UNIVERSIDAD TÉCNICA DE BABAHOYO FACULTAD

DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA.

PROCESO DE TITULACIÓN

DICIEMBRE 2022 – ABRIL 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 DE SEGURIDAD EN LA FACTURACIÓN ELECTRÓNICA: CASO DE ESTUDIO DE FACTURADOR CLOUD Y FACTUSOL

ESTUDIANTE:

JHONATAN MARTY DIAZ MONTOYA

TUTOR:

ING. ERICK MAGNO RICAURTE ZAMBRANO

AÑO 2023

CONTENIDO

INDICE

RESUMEN

Este caso de estudio se centra en realizar un análisis de seguridad en los sistemas de facturación electrónica de Facturador Cloud y FactuSOL, con el objetivo de identificar posibles vulnerabilidades y proponer medidas de mejora. Se utilizará un enfoque exploratorio y descriptivo mediante la recopilación, análisis y evaluación de información ya existente en fuentes documentales, encuestas y entrevistas realizadas a expertos en el área. La investigación se llevará a cabo utilizando el método cualitativo y se dividirá en tres fases: recopilación de datos, análisis de vulnerabilidades y evaluación de riesgos. El objetivo final es ofrecer una visión completa y detallada de la seguridad en la facturación electrónica para que las empresas y usuarios puedan tomar medidas preventivas y proteger sus datos de posibles ataques o violaciones de seguridad.

Es fundamental realizar un análisis exhaustivo de los sistemas de Facturador Cloud y FactuSOL, utilizando herramientas de ciberseguridad, para identificar posibles vulnerabilidades y así implementar medidas de seguridad que puedan reducir los riesgos de exposición de información confidencial. Esto incluye analizar los puertos abiertos en los servidores, verificar el código fuente en busca de vulnerabilidades, establecer políticas de seguridad claras, capacitar al personal y realizar evaluaciones periódicas de seguridad para mantener los niveles adecuados de seguridad y evitar posibles vulnerabilidades. Todo esto es crucial para proteger los datos de los clientes y mantener la confianza en los sistemas de facturación electrónica.

Palabras clave: análisis de seguridad, sistemas de facturación electrónica, vulnerabilidades, medidas de mejora, enfoque exploratorio, recopilación de datos, análisis de vulnerabilidades, evaluación de riesgos, herramientas de ciberseguridad, puertos abiertos, evaluaciones periódicas de seguridad, protección de datos.

PLANTEAMIENTO DEL PROBLEMA

La facturación electrónica se ha convertido en una herramienta indispensable para las empresas porque ahorra tiempo y recursos en el proceso de facturación. Sin embargo, su uso implica algunos riesgos de seguridad de la información que pueden poner en peligro la confidencialidad de los clientes.

En Ecuador, la facturación electrónica se ha convertido en una herramienta fundamental para la gestión de las finanzas de las empresas. La Agencia de Regulación y Control de Telecomunicaciones (ARCOTEL) es el organismo encargado de regular el uso de la facturación electrónica en el país y ha establecido una serie de normas y requisitos que las empresas deben cumplir para implementar este sistema.

Uno de los principales beneficios de la facturación electrónica es la rapidez y eficiencia que ofrece en el proceso de facturación, así como la reducción de costos y la disminución del impacto ambiental. Sin embargo, junto con estos beneficios, también surgen preocupaciones en torno a la seguridad de los datos de los clientes almacenados en estos sistemas.

La seguridad de los datos de los clientes es fundamental en cualquier sistema de facturación electrónica. La protección de la información personal y financiera de los clientes es crucial para prevenir el robo de identidad, el fraude y otros delitos cibernéticos. Además, como menciona ALONSO (2023) en Ecuador existe la Ley Orgánica de Protección de Datos Personales, que

establece la obligación de las empresas de proteger y garantizar la privacidad de los datos de sus clientes.

Por lo tanto, la seguridad de la facturación electrónica es un tema de gran importancia para las empresas que implementan este sistema en Ecuador, y es necesario llevar a cabo un análisis riguroso de los programas de facturación electrónica para garantizar la protección de los datos de los clientes y el cumplimiento de las normas y requisitos establecidos por las autoridades reguladoras.

En la situación actual, las empresas han tenido que adaptarse a una nueva forma de trabajo remoto debido a la pandemia del COVID-19. Esto ha incrementado el uso de facturas electrónicas para facilitar las compras en línea. Sin embargo, el mayor uso de la facturación electrónica también ha aumentado los riesgos de seguridad, especialmente cuando se procesan los datos de los clientes.

En este sentido, como modelo para el análisis de seguridad se utilizarán dos softwares de facturación electrónica, Facturador Cloud y FactuSOL, analizando los datos de los clientes que utilizan estos programas. El tema se centra en determinar si existen diferencias significativas en la seguridad de las facturas electrónicas entre ambos programas, especialmente cuando se trata de utilizar los datos de los clientes en el contexto del trabajo remoto.

Es importante tener en cuenta que la seguridad de los datos de los clientes es una preocupación crucial en la actualidad, y por lo tanto se evaluarán exhaustivamente los protocolos de seguridad utilizados por los softwares seleccionados. Además, también se considerará la capacidad de los usuarios para manejar la información de forma segura en un contexto de trabajo remoto. Se examinará cómo los usuarios manejan los datos confidenciales, si utiliza contraseñas

seguras y evitan el uso de redes inseguras, entre otros aspectos importantes para garantizar la protección de los datos de los clientes. En resumen, se llevará a cabo un análisis detallado y completo de la seguridad de los datos en el contexto de la facturación electrónica y el trabajo remoto.

Hubo en los últimos años aumento de ataques cibernéticos contra las empresas que utilizan la facturación electrónica, especialmente aquellas que intentan obtener de manera fraudulenta información confidencial sobre los clientes. Por tanto, el presente estudio tiene como objetivo identificar posibles vulnerabilidades en la seguridad de los datos de Facturador Cloud y facturación electrónica FactuSOL en relación con el trabajo remoto, a partir del análisis de los datos de los clientes, para proponer medidas de seguridad, mejora y protección de su información confidencial**.**

¿Cuáles son los niveles de seguridad presentes en los sistemas de facturación electrónica y cómo se comparan los programas Facturador Cloud y FactuSOL en términos de protección contra estas vulnerabilidades?

JUSTIFICACIÓN

La facturación electrónica se ha convertido en una herramienta fundamental para las empresas en todo el mundo, ya que permite una mayor eficiencia y seguridad en las transacciones comerciales. Sin embargo, con el aumento de la facturación electrónica también aumentan los riesgos y amenazas a la seguridad informática. En Ecuador, donde la facturación electrónica es obligatoria desde el 2014, se ha visto un crecimiento en el uso de estas herramientas y es importante garantizar que estas herramientas estén protegidas contra los riesgos y amenazas informáticas.

La seguridad en la facturación electrónica es esencial para garantizar la confidencialidad, integridad y disponibilidad de la información, y para prevenir el robo de identidad y la suplantación de identidad. Una brecha de seguridad en un sistema de facturación electrónica puede tener consecuencias graves para las empresas, como pérdida de confianza en el negocio, sanciones legales y pérdida de ingresos. Por lo tanto, es importante analizar la seguridad de las herramientas de facturación electrónica y proporcionar recomendaciones para mejorar la seguridad en las mismas.

En este sentido, el estudio de caso sobre la facturación electrónica y la seguridad informática es crucial para entender los riesgos y amenazas a la seguridad en las herramientas Facturador Cloud y FactuSOL, y cómo prevenirlos. El objetivo principal del estudio es analizar la seguridad de ambas herramientas, identificar los riesgos y amenazas más comunes y proporcionar recomendaciones para mejorar la seguridad en las mismas. Con esto se busca garantizar la confidencialidad, integridad y disponibilidad de la información, y proteger a las

empresas contra posibles consecuencias legales, pérdida de confianza en el negocio y pérdida de ingresos.

Además, el estudio tendrá un impacto positivo en la economía del país ya que contribuirá a mejorar la seguridad en las transacciones comerciales y aumentará la confianza en el uso de la facturación electrónica. Es por ello que el estudio es una herramienta valiosa para entender los riesgos y amenazas a la seguridad en las herramientas de facturación electrónica, y proporcionar recomendaciones para mejorar la seguridad en las mismas.

OBJETIVOS

Objetivo general

Realizar un análisis de seguridad en la facturación electrónica de Facturador Cloud y FactuSOL, con el objetivo de identificar posibles vulnerabilidades y proponer medidas de mejora.

Objetivos específicos

- Analizar la seguridad de la facturación electrónica en Facturador Cloud y FactuSOL, mediante el uso de herramientas de ciberseguridad, con el fin de identificar posibles vulnerabilidades.
- Evaluar los resultados de la investigación para determinar las implicaciones de las vulnerabilidades en la seguridad de la facturación electrónica de Facturador Cloud y FactuSOL.
- Diseñar una propuesta de investigación futura para seguir mejorando la seguridad de la facturación electrónica y adaptarse a las necesidades cambiantes de las empresas y los clientes en el futuro.

LÍNEAS DE INVESTIGACIÒN

La línea de investigación de Sistemas de información y comunicación, emprendimiento e innovación es fundamental para el estudio de caso del análisis de seguridad en la facturación electrónica de Facturador Cloud y FactuSOL. Esta línea de investigación se enfoca en los procesos de los sistemas de información y administración de una empresa, y cómo se pueden optimizar y mejorar para maximizar el rendimiento y minimizar los riesgos.

La sublínea de investigación de Redes y tecnologías inteligentes de software y hardware también es relevante para el estudio de caso, ya que la facturación electrónica requiere el uso de tecnologías de software y hardware para garantizar la seguridad y la eficiencia del proceso. En este sentido, se examinarán las tecnologías utilizadas por Facturador Cloud y FactuSOL para la facturación electrónica, y cómo estas tecnologías pueden ser mejoradas y actualizadas para mejorar la seguridad y la eficiencia del proceso.

En conclusión, la línea de investigación de Sistemas de información y comunicación, emprendimiento e innovación y la sublínea de investigación de Redes y tecnologías inteligentes de software y hardware son esenciales para el estudio de caso del análisis de seguridad en la facturación electrónica de Facturador Cloud y FactuSOL, ya que se enfocan en los procesos de los sistemas de información y administración de una empresa, y cómo se pueden optimizar y mejorar a través del uso de tecnologías de software y hardware.

MARCO CONCEPTUAL

Para llevar a cabo la ejecución del proyecto, se requiere de la comprensión de ciertos términos y conceptos que se relacionan con la facturación electrónica. En consecuencia, a continuación, se proporcionará una descripción detallada de aquellos que son relevantes para el desarrollo del mismo.

Facturación electrónica

La facturación electrónica es una herramienta tributaria mediante la cual se emiten y reciben facturas electrónicas en lugar de facturas en papel. En este proceso, se utilizan tecnologías de la información y la comunicación para crear, enviar, recibir y procesar las facturas, lo que permite a las empresas y organizaciones optimizar su gestión administrativa y mejorar su eficiencia. La facturación electrónica es una alternativa cada vez más popular a la facturación en papel debido a su eficiencia, seguridad y respeto al medio ambiente.

Arias Pérez & Cáceres Ortiz (2021) mencionan lo siguiente:

> La implementación de la facturación electrónica en empresas ha sido vista como una iniciativa para mejorar la conformidad fiscal en todo el mundo. Esto ha llevado a varios países a adoptar esta nueva forma de facturación, lo que ha permitido una mayor recaudación de impuestos para cada uno de ellos. (pág. 3)

La facturación electrónica es una herramienta que ha sido vista como un beneficio tanto para las entidades tributarias como para las personas que facturan. Su implementación en diferentes países ha demostrado ser efectiva para lograr un mayor cumplimiento tributario, lo que se traduce en un aumento en la recaudación de impuestos. Al utilizar la facturación electrónica, las empresas pueden tener un mejor control sobre sus facturas y reducir los errores, lo que a su vez mejora la calidad del servicio que ofrecen a sus clientes. La facturación electrónica no solo es una herramienta eficaz para las entidades tributarias, sino también para las empresas que buscan optimizar sus procesos y mejorar su relación con los clientes.

La facturación electrónica se ha extendido por toda latino América en la que cada país se ha ido adaptando a esta nueva modalidad junto con su normativa de seguridad y de acuerdo con los objetivos planteados por cada entidad tributaria.

> En abril de 2009, Ecuador inició el proceso de Facturación Electrónica a través de la RESOLUCIÓN Nº NACDGERCGC09-00288, que estableció las normas para la emisión de Comprobantes de Venta, Documentos Complementarios y Comprobantes de Retención. La Secretaría Nacional de la Administración Pública publicó una lista de empresas autorizadas para emitir comprobantes electrónicos ese mismo año. Después, el Servicio de Rentas Internas (SRI) implementó medidas normativas y tecnológicas para brindar servicios en línea de certificación, validación, autorización y almacenamiento. En 2012, se emitió la RESOLUCIÓN Nº NACDGERCGC12-00105, que estableció las normas para el nuevo esquema de emisión de comprobantes de venta, retención y documentos complementarios mediante mensajes de datos (Comprobantes electrónicos), aunque su uso seguía siendo voluntario. (DIAZ CORDOVA, COBA MOLINA, & BOMBÓN MAYORGA, 2020)

Con la implementación de la facturación electrónica en Ecuador en el 2009 el SRI (servicios de rentas internas) comienza en el 2012 un proceso de implementación de normativas tecnológicas para tener un desarrollo integral y un servicio tecnológico seguro y de calidad para poder ser implementadas en todas las empresas.

Seguridad informática

La seguridad informática es el conjunto de medidas y técnicas que se implementan para proteger los sistemas informáticos y la información que contienen de amenazas, riesgos y vulnerabilidades que pueden comprometer su confidencialidad, integridad y disponibilidad. Estas medidas y técnicas incluyen políticas de seguridad, controles de acceso, cifrado de datos, monitoreo de eventos, detección de intrusiones, entre otros aspectos relacionados con la gestión y protección de la información en el ámbito informático. La seguridad informática se ha vuelto cada vez más importante debido al creciente uso de sistemas informáticos y a la cantidad de información sensible que se maneja en ellos.

Ingeniería inversa

En informática, la ingeniería inversa es el proceso de desmontar un software o sistema para comprender su funcionamiento interno y diseño, con el fin de obtener información valiosa o realizar cambios en el mismo.” De manera general, la ingeniería inversa de un producto consiste en examinar un objeto con el objetivo de comprenderlo lo suficiente como para poder recrearlo y mejorarlo.” (Cedeño, 2022)

Análisis de vulnerabilidades

> Se considera una vulnerabilidad a cualquier fallo o deficiencia en el código de un software, aplicación o dispositivo. Si esta vulnerabilidad es explotada, puede afectar la confidencialidad, disponibilidad e integridad de los datos almacenados, permitiendo el acceso no autorizado, elevación de privilegios o denegación de servicio, lo que representa un riesgo para la organización. (Zapata, 2023)

Este proceso implica la identificación de vulnerabilidades, es decir, las debilidades que pueden ser explotadas por un atacante, y la evaluación de su impacto potencial en el sistema, red o aplicación en cuestión. El análisis de vulnerabilidades se realiza mediante el uso de herramientas de seguridad especializadas, como scanners de vulnerabilidades, y técnicas de hacking ético, para identificar los puntos débiles.

Normativa y regulaciones para la protección de los datos de los clientes:

La creación de la normativa es importante para la implementación de la facturación electrónica en el país, aunque es importante tener en cuenta que no aborda directamente la facturación electrónica en sí misma, sino más bien los aspectos tecnológicos y legales relacionados con ella, como los mensajes de datos, las firmas digitales y la contratación electrónica. Es positivo que se haya incluido la protección de los usuarios de estos sistemas en la normativa, ya que es fundamental garantizar la seguridad y privacidad de la información en el entorno digital. Sin embargo, es importante seguir trabajando en el desarrollo de normativas más específicas para la facturación electrónica, que permitan su correcta implementación y uso en beneficio de las empresas y la sociedad en general.

> La creación de esta regulación marca el inicio de la facturación electrónica, pero no de manera explícita, ya que solo establece normas para los mensajes de datos, las firmas digitales, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos a través de redes de información y la protección de los usuarios que utilizan estos sistemas. (Malavé, 2019)

En Ecuador, la facturación electrónica está regulada por la Resolución No. NAC-DGERCGC20-00000029 emitida por el Servicio de Rentas Internas (SRI). Esta resolución establece los requisitos técnicos y operativos que deben cumplir los contribuyentes que decidan utilizar la facturación electrónica, así como los procedimientos que deben seguirse para su implementación y uso.

> Según lo establecido en el artículo 73 del Código Tributario, la administración tributaria debe actuar basándose en los principios de simplificación, celeridad y eficacia. (SRI, 2021)

Además, la protección de datos personales está regulada por la Ley Orgánica de Protección de Datos Personales (LOPD) y su Reglamento, emitidos por la Agencia de Regulación y Control de Datos Personales (ARCO). Estas normativas establecen los principios y procedimientos que deben seguirse para la protección de los datos personales de los ciudadanos ecuatorianos, incluyendo los datos de los clientes que se manejan en la facturación electrónica.

Es importante que las empresas que utilizan la facturación electrónica en Ecuador cumplan con estas regulaciones y normativas para garantizar la protección de los datos personales de sus clientes y evitar sanciones por parte de las autoridades competentes.

Herramientas de ciberseguridad

Una herramienta de ciberseguridad es un software o dispositivo diseñado para proteger los sistemas informáticos y los datos contra amenazas de seguridad, como virus informáticos, malware, phishing, ataques de hackers y otras formas de ciberataques. Estas herramientas de seguridad incluyen antivirus, firewalls, sistemas de detección de intrusiones, sistemas de prevención de intrusiones, cifrado de datos, autenticación y gestión de contraseñas, entre otros. Las herramientas de ciberseguridad son básicas para garantizar la protección de la información confidencial y la privacidad de los usuarios en el entorno digital. “La tarea principal que desempeña es la supervisión del tráfico web, la identificación de usuarios y la prevención de accesos no autorizados.” (Bello, 2022)

Tipo de vulnerabilidad	Descripción	Posibles consecuencias
Ataques de fuerza bruta	Intentos repetitivos y automáticos para adivinar contraseñas o códigos de acceso	Acceso no autorizado a cuentas y datos sensibles
Inyección SQL	Inserción de código malicioso en un campo de entrada de datos para obtener acceso a la base de datos o alterar información	Modificación o eliminación de datos importantes, robo de información confidencial
Cross-site scripting (XSS)	Inserción de código malicioso en un sitio web para robar información de los usuarios o redirigir a sitios fraudulentos	Robo de datos personales y financieros de los usuarios

Tipo de vulnerabilidad	Descripción	Posibles consecuencias
Phishing	Envío de correos electrónicos o mensajes engañosos que parecen ser legítimos para obtener información confidencial	Robo de credenciales de inicio de sesión y datos bancarios
Ataques de denegación de servicio (DDoS)	Envío de múltiples solicitudes a un servidor para saturar y hacer que deje de funcionar	Interrupción del servicio, pérdida de ingresos y reputación

fuentes: Del autor

Virtual Box

VirtualBox es un software de virtualización de código abierto que permite crear y ejecutar máquinas virtuales en un sistema host. En otras palabras, VirtualBox permite crear un ambiente virtual dentro de una computadora donde se pueden instalar sistemas operativos adicionales, programas y aplicaciones que funcionan como si estuvieran instalados directamente en el sistema host.

El término "hipervisor de tipo 2" se refiere a un software que se utiliza para crear máquinas virtuales y virtualizar sistemas operativos dentro de un ordenador existente. A diferencia de los hipervisores de tipo 1, que funcionan directamente sobre el hardware o la máquina host, los hipervisores de tipo 2 necesitan un sistema operativo para operar. (Bercial, 2020)

VirusTotal

VirusTotal es un servicio en línea que permite analizar archivos sospechosos o desconocidos en busca de posibles amenazas de seguridad. Es una herramienta muy útil para los profesionales de la seguridad informática, ya que permite detectar rápidamente archivos maliciosos, virus y otros tipos de amenazas de seguridad en los archivos que se analizan.

> Virus Total es un servicio altamente confiable y valioso que utiliza una gran variedad de motores antivirus para analizar y detectar posibles amenazas de malware. En caso de dudas sobre una página web, tienda o archivo, Virus Total puede ser de gran ayuda al proporcionar información sobre si es seguro o no antes de proceder a analizar el archivo o visitar la página web en cuestión. Esto puede evitar la necesidad de analizar el archivo con nuestro antivirus local o visitar una página web potencialmente peligrosa. (Espinosa, 2019)

Kali Linux

Kali Linux es una distribución de Linux basada en Debian que se utiliza principalmente para pruebas de penetración y evaluación de seguridad. Es una herramienta muy útil para profesionales de la seguridad informática, así como para usuarios avanzados que desean realizar pruebas de seguridad en su propio sistema.

Kali Linux es un sistema muy completo que dispone de una amplia variedad de herramientas, tanto en modo gráfico como en modo de comandos, lo que lo convierte en una opción ideal tanto para los defensores que buscan un sistema más seguro como para los atacantes que buscan obtener información valiosa como cuentas, contraseñas y otros datos personales. (Altube, 2021)

Nmap

Nmap es una herramienta de escaneo de red de código abierto y gratuita que se utiliza para descubrir dispositivos en una red y para identificar los puertos y servicios que estos dispositivos están utilizando. También se puede utilizar para realizar pruebas de seguridad en una red.

> Se trata de una herramienta de descubrimiento de redes y auditoría de seguridad de código abierto y gratuita que es muy útil para los administradores de sistemas y redes. Además, se puede utilizar para llevar a cabo tareas como el inventario de la red, la gestión de actualizaciones de servicios y la supervisión del tiempo de actividad de los hosts y servicios. (Lyon, 2019)

Nmap funciona enviando paquetes de red a través de la red que se está escaneando y analizando las respuestas recibidas. La herramienta utiliza técnicas de escaneo avanzadas para identificar los dispositivos que están conectados a la red, los servicios que están ejecutando y los puertos que están abiertos en esos dispositivos.

Ghidra

Ghidra es una herramienta de ingeniería inversa y análisis de malware desarrollada por la Agencia de Seguridad Nacional (NSA) de los Estados Unidos y liberada al público en 2019 bajo la Licencia Apache 2.0. Es una herramienta de software libre y gratuita que se utiliza para descompilar y analizar binarios de programas para entender su funcionamiento interno.

> Se pueden encontrar en Ghidra una gran cantidad de características que incluyen, entre otras, la capacidad de desmontar y ensamblar, la descompilación, la creación de gráficos y

scripting. Además, es compatible con muchos conjuntos de instrucciones de procesador y formatos ejecutables, y se puede utilizar tanto en modo interactivo como automatizado. Los usuarios pueden desarrollar sus propias extensiones y scripts utilizando Java o Python. (Kurtz, 2019)

Facturador Cloud

Facturador Cloud es un software de facturación electrónica en línea desarrollado por la empresa Facturador Cloud S.A., que permite a las empresas generar, enviar y almacenar facturas electrónicas en cumplimiento con las normativas fiscales y tributarias de cada país. Este software cuenta con diversas funcionalidades como la creación de facturas personalizadas, el registro de clientes y proveedores, la integración con sistemas de contabilidad y la generación de reportes de facturación. Además, se caracteriza por ser accesible desde cualquier dispositivo con conexión a internet y contar con medidas de seguridad para la protección de los datos de los clientes. “Se trata de un software diseñado para pequeñas y medianas empresas, así como para autónomos, que buscan centralizar su facturación y contabilidad en un único lugar accesible a través de Internet. Esta herramienta resulta muy útil para llevar un control exhaustivo de la gestión empresarial y facilitar la toma de decisiones.” (FacturasCloud, 2023)

FactuSOL

FactuSOL es un software de facturación y gestión comercial diseñado para pequeñas y medianas empresas. Permite la gestión de facturas, presupuestos, albaranes, pedidos, control de stock, clientes, proveedores, entre otras funcionalidades relacionadas con la gestión empresarial.

FactuSOL se ha convertido en una herramienta popular en el mercado español debido a su facilidad de uso y capacidad de adaptación a las necesidades de cada empresa.

> FactuSOL es un programa informático que ofrece soluciones completas para facturación, gestión de clientes y proveedores, control de inventario y conciliación bancaria. Se le reconoce como uno de los mejores programas para facturar, por lo que es muy útil para pymes, autónomos y empresas, y puede ser empleado como software de gestión en diversos tipos de comercios y empresas de servicios. (cronomia, 2023)

Tabla comparativa

Característica	Facturador Cloud	FactuSOL
Tipo de software	Basado en la nube	Instalado en local
Accesibilidad	Accesible desde cualquier lugar con conexión a Internet	Accesible sólo desde el equipo en el que está instalado
Costo	Pago por suscripción mensual o anual	Pago único de licencia
Actualizaciones	Actualizaciones automáticas incluidas en la suscripción	Actualizaciones pagadas y programadas
Personalización	Limitada a las opciones proporcionadas por el proveedor de software	Altamente personalizable con opciones de programación y configuración
Seguridad	Depende del proveedor de software y su infraestructura de seguridad en la nube	Depende de la seguridad del sistema operativo y la red en la que se encuentra instalado
Integración con otras herramientas	Fácil integración con otras herramientas en la nube	Integración limitada a herramientas locales o de terceros

Característica	Facturador Cloud	FactuSOL
Escalabilidad	Escalable y adaptable a las necesidades del negocio	Limitado por las capacidades del equipo en el que está instalado
Soporte técnico	Soporte técnico proporcionado por el proveedor de software	Soporte técnico proporcionado por el proveedor de software y por terceros especializados en FactuSOL

fuentes: Del autor

Análisis de riesgos y amenazas si la información es vulnerada

Si los datos de un facturador electrónico son robados, puede ocurrir lo siguiente:

- Exposición de información confidencial: los datos personales, financieros y fiscales de los clientes pueden ser expuestos a terceros no autorizados, lo que podría llevar a un robo de identidad, fraude financiero u otros delitos.
- Interrupción del servicio: si los atacantes obtienen acceso al sistema de facturación electrónica, pueden causar interrupciones en el servicio o incluso bloquear completamente el acceso a la plataforma.
- Pérdida de la confianza del cliente: un incidente de seguridad puede afectar negativamente la confianza de los clientes en la empresa, lo que puede llevar a una pérdida de ingresos y daño a la reputación de la empresa.
- Incumplimiento legal: si se demuestra que la empresa no cumplió con las leyes y regulaciones de protección de datos, puede enfrentar multas y sanciones legales.

El empleo correcto de contraseñas y autenticaciones puede ser de gran ayuda. Según un estudio de Ponemon, alrededor del 59% de las personas encuestadas afirmaron que

> desconocen las prácticas de contraseñas utilizadas por sus empleados. Solo el 43% de las empresas tienen una política de contraseñas y, de estas, el 68% admite no ponerlas en práctica. (Lesonsky, 2019)

En resumen, la pérdida de datos de un facturador electrónico puede tener graves consecuencias para los clientes y la empresa, incluyendo exposición de información confidencial, interrupción del servicio, pérdida de la confianza del cliente e incumplimiento legal.

MARCO METODOLÓGICO

Metodología de la investigación

Esta metodología consiste en la recopilación, análisis y evaluación de información ya existente en fuentes documentales tales como libros, artículos, informes y otros documentos relevantes para el proyecto. En este caso, se recopiló información sobre casos de vulnerabilidades en facturadores electrónicos y medidas preventivas para evitarlas. La investigación documental permitirá obtener información valiosa para el proyecto y realizar un análisis exhaustivo de las vulnerabilidades en los facturadores electrónicos, así como sugerir medidas de seguridad para mitigar los riesgos.

Método cualitativo

Se utilizará el método cualitativo con el fin de analizar las vulnerabilidades de un facturador electrónico. La recolección de datos se realizará a partir de diferentes fuentes como artículos, tesis y trabajos presentados en fuentes oficiales relacionadas con la seguridad de la facturación electrónica. La información obtenida será interpretada y comparada para lograr una comprensión clara y precisa de los hallazgos del estudio. Se llevará a cabo un análisis de texto para identificar las conceptualizaciones y factores relevantes relacionados con las vulnerabilidades de los facturadores electrónicos.

Tipo de investigación

Investigación exploratorio descriptiva

El tipo de investigación utilizado para el presente proyecto es de carácter exploratorio y descriptivo, ya que se pretende analizar y comprender las posibles vulnerabilidades en los sistemas de facturación electrónica, específicamente en los Facturador Cloud y FactuSOL. A través de la revisión de fuentes documentales, encuestas y entrevistas realizadas a expertos en el área, se busca identificar las posibles amenazas y vulnerabilidades, así como las mejores prácticas de seguridad y herramientas que se pueden utilizar para prevenirlas o mitigar sus efectos. De esta manera, se pretende ofrecer una visión completa y detallada de la seguridad en la facturación electrónica, para que las empresas y usuarios puedan tomar medidas preventivas y proteger sus datos de posibles ataques o violaciones de seguridad.

Técnicas e instrumento

Se utilizó la entrevista como técnica de recolección de datos cualitativas a un grupo de personas que trabajan con la facturación electrónica para tener una comprensión de cómo se lleva la seguridad en la facturación en las empresas.

Preguntas

Entrevista dirigida a un grupo de personas que trabajan con la facturación electrónica

- ¿Qué medidas de seguridad adicionales toman para evitar el acceso no autorizado a los datos de los clientes?
- ¿Cómo manejan los posibles incidentes de seguridad relacionados con la facturación electrónica, como el robo de datos o el phishing (Hackeo)?

- ¿Cómo manejan los datos de los clientes que ya no son necesarios para la facturación?
- ¿Cómo está estructurado el equipo encargado de la facturación electrónica en su empresa? y ¿Hay una sola persona encargada o es un grupo de personas?
- ¿Cómo se asegura la privacidad y confidencialidad de los datos de los clientes durante la transmisión de información a través de Internet?

Fases para realizar análisis de seguridad

- Recopilación de datos: Se recopilaron los datos necesarios para el análisis de seguridad, entre ellos la configuración de los sistemas, el software utilizado, los tipos de datos que se procesan, entre otros.

- Análisis de vulnerabilidades: En esta fase se realizará el análisis de vulnerabilidades mediante la utilización de Nessus, una herramienta de ciberseguridad. Se identificarán las posibles vulnerabilidades en el facturador cloud y se evaluarán las consecuencias potenciales que podrían derivarse de ellas.

- Evaluación de riesgos: Se evaluarán los riesgos identificados durante el análisis de vulnerabilidades y se determinará su impacto en la seguridad de la facturación electrónica.

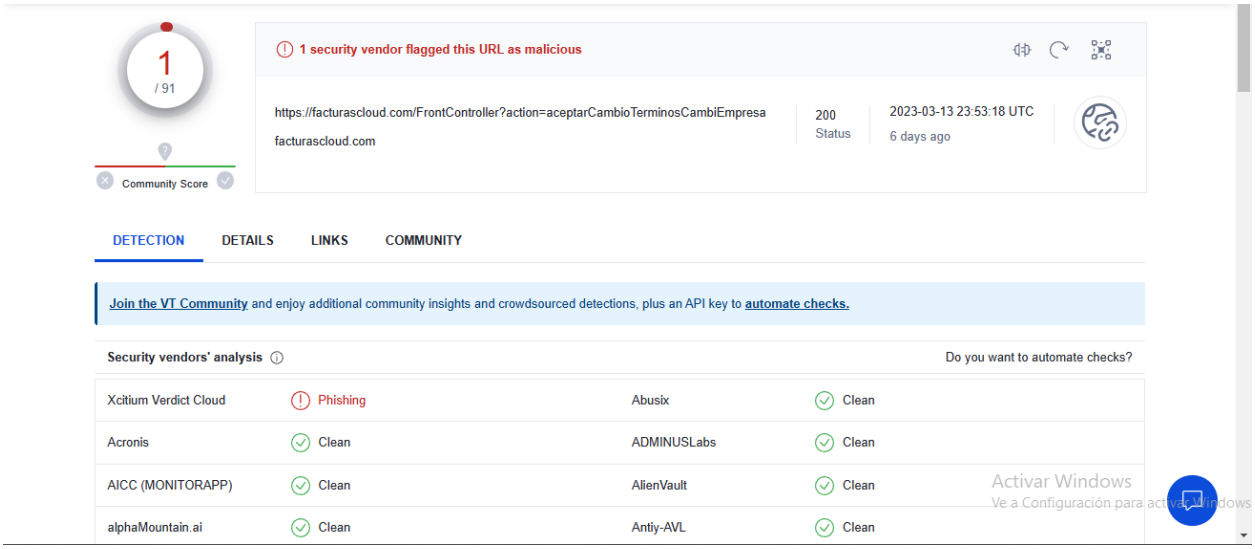
RESULTADOS

A través de la evaluación realizada, se identificaron posibles vulnerabilidades en la protección de la información confidencial de los clientes. Los resultados obtenidos permiten proponer medidas de mejora para garantizar la seguridad y protección de la información en la facturación electrónica.

Recopilación de datos

Facturador Cloud

Para recopilar los datos del facturador lo primero es averiguar la ip de la página y para eso se utiliza Virustotal que analiza la dirección URL revelando la ip.



Búsqueda de la ip de facturas cloud

fuentes: Del autor

History ⓘ

First Submission	2023-03-13 23:53:18 UTC
Last Submission	2023-03-13 23:53:18 UTC
Last Analysis	2023-03-13 23:53:18 UTC

HTTP Response ⓘ

Final URL

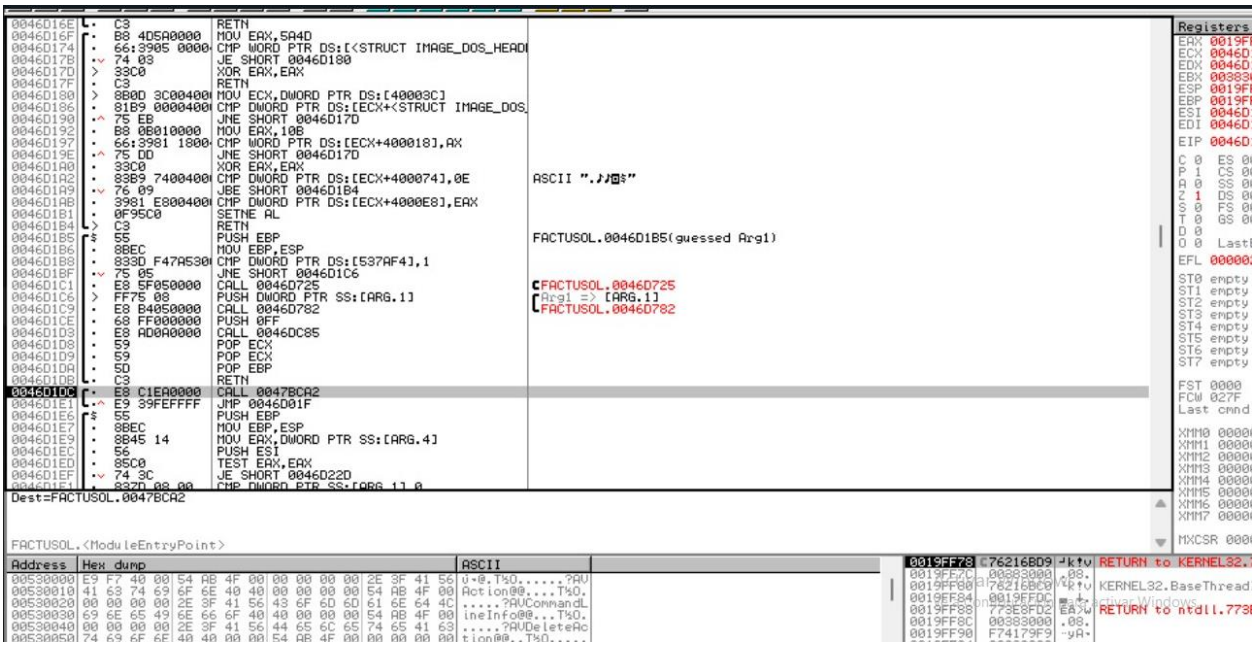
https://facturascloud.com/FrontController?action=aceptarCambioTerminosCambiEmpresa

Serving IP Address

35.187.49.57

fuentes: Del autor

FactuSOL



fuentes: Del autor

Análisis de vulnerabilidades

Facturador Cloud

Ingresamos la ip de facturador cloud en Nmap con la siguiente sintaxis nmap -sV

```
┌──(usuario㉿usuario)-[~]
└─$ nmap -sV 35.187.49.57
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-22 20:18 -05
Nmap scan report for 57.49.187.35.bc.googleusercontent.com (35.187.49.57)
Host is up (0.18s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE  VERSION
80/tcp    open  http     Apache httpd 2.4.54 ((Debian))
85/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
443/tcp   open  ssl/http Apache httpd 2.4.54 ((Debian))
10000/tcp open  http     Apache httpd 2.4.54
Service Info: Host: facturascloud.com; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 57.83 seconds
```

Ilustración 1 análisis de ip

fuentes: Del autor

FactuSOL

```
76223F3F  CC           INT3
76223F40  FF25 00102876  JMP DWORD PTR DS:[<&api-ms-win-core-fil  BOOL KERNEL32.FlushFileBuffers(hFile)
76223F46  CC           INT3
76223F47  CC           INT3
76223F48  CC           INT3
```

fuentes: Del autor

```
76217F8F  CC           INT3
76217F90  8BFF         MOV EDI,EDI   HANDLE KERNEL32.OpenProcess(Access,InheritHandle,ProcessID)
76217F92  55           PUSH EBP
```

fuentes: Del autor

Evaluación de riesgo

Facturador cloud

Se refleja 4 puertos abiertos para analizar las siguientes consecuencias:

Si el puerto 80 (http) en un servidor de facturación electrónica en la nube está abierto, puede tener algunas consecuencias no deseadas, ya que este puerto se utiliza comúnmente para el tráfico web y la comunicación HTTP. Algunas posibles consecuencias son:

- Exposición de la información confidencial: Si un atacante encuentra una vulnerabilidad en el servidor de Apache httpd, puede utilizarla para acceder a la información confidencial almacenada en el servidor, como los datos de facturación electrónica, los registros de clientes, las credenciales de usuario, etc.
- Exposición de las vulnerabilidades de Apache httpd: Si se ejecuta una versión antigua o vulnerable de Apache httpd en el servidor, puede ser susceptible a ataques como inyección de código o denegación de servicio (DoS), que pueden afectar la disponibilidad y la integridad de los datos del servidor.
- Ataques de phishing y spear phishing: Si un atacante logra comprometer el servidor de facturación electrónica, puede utilizar la información obtenida para realizar ataques de phishing y spear phishing contra los clientes del servicio de facturación.
- Interrupción del servicio: Si se produce una interrupción del servicio en el servidor, los clientes pueden verse afectados y no ser capaces de acceder a sus facturas electrónicas.

Si el puerto 85/tcp está abierto y disponible en un facturador electrónico y se utiliza para el servicio SSH, esto puede tener algunas consecuencias, como se detallan a continuación:

- Posible acceso no autorizado: Si el puerto 85/tcp está abierto y se utiliza para SSH, cualquier persona con acceso a la red podría intentar conectarse a la máquina utilizando herramientas de fuerza bruta para descubrir contraseñas débiles. Si logran obtener acceso, podrían robar información sensible o comprometer la integridad del sistema.

- Riesgo de acceso remoto no seguro: Si el servicio SSH no se configura de manera segura, podría permitir el acceso remoto no seguro. Por ejemplo, si el sistema no está configurado para utilizar autenticación de clave pública y solo depende de contraseñas, el acceso a la máquina podría ser comprometido.

- Riesgo de malware: Si un atacante logra acceder al sistema a través de SSH, podrían instalar malware en la máquina, que podría ser utilizado para realizar ataques adicionales o recopilar información confidencial.

Si el puerto 443/tcp visible y abierto puede tener varias consecuencias, algunas de las cuales son las siguientes:

- Vulnerabilidades de seguridad: Si el puerto 443/tcp está abierto, esto significa que el servidor web Apache está siendo utilizado para el facturador electrónico y que el sitio web utiliza HTTPS para comunicaciones seguras. Es importante asegurarse de que el software Apache esté actualizado y protegido contra vulnerabilidades conocidas para evitar posibles ataques de hackers.

- Riesgo de ataques de inyección SQL: Si el sitio web del facturador electrónico no está correctamente asegurado, podrían estar expuestas a ataques de inyección SQL. Un atacante podría aprovechar esta vulnerabilidad para modificar la base de datos del facturador electrónico y alterar o robar información confidencial.

- Exposición de información: Si el facturador electrónico es accesible a través del puerto 443/tcp, es posible que la información del sistema, como la versión del software y la configuración del servidor, esté expuesta a cualquier persona que tenga acceso a la red. Esto puede facilitar que un atacante identifique vulnerabilidades y explote el sistema.
-

- Riesgo de ataques DDoS: Los ataques de denegación de servicio distribuidos (DDoS) pueden tener como objetivo inundar el servidor web Apache y provocar que el sistema no esté disponible para los usuarios legítimos. Si el facturador electrónico se encuentra en el mismo servidor web Apache que otros sitios web, un ataque DDoS dirigido a uno de los sitios web también puede afectar la disponibilidad del facturador electrónico.

Si el puerto 10000/tcp está abierto en un facturador electrónico y se utiliza para el servicio web Apache, esto puede tener algunas consecuencias, como se detallan a continuación:

- Posible acceso no autorizado: Si el puerto 10000/tcp está abierto y se utiliza para el servicio web, cualquier persona con acceso a la red podría intentar conectarse a la máquina utilizando herramientas de fuerza bruta para descubrir contraseñas débiles. Si logran obtener acceso, podrían robar información sensible o comprometer la integridad del sistema.

- Riesgo de acceso remoto no seguro: Si el servicio web no se configura de manera segura, podría permitir el acceso remoto no seguro. Por ejemplo, si el sistema no está configurado para utilizar HTTPS y solo depende de HTTP, el acceso a la máquina podría ser comprometido.

- Riesgo de malware: Si un atacante logra acceder al sistema a través del servicio web, podrían instalar malware en la máquina, que podría ser utilizado para realizar ataques adicionales o recopilar información confidencial.

FactuSOL

BOOL KERNEL32.FlushFileBuffers(hFile)

Esta función es importante para garantizar que los datos se escriban correctamente y de manera segura en un medio de almacenamiento, lo que puede ser relevante para la seguridad informática en casos donde la integridad y la confidencialidad de los datos son críticas.

KERNEL32.OpenProcess(Access,InheritHandle,ProcessID)

La función OpenProcess se utiliza para obtener un identificador de acceso al proceso de Windows en ejecución para realizar operaciones como la lectura o escritura de memoria, la terminación del proceso o la obtención de información de depuración. Esta función es útil en situaciones donde es necesario interactuar con el proceso en tiempo de ejecución, como puede ser el caso de herramientas de análisis de software o de depuradores.

Sin embargo, el uso de esta función puede ser peligroso en algunos casos, especialmente si se utiliza de manera malintencionada o si se accede a áreas sensibles de la memoria del proceso. Por lo tanto, es importante considerar la seguridad e integridad de los datos y los procesos involucrados en el uso de esta función.

Análisis de las Entrevista

En el proceso de análisis, se utiliza una metodología sistemática para interpretar los datos obtenidos en las entrevistas. Se identificaron patrones y tendencias en las respuestas de los participantes, los cuales permitieron obtener una visión general del nivel de seguridad de la facturación electrónica y del conocimiento de seguridad informática de los entrevistados.

En cuanto al análisis del nivel de seguridad de la facturación electrónica, se evidenció que muchos de los participantes no conocían los estatutos asociados a la seguridad informática para la facturación electrónica y cómo proteger sus datos personales. Algunos entrevistados mostraron preocupación por la posibilidad de que sus datos pudieran ser robados o utilizados de manera fraudulenta, mientras que otros no estaban seguros de cómo proteger sus datos en línea.

En cuanto al análisis del conocimiento de seguridad informática, algunos participantes tenían un conocimiento básico de las buenas prácticas de seguridad informática, mientras que otros carecían de conocimientos básicos en esta área. Algunos entrevistados se mostraron conscientes de la necesidad de proteger sus datos personales y emplearon medidas básicas de seguridad, como la configuración de contraseñas seguras o la instalación de software de protección contra virus y malware. Otros, por el contrario, se mostraron poco informados sobre la importancia de estas medidas de seguridad.

Puntos en común de la entrevista

¿Qué medidas de seguridad adicionales toman para evitar el acceso no autorizado a los datos de los clientes?

La utilización de contraseñas de acceso autorizado se consideró como una medida efectiva para garantizar que sólo los usuarios autorizados pudieran acceder a los datos de los clientes. De esta forma, se evita que personas no autorizadas puedan acceder a información confidencial y se aumenta el control sobre la seguridad de los datos.

¿Cómo manejan los posibles incidentes de seguridad relacionados con la facturación electrónica, como el robo de datos o el phishing (Hackeo)?

En el análisis de las respuestas obtenidas, se observó un punto en común que consistía en que muchos participantes dejaban la responsabilidad de manejar estos incidentes a la institución

o empresa proveedora del facturador electrónico o al departamento de informática de su organización.

¿Cómo manejan los datos de los clientes que ya no son necesarios para la facturación?

En el análisis de las respuestas obtenidas, se observó que muchos participantes indicaron que almacenan los datos de los clientes por un período de tiempo menor a un año.

Al limitar el tiempo de retención de los datos, se reduce el riesgo de que los datos sean comprometidos por amenazas externas o internas.

¿Cómo está estructurado el equipo encargado de la facturación electrónica en su empresa? y ¿Hay una sola persona encargada o es un grupo de personas?

En el análisis de las respuestas obtenidas, se observó que la mayoría de los participantes indicaron que más de una persona está involucrada en el proceso de facturación electrónica en sus respectivas empresas.

¿Cómo se asegura la privacidad y confidencialidad de los datos de los clientes durante la transmisión de información a través de Internet?

En general, los participantes suponían que el departamento de sistemas o informática de la empresa se encargaba de la protección de los datos durante la transmisión de información a través de Internet. Sin embargo, no se proporcionó información clara sobre las medidas específicas que se tomaban para asegurar la privacidad y confidencialidad de los datos de los clientes durante la transmisión de información a través de Internet.

DISCUSIÓN DE RESULTADOS

Resultados del análisis de los facturadores

El uso de tecnologías de facturación electrónica como el Facturador Cloud y FactuSOL se ha vuelto cada vez más común en las empresas. Ambas aplicaciones ofrecen una solución para la gestión de facturación, pero presentan algunas diferencias notables.

Facturador Cloud, como su nombre lo indica, es una aplicación en línea que se ejecuta completamente en la nube. Esto significa que no es necesario instalar nada en la máquina del usuario, lo que conlleva a una ventaja considerable en términos de accesibilidad y portabilidad. Además, dado que la aplicación se ejecuta en servidores remotos, no utiliza recursos del equipo del usuario, lo que puede mejorar el rendimiento y la velocidad de la máquina.

Por otro lado, FactuSOL es un software de escritorio que se instala en la máquina del usuario. Esto implica que el software utiliza recursos de la máquina, lo que puede afectar su rendimiento. Sin embargo, esta característica también puede ser vista como una ventaja, ya que el acceso a la información de facturación se limita solo a los usuarios que tienen acceso físico a la máquina. De esta manera, se reduce el riesgo de vulnerabilidades de seguridad, como el acceso no autorizado a la información.

La encuesta realizada ha sido de gran ayuda para comprender la importancia de la seguridad en la facturación electrónica. Los resultados obtenidos evidencian la necesidad de que los encuestados conozcan en detalle el proceso que se lleva a cabo para garantizar la seguridad informática de los datos de los clientes. Con esto, se podrán proponer ideas innovadoras para mejorar la calidad de trabajo con la facturación electrónica, y así, asegurar una gestión más efectiva y segura de los datos de los clientes. En resumen, la encuesta ha permitido tomar conciencia sobre la relevancia de la seguridad informática en el ámbito de la facturación electrónica, y ha demostrado la necesidad de seguir trabajando en la implementación de medidas de seguridad más efectivas y actualizadas.

En relación a las limitaciones del presente estudio, es importante reconocer que la falta de un computador con mayores recursos limitó la profundidad del análisis en algunos aspectos. Sin embargo, a pesar de esta limitación, los resultados obtenidos fueron suficientes para cumplir con los objetivos planteados. Asimismo, se debe destacar que la muestra seleccionada fue limitada y no necesariamente representa la totalidad de la población objetivo.

Se considera las siguientes propuestas para enfrentar las amenazas que tienen los facturadores electrónicos:

- Identificar los puertos abiertos y restringir el acceso: Es importante identificar los puertos abiertos y restringir el acceso a ellos para evitar que los atacantes puedan acceder al sistema y robar información confidencial. Esto se puede hacer a través de la configuración de un firewall que bloquee el tráfico no deseado y solo permita el acceso a los puertos necesarios para el funcionamiento del sistema.

- Mantener actualizado el software y parchear las vulnerabilidades conocidas: Es importante mantener actualizado el software utilizado en Facturador Cloud y FactuSOL y aplicar parches de seguridad cuando estén disponibles para corregir las vulnerabilidades conocidas.

- Implementar la autenticación de dos factores (2FA): La autenticación de dos factores es una medida de seguridad efectiva que agrega una capa adicional de protección al sistema. Al requerir un segundo factor de autenticación, como un código enviado a un dispositivo móvil, se puede prevenir el acceso no autorizado al sistema incluso si se conocen las credenciales de inicio de sesión.

- Realizar auditorías de seguridad periódicas: Las auditorías de seguridad periódicas pueden ayudar a identificar posibles vulnerabilidades y brechas de seguridad en el sistema. Estas auditorías pueden ser realizadas por un equipo de seguridad interno o por un tercero especializado en seguridad de la información.

- Capacitar al personal sobre seguridad de la información: Es importante que el personal de la empresa esté capacitado y consciente de las amenazas de seguridad y las mejores prácticas de seguridad. La capacitación puede incluir la creación de contraseñas seguras, la identificación de correos electrónicos de phishing y la comprensión de la importancia de mantener actualizado el software utilizado en el sistema.

Es importante mencionar también que la metodología utilizada, aunque rigurosa, puede presentar algunas debilidades en cuanto a la subjetividad en la interpretación de las respuestas de los entrevistados. En definitiva, se debe tener en cuenta que cualquier estudio posee limitaciones y debilidades que pueden afectar la validez de los resultados obtenidos, pero que estas limitaciones no invalidan la utilidad de los hallazgos para futuras investigaciones y mejoras en la práctica profesional.

CONCLUSIONES

Es fundamental realizar un análisis exhaustivo de los sistemas de Facturador Cloud y FactuSOL, utilizando herramientas de ciberseguridad, para identificar posibles vulnerabilidades y así implementar medidas de seguridad que puedan reducir los riesgos de exposición de información confidencial. Esto incluye analizar los puertos abiertos en los servidores, verificar el código fuente en busca de vulnerabilidades, establecer políticas de seguridad claras, capacitar al personal y realizar evaluaciones periódicas de seguridad para mantener los niveles adecuados de seguridad y evitar posibles vulnerabilidades. Todo esto es crucial para proteger los datos de los clientes y mantener la confianza en los sistemas de facturación electrónica.

En la evaluación de las vulnerabilidades en la seguridad de la facturación electrónica de Facturador Cloud y FactuSOL, se identificaron posibles daños que pueden ocurrir si no se consideran adecuadamente las implicaciones de las vulnerabilidades en la seguridad. Por ejemplo, si el puerto SSH no está protegido adecuadamente, los atacantes podrían acceder a los datos del servidor y robar información confidencial del sistema. Es importante tener en cuenta estos posibles daños al evaluar los resultados de la investigación y establecer medidas de seguridad adecuadas para proteger la facturación electrónica y la información confidencial de los clientes.

Se delinea una propuesta de investigación futura para mejorar la seguridad de la facturación electrónica y adaptarse a las necesidades cambiantes de las empresas y los clientes en el futuro, se podrán identificar y abordar las amenazas emergentes y las vulnerabilidades del sistema a medida que cambian las necesidades de las empresas y los clientes. Esto permitirá mantener la seguridad

del sistema actualizada y efectiva en el tiempo, lo que es esencial para proteger la información confidencial y garantizar la continuidad del negocio.

RECOMENDACIONES

Realizar medidas de seguridad adecuadas para reducir los riesgos de exposición de información confidencial en los sistemas de Facturador Cloud y FactuSOL. Esto debe incluir el análisis de los puertos abiertos en los servidores, la verificación del código fuente en busca de vulnerabilidades, la implementación de políticas de seguridad claras, la capacitación del personal y la realización de evaluaciones periódicas de seguridad. Al hacerlo, se puede garantizar la protección de los datos de los clientes y mantener la confianza en los sistemas de facturación electrónica, lo que es fundamental para garantizar la continuidad del negocio y proteger la información confidencial.

Implementar medidas de seguridad adecuadas para proteger los sistemas de facturación electrónica y la información confidencial de los clientes, considerando las posibles vulnerabilidades identificadas en la evaluación de riesgos. Es importante proteger adecuadamente los puertos abiertos, especialmente el puerto SSH, para evitar que los atacantes puedan acceder a los datos del servidor y robar información confidencial del sistema. Además, se deben establecer políticas de seguridad claras, capacitar al personal y realizar evaluaciones periódicas de seguridad para mantener los niveles adecuados de seguridad y evitar posibles vulnerabilidades en el futuro.

Seguir desarrollando e implementando la propuesta de investigación futura para mejorar la seguridad de la facturación electrónica. Es importante realizar un seguimiento constante de las nuevas amenazas y vulnerabilidades en el sistema, adaptando y actualizando continuamente

las medidas de seguridad para mantenerse al día y garantizar la protección efectiva de la información confidencial. Esto permitirá a las empresas y clientes tener confianza en la seguridad del sistema de facturación electrónica, lo que a su vez garantizará la continuidad del negocio y la protección de los datos de los clientes.

REFERENCIAS

ALONSO, C. (22 de FEBRERO de 2023). Claves de la Ley Orgánica de Protección de Datos Personales de Ecuador. *Ley Orgánica de Protección de Datos Personales de Ecuador (LOPDP)*. Obtenido de https://www.globalsuitesolutions.com/es/claves-proyecto-ley-organica-proteccion-de-datos-personales-ecuador/

Altube, R. (5 de noviembre de 2021). Kali Linux: Qué es y características principales. Obtenido de https://openwebinars.net/blog/kali-linux-que-es-y-caracteristicas-principales/

Arias Pérez, M., & Cáceres Ortiz, A. (2021). *FACTURACIÓN ELECTRÓNICA UN MECANISMO DE CONTROL PARA EL CUMPLIMIENTO TRIBUTARIO, CASO SECTOR CARROCERO.* Ambato. doi:http://doi.org/10.22370/riace.2021.10.1.2987

BAHO, S. A., & ABAWAJY, J. (28 de febrero de 2023). Análisis de los marcos de cuantificación de vulnerabilidades de dispositivos IoT de consumo. geelong, Australia.

Bello, E. (20 de octubre de 2022). Conoce las herramientas de ciberseguridad para proteger tu empresa. Obtenido de https://www.iebschool.com/blog/herramientas-ciberseguridad-digital-business/#:~:text=Su%20funci%C3%B3n%20principal%20es%20inspeccionar%20el%20tr%C3%A1fico%20de,como%20hardware%2C%20software%20o%20una%20combinaci%C3%B3n%20de%20ambos.

Bercial, J. (24 de abril de 2020). VirtualBox: ¿Qué es y para qué sirve? Obtenido de https://www.geeknetic.es/VirtualBox/que-es-y-para-que-sirve

Cedeño, C. (28 de octubre de 2022). Ingeniería inversa: beneficios y ejemplos reales de un ingenioso enfoque para diseñar productos. Obtenido de https://www.cinconoticias.com/ingenieria-inversa/

cronomia. (2023). *CRONOMIA*. Obtenido de https://www.cronomia.com/software/factusol

DIAZ CORDOVA, J., COBA MOLINA, E., & BOMBÓN MAYORGA, A. (2020). *Facturación electrónica versus facturación clásica. Un estudio en el comportamiento financiero mediante estudios de casos.* AMBATO.

Espinosa, O. (30 de octubre de 2019). Conoce todas las opciones de análisis de VirusTotal para comprobar si tienes malware. Obtenido de https://www.redeszone.net/tutoriales/seguridad/virustotal-analisis-archivos-webs-malware/

FacturasCloud. (2023). El software de facturación que te ayuda a controlar tu negocio. Obtenido de https://facturascloud.com/

Kurtz, R. (5 de marzo de 2019). *github*. Obtenido de https://github.com/NationalSecurityAgency/ghidra

Lesonsky, R. (15 de mayo de 2019). Las principales amenazas a la seguridad electrónica y cómo proteger tu negocio. Obtenido de https://negocioseideas.blogs.xerox.com/2019/05/15/las-principales-amenazas-a-la-seguridad-electronica-y-como-proteger-tu-negocio/

Lyon, G. (2019). Nmap: Descubre tu red. Obtenido de https://nmap.org/

Malavé, L. (29 de abril de 2019). *facturacion-electronica*. Obtenido de https://facturacion-electronica.ec/bases-legales-de-la-facturacion-electronica/#comment-17

SRI. (18 de mayo de 2021). RESOLUCIÓN Nro. NAC-DGERCGC21-00000029. Obtenido de https://b2142226-1925-42c3-b5df-38d50682f540.usrfiles.com/ugd/b21422_848db41d9ea24d26b4f664f92ff59418.pdf

Zapata, D. (23 de enero de 2023). ¿Qué es un análisis de vulnerabilidad? Obtenido de https://blogs.manageengine.com/espanol/2023/01/23/analisis-vulnerabilidad.html

ANEXOS

Entrevista sobre la seguridad informática en los datos de los clientes en la facturación electronica

En esta entrevista hablaremos sobre la facturación electrónica y la importancia de proteger los datos de los clientes en este proceso.

Antes de comenzar con la entrevista, es importante mencionar que cualquier información compartida durante la misma será utilizada únicamente con fines académicos y de investigación. Todos los datos y opiniones proporcionados serán tratados de manera confidencial y solo se utilizarán para el desarrollo de este proyecto. Siéntete libre de compartir todo lo que consideres relevante para la investigación, y si en algún momento sientes que no deseas responder alguna pregunta, estás en todo tu derecho de hacerlo. Agradecemos tu disposición y colaboración en este estudio. *

(●) ACEPTO DAR INFORMACION PARA EL PROYECTO

NOMBRE Y APELLIDO *

Josué Montoya

CARGO EN LA EMPRESA *

Facturación

¿Qué medidas de seguridad adicionales toman para evitar el acceso no autorizado a los datos de los clientes? *

Contraseñas de acceso autorizado

¿Cómo manejan los posibles incidentes de seguridad relacionados con la facturación electrónica, como el robo de datos o el phishing (Hakeo)? *

Reglamentos internos de uso de información confidencial

¿Cómo manejan los datos de los clientes que ya no son necesarios para la facturación? *

Actualización cada 6 meses

¿Cómo está estructurado el equipo encargado de la facturación electrónica en su empresa? * y ¿Hay una sola persona encargada o es un grupo de personas?

Dos personas

¿Cómo aseguran la privacidad y confidencialidad de los datos de los clientes durante la transmisión de información a través de Internet? *

Usuarios de red

Entrevista sobre la seguridad informática en los datos de los clientes en la facturación electronica

En esta entrevista hablaremos sobre la facturación electrónica y la importancia de proteger los datos de los clientes en este proceso.

Antes de comenzar con la entrevista, es importante mencionar que cualquier información compartida durante la misma será utilizada únicamente con fines académicos y de investigación. Todos los datos y opiniones proporcionados serán tratados de manera confidencial y solo se utilizarán para el desarrollo de este proyecto. Siéntete libre de compartir todo lo que consideres relevante para la investigación, y si en algún momento sientes que no deseas responder alguna pregunta, estás en todo tu derecho de hacerlo. Agradecemos tu disposición y colaboración en este estudio. *

- (●) ACEPTO DAR INFORMACION PARA EL PROYECTO

NOMBRE Y APELLIDO *

Elsa Zambrano

CARGO EN LA EMPRESA *

Directora administrativa financiera

¿Qué medidas de seguridad adicionales toman para evitar el acceso no autorizado a los datos de los clientes? *

Nube

¿Cómo manejan los posibles incidentes de seguridad relacionados con la facturación electrónica, como el robo de datos o el phishing (Hakeo)? *

Validación de sri

¿Cómo manejan los datos de los clientes que ya no son necesarios para la facturación? *

Se valida en el sistema comercial el catastro

¿Cómo está estructurado el equipo encargado de la facturación electrónica en su empresa? * y ¿Hay una sola persona encargada o es un grupo de personas?

3 personas

¿Cómo aseguran la privacidad y confidencialidad de los datos de los clientes durante la transmisión de información a través de Internet? *

El área de sistemas y comercial

Entrevista sobre la seguridad informática en los datos de los clientes en la facturación electronica

En esta entrevista hablaremos sobre la facturación electrónica y la importancia de proteger los datos de los clientes en este proceso.

Antes de comenzar con la entrevista, es importante mencionar que cualquier información compartida durante la misma será utilizada únicamente con fines académicos y de investigación. Todos los datos y opiniones proporcionados serán tratados de manera confidencial y solo se utilizarán para el desarrollo de este proyecto. Siéntete libre de compartir todo lo que consideres relevante para la investigación, y si en algún momento sientes que no deseas responder alguna pregunta, estás en todo tu derecho de hacerlo. Agradecemos tu disposición y colaboración en este estudio. *

- (●) ACEPTO DAR INFORMACION PARA EL PROYECTO

NOMBRE Y APELLIDO *

Lilivette Estefanía Troya Proaño

CARGO EN LA EMPRESA *

Asistente de contaduría

¿Qué medidas de seguridad adicionales toman para evitar el acceso no autorizado a los datos de los clientes? *

Software para detectar firewall malicioso

¿Cómo manejan los posibles incidentes de seguridad relacionados con la facturación electrónica, como el robo de datos o el phishing (Hakeo)? *

Asegurarse de que los correos recibidos sean seguros.

¿Cómo manejan los datos de los clientes que ya no son necesarios para la facturación? *

Quedan guardados en archivos donde se especifica el tipo.

¿Cómo está estructurado el equipo encargado de la facturación electrónica en su empresa? * y ¿Hay una sola persona encargada o es un grupo de personas?

Asistente y contadora. Solo dos.

¿Cómo aseguran la privacidad y confidencialidad de los datos de los clientes durante la transmisión de información a través de Internet? *

Contraseñas seguras

Entrevista sobre la seguridad informática en los datos de los clientes en la facturación electronica

En esta entrevista hablaremos sobre la facturación electrónica y la importancia de proteger los datos de los clientes en este proceso.

Antes de comenzar con la entrevista, es importante mencionar que cualquier información compartida durante la misma será utilizada únicamente con fines académicos y de investigación. Todos los datos y opiniones proporcionados serán tratados de manera confidencial y solo se utilizarán para el desarrollo de este proyecto. Siéntete libre de compartir todo lo que consideres relevante para la investigación, y si en algún momento sientes que no deseas responder alguna pregunta, estás en todo tu derecho de hacerlo. Agradecemos tu disposición y colaboración en este estudio. *

- (●) ACEPTO DAR INFORMACION PARA EL PROYECTO

NOMBRE Y APELLIDO *

Andrea rivera

CARGO EN LA EMPRESA *

Trabajador operativo

¿Qué medidas de seguridad adicionales toman para evitar el acceso no autorizado a los datos de los clientes? *

Solo personal autorizado

¿Cómo manejan los posibles incidentes de seguridad relacionados con la facturación electrónica, como el robo de datos o el phishing (Hakeo)? *

Revisar bien las facturas

¿Cómo manejan los datos de los clientes que ya no son necesarios para la facturación? *

Se cierra la pestaña o si es en físico se guardan

¿Cómo está estructurado el equipo encargado de la facturación electrónica en su empresa? * y ¿Hay una sola persona encargada o es un grupo de personas?

Un grupo

¿Cómo aseguran la privacidad y confidencialidad de los datos de los clientes durante la transmisión de información a través de Internet? *

Solo la persona que efectúa la transacción

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

Babahoyo, 4 de abril de 2023

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

En mi calidad de Tutor del Trabajo de la Investigación del Sr: **DIAZ MONTOYA JHONATAN MARTY**, cuyo tema es: ***ANÁLISIS DE SEGURIDAD EN LA FACTURACIÓN ELECTRÓNICA: CASO DE ESTUDIO DE FACTURADOR CLOUD Y FACTUSOL***, certifico que este trabajo investigativo fue analizado por el Sistema Antiplagio COMPILATIO, obteniendo como porcentaje de similitud de **[5%]**, 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. Erick Ricaurte Zambrano, MSIG, MBA.
DOCENTE DE LA FAFI.