informáticas a los que están expuestos los sitios web de las entidades financieras.
- Proponer recomendaciones para mejorar la seguridad de los sitios web de las entidades financieras y reducir el riesgo de amenazas informáticas.

LÍNEAS DE INVESTIGACIÓN

En cuanto la línea de investigación que está enfocado a este caso de estudio es Sistemas de información y comunicación, emprendimiento e innovación, de esta manera el estudio de las amenazas informáticas también puede llevar a la identificación de nuevas oportunidades de innovación en el campo de la seguridad informática. Y la sublíena de investigación es Redes tecnologías inteligentes de software y hardware, por lo tanto, ayuda a contribuir al desarrollo y mejora de las tecnologías inteligentes de software y hardware que se utilizan en la protección de la información y la prevención de ataques cibernéticos.

MARCO CONCEPTUAL

SISTEMA FINANCIERO

El sistema financiero actúa como un intermediario entre aquellos individuos que tienen ahorros disponibles y aquellos que necesitan financiamiento para sus actividades. Los intermediarios financieros cumplen el rol de intermediarias entre estos dos grupos, es necesario instrumentos financieros que les permitan mantener su riqueza. A través del financiamiento que se obtiene del sistema financiero, tanto emprendedores como empresas e instituciones gubernamentales pueden realizar inversiones productivas que contribuyen al desarrollo económico. Las entidades bancarias realizan diversas funciones, incluyendo la capacitación y promoción del ahorro, la canalización de los fondos hacia diferentes agentes económicos, la facilitación del intercambio de bienes y servicios, la gestión de medios de pago y el fomento del crecimiento económico de la población. (Ordóñez-Granda, Narváez-Zurita, & Erazo-Álvarez, 2020)

TEORÍA DE LA SEGURIDAD INFORMÁTICA

La seguridad de la información es una disciplina de la informática que se concentra en salvaguardar la infraestructura computacional y los datos que se encuentran almacenados o transmitiéndose por medio de ella. Para este propósito, se emplean una variedad de estándares, protocolos, técnicas, reglas, herramientas y leyes diseñados para reducir los posibles riesgos para la infraestructura y la información. Cada organización puede tener necesidades específicas en cuanto a la seguridad informática, por lo que lo que es apropiado para una empresa puede no serlo para otra. (Terán Pérez, 2018)

Algunos de estos conceptos incluyen:

Confidencialidad: Se logra a través de técnicas como la encriptación de datos y la autenticación de usuarios.

Integridad: Se logra a través de técnicas como la verificación de datos y la utilización de sistemas de control de versiones.

Disponibilidad: Se logra a través de técnicas como la redundancia de datos y la implementación de sistemas de recuperación ante desastres.

Autenticación: Se logra a través de técnicas como el uso de contraseñas, la autenticación de dos factores y el reconocimiento de voz o huella dactilar.

Autorización: Se logra a través de técnicas como la configuración de roles y permisos y la implementación de políticas de seguridad.

Seguridad en la red: Se logra a través de técnicas como la utilización de firewalls y sistemas de detección de intruso

Seguridad física: Se logra a través de técnicas como la instalación de cerraduras y sistemas de vigilancia.

Políticas de seguridad: Se lograron a través de la implementación de políticas de contraseñas, la formación de los empleados y la realización de pruebas regulares de seguridad.

Gestión de riesgos: Se logra a través de la realización de evaluaciones de riesgos y la implementación de medidas de mitigación.

AMENAZAS INFORMÁTICAS

Acciones malintencionadas en el ámbito informático abarcan el acceso a información, alteración o eliminación de datos, perjudicar el funcionamiento de la computadora o disminuir su desempeño. Los ataques informáticos se enfocan principalmente en la recolección de información, aumentan los privilegios de acceso, aprovechan vulnerabilidades de desbordamiento de memoria, acceden remotamente sin autorización y ejecutan ataques de denegación de servicio. Dentro de los ataques informáticos, se encuentran aquellos que se dirigen a la red, específicamente a los sistemas informáticos que conforman la infraestructura de comunicaciones. En este sentido, la red puede servir como medio para ejecutar un ataque o ser el objetivo del mismo. (Thomas, Fraga-Lamas, & Fernández-Caramés, 2020)

IMPORTANCIA DE LA SEGURIDAD INFORMÁTICA EN EL SECTOR FINANCIERO

Las empresas financieras necesitan implementar medias de seguridad informática adecuadas para prevenir y mitigar los riesgos asociados a posibles ataques cibernéticos y fraudes informáticos. Esto implica la implementación de políticas de seguridad, la utilización de tecnólogas de seguridad avanzadas, la formación de empleados y la realización de pruebas y auditorias regulares para garantizar la protección y privacidad de la información. (Ríos Insua & Camacho, 2020)

AMENAZAS INFORMÁTICAS MAS COMUNES EN LAS ENTIDADES FINANCIERAS

Las instituciones financieras se ven expuestas a diversos riesgos cibernéticos, entre los que se incluyen ataques informáticos, amenazas a proveedores externos, vulneraciones de datos, lavado de dinero, riesgos de identidad digital y riesgos de seguridad informática basados en la nube. (Bautista, Gaudiot, & Ching L, 2022)

SITIOS WEB DE ENTIDADES FINANCIERAS

En la actualidad, es común encontrar sistemas de autenticación multifactor en sitios web de entidades financieras y comercio electrónico. En este artículo se examinaron apartados, informes e informaciones para analizar la importancia de la autenticación multifactor para el usuario final en un entorno financiero. Con el objetivo de lograr este propósito, se analizaron los ataques a los sistemas de autenticación, así como los métodos y su clasificación, y se exploró la forma óptima de implementar los sistemas de autenticación multifactor considerando el costo, la complejidad y la interacción con el usuario final. Como resultado, se concluye que el uso de los sistemas de autenticación multifactor en los sitios web de empresas en el entorno financiero se ha convertido en una necesidad para garantizar la seguridad de la información de sus clientes y prevenir el robo de dinero. (Mendoza Arteaga et al. 2020)

VULNERABILIDAD

En términos generales, se puede definir una vulnerabilidad como un defecto en un sistema que puede ser aprovechado por un atacante para generar un riesgo para la organización o para el propio sistema. (Romero Castro et al. 2018)

Las vulnerabilidades de sitio web son una preocupación importante para las entidades financieras, ya que pueden dar lugar a la exposición de datos sensibles de los clientes y dañar la reputación de la institución financiera.

CIBERSEGURIDAD

Es importante tener en cuenta que definir la ciberseguridad ha sido un tema de debate académico sin fin, ya que ha sido analizada desde diferentes perspectivas. Actualmente, el término se utiliza de manera generalizada y existen tantas definiciones como autores, muchas de las cuales son subjetivas y de escaso valor informativo. En mi opinión, lo más acertado es elegir definiciones precisas del ámbito y jurídico, al igual que en el caso de los diccionarios, seleccionar lo útil y descartar lo erróneo o necesario. Se trata de equilibrar dos intereses contrapuestos: por un lado, realizando una definición breve y precisa, y por otro, que la misma contenga el mayor nivel de detalle posible sin comprometer su calidad. (CONAL FUERTES, 2022)

CRIPTOGRAFÍA

En realidad, la Criptografía moderna utiliza técnicas matemáticas para proteger la información digital, los sistemas de procesamiento y la computación distribuida de ataques de terceros. Esta tecnología asegura la confidencialidad de las comunicaciones, la integridad de los mensajes intercambiados y la autenticación de los participantes y mensajes. Además, es posible crear protocolos de seguros para bases de datos distribuidos, dinero digital, subastas electrónicas, juegos en línea y votaciones electrónicas. En resumen, la Criptografía moderna es un instrumento vital que garantiza la confianza en la actividad y los procesos digitales que hemos desarrollado o creado. (GONZÁLEZ VASCO & PÉREZ DEL POZO, 2022)

INGENIERÍA SOCIAL

La ingeniería social es un tema muy interesante, ya que desafía la creencia común de que la información solo puede ser robada o vulnerada a través de ataques informáticos como malware o phishing. Muchas personas creen que solo los hackers o atacantes pueden inyectar código malicioso o virus en el sistema para robar información, pero la ingeniería social demuestra que esto no es siempre el caso. Esta técnica busca obtener información valiosa persuadiendo a las personas a divulgarla, utilizando estrategias basadas en la confianza, en lugar de vulnerar la seguridad informática a través de ataques externos. La ingeniería social utiliza técnicas de persuasión para obtener información valiosa, como contraseñas o cuentas bancarias, a través de la confianza que las personas depositan en otros. Los estafadores y ladrones utilizan esta técnica para engañar a las personas, ya que es más fácil persuadir a alguien que revelar información importante que intentar vulnerar la seguridad del sistema informático. (Picado Corao & Pérez Vanegas, 2021)

AUTENTICACIÓN

Es importante mencionar los servicios de autenticación de sitios web, los cuales ofrecen un medio para garantizar que el sitio web está respaldado por una entidad auténtica y legítima, lo que generará mayor confianza en los usuarios. Para llevar a cabo la autenticación, los proveedores y servicios deben cumplir con ciertas obligaciones mínimas de seguridad y responsabilidad, de acuerdo con las iniciativas del Foro de Autoridades de Certificación y Navegadores-CA/B Forum. Sin embargo, el Reglamento establece que la utilización de estos servicios es opcional y se pueden utilizar otros métodos de autenticación no regulados en el Reglamento, o servicios de proveedores de autenticación de sitios web de terceros países para clientes en la Unión. El Reglamento permite que los sitios web utilicen servicios de autenticación, pero también deja en claro que esto es una

opción voluntaria. Los sitios web también tienen la libertad de utilizar otros métodos de autenticación que no están regulados en el Reglamento, o pueden utilizar servicios de autenticación prestados por proveedores de terceros países para clientes en la Unión Europea. (Grande Sanz, 2021)

SISTEMA DE SEGURIDAD EN LÍNEA

Se pueden encontrar algunos beneficios en el uso de la tecnología en el sector financiero, pero también hay preocupaciones acerca de la seguridad de la información personal y confidencial en un entorno global y masivo. Las instituciones financieras están invirtiendo en sistemas complejos y adoptando múltiples medidas de seguridad para prevenir el acceso no autorizado por parte de organizaciones fraudulentas o piratas informáticos a las operaciones que sus clientes realizan con ellas. (Jiménez García, 2021)

Las entidades financieras utilizan diversos sistemas de seguridad en línea para proteger los datos de sus clientes y prevenir el fraude en línea. Algunos de los sistemas de seguridad más comunes incluyen:

Encriptación de datos: este sistema de seguridad en línea convierte la información en un código que solo puede ser decodificado por la entidad financiera o el destinatario deseado. La encriptación de datos se utiliza para proteger la información de las transacciones financieras en línea, como las contraseñas y los datos de la tarjeta de crédito.

Autenticación de dos factores: también conocida como autenticación de dos pasos, este sistema de seguridad en línea requiere que los usuarios ingresen dos formas de identificación para acceder a su cuenta. Por ejemplo, una contraseña y un código enviado al teléfono móvil del usuario.

La autenticación de dos factores ayuda a prevenir el acceso no autorizado a la cuenta de un usuario, incluso si un tercero ha obtenido su contraseña.

Firewalls: un firewall es un sistema de seguridad en línea que actúa como una barrera entre la red de la entidad financiera y el resto de Internet. El firewall ayuda a prevenir el acceso no autorizado a la red y protege los datos de los usuarios.

Detección de fraude: la mayoría de las entidades financieras utilizan sistemas de detección de fraude para identificar y prevenir actividades fraudulentas. Estos sistemas analizan los patrones de transacciones y alertan al equipo de seguridad si se detecta algo sospechoso.

Actualizaciones de seguridad: las entidades financieras mantienen sus sistemas de seguridad en línea actualizados para protegerse contra nuevas amenazas y vulnerabilidades. Las actualizaciones de seguridad son esenciales para garantizar que los sistemas de seguridad estén a la altura de las amenazas en constante evolución.

MODELO DE GESTIÓN DE SEGURIDAD INFORMÁTICA

La gestión de riesgos es un procedimiento constante que consiste en reconocer, valorar y responder a los riesgos. Para poder gestionar los riesgos, las entidades necesitan entender qué tan probable es que ocurra un evento y cuál sería su impacto. Utilizando esta información, las organizaciones pueden establecer el nivel de riesgo que están dispuestas a aceptar en la prestación de sus servicios, lo cual se puede expresar como su grado de tolerancia al riesgo. (ORTEGA CANDEL, 2021)

Las entidades financieras pueden utilizar estos modelos de gestión de seguridad informática para mejorar su seguridad cibernética de diversas maneras. Por ejemplo, pueden

evaluar su nivel actual de seguridad y definir un plan para mejorar en las áreas clave identificadas por el modelo. También pueden utilizar estos modelos como marcos de referencia para desarrollar políticas y procedimientos de seguridad informática, mejorar la formación y concienciación de su personal, y establecer controles de seguridad más robustos para proteger sus sistemas y datos sensibles.

¿QUE ES ATAQUE EN LOS SITIOS WEB DE LAS ENTIDADES FINANCIERAS?

Un ataque en los sitios web de las entidades financieras es un intento malicioso de acceder, dañar o manipular la información almacenada en los sistemas informáticos de una entidad financiera a través de su sitio web. Estos ataques pueden tener diferentes objetivos, como robar información financiera de los clientes, interrumpir el servicio, o incluso realizar transferencias de fondos no autorizadas.

Los ataques DDoS representan una amenaza para las instituciones financieras, independientemente de su tamaño. Si un banco está atacado, puede enfrentarse a varios riesgos, incluidos riesgos operativos y de reputación. Además, el ataque puede ser utilizado como una distracción por parte de los hackers, mientras intentan llevar a cabo otros tipos de fraude. (Nguyen, 2018)

TRANSACCIÓN EN LÍNEA

En la actualidad, muchas empresas y comercios han adoptado la venta en línea mediante tiendas virtuales, tiendas en línea o tiendas electrónicas. Estas transacciones se llevan a cabo a través de un sitio web o una aplicación conectada a Internet, que generalmente requiere la creación

de un usuario con información personal como nombre, teléfono, número de identificación, dirección postal y correo electrónico. La forma más común de pago en estas tiendas virtuales es a través de tarjetas bancarias (débito/crédito), utilizando un Terminal Punto de Venta (TPV) o pasarela de pago virtual específica del comercio en cuestión. (Castillo Parrilla, et al 2019)

ANÁLISIS DE AMENAZAS Y VULNERABILIDADES DEL SITIIO WEB DEL:

BANCO PICHINCHA

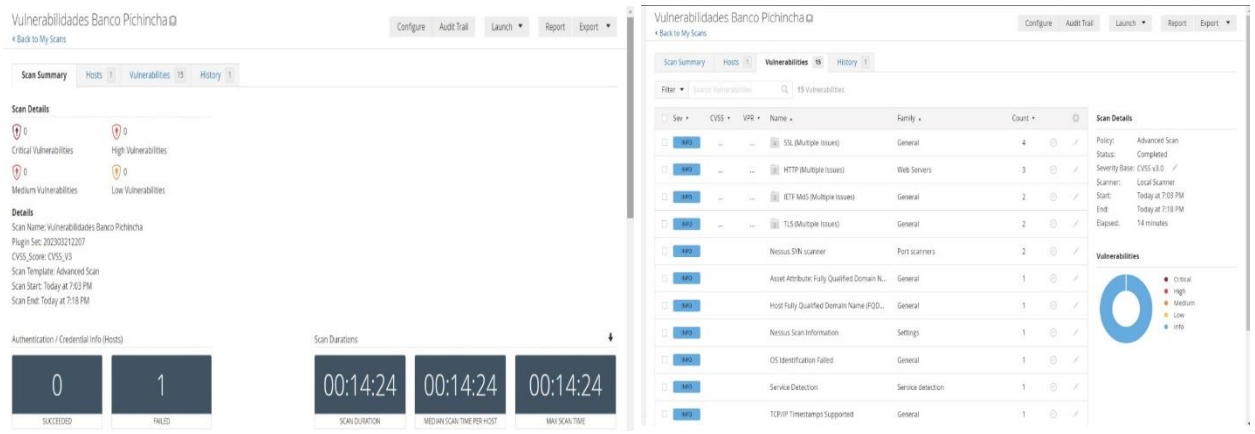

Ilustración 1 análisis de las vulnerabilidades de la herramienta Nessus

Ilustración 2 vulnerabilidades encontradas

Fuente: La Autora

- Se encontraron 15 vulnerabilidades en total.
- La mayoría de las vulnerabilidades son del tipo “información recopilada”, lo que indica que la configuración del servidor web permite a un atacante obtener información sobre el sistema.
- Otras vulnerabilidades incluyen “falsificación de petición en sitios cruzados” y “problema de inyección de SQL”

BANCO GUAYAQUIL

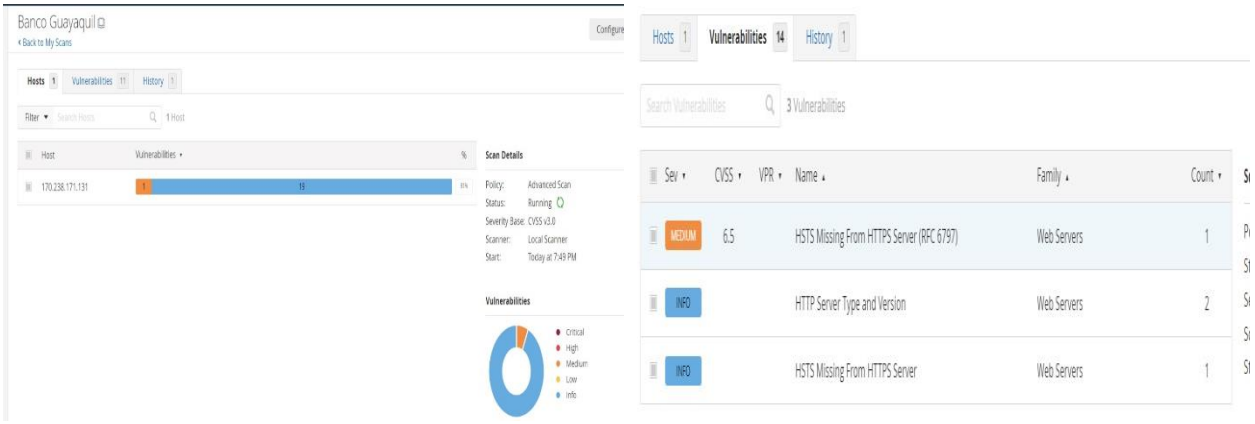

Ilustración 3 análisis de las vulnerabilidades de la herramienta Nessus

Ilustración 4 vulnerabilidades encontradas

Fuente: La Autora

- Se encontraron 14 vulnerabilidades en total y 1 vulnerabilidad MEDIA
- Las vulnerabilidades más comunes son “información recopilada” y “problemas de inyección de SQL”
- También se encontraron algunas vulnerabilidades relacionadas con “Acceso no autorizado” y “Falsificación de petición en sitios cruzados”

BANCO INTERNACIONAL

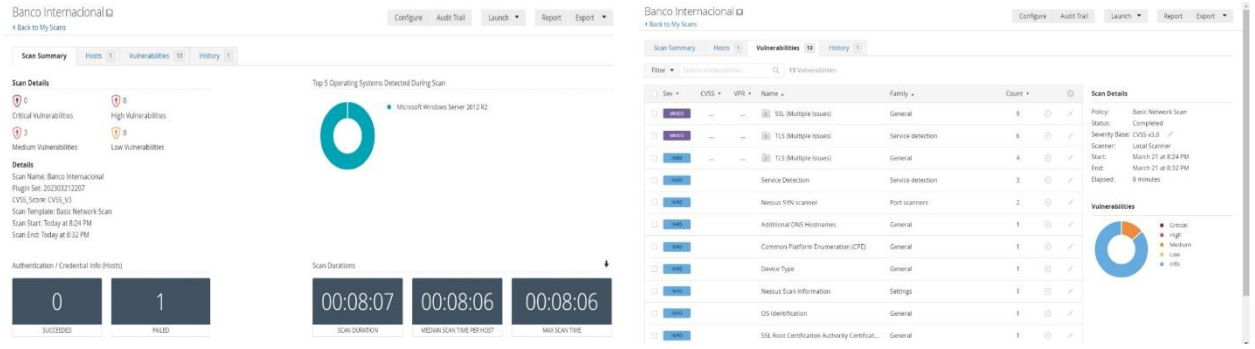

Ilustración 5 análisis de las vulnerabilidades de la herramienta Nessus

Ilustración 6 vulnerabilidades encontradas

Fuente: La Autora

- Se encontraron 13 vulnerabilidades en total y 3 vulnerabilidades MEDIA
- Las vulnerabilidades más comunes son “información recopilada” y “problemas de inyección de SQL”
- También se encontraron algunas vulnerabilidades relacionadas con “Acceso no autorizado” y “Falsificación de petición en sitios cruzados”

BANCO PACÍFICO

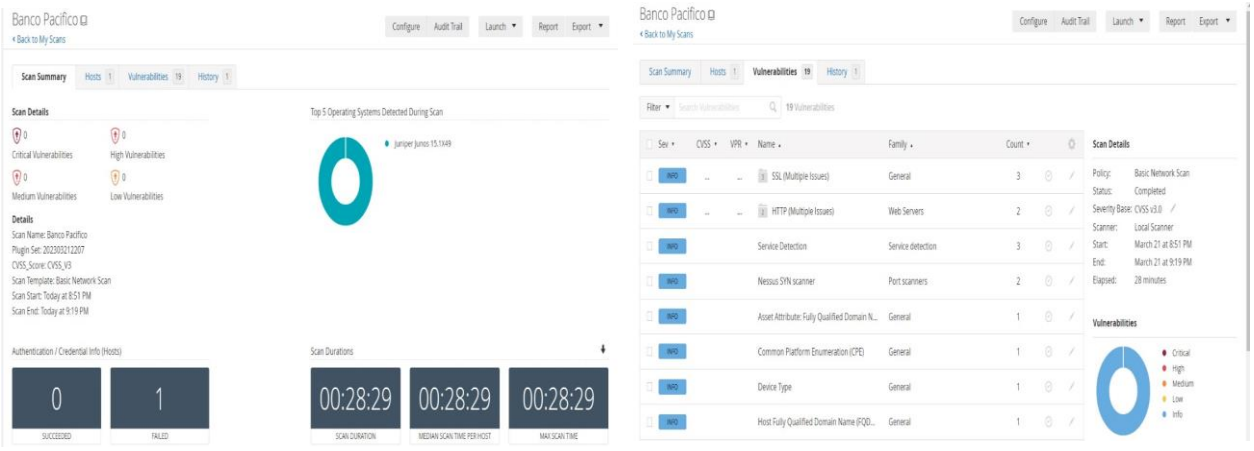

Ilustración 7 análisis de las vulnerabilidades de la herramienta Nessus

Ilustración 8 vulnerabilidades encontradas

Fuente: La Autora

- Se encontraron 19 vulnerabilidades en total.
- La mayoría de las vulnerabilidades son del tipo “información recopilada”, lo que indica que la configuración del servidor web permite a un atacante obtener información sobre el sistema.
- También se encontraron algunas vulnerabilidades relacionadas con “Acceso no autorizado” y “Falsificación de petición en sitios cruzados”

BANCO BOLIVARIANO

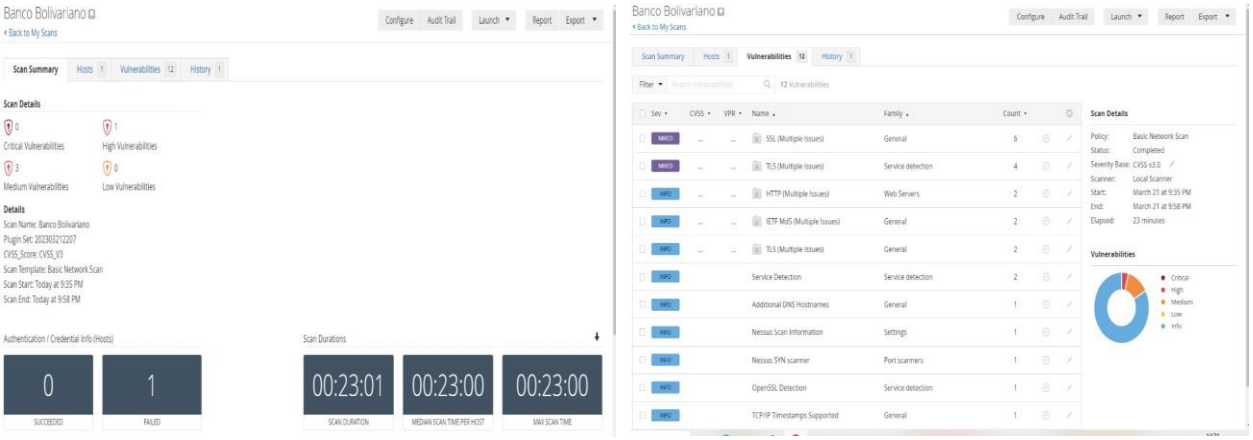

Ilustración 9 análisis de las vulnerabilidades de la herramienta Nessus

Ilustración 10 vulnerabilidades encontradas

Fuente: La Autora

- Se encontraron 12 vulnerabilidades en total, 1 vulnerabilidad media y 3 Criticas
- Las vulnerabilidades más comunes son “información recopilada” y “problemas de inyección de SQL”
- También se encontraron algunas vulnerabilidades relacionadas con “Acceso no autorizado” y “Falsificación de petición en sitios cruzados”

MARCO METODOLÓGICO

El enfoque utilizado en el siguiente estudio de caso es realizar y determinar la comparación de las amenazas informáticas a los sitios web de las entidades financieras en el desarrollo de herramientas tecnológicas.

A continuación, se utilizó el método cuantitativo, en la que ayuda a identificar las principales amenazas informáticas, se puede realizar una revisión sistemática bibliográfica y análisis documental de casos reales de ataques informáticos a sitios web de entidades financieras. Esto implicara en revisar y analizar información relevante, como artículos científicos, informes y documentos relacionado con la seguridad informática de estas entidades financieras.

Así misma investigación descriptiva se enfoca en describir las características de las situaciones de las amenazas informáticas que están expuestas a los sitios web de las entidades financieras. Esta metodología se basa en la observación y medición de variables para el objeto de estudio, para buscar relaciones entre ellas para explicar y comprender la situación que está basada a las vulnerabilidades de estos sitios web.

Para llevar a cabo una investigación descriptiva en el estudio de caso, se deberá recopilar datos y realizar un análisis detallado de los diferentes tipos de amenazas informáticas, así como de las medidas de seguridad existentes en los sitios web de las entidades financieras.

RESULTADOS

Los resultados del estudio indican durante la revisión sistemática bibliográfica y de los análisis documentales se identificó que los sitios web de las entidades financieras están expuestos a una variedad de amenazas informáticas. Entre las amenazas identificadas se encuentran ataques de phishing, malware, denial of service (DoS), cross-site scripting (XSS), entre otros. Estos ataques pueden tener consecuencias graves, como la pérdida de información confidencial, la interrupción de los servicios en línea, el robo de identidad y la pérdida financiera.

Por otro lado, los resultados obtenidos a través del análisis detallado de las entidades financieras son vulnerables a los ataques de fuerza bruta, lo que indica que estas amenazas son comunes en la mayoría de los sitios web de las entidades financieras. Sin embargo, el alcance de estas vulnerabilidades puede variar significativamente entre las distintas entidades.

Tabla 1 Cuadro comparativo de los diferentes tipos de amenazas que están expuestos los sitios web de los bancos mencionados.

Tipo de amenaza	Banco Pichincha	Banco Guayaquil	Banco internacional	Banco Pacifico	Banco Bolivariano
Ataques de fuerza bruta	Bajo	Medio	Medio	Medio	Bajo
Inyección SQL	Medio	Alto	Alto	Medio	Medio
Cross-site scripting (XSS)	Medio	Medio	Alto	Medio	Medio
Ataques de phishing	Medio	Medio	Medio	Alto	Alto
Ataques DDoS	Alto	Alto	Alto	Alto	Alto
Exposición de información confidencial	Alto	Medio	Medio	Medio	Medio
Vulnerabilidades en aplicaciones web	Alto	Alto	Alto	Alto	Alto

Elaborada por: Paulina Avegno

DISCUSIÓN DE LOS RESULTADOS

Las amenazas informáticas son una preocupación para las entidades financieras y requieren importantes medidas de seguridad efectivas para proteger la información confidencial de los clientes y evitar interrupciones en los servicios en línea.

Primero, es importante destacar que cada banco puede enfrentar amenazas diferentes y tener diferentes niveles de vulnerabilidad en función de su tamaño, infraestructura, políticas de seguridad, entre otros factores.

Por lo tanto, se puede observar que los 5 bancos presentan vulnerabilidades comunes, siendo las más frecuentes las relacionadas con la "Información recopilada" y los "Problemas de inyección de SQL". Sin embargo, es importante destacar que la cantidad de vulnerabilidades encontradas varía significativamente entre los bancos, siendo el Banco Bolivariano el que presentó la mayor vulnerabilidad y en situación crítica detectadas por Nessus.

En cuanto a las vulnerabilidades relacionadas con "Acceso no autorizado" y "Falsificación de petición en sitios cruzados", estos son comunes en todos los bancos, aunque en menor medida que las vulnerabilidades mencionadas anteriormente.

Según la herramienta Nessus dio una explicación sobre la vulnerabilidad MEDIA que tiene el banco de guayaquil es que el servidor web remoto no aplica HSTS, según lo define RFC 6797. HSTS es un encabezado de respuesta opcional que se puede configurar en el servidor para indicarle al navegador que solo se comunique a través de HTTPS. La falta de HSTS permite ataques de degradación, ataques de hombre en el medio que eliminan SSL y debilita las protecciones de secuestro de cookies.

Sin embargo, Nessus da una breve descripción de una de las vulnerabilidades media que tiene el banco internacional ya que esta situación puede hacer que sea difícil para los usuarios verificar la autenticidad e identidad del servidor web y, por lo tanto, aumentar el riesgo de ataques man-in-the-middle. Es importante solucionar esta situación para garantizar la seguridad de la comunicación y la integridad de los datos transmitidos.

Además, el servicio remoto del banco internacional acepta conexiones cifradas mediante TLS 1.1. TL5 1,1 carece de soporte para conjuntos de cifrado actuales y recomendados. Los cifrados que admiten el cifrado antes del cómputo MAC y los modos de cifrado autenticado, como GCM, no se pueden usar con TLS 1.1. A partir del 31 de marzo de 2020, los puntos finales que no estén habilitados para TLS 1.2 y superior ya no funcionarán correctamente con los principales navegadores web y los principales proveedores.

Por otro lado, se observó el nivel de vulnerabilidad ALTA que obtuvo el Banco Bolivariano mediante el uso del escaneo de la herramienta Nessus indica que el host remoto admite el uso de cifrados SSL que ofrecen cifrado de nivel medio. Nessus considera que la encriptación de nivel medio es cualquier encriptación que use longitudes de clave de al menos 64 bits y menos de 112 bits, o que use el cifrado 3DES. Tenga en cuenta que es considerablemente más fácil eludir el encriptado de nivel medio si el atacante está en la misma red física.

CONCLUSIONES

Se identifico las principales amenazas informáticas, las cuales son: phishing, malware, denial of service (DoS), cross-site scripting (XSS), entre otros. La seguridad de los sitios web de las entidades financieras es un aspecto crucial en la actualidad, ya que el acceso a información confidencial y los servicios financieros en línea se han vuelto cada vez más populares.

Se realizó la comparación de los diferentes tipos de amenazas informáticas como ataques de fuerza bruta, inyección SQL, cross-site scripting (XSS), ataques de phishing, exposición de información confidencial, vulnerabilidades en aplicaciones web, es importante destacar que estas amenazas tienen consecuencias graves y pueden afectar tanto a los clientes como a la propia entidad financiera, en términos de pérdida de información confidencial, interrupción de los servicios en línea, robo de identidad y pérdida financiera

Como conclusión se propone utilizar herramientas como los son: Nessus, Nmap, OpenVas, Metasploit, Snor, porque es importante que las entidades financieras utilicen las herramientas de seguridad adecuadas para proteger sus sistemas y aplicaciones. Las evaluaciones periódicas son de gran utilidad para que las entidades bancarias reduzcan el riesgo de las amenazas informáticas y así asegurarse que las medidas de seguridad sean efectivas y estén constantemente actualizadas.

.

RECOMENDACIONES

Estas recomendaciones ayudarán a mejorar la seguridad de los sitios web de las entidades financieras y reducir el riesgo de amenazas informáticas.

Realizar análisis regulares de malware en el sitio web y en la red de la entidad financiera, y contar con software de seguridad actualizado para detectar y bloquear ataques de malware, del mismo modo se pueden establecer planes de contingencia para prevenir y responder a ataques de Denial of Service (DoS), incluyendo la implementación de herramientas de mitigación de DoS.

Implementar medidas de seguridad robustas y actualizadas para proteger los sitios web de las entidades financieras de las amenazas informáticas. Esto podría incluir la utilización de software de seguridad como Nessus para identificar y corregir las vulnerabilidades. Por otra parte, se fomentaría la conciencia de seguridad informática entre los clientes, utilizar información y consejos útiles sobre cómo mantener seguras sus cuentas y cómo detectar los intentos de phishing.

Se sugiere que las entidades financieras implementen políticas de seguridad sólidas y capacitaciones periódicas para el personal en temas relacionados con la seguridad informática, para que estén al tanto de las últimas amenazas y cómo prevenirlas. También se recomienda que se realicen pruebas de penetración y evaluaciones de vulnerabilidades de manera regular, para detectar y corregir cualquier posible brecha de seguridad en los sistemas y aplicaciones.

REFERENCIAS

Bautista, E., Gaudiot, J.-L., & Ching L, K. (2022). *Cybersecurity and High-Performance Computing Environments: Integrated Innovations, Practices, and Applications.* CRC Press. https://www.google.com.ec/books/edition/Cybersecurity_and_High_Performance_Compu/SNJkEAAAQBAJ?hl=es-419&gbpv=1

Castillo Parrilla, J. A., Castaños Castro, P., Cámara Lapuente, S., Merchán Murillo, A., & Calvo Vérgez, J. (2019). *El mercado digital en la Unión Europea.* Editorial Reus S.A. https://www.google.com.ec/books/edition/El_mercado_digital_en_la_Uni%C3%B3n_Europea/ujajDwAAQBAJ?hl=es419&gbpv=1&dq=Transacci%C3%B3n+en+l%C3%ADnea+DE+LOS+SITIOS+WEB+DE+LAS+ENTIDADES+FINANCIERAS&pg=PA614&printsec=frontcover

CONAL FUERTES, I. (2022). *Ciberseguridad y Derecho penal.* ARANZADI / CIVITAS. https://books.google.com.ec/books?id=bumEAAAQBAJ&pg=PT54&dq=que+es+ciberseguridad+en+la+pagina+web+de+las+entidades+financieras&hl=es419&sa=X&ved=2ahUKEwjHpf2cs9z9AhWrQzABHbaYCg0Q6AF6BAgKEAI#v=onepage&q=que%20es%20ciberseguridad%20en%20la%20pagina%20web%20de%20las%20entidades%20financieras&f=false

GONZÁLEZ VASCO, M. I., & PÉREZ DEL POZO, Á. L. (2022). *Criptografía esencial: Principios básicos para el diseño de esquemas y protocolos seguros.* Ediciones de la U. https://www.google.com.ec/books/edition/Criptograf%C3%ADa_esencial/jANcEAAAQBAJ?hl=es-419&gbpv=1&dq=que+es+criptografia&printsec=frontcover

Grande Sanz, M. (2021). *El convenio arbitral electrónico y su prueba.* ARANZADI / CIVITAS. https://www.google.com.ec/books/edition/El_convenio_arbitral_electr%C3%B3nico_y_su_p/YTc0EAAAQBAJ?hl=es419&gbpv=1&dq=que+es+Autenticaci%C3%B3n+SITIOS+WEB&pg=PT437&printsec=frontcover

Jiménez García, A. (2021). *Gestión auxiliar de documentación económico-administrativa y comercial.* IC Editorial. https://www.google.com.ec/books/edition/Gesti%C3%B3n_auxiliar_de_documentaci%C3%B3n_econ/ToBJEAAAQBAJ?hl=es419&gbpv=1&dq=que+es+Sistema+de+seguridad+en+l%C3%ADnea+SITIOS+WEB+en+las+entidades+financieras&pg=PT209&printsec=frontcover

Mendoza Arteaga, A., Bolaños Burgos, F., Cedeño Sarmiento, C., & Rafael Saltos Rivas, W. (2020). La importancia de la autenticación multifactor para el usuario final en un. *Informática y Sistemas*, 1. https://webcache.googleusercontent.com/search?q=cache:PeWtZ2X9KZAJ:https://revistas.utm.edu.ec/index.php/Informaticaysistemas/article/download/2347/2560/&cd=3&hl=es-419&ct=clnk&gl=ec

Nguyen, N. (2018). *Essential Cyber Security Handbook In Spanish: Manual esencial de seguridad cibernética en español.*

https://www.google.com.ec/books/edition/Essential_Cyber_Security_Handbook_In_Spa/lUJKDwAAQBAJ?hl=es-419&gbpv=1

Ordóñez-Granda, E. M., Narváez-Zurita, C. I., & Erazo-Álvarez, J. C. (2020). El sistema financiero en Ecuador. Herramientas innovadoras y nuevos modelos. *KOINONIA.*

https://dialnet.unirioja.es/servlet/articulo?codigo=7439111

ORTEGA CANDEL, J. M. (2021). *Ciberseguridad. Manual práctico.* Ediciones Paraninfo, S.A.

Picado Corao, F., & Pérez Vanegas, M. (2021). *Administración de servicios web: Anatomía del internet.* Alpha Editorial.

https://www.google.com.ec/books/edition/Administraci%C3%B3n_de_servicios_web/s816EAAAQBAJ?hl=es419&gbpv=1&dq=que+es++INGENIER%C3%8DA+SOCIAL+en+una+entidad+financiera&pg=PA201&printsec=frontcover

Ríos Insua, D., & Camacho, M. J. (2020). *Modelos matemáticos para la gestión de la ciberseguridad.* Madrid.

https://webcache.googleusercontent.com/search?q=cache:H_gAOfou0V8J:https://rac.es/ficheros/doc/4feddd360e70e12af.pdf&cd=1&hl=es-419&ct=clnk&gl=ec

Romero Castro, M. I., Figueroa Moràn, G. L., Vera Navarrete, D. S., Álava Cruzatty, J. E., Parrales Anzúles, G. R., Álava Mero, C. J., . . . Castillo Merino, M. A. (2018). *INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES.* ÁREA DE INNOVACIÓN Y DESARROLLO, S.L.

https://books.google.com.ec/books?id=5Z9yDwAAQBAJ&printsec=frontcover&dq=que+es+vulnerabilidad+en+los+sitios+web+de+entidades+financieras&hl=es419&sa=X&ved=2ahUKEwjOgc3HkNz9AhVRSTABHRFmD8MQ6AF6BAgCEAI#v=onepage&q&f=false

Terán Pérez, D. M. (2018). *Administración y seguridad: En redes de computadoras.* Alpha Editorial.

https://www.google.com.ec/books/edition/Administraci%C3%B3n_y_seguridad/8H14EAAAQBAJ?hl=es-419&gbpv=1

Thomas, C., Fraga-Lamas, P.-L., & Fernández-Caramés, T. (2020). *Computer Security Threats.* Reino Unido: IntechOpen.

https://www.google.com.ec/books/edition/Computer_Security_Threats/CJYtEAAAQBAJ?hl=es-419&gbpv=1

ANEXOS

UNIVERSIDAD TÉCNICA DE BABAHOYO
FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA
CARRERA DE SISTEMAS DE INFORMACION

Babahoyo, 29 de marzo del 2022

CERTIFICACIÓN DE PORCENTAJE DE SIMILITUD CON OTRAS FUENTES EN EL SISTEMA DE ANTIPLAGIO

En mi calidad de Tutor del Trabajo de la Investigación de: el/la, Sr./Sra./ Srta.: **Avegno Tenorio Paulina Evelina**, cuyo tema es: **ANALISIS COMPARATIVO DE LAS AMENAZAS INFORMATICAS SUSCITADA A LOS SITIOS WEB DE LAS ENTIDADES BANCARIAS**, certifico que este trabajo investigativo fue analizado por el Sistema Antiplagio Urkund, obteniendo como porcentaje de similitud de **[4%]**, resultados que evidenciaron las fuentes principales y secundarias que se deben considerar para ser citadas y referenciadas de acuerdo a las normas de redacción adoptadas por la institución y Facultad.

Considerando que, en el Informe Final el porcentaje máximo permitido es el 10% de similitud, queda aprobado para su publicación.

Por lo que se adjunta una captura de pantalla donde se muestra el resultado del porcentaje indicado.

Ing. Enrique Ismael Delgado Cuadro, MeT.
DOCENTE DE LA FAFI.