UNIVERSIDAD ANDINA DEL CUSCO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS

“PROPUESTA DE MITIGACION DE RIESGOS EN EL SISTEMA IFACTURACION DE LA EMPRESA PALE CONSULTORES HACIENDO USO DE LA ADAPTACION DE LAS METODOLOGIAS PENTESTING STANDART Y NIST-SP 800-30 – 2022”.

TESIS PARA OPTAR EL TÍTULO DE INGENIERO DE SISTEMAS

Presentado por:

Bach. Carlos Frankbel Schiavonne Hurtado

ASESOR: Mg. De la Vega Bellido, Vivian Luz

CUSCO – PERU

2022

Índice de Tablas

Índice de Figuras

Introducción

Desde hace varios años los sistemas de información se volvieron indispensables en las empresas para que sea competitiva en el mercado local, nacional, internacional, los sistemas de información facilitan en gran medida el desempeño de la empresa, pero no todas son ventajas debido a que un sistema contiene información confidencial para la empresa, como son: datos contables, información personal sensible, secretos de negocio, etc.

El hecho de que los sistemas de información manejen información tan importante para la empresa la vuelve un objetivo codiciado para personas o entidades mal intencionadas, si alguien llega a tomar el control o roba esta información puede extorsionar o simplemente eliminar esta información provocando que la empresa pierda dinero y la confiabilidad de los clientes, generando de esta manera pérdida de confianza de los clientes de la empresa.

Existen múltiples maneras de descubrir los riesgos a los cuales está expuesto un sistema de información, se puede usar Pentesting, hacking ético, análisis de vulnerabilidades o auditorias en seguridad para tener conocimiento acerca de las vulnerabilidades y la manera en la cual impactaría al sistema si un ataque se diera a cabo.

En la actualidad las empresas están siendo obligadas por la SUNAT a tener facturación Electrónica, por esta razón en las últimas décadas se crearon múltiples empresas que ofrecen este servicio a través de sistemas que realicen la facturación de manera automática, en consecuencia, este mercado se expandió con el desarrollo de sistemas que integren la facturación y otros servicios adicionales como pueden ser declaraciones de boletas de venta hacia la SUNAT.

El objetivo de este trabajo de investigación es evaluar los riesgos a los que está expuesto el sistema IFacturacion de la empresa Pale Consultores, IFacturacion es el sistema principal de la empresa, IFacturacion realiza como tarea principal facturación electrónica para grifos, restaurantes y farmacias, también gestiona el inventariado, entre otros.

El trabajo de investigación se estructura en cuatro partes la primera de ellas se describirá la problemática y los objetivos, en la segunda se describirá el marco teórico el cual sentara las bases de la investigación, en la tercera parte se describirá el desarrollo del trabajo de investigación, como se hará y lo que implicara el desarrollo del trabajo de investigación, en la cuarta parte se describen los resultados del trabajo de investigación, se verifica el cumplimiento de los objetivos planteados y la prospectiva, también se verifica las contribuciones del trabajo de investigación.

Resumen

En la presente investigación se desarrolla la propuesta de mitigación de riesgos de riesgos en el Sistema IFacturacion para la empresa Pale Consultores haciendo uso de las metodologías Pentesting Standard y NIST SP 800-30, para el desarrollo de esta propuesta se usó las tablas propuestas por la metodologia de NIST SP800-30 y las herramientas y recomendaciones que propone la metodologia del Pentesting Standard.

En el Capítulo I – Problema de Investigación, se hizo referencia al área de dominio de la propuesta, la línea de investigación, luego se planteó la descripción del problema y los objetivos de la propuesta.

En el Capítulo II – Marco teórico, se da las bases teóricas para poder entender la propuesta, asimismo se desarrollaron los antecedentes nacionales e internacionales que sirvieron para realizar la presente propuesta.

En el Capítulo III – Prospectiva Tecnológica, se describe como se hará, que se hará y con qué herramientas se realizará la presente propuesta.

En el Capítulo IV – Resultados, se describe cuáles fueron los resultados de la prospectiva tecnológica, la comprobación de los objetivos planteados y el impacto que tiene la presente propuesta en la empresa.

ABSTRACT

This research develops the proposal for risk mitigation of risks in the IFacturacion System for the company Pale Consultores using the Pentesting Standard and NIST SP 800-30 methodologies, for the development of this proposal the tables proposed by the NIST SP800-30 methodology, and the tools and recommendations proposed by the Pentesting Standard methodology were used.

In Chapter I - Research Problem, reference was made to the domain area of the proposal, the line of research, then the description of the problem and the objectives of the proposal were presented.

In Chapter II - Theoretical Framework, the theoretical basis for understanding the proposal is given, as well as the national and international background that served to develop this proposal.

Chapter III - Technological Prospective describes how the proposal will be made, what will be done and with what tools it will be carried out.

Chapter IV - Results, describes the results of the technology foresight, the verification of the proposed objectives and the impact of this proposal on the company.

CAPITULO 1 - Problema de investigación

1.1. Ámbito de influencia.

1.1.1. Ámbito de influencia teórica.

La seguridad de la información empieza con políticas las cuales describen quien está autorizado a hacer que, con la información sensible; una vez definida la política esta debe ser reforzada, para esto los negocios desarrollan procesos y mecanismos que se dividen en cuatro categorías.

- Las medidas de protección que tienen por objetivo prevenir que ocurran eventos adversos.
- Las medidas de detección alertan al negocio cuando ocurren eventos adversos.
- Las medidas de respuesta abordan las consecuencias de los eventos adversos y devuelven el negocio a una condición segura después de que se ha resuelto un evento.
- Medidas de aseguramiento validar la efectividad y buen funcionamiento de los protocolos de protección, detección y respuesta.

La tarea final de la seguridad de la información es una auditoria que consienta determinar la efectividad de las medidas tomadas para la proteger la información contra el riesgo (Blakley et al., s. f.)

1.1.2. Área de Dominio.

Hacer una propuesta de mitigación de riesgos implica una evaluación de riesgos en un sistema de información el cual corresponde al dominio de tecnologías de la comunicación debido al desarrollo que conlleva, al realizar un análisis de vulnerabilidades se verá involucrado el sistema de información y la base de datos con la que se relaciona el sistema de información.

1.1.3. Línea de Investigación.

Una propuesta de mitigación de riesgos está claramente conectada con la seguridad de la información debido a que el fin de este, es que la empresa sujeta a evaluación sea consciente de los riesgos a los que está expuesto por lo que la línea de investigación de acuerdo con los lineamientos de la Escuela Profesional de ingeniería de Sistemas (EPIS) es Seguridad en Tecnologías de información y comunicación

1.2. Planteamiento del problema.

Pale Consultores es una empresa que inicio sus actividades en el año de 2013 en la ciudad del Cusco, es una empresa que tiene como principal servicio la facturación electrónica, asimismo ofrece distintos servicios como: consultoría, venta de hardware, venta de software, diseño de páginas web, soporte de software. Pale Consultores tiene un promedio de 20 clientes, siendo en su mayoría grifos y estaciones de servicio sin embargo entre estos se encuentran también restaurantes y farmacias.

La innovación tecnológica, cambios de tecnología y la creciente necesidad de facturación electrónica por parte de las empresas exigió que Pale Consultores sea más competitivo en el mercado, por lo que el gerente general estableció políticas de seguridad implementadas en la empresa sin embargo estas no fueron registradas y se enfocaron únicamente en la base de datos del sistema de IFacturacion basados en el criterio del gerente general y del equipo a cargo del desarrollo y configuración de la base de datos.

La seguridad de la información del sistema IFacturacion quedo en segundo plano, esto se verifico realizando una entrevista al gerente general de Pale Consultores luego de la cual se han identificado algunos inconvenientes respecto a la seguridad de la información del sistema IFacturacion, por ejemplo: no hay restricción de ingreso a internet, contraseñas poco seguras para acceso a la red interna, no hay procesos de contingencia en caso de un ataque, no tiene documentación de la red empresarial. Por esta razón surge la necesidad de realizar una propuesta de mitigación de riesgos en el sistema de IFacturacion de la empresa Pale Consultores.

1.2.1. Descripción de la situación actual del lugar de intervención.

Pale Consultores es una empresa privada que se dedica al negocio de facturación electrónica, consultorías, venta de hardware, desarrollo de soluciones entre otras actividades a fines del desarrollo de tecnología. Actualmente los clientes de esta empresa son instituciones privadas en su mayoría estaciones de servicios y grifos las cuales brindan información contable e información relacionada a los clientes de las empresas asociadas a Pale Consultores, en caso el sistema sea vulnerable se expondría esta información a personas no autorizadas.

La empresa cuenta con un sistema principal llamado IFacturacion que maneja los datos de las empresas asociadas a Pale Consultores, se encarga principalmente de la facturación electrónica de las empresas asociadas, sin embargo, tiene otras funcionalidades como son la gestión de los movimientos en la caja, los arqueos, inventarios, reportes mensuales de ventas, etc.

IFacturacion es un sistema desarrollado en el lenguaje de programación C# para plataformas Desktop, es decir el sistema IFacturacion es instalado en la máquina del cliente y se le enlaza con un identificador designado en la base de datos, dicho proceso es realizado por el área de soporte de Pale Consultores.

El sistema IFacturacion cuenta con catorce módulos principales enumerados a continuación:

1. Módulo de Ventas
2. Módulo Contable
3. Módulo Movimientos caja
4. Módulo de Clientes
5. Módulos de Arqueos
6. Módulo Almacén
7. Módulos de Administración
8. Módulo de Reportes
9. Módulo de Asistencia al Cliente
10. Módulo de Asistencia Sistema
11. Módulo de Gateway
12. Módulo de Configuración
13. Módulo de Configuración Sistema

La empresa cuenta con 7 Áreas las cuales son Gerencia, Administración, Desarrollo, Ventas, Soporte, Contabilidad y Capacitación las actividades que se desarrollan en cada área se describen a continuación:

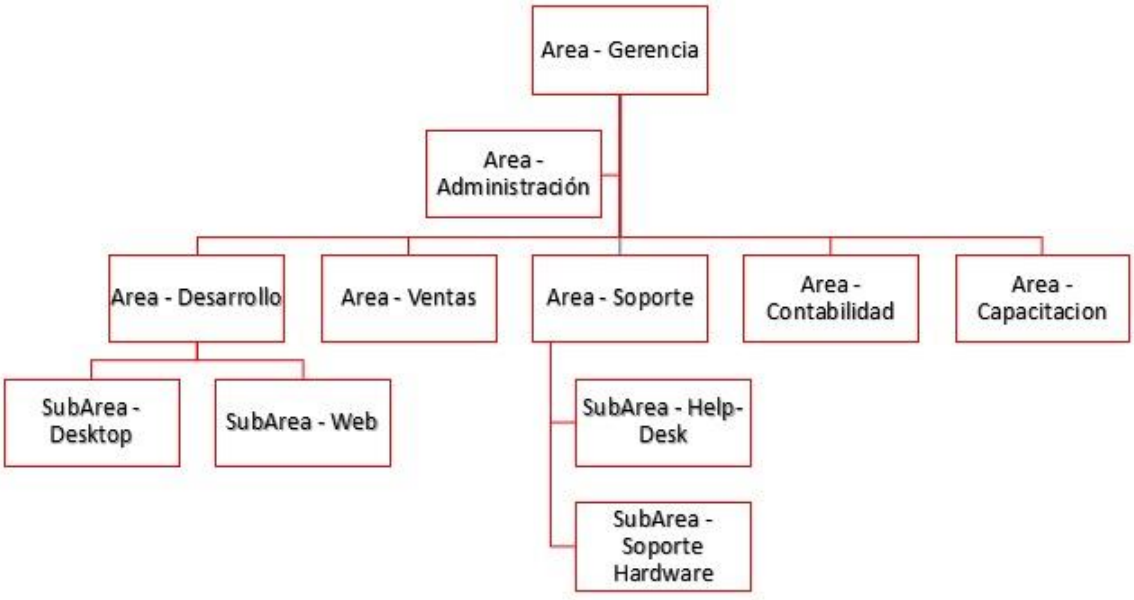


Figura 1 Organigrama de Pale Consultores

Gerencia.

Esta área es donde se alcanzan las propuestas para la mejora de la empresa, también se encarga de recibir y evaluar al personal después de realizar una prueba para el área que haya postulado, por último, en esta área se aprueban las decisiones administrativas.

Desarrollo.

Se encarga del desarrollo de aplicaciones a la fecha son aplicaciones web las cuales están desarrolladas en React JS como front-end y nodejs como backend, aplicaciones de escritorio las cuales están desarrolladas en C# y SQL Server, en esta área hay un promedio de diez desarrolladores de los cuales aproximadamente cuatro están dedicados al desarrollo de aplicaciones web, cuatro a desarrollo de aplicaciones de escritorio y dos de apoyo a las necesidades de la empresa como innovación tecnológica o de apoyo a alguno de los dos equipos de desarrollo previamente descritos**.**

Soporte.

Se encarga de brindar soporte técnico a los clientes que cuenten con el sistema de IFacturacion, esta área recibe llamadas de los clientes y les entrega soluciones a sus problemas expuestos por esto, en caso de ser necesario se les brinda soporte técnico a través del software de Team Viewer el cual permite controlar remotamente la computadora de otro usuario en este caso los clientes para realizar las labores requeridas por los mismos.

Capacitación.

Se encarga de capacitar a los empleados acerca de las actualizaciones de software que se van adoptando en la empresa, a su vez esta área se encarga de evaluar al personal nuevo de la empresa.

Esta área cuenta con equipos informáticos dentro de la red empresarial los cuales están destinados únicamente a las tareas previamente descritas.

Ventas.

Se encarga de la relación directa con los clientes ellos son los que atienden a los clientes y dan los requerimientos a gerencia general para que se derive al área que se encargara de cumplir con los requerimientos dados, son el área que brinda la información del producto que ofrece Pale Consultores a los clientes.

Administración.

Esta área que se encarga de emitir, archivar y revisar todo tipo de documento que llegue a la empresa, también se encarga de proponer manuales y guías administrativas que serán emitidas a gerencia.

Contabilidad.

Se encarga de manejar las boletas y facturas de la empresa también está el área que se encarga de alcanzar la subvención a los empleados de la empresa.

1.2.2. Descripción del Problema.

El sistema de IFacturacion no tiene antecedentes de ataques informáticos ni robo de información, tampoco tiene registros de auditorías en seguridad previos o algún otro tipo de verificación de la seguridad de la información en el sistema, además de no contar con firewall o dispositivos de seguridad perimetral. Al no tener ningún tipo de investigación relacionada a la seguridad de la información en IFacturacion y gracias a la entrevista realizada con el gerente podemos deducir que es muy probable que la información que administra sistema IFacturacion este expuesto a riesgos.

IFacturacion es un software desarrollado por Pale Consultores el sistema IFacturacion tiene por objetivo principal administrar la facturación electrónica del cliente, para ello el sistema es instalado en una computadora local del cliente, en la computadora que se instale el sistema también se instalan las dependencias que requiere el sistema como Fast Report, SQLite, entre otros. Los datos que genere el usuario son enviados a la base de datos administrada por Pale Consultores, siendo esta la que administra y guarda los datos de sus clientes, a su vez ellos se encargan de enviar mensualmente el reporte de la facturación hecha a través del sistema.

La información que maneja IFacturacion puede estar expuesto a diferentes riesgos pero Pale Consultores no es consciente de si esto puede o no generar daños colaterales o directos, la problemática es no tener conocimiento del riesgo al que está expuesto ni las vulnerabilidades latentes, lo que puede generar perdida de información, caída o inoperatividad del sistema, intercepción de información, escalar privilegios entre otros, esto podría conllevar efectos como pérdida de confianza de los clientes, robo de propiedad intelectual, pérdidas económicas, pero existen contramedidas como las técnicas de evaluación de riesgos, pentesting y múltiples maneras de comprobar las amenazas, riesgos y vulnerabilidades a las que posiblemente están expuestas los activos de información de la empresa.

Las empresas generalmente optan por modelos de gestión de seguridad, sin embargo, estos modelos en su mayoría están orientado a los procesos de negocio mas no a la seguridad integral de los o el sistema de información, para esto se opta por el pentesting, auditoria de sistemas de información, evaluación de riesgos, entre otros, estos métodos están orientados a asegurar los activos del sistema de información presentes en el objetivo mediante tareas o practicas sugeridas.

La alternativa de solución es proponer mitigar los riesgos mediante el uso de la adaptación de NIST SP 800-30 y Pentesting Standard, ya que NIST SP 800-30 provee una guía para la evaluación de riesgos, así como cuadros guía de los valores que se le darán a los riesgos, probabilidad de inicio, probabilidad de impacto, condiciones predispuestas, y enfoques adversariales como no adversariales, para de esta manera cubrir los escenarios posibles de ataques, mientras que el Pentesting Standard provee de las pautas necesarias para obtener las vulnerabilidades, mediante herramientas que ayuden a la recopilación de información, comandos que pueden ser útiles y una guía de las vulnerabilidades más comunes y como encontrarlas. Haciendo uso de ambas metologias se asegurará que los resultados de la evaluación de riesgos son los más cercanos a la realidad y que permitirán tomar decisiones de negocio respecto a IFacturacion.

1.2.3. Formulación del problema.

El manejo inadecuado de la seguridad de la información en Pale Consultores, implica que actualmente el sistema IFacturacion tiene vulnerabilidades latentes. Por lo que se requiere una evaluación de riesgos que permita a Pale Consultores ser consciente de los riesgos a los que está expuesto IFacturacion.

¿El sistema IFacturacion presenta riesgos latentes que puedan comprometer la seguridad de la información?

1.2.4. Objetivos.

General.

Evaluar los riesgos y proponer mitigaciones en el sistema IFacturacion de la empresa Pale Consultores haciendo uso de la adaptación de las metodologías Pentesting Standard y NIST SP 800-30.

Específicos.

- Definir el uso de las de las metodologías de Seguridad de la información dependiendo de la etapa del trabajo de investigación.
- Recolectar información respecto al sistema IFacturacion de la empresa Pale Consultores.
- Realizar el análisis de las vulnerabilidades en el sistema IFacturacion haciendo uso de la metodologia de Pentesting Standard.
- Identificar los riesgos basado en los eventos de amenaza haciendo uso de la metodologia NIST SP 800-30.
- Elaborar el reporte de la evaluación de riesgo con el impacto que representa cada evento de amenaza.
- Generar la propuesta de mitigación a partir de las vulnerabilidades evaluadas previamente haciendo uso de NTP ISO/IEC 27001:2008.

1.2.5. Justificación.

La seguridad de la información es algo que no puede pasar desapercibido o ser ignorado debido a que el activo más importante de cualquier empresa es la información por lo cual todas las empresas deberían aplicar una metodología, políticas o reglamentos que permita asegurar o tener un plan de contingencia para los riesgos latentes. Los sistemas de facturación electrónica tienen una relación cercana con la SUNAT dado que esta institución pública obliga a las empresas a usar facturación electrónica.

La facturación es un tipo de comprobante de pago lo que implica que los sistemas que manejen este tipo de comprobante tienen en su poder los ingresos económicos de las entidades, si esta información cae en manos de un atacante este puede despertar su interés o publicar dicha información con el fin de deteriorar la imagen de la entidad, también puede dar esta información a los competidores, en cualquiera de los casos la información dada por la facturación electrónica debe evitar ser divulgada.

En el ESET Security Report 2018 ha publicado una infografía respecto a la seguridad de las empresas en el Perú, según esta infografía una de cada 5 empresas había sufrido un acceso indebido a su información como se ve en la figura 1 tenemos un alto porcentaje de vulnerabilidades encontradas.(*Estado de la seguridad en las empresas de Perú | WeLiveSecurity*, s. f.)

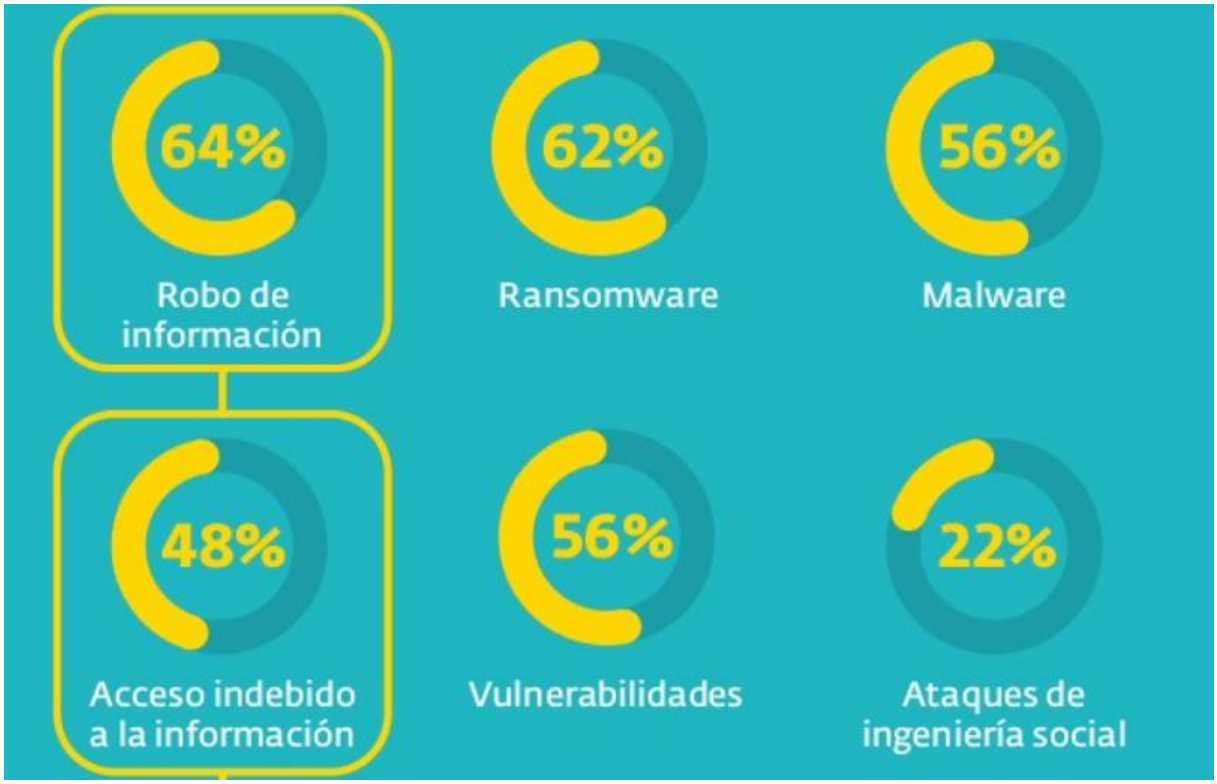


*Figura 2 Preocupaciones en la seguridad informática en el Perú (*Estado de la seguridad en las empresas de Perú | WeLiveSecurity, *s. f.)*

Se puede decir que las empresas en el Perú están expuestas a ataques ya que según los datos proporcionados por ESET solo el 50% de las empresas en el Perú tienen políticas de seguridad, un 81% de las empresas aplican prácticas de gestión y un 3.3% de las empresas no aplican ningún control de seguridad.(*Estado de la seguridad en las empresas de Perú | WeLiveSecurity*, s. f.)

El presente trabajo de investigación responde a la necesidad de la empresa Pale Consultores de estar conscientes de los riegos a los que está expuesto el sistema de IFacturacion haciendo uso del Pentesting Standard para analizar las vulnerabilidades en el sistema IFacturacion Y NIST SP 800-30 nos permitirá evaluar los riegos y proponer mitigaciones basado en el impacto de cada riesgo.

1.2.6. Alcances y Limitaciones.

La presente tesis se encargará de la evaluación de riesgos para luego realizar una propuesta de mitigaciones hacia el sistema IFacturacion, en un escenario de pruebas entregado al tesista, este escenario de pruebas tiene los mismos permisos que tienen los clientes a los que se le entrega el sistema IFacturacion con el objetivo de que el estudio se realice desde la perspectiva del cliente, permitiendo saber de esta manera si un cliente con malas intenciones representa un riesgo para el sistema IFacturacion.

Dentro de las limitaciones se encuentran los tipos de ataque que no se pueden realizar en esta investigación que son los de fuerza bruta debido a que la naturaleza de estos ataques perjudicaría a la empresa y el escenario de pruebas alcanzado no está preparado para dichos ataques.

CAPITULO 2 - Marco Teórico

2.1. Antecedentes del desarrollo, implementación o transferencia tecnológica

2.1.1. Antecedentes Nacionales

"Modelo de gestión de riesgos de seguridad de la información para pymes en el Perú", elaborado por García Porras, J., Huamani Pastor, S., & Lomparte Alvarado, R.

Resumen:

Para poder preservar la información de una empresa, se debe determinar la exposición de esta al riesgo, normalmente se recomienda hacer uso de metodologías, marcos de referencia o estándares que permitan el análisis de riesgo de seguridad de la información. El presente proyecto en referencia radica en efectuar un modelo de gestión de riesgos referido a la seguridad de la información para Pymes, usando e integrando la metodología OCTAVE-S y la norma ISO/IEC 27005. En el proyecto se realizó un estudio de las metodologías y normas de gestión de riesgos así como el diseño de un modelo de gestión de riesgos de seguridad de la información y por último se validó el modelo en una Pyme.

Aporte:

Este trabajo de investigación me aportó una vista de la gestión de riesgo desde la vista de OCTAVE-S y la norma ISO/IEC 27005 permitiendo comparar estas metodologías con otras anteriormente vistas y poder evaluar de mejor manera que metodología se usara en el presente trabajo.

“Diseño de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001:2013 para la Municipalidad Distrital de El Agustino”, diseñado por Monteza Mera y Lisbet Odelly.

Resumen:

Describe el esbozo de un SGSI apoyado en la norma ISO/IEC 207001:2013 con el objetivo de resguardar los activos de información coligados a los procesos de: recaudo y investigación tributaria de la Municipalidad Distrital de El Agustino. Así como sugiere la ISO 27001 se cazó al ciclo de Deming, la primera etapa consto de realizar el diagnóstico inicial de la entidad respecto a la norma ISO/IEC 27001:2013; la segunda etapa consto en establecer el contexto de la organización; la tercera consto en seguir la metodología de estudio y gestión de riesgos.

Bajo la norma ISO/IEC 31000 se identificó, catalogo, y estimo los activos de información con el fin de realizar un plan de tratamiento de riesgos asimilando a los controles provistos de la norma ISO/IEC 27002:2013 finalmente se confeccionó el documento del Manual SGSI.

Aporte:

El aporte de esta tesis fue facilitar una guía de cómo aplicar los controles ofrecidos por la norma ISO/IEC 27001, así como las bases normativas que se deberían tomar en cuenta para poder usar los controles.

2.1.2. Antecedentes Internacionales:

“Vulnerabilities Analysis”, investigado por Matt Bishop.

Resumen:

Este articulo presenta un nuevo modelo para clasificar las vulnerabilidades en los sistemas informáticos. El modelo es estructuralmente diferente de los modelos anteriores. Descompone las vulnerabilidades en partes pequeñas, llamadas "condiciones primitivas". la hipótesis del artículo es que, al examinar los sistemas para estas condiciones, podemos detectar vulnerabilidades. Al evitar que se cumplan estas condiciones, podemos evitar que se produzcan vulnerabilidades, incluso si no sabemos que existe la vulnerabilidad. Se presenta una base formal para este modelo.

Aporte:

Este artículo aporta los conceptos introductorios a el análisis de vulnerabilidades como son la descomposición de vulnerabilidades, RISOS (Research Into Secure Operating Systems) lo cual presenta siete clases de banderas de seguridad y la PA que presenta otras nueve clases de banderas de seguridad todo esto como conocimiento para posibles mitigaciones de vulnerabilidades.

"Diseño de un modelo de seguridad de la información, basado en OSSTMMV3, NIST SP 800-30 E ISO 27001, para centros de educación: caso de estudio Universidad Regional Autónoma de los Andes, extensión Tulcán", diseñado por Elva Gioconda Lara Guijarro

Resumen:

Hoy en dia existen diferentes modelos de seguridad de la información, éstos sirven para resguardar información privada de personas que tengan por objetivo apoderarse de estos datos. El objetivo del trabajo es establecer las mejores políticas de seguridad a usar en la institución, se tomó en cuenta que no todas las empresas tienen las mismas necesidades respecto a su información. Se realizó un piloto del modelo de seguridad de la información para la Universidad Regional Autónoma de los Andes, extensión Tulcán, haciendo uso de dos modelos de seguridad de la información como son: primero el modelo OSSTMMv3 (Open Source Security Testing Methodology), luego el marco de trabajo NIST 800-30 (National Institute of Standards and Technology) y por último el estándar ISO 27001. Finalmente, se ejecutaron encuestas a los interesados de la red de información como son alumnos, docentes, personal administrativo y responsables de TI.

Aporte:

Esta tesis dio un panorama de como poder usar la norma NIST 800-30 para la evaluación de riesgos en una empresa, también como poder combinar varias metodologías de gestión de riesgos sin intervenir unas entre tras permitiendo de esta manera una visión más amplia respecto a la gestión de riesgos.

2.2. Bases Teórica Científicas

2.2.1. Seguridad de la Información

La seguridad de la información se puede entender como el estado de bienestar de esta, se entiende que la información es segura si la posibilidad de irrupción es muy baja o tolerable en su defecto.

La seguridad en redes es la información que fluye en la red segura, a través de instrucciones fundados en una política de seguridad informática. En caso ocurra un hacking, perturbará cualquier activo de seguridad esencial. La seguridad se apoya en 4 pilares el primero es confidencialidad, segundo autenticidad, tercero integridad y por ultimo disponibilidad. (Instituto Superior Tecnológico Sistemas del Sur, 2020)

2.2.2. Seguridad Informática y Seguridad de la Información

Ambos conceptos son diferentes pero relacionados mientras que la seguridad de la informática es la parte táctica y operacional, la seguridad de la información es la parte estratégica de la seguridad. (*¿Seguridad informática o seguridad de la información?*, s. f.)

La definición de seguridad informática según ISO tools Excellence, es la norma que se encarga de la ejecución que permite proteger la información, la dispersión de las tecnologías que aseguran en la medida de lo posible las situaciones de fallas parciales o totales, cuando la información es el activo que se encuentra en riesgo. (*¿Qué Sistema de Gestión de Seguridad de la Información ISO 27001?*, s. f.)

En ese sentido, la seguridad de la información es la disciplina que habla de los riesgos, amenazas, análisis de escenarios, buenas prácticas y esquemas normativos, que permite visualizar los niveles de seguridad de procesos y tecnología para elevar el nivel de confianza de la información. (*¿Seguridad informática o seguridad de la información?*, s. f.)

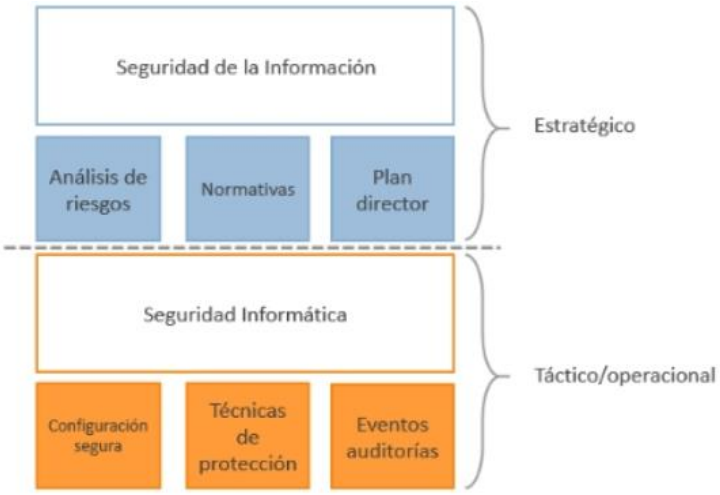


Figura 3 Diferencia Seguridad informática y Seguridad de la Información (¿Seguridad informática o seguridad de la información?, *s. f.)*

2.2.3. Métodos de análisis de la Seguridad de la Información

2.2.3.1. Análisis de Vulnerabilidades

En este proceso se determina el nivel de exposición y la predisposición a la pérdida de un activo o varios activos de información ante una amenaza. La mayoría de las metodologías que tienen en cuenta el análisis de vulnerabilidades valoran desde la amenaza más baja hasta la más alta. (Romero Castro et al., 2018)

2.2.3.2. Pentesting

Una prueba de penetración es un ataque simulado y autorizado contra un sistema informático en un ambiente controlado con el objetivo de evaluar la seguridad del sistema. Mientras que dure el pentesting, se emparejan las vulnerabilidades en el sistema y se explotan tal como haría un atacante. Esto permite al pentester ejecutar la evaluación de riesgos basándose en los derivaciones de la prueba y por ende proponer un plan de medidas correctivas. (Zafra, s. f.)

2.2.3.3. Hacking Ético

El Hacking Ético es definido por los profesionales que se ofrecen el servicio. Estos profesionales son contratadas para hackear un sistema e identificar y subsanar las posibles vulnerabilidades, lo cual advierte la explotación por hackers maliciosos, la eficacia de la identificación depende de la experiencia del hacker en la mayoría de los casos, estos profesionales se especializan en las pruebas de penetración de sistemas informáticos con el fin de valorar, fortalecer y optimizar la seguridad en estos. (Alonso Cebrian Jose Maria, s. f.)

2.2.4. Cualidades de la seguridad de la información

2.2.4.1. Confidencialidad

En esta cualidad solo las personas autorizadas deben acceder a los activos de información. Se debe evitar en la medida de lo posible cualquier obstrucción, los activos de información se tienen que encriptar y solo los actores de la transacción deben tener la clave para observar los datos. (Instituto Superior Tecnológico Sistemas del Sur, 2020)

2.2.4.2. Autentificación

En esta cualidad se restringe el acceso a las personas autorizadas. Se tiene que certificar la identidad de un usuario antes de realizar el intercambio de activos de información.(Instituto Superior Tecnológico Sistemas del Sur, 2020)

2.2.4.3. Integridad

En esta cualidad se tiene que garantizar a todas horas que los activos de información que transitan por la red son los que se entiende que son y que no se han trastornado (voluntariamente o no) durante su transmisión. (Instituto Superior Tecnológico Sistemas del Sur, 2020)

2.2.4.4. Disponibilidad

En esta cualidad se tiene que garantizar el correcto funcionamiento del sistema y el acceso a sus recursos a cualquier hora. (Instituto Superior Tecnológico Sistemas del Sur, 2020)

2.2.5. Términos esenciales

2.2.5.1. Intrusión

Son un conjunto de acciones que pretenden comprometer o poner en peligro las cualidades de un sistema informático. (Inspector Pablo Alonso, 2019)

2.2.5.2. Vulnerabilidad

Es un aspecto del sistema o de sus aplicaciones que es susceptible de ser víctima de un ataque. Representan debilidades o puntos de acceso en un sistema informático. (Inspector Pablo Alonso, 2019)

2.2.5.3. Diferencia Vulnerabilidad y Debilidad

Una debilidad es un error que puede conducir a una vulnerabilidad mientras que una vulnerabilidad es una equivocación en el software que puede ser directamente usada por un hacker para ganar acceso al sistema o red. (*CWE - Common Weakness Enumeration*, s. f.)

2.2.5.4. Técnicas, Tácticas, y procedimientos (TTPs)

Patrones de actividades y métodos asociados con amenazas especificas actores o grupos de actores de amenaza. (Friedman & Bouchard, 2015)

2.2.5.5. Exploit

Un exploit es cuando hay un fallo en un sistema o aplicación que permita acceder al sistema o aplicación pasando de esta manera a través de la seguridad del sistema, a través de un exploit se puede obtener los consentimientos requeridos para poder ejecutar código malicioso en un sistema e infectarlo aprovechando las o la vulnerabilidad sin embargo un exploit en sí mismo no es malicioso. (*¿Sabes qué es un exploit y cómo funciona? | WeLiveSecurity*, s. f.)

2.2.5.6. Programa maligno

El programa maligno es un tipo dañino de software que fue programado para acceder a un dispositivo de forma inadvertida. Los tipos de programa maligno pueden ser o incluir spyware, adware, virus, troyanos, gusanos, rootkits, ransomware y secuestradores del navegador, estos tipos de programas malignos son clasificados dependiendo de su finalidad. (*Mitos sobre malware #5: exploit es lo mismo que malware | WeLiveSecurity*, s. f.)

2.2.5.7. Amenaza

Una amenaza es un evento que puede dañar o destruir uno o más activos del sistema. (Instituto Superior Tecnológico Sistemas del Sur, 2020)

2.2.5.8. Riesgo

Según la Organización Internacional de Normalización (ISO) un riesgo es la probabilidad de que una amenaza explícita explote las vulnerabilidades de un activo o grupo de activos y por lo cual causar daño a la organización (ISO. 2019).

2.2.5.9. Medición de Riesgo

Para poder medir los riesgos no solo se usa la probabilidad sino también los efectos que vayan a causar, estos a su vez varían dependiendo de la organización y el contexto de esta, también puede ocurrir que ciertos riesgos sean de fácil solución y existen otros que pueden generar perdidas inmensas a la organización sin embargo en el mundo profesional los riesgos se miden por el coste que estos representen para la organización sea económico, recursos o algún otro tipo de inversión.(Joint Task Force Transformation Initiative, 2012).

2.2.5.10. Impacto

El impacto indica el daño que puede ocasionar una vulnerabilidad cuando las amenazas se materializan sobre un activo. El impacto se estima conociendo el valor de los activos de información y el daño causado por las amenazas. (Instituto Superior Tecnológico Sistemas del Sur, 2020).

2.2.5.11. Mitigar

Según la RAE la definición de mitigar es Moderar, aplacar, disminuir o suavizar algo riguroso o áspero, por lo que aplicado al ámbito de la seguridad podemos decir que mitigar es aplacar o disminuir el riesgo que representan determinadas amenazas en la empresa.(Instituto Superior Tecnológico Sistemas del Sur, 2020).

2.2.5.12. IDS y Firewall

El Firewall actúa como un filtro de paquetes. Examina todos los paquetes entrantes y salientes de una red a la que esté conectado. Los paquetes que cumplen el criterio descrito en las reglas establecidas por el administrador de la red se envían en forma normal. Los que no cumplan la regla se descartan. (Tanenbaum et al., 2016).

2.2.5.13. Ofuscar

El ofuscamiento permite ocultar información sobre cómo fueron desarrolladas las aplicaciones y a que datos se acceden en la misma. También el ofuscar puede ser utilizado para encriptar o dejar en código de maquina el código fuente. (Sutherland, s. f.)

2.2.6. Tipos de ataques hackers y sus modalidades

2.2.6.1. Ataques a nivel de aplicación

Los ataques a nivel aplicación generalmente se dan cuando los programadores encargados no terminar de realizar la fase de pruebas unitarias de seguridad de la aplicación ni pruebas de calidad del software. (Gutierrez Salazar Pablo, 2019)

2.2.6.2. Phishing

Es una técnica para obtener información específica de una persona o compañía de manera fraudulenta, existen muchas maneras de realizar este ataque la manera normal de hacerlo es enviando un email al objetivo haciéndose pasar por la tercera parte, pidiendo información para fines de verificación.
Otro modo común de usar phishing es un enlace de un sitio web fraudulento que supuestamente está relacionado con el real en un pre-login. (Gutierrez Salazar Pablo, 2019)

2.2.6.3. Ataques a códigos prefabricados

Las aplicaciones que vienen preinstaladas en los Sistemas Operativos vienen con múltiples scripts de instalaciones de ejemplo, las cuales son usadas por los administradores de redes con el fin de facilitarles el trabajo.
El inconveniente con estos scripts es que los administradores de redes en su mayoría no personalizan ni revisan estos scripts y los dejan por defecto sin tener en cuenta que estos scripts se distribuyen de esa manera en los Sistemas Operativos que obtienen los Crackers, lo cual le permite a los Crackers realizar ataques con mayor exactitud conocidos como “Shrink Wrap Code Attacks”. (Gutierrez Salazar Pablo, 2019)

2.2.6.4. Reingeniería

La reingeniería de procesos es una herramienta la cual consiste en analizar los procesos de empresas de cualquier sector, a través de la cual se pueden rediseñar dichos procesos.

Para llevar a cabo una reingeniería exitosa se debe tener un conocimiento claro de las metas que quiere alcanzar la empresa para que de esta manera se pueda estudiar los procesos y de construirlos para su mejora en el mejor de los casos o para analizar el código con fines maliciosos. (Pérez Andrés et al., 2017)

2.2.6.5. SQL Injection

Este método de ataque es uno de los más comunes, este ataque se usa cuando existe una base de datos detrás de la aplicación, su nombre proviene debido a que se introduce código SQL en los campos de entrada de datos para de esta manera acceder al servidor sin autorización. (Gutierrez Salazar Pablo, 2019)

2.2.6.6. Man in the Middle

En el proceso de comunicación de datos, aunque los datos se han cifrado, existe la posibilidad de que otros puedan conocer dichos datos. Una posibilidad es que la persona intercepte el medio de comunicación utilizado por las dos personas que se están comunicando. Esta técnica se llama ataque de hombre en el medio.(Gutierrez Salazar Pablo, 2019)

2.2.6.7. CVE, CWE y NVD

Common Vulnerabilities and Exposures (CVE) es una página web que se encarga de recolectar las vulnerabilidades reportadas por la comunidad, es una de las más grandes a la fecha actual por lo que se encuentran miles de vulnerabilidades en los diferentes productos de software, cada una de estas vulnerabilidades al ser reportadas se les genera un ID el cual tiene la siguiente estructura. (*CVE - Common Vulnerabilities and Exposures (CVE)*, s. f.)

*Figura 4 Estructura del CVE ID (*CVE - Common Vulnerabilities and Exposures (CVE), *s. f.)*

National Vulnerability Database (NVD) tiene una estrecha relación con CVE dicha relación es que CVE alimenta la NVD esto quiere decir que cada vez que se crea un CVE ID se actualiza en la NVD con su puntuación de impacto y puntuación de severidad de manera más detallada, NVD también provee una búsqueda más personalizada como puede ser por producto, nombre de vendedor, tipo de vulnerabilidad, etc. (*NVD - Home*, s. f.)

Common Weakness and Exposures (CWE) se encarga de recolectar las debilidades en un determinado producto, CWE usa el CVE ID para encontrar las debilidades respecto a esa vulnerabilidad, estas debilidades están centradas en mayor medida a el código o el fragmento de código que genera la debilidad, proporciona ejemplos o posibles escenarios del código que puede tener dicha debilidad.(*CWE - Common Weakness Enumeration*, s. f.)

2.2.7. Clasificación de los hackers

2.2.7.1. Black Hat Hackers

Este tipo de atacantes penetran rompiendo los sistemas, con un interés personal y/o lucrativo. En este grupo se encuentran los crackers, que son los protagonistas del software pirata. Los crackers son por ejemplo los que le dieron origen a los virus, los troyanos y el spyware. (Gutiérrez Pablo, 2019)

2.2.7.2. White Hat Hackers

En el caso de los white hackers intentan ayudar a aseverar el sistema, no buscan sacar utilidad de manera ilícita. Analizan los sistemas informáticos para revelar vulnerabilidades aun sin conocer o aun sin publicar, los denominados 0 day exploit. En su mayoría los white hacker son profesionales que se especializan con el unico objetivo de proteger el sistema de las vulnerabilidades que van siendo descubiertas. (Gutiérrez Pablo, 2019)

2.2.7.3. Gray Hat Hackers

Es un hacker, que opera algunas veces con la actitud de un white hat, pero con una filosofía de divulgación diferente. Su propósito no es necesariamente malo, aunque es probable que de vez en cuando cometa algún delito.

Por ejemplo, puede intentar entrar ilegalmente en un sistema solo por curiosidad. Si ha encontrado un fallo, normalmente no buscara dañar el sistema. Sin embargo, el hecho de entrar en una red privada ajena y de la cual no tiene la propiedad o sin la aprobación de este es ilegal en la mayoría de los países. (Gutiérrez Pablo, 2019)

2.2.7.4. Script Kiddies

En este caso no son hacker ni personas capacitadas son individuos que recuperan los exploits publicados por los white hats en las herramientas públicas y los ejecutan en máquinas sin contemplar las consecuencias ni lo que implica ese exploit, los llamados mass-root. (Gutiérrez Pablo, 2019)

2.2.8. Tipos de Escenario de Pruebas

2.2.8.1. Black Box

En este caso, el hacker que audita el sistema sin poseer ninguna información del sistema ni sus activos. Actuará como si fuera un atacante real, probando diferentes técnicas y/o procesos en busca de una vulnerabilidad que pueda explotar. (Gutiérrez Pablo, 2019)

2.2.8.2. White Box

El que audita él tiene acceso total al sistema. Debido a esto, se tiene que experimentar cada servicio y activo, comprobar su configuración, así como sus posibles vulnerabilidades y realizar una revisión completa para avalar la seguridad en el sistema. (Gutiérrez Pablo, 2019)

2.2.8.3. Gray Box

El que audita el sistema posee información limitada. Este tipo de auditoría permite realizar otras pruebas teniendo en cuenta solo los activos que estén más expuestos, sin tener que averiguar toda la información. (Gutiérrez Pablo, 2019)

2.2.8.4. Metadatos

Los metadatos son la data de la data según Pomerantz esto se define de mejor manera diciendo que la metadata es un “objeto potencial de información que describe otro objeto potencial de información”, teniendo en cuenta que la data es solo “información potencial”. por ejemplo, cuando uno ve un libro no sabe lo que este contiene, pero si se el autor, resumen entre otros datos, estos datos son la metadata del libro.(Pomerantz Jeffrey, 2015)

Aplicada a la informática se vuelve un poco más complejo ya que todo lo que hacemos como software tiene metadata asociada por lo que puede llegar a ser un ciclo de metadata sin embargo en el ámbito de la seguridad de la información la metadata cumple un rol importante, siendo que la metadata del software en algunas ocasiones da más información de la que debería, esto lo pueden usar algunos atacantes como el punto de partida o u medio para el punto de partida. (Pomerantz Jeffrey, 2015)

2.2.9. Pentesting Standard

El Pentesting standard tiene siete procesos principales. Estos resguardan todo lo relacionado a una prueba de penetración: comenzando en la comunicación inicial y el razonamiento detrás de un pentesting, la recopilación de inteligencia y fases de modelado de amenazas.(The PTES Team, s. f.)

Las secciones del estándar pentesting son:

- **Interacciones preliminares**

  El objetivo de esta sección es presentar y declarar las herramientas y técnicas aprovechables que podrían usarse en la pentesting, previo al inicio de una prueba de penetración. La información dentro de esta sección es la consecuencia de muchos años de experiencia mezclada con algunos de los profesionales de pentesting más exitosos del mundo.

- **Recolección de información**

  Para la recolección de información se realiza un reconocimiento contra un objetivo para recopilar tanta información como sea posible, dicha información se utilizará al momento de explotar las vulnerabilidades en el objetivo durante las fases de evaluación de vulnerabilidad y explotación.

- **Modelado de amenazas**

  Esta sección define el enfoque de amenaza es decir hasta qué punto la organización está dispuesta a aceptar una amenaza y mitigar otra, en esta fase se responde a las preguntas siguientes:

  - ¿Qué activos son los más importantes?
  - ¿Qué comunicados de amenaza son más importantes?

  Esto permite que el tester pueda enfocarse en cumplir el compromiso y usar las herramientas y técnicas que mejor se ajusten al compromiso previamente establecido.

- **Análisis de Vulnerabilidades**

  El análisis de vulnerabilidades es el proceso de revelar fallas en sistemas y aplicaciones que pueden ser usadas por un agresor. Estas fallas pueden ser muy variadas, desde una configuración incorrecta del host y el servicio hasta el diseño de la aplicación.

  No obstante, el proceso manejado para buscar defectos varía y depende en gran medida del componente particular que se prueba, una vez completada esta fase debería de tenerse una lista de objetivos de alto valor, esta lista será usada para la fase siguiente permitiendo enfocarse en lo que impactara en mayor medida a la empresa.

- **Explotación**

  La fase de explotación se concentra únicamente en crear un punto de acceso a un sistema o recurso evitando la seguridad instalada. Si la fase del análisis de vulnerabilidades se realizó correctamente, esta fase debería estar bien planeada y el ataque debería ser preciso, es decir la explotación de la vulnerabilidad debería estar controlada y sin efectos adversos.

  El enfoque principal es asemejar un punto de entrada a la organización para identificar los activos que sean de un valor alto para la organización, el vector de ata que se use debe ser el que tenga mayor tasa de éxito e impacto en la organización.

- **Post Explotación**

  El propósito de la fase post explotación es comprobar el valor de la máquina envuelta y mantener bajo control la máquina para uso posterior.

  El valor de una máquina está dado por la sensibilidad de los datos almacenados en esta y la utilidad de estos para comprometer aún más dispositivos en la red. Esta fase está destinada a ayudar al tester a identificar y evidenciar datos confidenciales, identificar archivos de configuración, canales de comunicación y relaciones con otros dispositivos de red.

- **Reporte**

  Esta sección se comunicará al contratista, los objetivos específicos y los resultados de la prueba de penetración.

  La audiencia prevista será con aquellos individuos que estén encargados de la supervisión y visión estratégica del programa de seguridad en la organización, así como cualquier miembro de la organización que pueda percibir afectado por las identificadas y/o confirmadas amenazas. (The PTES Team, s. f.)

2.2.10. Metodología NIST-SP 800-30

NIST por sus siglas en ingles es National Institute of Standards and Technology es parte del ministerio de Comercio de Estados Unidos, está encargada de proporcionar estándares, la serie SP 800 sobre la seguridad de la información, en esta serie se encuentra la SP 800-30 está estándar en particular presenta una metodología para la evaluación de riesgos, de esta metodología se usara el paso dos en el trabajo de investigación ya que esta comprende la evaluación de riesgos, los pasos de la metodología se describen a continuación. (Joint Task Force Transformation Initiative, 2012)

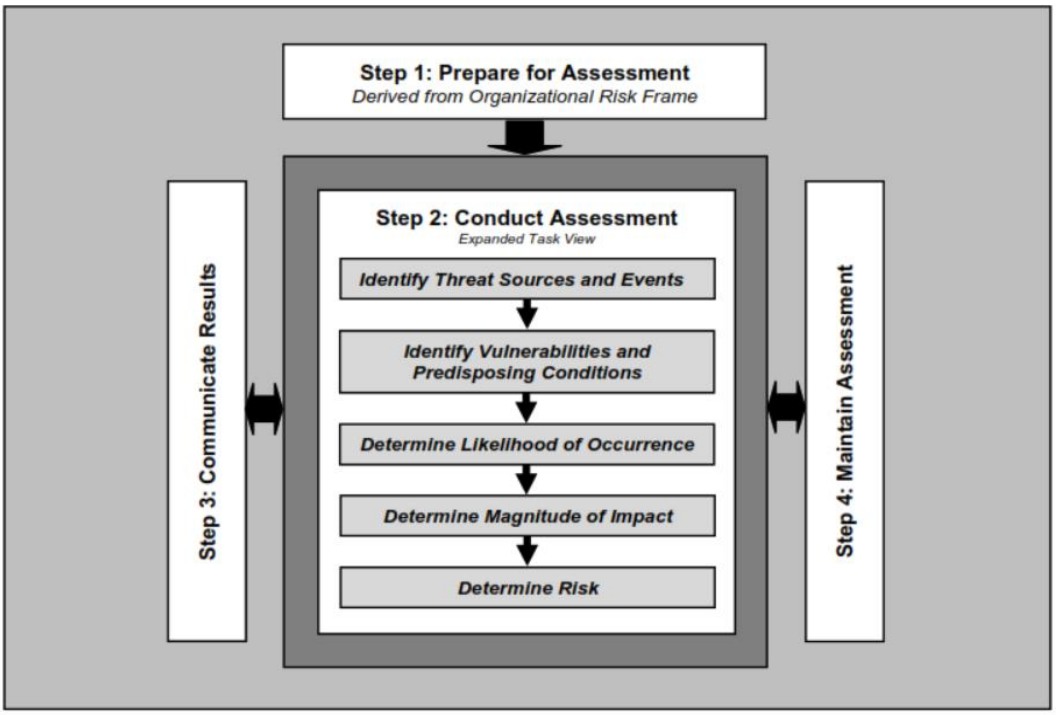


Figura 5 Proceso de la Evaluación de Riesgos (Joint Task Force Transformation Initiative, 2012)

2.2.10.1. Jerarquía de la administración de riesgos

La jerarquía de administración de riesgos fue definida en NIST SP 800-39, el cual provee múltiples perspectivas de riesgos desde el nivel estratégico hasta el nivel táctico en la **Figura 6** se observa una imagen referencial y como se trata la jerarquía en NIST SP 800-30.

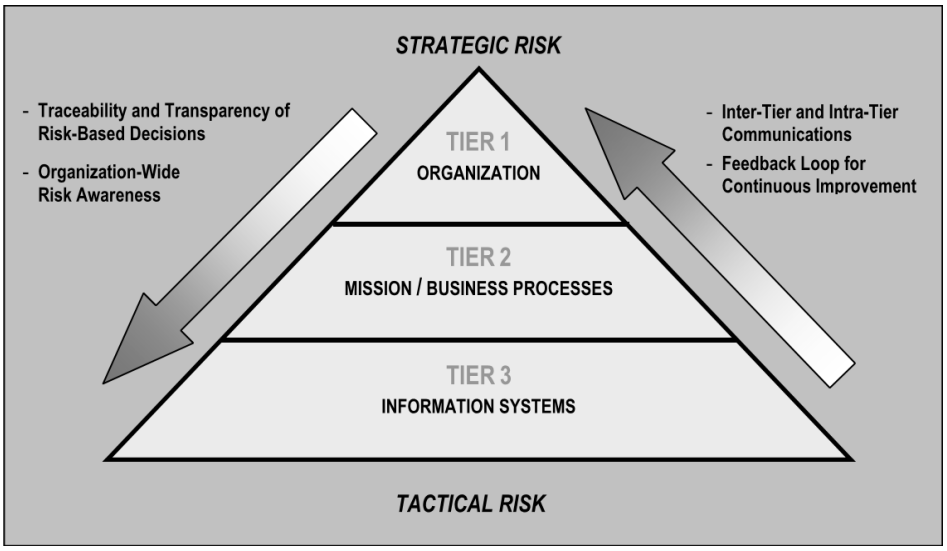


Figura 6 Jerarquía de administración de riesgos (Joint Task Force Transformation Initiative, 2012)

En el tier 1, la evaluación de riesgos puede afectar, por ejemplo:

1. Programas, políticas, procedimientos y orientaciones de seguridad de la información en toda la organización.
2. Los tipos de respuestas adecuadas al riesgo.
3. Decisión de inversión para tecnologías de información.
4. Adquisiciones.

En el tier 2, la evaluación de riesgos puede afectar, por ejemplo:

1. Las decisiones de diseño de la arquitectura empresarial/de seguridad.
2. la selección de proveedores, servicios y contratistas para apoyar la selección de proveedores, servicios y contratistas para apoyar las misiones y funciones de la organización.

En el tier 3, la evaluación de riesgos puede afectar, por ejemplo:

1. Las decisiones de diseño (incluida la selección, adaptación y complementación de los controles de seguridad y la selección de productos de tecnología de la información para los sistemas de información de la organización) de la tecnología de la información para los sistemas de información de la organización.
2. Las decisiones de implementación (incluyendo si los productos de tecnología de la información o las configuraciones de los productos cumplen con los requisitos de control de seguridad).
3. Decisiones operativas (incluyendo el nivel requerido de actividad de supervisión, la frecuencia de las autorizaciones continuas del sistema de información, y las decisiones de mantenimiento del sistema).

2.2.10.2. Prepararse para la evaluación:

Primer se preparará la información requerida para la valoración, este paso busca establecer un contexto para la evaluación de riesgos.

La elaboración de una evaluación de riesgos contiene las siguientes tareas:

- Identificacion del designio de la evaluación.
- Identificacion de la importancia de la evaluación.
- Identificacion de los supuestos y limitaciones relacionado con la evaluación.
- Identificacion de las fuentes de información que se manejarán como insumos para la valoración.
- Identificacion del modelo de riesgo y los enfoques analíticos (es decir, enfoques de evaluación y análisis) para ser usado durante la valoración.

2.2.10.3. Conducir la Evaluación de Riesgos

El segundo paso en el proceso de evaluación de riesgos es el que se usara en el trabajo de investigación. El objetivo de este paso es obtener una lista de riesgos que puedan priorizarse por nivel de riesgo y usarse para informar las decisiones. Para lograr esto, la organización deberá analizar las amenazas, vulnerabilidades, impactos, probabilidades y la incertidumbre asociada con la evaluación de riesgos.(Joint Task Force Transformation Initiative, 2012)

La perspectiva para la evaluación de riesgos es cubrir apropiadamente todo el espacio de amenaza siguiendo los esclarecimientos específicos, orientación y dirección establecidas durante el paso de preparación.

La realización de conducir la evaluación de riesgos incluye las siguientes tareas:

- Identificacion de las fuentes de amenazas que son distinguidas para las organizaciones y nivelar eventos de amenaza que podrían ser producidos por esas fuentes.
- Identificacion de vulnerabilidades dentro de las organizaciones que tienen una posibilidad de ser explotadas por fuentes de amenazas mediante eventos de amenazas y las condiciones predisponentes que podrían afectar de manera positiva o negativa la explotación exitosa.
- Determinación de la probabilidad que las fuentes de amenaza reconocidas inicien eventos de amenaza y la posibilidad de que los eventos de amenaza resulten en exitosos.
- Determinación de los impactos adversos para las operaciones y los activos de la organización, individuos y otras organizaciones tales como el resultado de la explotación de vulnerabilidades por fuentes de amenazas.
- Determinación de los riesgos de seguridad de la información como una mezcla de probabilidad de explotación, vulnerabilidades y impacto resultante de la explotación, incluidas las incertidumbres coligadas con la determinación de riesgos.

2.2.10.4. Comunicar y Compartir Información de Evaluación de Riesgos

En este paso se comunican los resultados de la evaluación, así como compartir información relacionada con los riesgos identificados.
El fin de este paso es certificar que los responsables de la toma de decisiones en toda la organización estén informados de manera que puedan tomar medidas correctivas o no referentes a los riesgos. (Joint Task Force Transformation Initiative, 2012)

La comunicación de información manifiesta de las siguientes tareas:

- Comunicación de los resultados de la evaluación de riesgos.
- Compartir la información resultante en la ejecución de la evaluación de riesgos, para apoyar otras actividades de gestión de riesgos.

2.2.10.5. Mantenimiento de la Evaluación de Riesgos

En este paso busca mantener actualizado el conocimiento resultante de la evaluación de riesgos. Los resultados de las evaluaciones de riesgos comunican las decisiones de gestión de riesgos y guían las respuestas correctas a los riesgos. Para proteger la revisión continua de las decisiones, las organizaciones conservan evaluaciones de riesgos para unir cualquier cambio detectado a través del monitoreo de riesgos. (Joint Task Force Transformation Initiative, 2012)

El monitoreo de los riesgos suministra a las organizaciones los medios necesarios para mantener una comunicación de manera continua:

- Determinación de la efectividad de las respuestas al riesgo.
- Identificacion de los cambios que afectan al riesgo en los sistemas de información organizacional y ambientes en los que operan esos sistemas
- Verificación del cumplimiento.

El mantenimiento de las evaluaciones de riesgos incluye las siguientes tareas:

- Monitoreo de los factores de riesgo identificados previamente de manera continua y comprender los cambios posteriores a esos factores

- Actualización de los componentes de las evaluaciones de riesgos que reflejan las actividades de monitoreo llevadas a cabo por las organizaciones.

2.2.11. Facturación Electrónica

Una factura es un tipo de comprobante de pago, el cual es emitido por una empresa a través de un sistema programado por la misma empresa o un software de terceros que se encargara de la facturación de la empresa, el sistema debe de emitir a su vez las Notas de Débito y Crédito vinculadas a la Factura Electrónica. (*Factura Electrónica - ¿Qué es la factura electrónica ?*, s. f.)

Características:

- La emisión se realiza desde un software especializado, por lo que no es necesario a ingresar a la web de la SUNAT, sin embargo, se debe verificar fiabilidad del sistema.
- Es un documento electrónico que tiene todos los efectos tributarios una factura, es decir funciona de igual manera que una factura tradicional, por lo que con tiene los datos necesarios como son: sustenta costo, gasto, crédito fiscal para efectos tributarios.
- La serie de una factura electrónica siempre empezara por la letra F.
- La numeración de una factura electrónica es correlativa e independiente a la numeración de la factura física.

CAPITULO 3 - Desarrollo de la propuesta de Evaluación de Riesgos en el Sistema IFacturacion.

Para el desarrollo de la propuesta de Evaluación de Riesgos en el Sistema IFacturacion, se hizo uso de las Metologias NIST SP 800-30, Pentesting standard y NTP ISO/IEC 27001:2008, dichas metodologías se usaron dependiendo de la fase en la cual se encuentre la propuesta, es decir en cada fase se usó una metodologia base que servirá para guiar la fase a su vez se usaron pautas proporcionadas por la otra metodologia reforzando de esta manera el resultado de la fase, para definir las fases se creó el siguiente modelo.

Definir el uso de las Metodologías de Seguridad de la Informacion en la propuesta

Para definir el uso de metodologías se creó la

Figura 7 en la que se representa todas las fases que se seguirá a lo largo de la investigación y se también se define cuál de las metodologías se usará en cada fase.

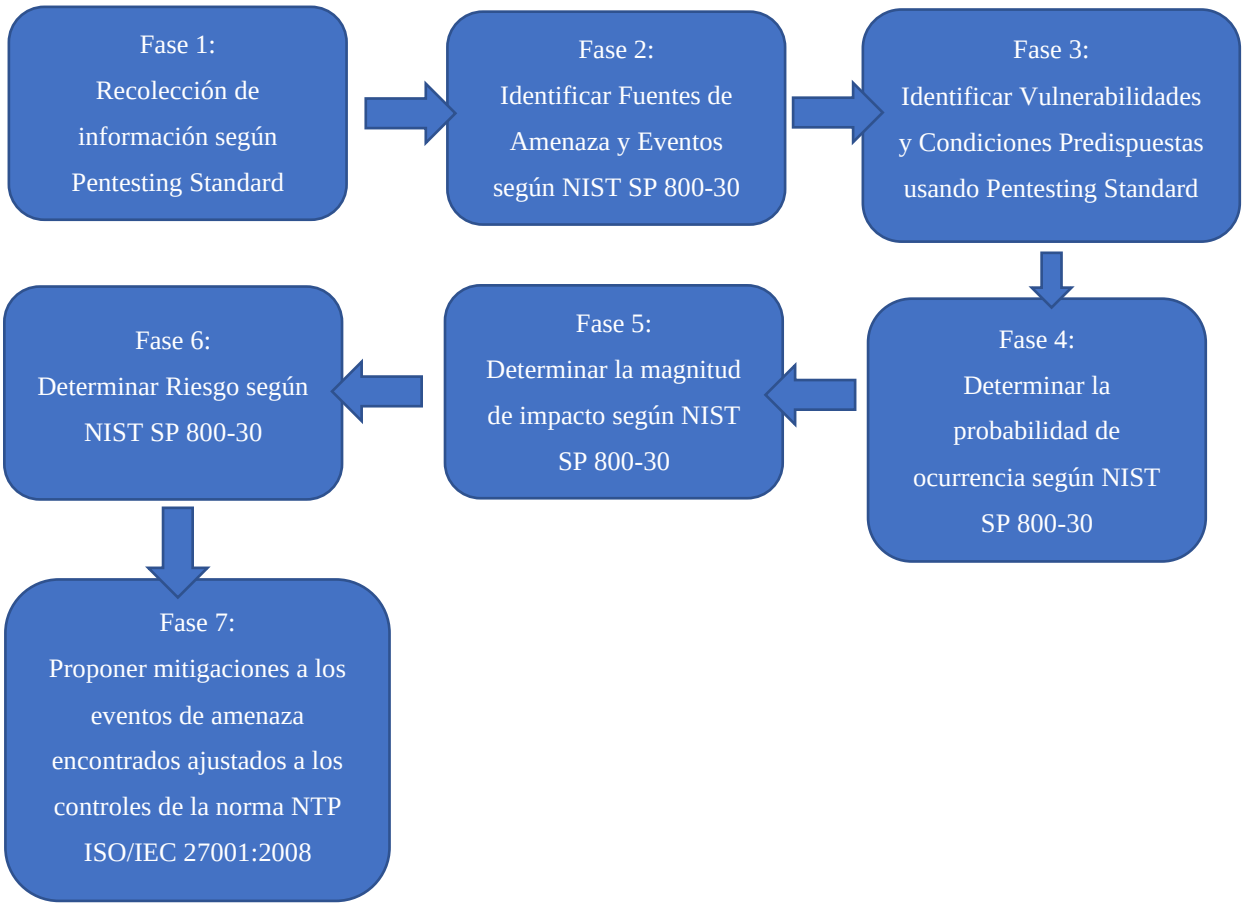


Figura 7 Definir fases para la propuesta
Fuente: Elaboración propia

Cabe señalar que, en el caso de la metodologia NIST SP 800-30 se siguió las partes referidas al tier 3 de la pirámide ofrecida por la metodologia, debido a que el tier 3 ofrece las pautas necesarias para sistemas de información.

3.1. Primera Fase – Recolección de Informacion.

Se usó la primera etapa del Pentesting al sistema IFacturacion con el objetivo de identificar las fuentes de amenazas que puedan existir en el sistema, siguiendo con la metodologia de Pentesting Standard.

3.1.1. Análisis de Trafico con WireShark

Para empezar la recolección de información la metodologia nos sugiere usar OSINT (Open Source Intelligence), el cual tiene tres formas: Recolección de Información Pasiva, Recolección de Información Semi-Pasiva, Recolección de Información Activa, para el caso de la propuesta se usara la recolección de información activa ya que permitirá obtener información relevante en un sistema desktop, para empezar se examinaron los puertos que se usan generalmente para la comunicación de diferentes protocolos como son los puertos: 21, 80, 443, etc.

En la Figura 8 se muestra que el análisis de tráfico del protocolo FTP que usa el puerto 21, tiene un usuario y una contraseña, como también el directorio raíz y el directorio al que realiza la consulta, por último, nos indica que el servidor FTP está en modo pasivo. En la Figura 9 se muestra el análisis de tráfico del protocolo HTTP que usa el puerto 80, en el cual se puede ver una consulta GET que tiene como host la SUNAT, así como el formato de archivo x-ms-application consultado. En la Figura 10 se muestra el análisis de tráfico del protocolo HTTPS que usa el puerto 443, en este caso no se puedo observar mucho más allá de las repuestas ACK del servidor ya que la mayoría de los datos están encriptados por el protocolo criptográfico TLSv1.2. En las Figuras 10,11,12 y 13 se puede observar el Trafico TCP Stream obtenido por WireShark, dichos flujos de tráfico contienen datos relacionados con el sistema sin embargo la mayoría de estos datos están encriptados

con encriptación asimétrica es decir tienen una llave publica y una privada para la desencriptación, por lo que en su mayoría deberían ser datos ilegibles.

tcp.port == 21

No.	Time	Source	Destination	Protocol	Length	Info
1972	38.113003	192.168.1.8	184.168.152.2	TCP	66	52587 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1975	38.268601	184.168.152.2	192.168.1.8	TCP	66	21 → 52587 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
1976	38.268667	192.168.1.8	184.168.152.2	TCP	54	52587 → 21 [ACK] Seq=1 Ack=1 Win=262656 Len=0
1978	38.426304	184.168.152.2	192.168.1.8	FTP	81	Response: 220 Microsoft FTP Service
1979	38.426758	192.168.1.8	184.168.152.2	FTP	71	Request: USER [redacted]
1980	38.590485	184.168.152.2	192.168.1.8	FTP	93	Response: 331 Password required for facemusica.
1981	38.590595	192.168.1.8	184.168.152.2	FTP	73	Request: PASS [redacted]
1982	38.945824	184.168.152.2	192.168.1.8	TCP	60	21 → 52587 [ACK] Seq=67 Ack=37 Win=65536 Len=0
1993	39.788596	184.168.152.2	192.168.1.8	FTP	124	Response: 230-FTP-SSL (AUTH TLS, Explicit FTPS or FTPES) security is available
1994	39.788653	184.168.152.2	192.168.1.8	FTP	75	Response: 230 User logged in.
1995	39.788671	192.168.1.8	184.168.152.2	TCP	54	52587 → 21 [ACK] Seq=37 Ack=158 Win=262400 Len=0
1996	39.788711	192.168.1.8	184.168.152.2	FTP	68	Request: OPTS utf8 on
1997	39.963702	184.168.152.2	192.168.1.8	FTP	112	Response: 200 OPTS UTF8 command successful - UTF8 encoding now ON.
1998	39.963816	192.168.1.8	184.168.152.2	FTP	59	Request: PWD
1999	40.120497	184.168.152.2	192.168.1.8	FTP	85	Response: 257 "/" is current directory.
2000	40.120611	192.168.1.8	184.168.152.2	FTP	62	Request: TYPE I
2001	40.283250	184.168.152.2	192.168.1.8	FTP	74	Response: 200 Type set to I.
2002	40.283360	192.168.1.8	184.168.152.2	FTP	60	Request: PASV
2003	40.440878	184.168.152.2	192.168.1.8	FTP	106	Response: 227 Entering Passive Mode (184,168,152,2,196,232).
2005	40.482768	192.168.1.8	184.168.152.2	TCP	54	52587 → 21 [ACK] Seq=70 Ack=319 Win=262400 Len=0
2008	40.606692	192.168.1.8	184.168.152.2	FTP	103	Request: RETR /Palerp/CERTIFICADOS/MPS20191201133400.pfx
2009	40.785328	184.168.152.2	192.168.1.8	FTP	103	Response: 550 The system cannot find the file specified.
2010	40.787648	192.168.1.8	184.168.152.2	TCP	54	52587 → 21 [FIN, ACK] Seq=119 Ack=368 Win=262400 Len=0
2022	40.959444	184.168.152.2	192.168.1.8	TCP	60	21 → 52587 [ACK] Seq=368 Ack=120 Win=65536 Len=0
2023	40.959472	184.168.152.2	192.168.1.8	TCP	60	21 → 52587 [FIN, ACK] Seq=368 Ack=120 Win=65536 Len=0
2024	40.959496	192.168.1.8	184.168.152.2	TCP	54	52587 → 21 [ACK] Seq=120 Ack=369 Win=262400 Len=0

```
> Frame 2024: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{8A546A8B-440D-425A-BE81-756BF9688FE8}, id 0
> Ethernet II, Src: ASUSTekC_5c:e7:ac (24:4b:fe:5c:e7:ac), Dst: HonHaiPr_dd:83:9f (18:4f:32:dd:83:9f)
> Internet Protocol Version 4, Src: 192.168.1.8, Dst: 184.168.152.2
> Transmission Control Protocol, Src Port: 52587, Dst Port: 21, Seq: 120, Ack: 369, Len: 0
```

```
0000  18 4f 32 dd 83 9f 24 4b  fe 5c e7 ac 08 00 45 00   ·O2···$K ·\····E·
0010  00 28 7b 12 40 00 80 06  00 00 c0 a8 01 08 b8 a8   ·({·@··· ········
0020  98 02 cd 6b 00 15 52 85  e6 b3 c8 c6 34 66 50 10   ···k··R· ····4fP·
0030  04 01 12 76 00 00                                 ···v··
```

Figura 8 Filtrado del Puerto 21 en el proceso de login

tcp.port == 80 || udp.port == 80

No.	Time	Source	Destination	Protocol	Length	Info
16	5.782984	192.155.108.5	192.168.1.8	TCP	60	80 → 50549 [ACK] Seq=1 Ack=1 Win=501 Len=0
17	5.783019	192.168.1.8	192.155.108.5	TCP	54	[TCP ACKed unseen segment] 50549 → 80 [ACK] Seq=1 Ack=2 Win=1024 Len=0
1010	14.847791	192.168.1.8	184.168.152.2	TCP	66	52565 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1028	15.002128	184.168.152.2	192.168.1.8	TCP	66	80 → 52565 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
1029	15.002200	192.168.1.8	184.168.152.2	TCP	54	52565 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
1030	15.002968	192.168.1.8	184.168.152.2	HTTP	192	GET /palerp/fact/eFacturacion/PALERPinterfaz.application HTTP/1.1
1080	15.177369	184.168.152.2	192.168.1.8	TCP	1514	80 → 52565 [ACK] Seq=1 Ack=139 Win=65536 Len=1460 [TCP segment of a reassembled PDU]
1081	15.177681	184.168.152.2	192.168.1.8	TCP	1514	80 → 52565 [ACK] Seq=1461 Ack=139 Win=65536 Len=1460 [TCP segment of a reassembled PDU]
1082	15.177697	192.168.1.8	184.168.152.2	TCP	54	52565 → 80 [ACK] Seq=139 Ack=2921 Win=262656 Len=0
1084	15.332746	184.168.152.2	192.168.1.8	TCP	1514	80 → 52565 [ACK] Seq=2921 Ack=139 Win=65536 Len=1460 [TCP segment of a reassembled PDU]
1085	15.333058	184.168.152.2	192.168.1.8	TCP	1514	80 → 52565 [ACK] Seq=4381 Ack=139 Win=65536 Len=1460 [TCP segment of a reassembled PDU]
1086	15.333058	184.168.152.2	192.168.1.8	HTTP	598	HTTP/1.1 200 OK (application/x-ms-application)
1087	15.333076	192.168.1.8	184.168.152.2	TCP	54	52565 → 80 [ACK] Seq=139 Ack=6385 Win=262656 Len=0
1117	16.019843	192.155.108.5	192.168.1.8	TCP	60	[TCP Dup ACK 16#1] 80 → 50549 [ACK] Seq=1 Ack=1 Win=501 Len=0
1118	16.019879	192.168.1.8	192.155.108.5	TCP	54	[TCP Dup ACK 17#1] [TCP ACKed unseen segment] 50549 → 80 [ACK] Seq=1 Ack=2 Win=1024 Len=0
1509	26.259259	192.155.108.5	192.168.1.8	TCP	60	[TCP Dup ACK 16#2] 80 → 50549 [ACK] Seq=1 Ack=1 Win=501 Len=0
1510	26.259272	192.168.1.8	192.155.108.5	TCP	54	[TCP Dup ACK 17#2] [TCP ACKed unseen segment] 50549 → 80 [ACK] Seq=1 Ack=2 Win=1024 Len=0
1556	27.159721	192.168.1.8	200.60.136.89	TCP	55	52504 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=1
1568	27.251746	192.168.1.8	23.211.233.221	TCP	55	52511 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=1
1649	29.382787	192.168.1.8	192.155.108.5	TCP	55	[TCP Keep-Alive] [TCP ACKed unseen segment] 50549 → 80 [ACK] Seq=0 Ack=2 Win=1024 Len=1
1650	29.557519	192.155.108.5	192.168.1.8	TCP	66	[TCP Previous segment not captured] 80 → 50549 [ACK] Seq=2 Ack=1 Win=501 Len=0 SLE=0 SRE=1
1753	36.407898	192.168.1.8	161.132.21.8	TCP	66	52584 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
1754	36.437355	161.132.21.8	192.168.1.8	TCP	66	80 → 52584 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 WS=1 SACK_PERM=1
1755	36.437411	192.168.1.8	161.132.21.8	TCP	54	52584 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
1756	36.437847	192.168.1.8	161.132.21.8	HTTP	437	GET /cl-at-ittipcam/tcS01Alias?anho=2020&mes=10 HTTP/1.1
1757	36.462256	161.132.21.8	192.168.1.8	TCP	60	80 → 52584 [ACK] Seq=1 Ack=384 Win=14983 Len=0

```
> Frame 2933: 1502 bytes on wire (12016 bits), 1502 bytes captured (12016 bits) on interface \Device\NPF_{8A546A8B-440D-425A-BE81-756BF9688FE8}, id 0
> Ethernet II, Src: HonHaiPr_dd:83:9f (18:4f:32:dd:83:9f), Dst: ASUSTekC_5c:e7:ac (24:4b:fe:5c:e7:ac)
> Internet Protocol Version 4, Src: 8.36.80.212, Dst: 192.168.1.8
v Transmission Control Protocol, Src Port: 80, Dst Port: 52597, Seq: 20273, Ack: 140, Len: 1448
    Source Port: 80
    Destination Port: 52597
    [Stream index: 128]
    [TCP Segment Len: 1448]
```

Figura 9 Filtrado del Puerto 80 en el proceso de login

tcp.port == 443

No.	Time	Source	Destination	Protocol	Length	Info
7	1.946766	192.168.1.8	96.6.194.117	TCP	55	52513 → 443 [ACK] Seq=1 Ack=1 Win=1024 Len=1 [TCP segment of a reassembled PDU]
8	2.119796	192.168.1.8	69.192.141.221	TCP	55	52494 → 443 [ACK] Seq=1 Ack=1 Win=1026 Len=1 [TCP segment of a reassembled PDU]
9	2.134745	192.168.1.8	23.222.24.138	TCP	55	52510 → 443 [ACK] Seq=1 Ack=1 Win=1024 Len=1 [TCP segment of a reassembled PDU]
10	2.213767	192.168.1.8	13.35.109.62	TCP	55	52524 → 443 [ACK] Seq=1 Ack=1 Win=1026 Len=1 [TCP segment of a reassembled PDU]
11	2.244748	192.168.1.8	23.54.149.245	TCP	55	52493 → 443 [ACK] Seq=1 Ack=1 Win=1024 Len=1 [TCP segment of a reassembled PDU]
12	2.302613	13.35.109.62	192.168.1.8	TCP	66	443 → 52524 [ACK] Seq=1 Ack=2 Win=123 Len=0 SLE=1 SRE=2
13	2.322760	192.168.1.8	23.83.76.35	TCP	55	52487 → 443 [ACK] Seq=1 Ack=1 Win=1023 Len=1 [TCP segment of a reassembled PDU]
14	4.304851	192.168.1.8	52.109.112.91	TLSv1.2	89	Application Data
15	4.732191	52.109.112.91	192.168.1.8	TCP	60	443 → 51036 [ACK] Seq=1 Ack=36 Win=1024 Len=0
18	5.834393	162.159.133.234	192.168.1.8	TLSv1.2	171	Application Data
19	5.890331	192.168.1.8	162.159.133.234	TCP	54	51139 → 443 [ACK] Seq=1 Ack=118 Win=1025 Len=0
20	7.021115	192.168.1.8	35.186.224.47	TLSv1.2	97	Application Data
21	7.068786	192.168.1.8	192.16.58.25	TCP	55	52508 → 443 [ACK] Seq=1 Ack=1 Win=1024 Len=1 [TCP segment of a reassembled PDU]
22	7.068838	192.168.1.8	54.145.39.178	TCP	55	52495 → 443 [ACK] Seq=1 Ack=1 Win=1024 Len=1 [TCP segment of a reassembled PDU]
23	7.084735	192.168.1.8	68.67.161.206	TCP	55	52491 → 443 [ACK] Seq=1 Ack=1 Win=63951 Len=1 [TCP segment of a reassembled PDU]
24	7.084736	192.168.1.8	54.236.73.186	TCP	55	52519 → 443 [ACK] Seq=1 Ack=1 Win=1024 Len=1 [TCP segment of a reassembled PDU]
25	7.084766	192.168.1.8	3.23.83.219	TCP	55	52496 → 443 [ACK] Seq=1 Ack=1 Win=1024 Len=1 [TCP segment of a reassembled PDU]
26	7.084850	35.186.224.47	192.168.1.8	TCP	60	443 → 50579 [ACK] Seq=1 Ack=44 Win=267 Len=0
27	7.101738	192.168.1.8	54.86.139.136	TCP	55	52518 → 443 [ACK] Seq=1 Ack=1 Win=1026 Len=1 [TCP segment of a reassembled PDU]
28	7.239140	35.186.224.47	192.168.1.8	TLSv1.2	94	Application Data
29	7.280607	162.159.133.234	192.168.1.8	TLSv1.2	106	Application Data
30	7.291781	192.168.1.8	35.186.224.47	TCP	54	50579 → 443 [ACK] Seq=44 Ack=41 Win=1023 Len=0
31	7.323798	192.168.1.8	162.159.133.234	TCP	54	51139 → 443 [ACK] Seq=1 Ack=170 Win=1024 Len=0
32	7.804627	192.168.1.8	204.79.197.200	TLSv1.2	124	Application Data
33	7.859442	192.168.1.8	204.79.197.200	TLSv1.2	1385	Application Data
34	7.859504	192.168.1.8	204.79.197.200	TLSv1.2	127	Application Data

> Frame 8582: 276 bytes on wire (2208 bits), 276 bytes captured (2208 bits) on interface \Device\NPF_{8A546A8B-440D-425A-BE81-756BF9688FE8}, id 0
> Ethernet II, Src: ASUSTekC_5c:e7:ac (24:4b:fe:5c:e7:ac), Dst: HonHaiPr_dd:83:9f (18:4f:32:dd:83:9f)
> Internet Protocol Version 4, Src: 192.168.1.8, Dst: 52.184.213.21
> Transmission Control Protocol, Src Port: 52607, Dst Port: 443, Seq: 1, Ack: 1, Len: 222
> Transport Layer Security

Figura 10 Filtrado del Puerto 443 en el proceso de login

tcp.stream eq 65

No.	Time	Source	Destination	Protocol	Length	Info
1354	20.564904	192.168.1.8	190.119.206.197	TCP	66	52572 → 1433 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1359	20.616881	190.119.206.197	192.168.1.8	TCP	66	1433 → 52572 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
1360	20.616928	192.168.1.8	190.119.206.197	TCP	54	52572 → 1433 [ACK] Seq=1 Ack=1 Win=262656 Len=0
1361	20.621802	192.168.1.8	190.119.206.197	TDS	148	TDS7 pre-login message
1362	20.675818	190.119.206.197	192.168.1.8	TDS	108	Response
1363	20.677187	192.168.1.8	190.119.206.197	TDS	237	TDS7 pre-login message
1364	20.732817	190.119.206.197	192.168.1.8	TDS	1238	TDS7 pre-login message
1365	20.733807	192.168.1.8	190.119.206.197	TDS	155	TDS7 pre-login message
1366	20.787567	190.119.206.197	192.168.1.8	TDS	113	TDS7 pre-login message
1367	20.791152	192.168.1.8	190.119.206.197	TDS	432	TLS exchange
1368	20.842820	190.119.206.197	192.168.1.8	TDS	564	Response
1369	20.849658	192.168.1.8	190.119.206.197	TDS	280	Remote Procedure Call
1370	20.910613	190.119.206.197	192.168.1.8	TDS	784	Response
1371	20.911880	192.168.1.8	190.119.206.197	TDS	161	Remote Procedure Call
1372	20.963171	190.119.206.197	192.168.1.8	TCP	1514	1433 → 52572 [ACK] Seq=2538 Ack=1090 Win=64512 Len=1460 [TCP segment of a reassembled PDU]
1373	20.963494	190.119.206.197	192.168.1.8	TCP	1514	1433 → 52572 [ACK] Seq=3998 Ack=1090 Win=64512 Len=1460 [TCP segment of a reassembled PDU]
1374	20.963494	190.119.206.197	192.168.1.8	TCP	1514	1433 → 52572 [ACK] Seq=5458 Ack=1090 Win=64512 Len=1460 [TCP segment of a reassembled PDU]
1375	20.963515	192.168.1.8	190.119.206.197	TCP	54	52572 → 1433 [ACK] Seq=1090 Ack=6918 Win=262656 Len=0
1376	20.963715	190.119.206.197	192.168.1.8	TCP	1514	1433 → 52572 [ACK] Seq=6918 Ack=1090 Win=64512 Len=1460 [TCP segment of a reassembled PDU]
1377	20.963715	190.119.206.197	192.168.1.8	TCP	1514	1433 → 52572 [ACK] Seq=8378 Ack=1090 Win=64512 Len=1460 [TCP segment of a reassembled PDU]
1378	20.963728	192.168.1.8	190.119.206.197	TCP	54	52572 → 1433 [ACK] Seq=1090 Ack=9838 Win=262656 Len=0
1379	20.963926	190.119.206.197	192.168.1.8	TDS	754	Response (Not last buffer)
1380	20.963933	192.168.1.8	190.119.206.197	TCP	54	52572 → 1433 [ACK] Seq=1090 Ack=10538 Win=261888 Len=0
1381	20.964131	190.119.206.197	192.168.1.8	TDS	1454	Response
1382	21.004747	192.168.1.8	190.119.206.197	TCP	54	52572 → 1433 [ACK] Seq=1090 Ack=11938 Win=262656 Len=0
2266	50.969698	192.168.1.8	190.119.206.197	TCP	55	[TCP Keep-Alive] 52572 → 1433 [ACK] Seq=1089 Ack=11938 Win=262656 Len=1

> Frame 1354: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{8A546A8B-440D-425A-BE81-756BF9688FE8}, id 0
> Ethernet II, Src: ASUSTekC_5c:e7:ac (24:4b:fe:5c:e7:ac), Dst: HonHaiPr_dd:83:9f (18:4f:32:dd:83:9f)
> Internet Protocol Version 4, Src: 192.168.1.8, Dst: 190.119.206.197
> Transmission Control Protocol, Src Port: 52572, Dst Port: 1433, Seq: 0, Len: 0

Figura 11 Filtrado de Flujo TCP Stream 65

tcp.stream eq 79

No.	Time	Source	Destination	Protocol	Length	Info
1598	27.898105	192.168.1.8	190.119.206.197	TCP	66	52580 → 1433 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1599	27.946395	190.119.206.197	192.168.1.8	TCP	66	1433 → 52580 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
1600	27.946458	192.168.1.8	190.119.206.197	TCP	54	52580 → 1433 [ACK] Seq=1 Ack=1 Win=262656 Len=0
1601	27.946609	192.168.1.8	190.119.206.197	TDS	148	TDS7 pre-login message
1602	28.001017	190.119.206.197	192.168.1.8	TDS	108	Response
1603	28.001254	192.168.1.8	190.119.206.197	TDS	236	TDS7 pre-login message
1604	28.057839	190.119.206.197	192.168.1.8	TDS	1238	TDS7 pre-login message
1605	28.058751	192.168.1.8	190.119.206.197	TDS	155	TDS7 pre-login message
1606	28.112316	190.119.206.197	192.168.1.8	TDS	113	TDS7 pre-login message
1607	28.112684	192.168.1.8	190.119.206.197	TDS	434	TLS exchange
1608	28.166925	190.119.206.197	192.168.1.8	TDS	572	Response
1609	28.167156	192.168.1.8	190.119.206.197	TDS	308	Remote Procedure Call
1610	28.249924	190.119.206.197	192.168.1.8	TCP	60	1433 → 52580 [ACK] Seq=1816 Ack=1012 Win=64768 Len=0
1611	28.316319	190.119.206.197	192.168.1.8	TDS	744	Response
1612	28.316515	192.168.1.8	190.119.206.197	TDS	154	Remote Procedure Call
1613	28.379782	190.119.206.197	192.168.1.8	TDS	155	Response
1616	28.422766	192.168.1.8	190.119.206.197	TCP	54	52580 → 1433 [ACK] Seq=1112 Ack=2607 Win=261888 Len=0
1633	28.640866	192.168.1.8	190.119.206.197	TDS	175	Remote Procedure Call
1635	28.696402	190.119.206.197	192.168.1.8	TDS	954	Response[Malformed Packet]
1637	28.751751	192.168.1.8	190.119.206.197	TCP	54	52580 → 1433 [ACK] Seq=1233 Ack=3507 Win=262656 Len=0
1709	32.225202	192.168.1.8	190.119.206.197	TDS	174	Remote Procedure Call
1711	32.284169	190.119.206.197	192.168.1.8	TDS	633	Response[Malformed Packet]
1712	32.284617	192.168.1.8	190.119.206.197	TDS	174	Remote Procedure Call
1713	32.337726	190.119.206.197	192.168.1.8	TDS	633	Response[Malformed Packet]
1714	32.391753	192.168.1.8	190.119.206.197	TCP	54	52580 → 1433 [ACK] Seq=1473 Ack=4665 Win=261632 Len=0
1725	35.842294	192.168.1.8	190.119.206.197	TDS	174	Remote Procedure Call

```
> Frame 1601: 148 bytes on wire (1184 bits), 148 bytes captured (1184 bits) on interface \Device\NPF_{8A546A8B-440D-425A-BE81-756BF9688FE8}, id 0
> Ethernet II, Src: ASUSTekC_5c:e7:ac (24:4b:fe:5c:e7:ac), Dst: HonHaiPr_dd:83:9f (18:4f:32:dd:83:9f)
> Internet Protocol Version 4, Src: 192.168.1.8, Dst: 190.119.206.197
> Transmission Control Protocol, Src Port: 52580, Dst Port: 1433, Seq: 1, Ack: 1, Len: 94
> Tabular Data Stream
```

Figura 12 Filtrado de Flujo TCP Stream 79

tcp.stream eq 80

No.	Time	Source	Destination	Protocol	Length	Info
1614	28.381326	192.168.1.8	190.119.206.197	TCP	66	52581 → 1433 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1617	28.432117	190.119.206.197	192.168.1.8	TCP	66	1433 → 52581 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
1618	28.432155	192.168.1.8	190.119.206.197	TCP	54	52581 → 1433 [ACK] Seq=1 Ack=1 Win=262656 Len=0
1619	28.432277	192.168.1.8	190.119.206.197	TDS	148	TDS7 pre-login message
1622	28.482550	190.119.206.197	192.168.1.8	TDS	108	Response
1623	28.482796	192.168.1.8	190.119.206.197	TDS	268	TDS7 pre-login message
1624	28.531025	190.119.206.197	192.168.1.8	TDS	203	TDS7 pre-login message
1625	28.531297	192.168.1.8	190.119.206.197	TDS	113	TDS7 pre-login message
1626	28.531375	192.168.1.8	190.119.206.197	TDS	434	TLS exchange
1629	28.581668	190.119.206.197	192.168.1.8	TCP	60	1433 → 52581 [ACK] Seq=204 Ack=748 Win=65024 Len=0
1630	28.584045	190.119.206.197	192.168.1.8	TDS	572	Response
1631	28.584221	192.168.1.8	190.119.206.197	TDS	282	Remote Procedure Call
1632	28.640683	190.119.206.197	192.168.1.8	TDS	800	Response
1634	28.688669	192.168.1.8	190.119.206.197	TCP	54	52581 → 1433 [ACK] Seq=976 Ack=1468 Win=262656 Len=0
1707	32.161117	192.168.1.8	190.119.206.197	TDS	282	Remote Procedure Call
1708	32.225017	190.119.206.197	192.168.1.8	TDS	808	Response
1710	32.266571	192.168.1.8	190.119.206.197	TCP	54	52581 → 1433 [ACK] Seq=1204 Ack=2222 Win=261888 Len=0
1727	35.895969	192.168.1.8	190.119.206.197	TDS	290	Remote Procedure Call
1729	35.950995	190.119.206.197	192.168.1.8	TDS	804	Response
1731	35.997752	192.168.1.8	190.119.206.197	TCP	54	52581 → 1433 [ACK] Seq=1440 Ack=2972 Win=262656 Len=0
1745	36.127668	192.168.1.8	190.119.206.197	TDS	306	Remote Procedure Call
1746	36.182589	190.119.206.197	192.168.1.8	TDS	858	Response
1748	36.234755	192.168.1.8	190.119.206.197	TCP	54	52581 → 1433 [ACK] Seq=1692 Ack=3776 Win=261888 Len=0
1836	36.733174	192.168.1.8	190.119.206.197	TDS	292	Remote Procedure Call
1837	36.785168	190.119.206.197	192.168.1.8	TDS	808	Response
1839	36.829739	192.168.1.8	190.119.206.197	TCP	54	52581 → 1433 [ACK] Seq=1930 Ack=4530 Win=262656 Len=0

> Frame 1614: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{8A546A8B-440D-425A-BE81-756BF9688FE8}, id 0
> Ethernet II, Src: ASUSTekC_5c:e7:ac (24:4b:fe:5c:e7:ac), Dst: HonHaiPr_dd:83:9f (18:4f:32:dd:83:9f)
> Internet Protocol Version 4, Src: 192.168.1.8, Dst: 190.119.206.197
> Transmission Control Protocol, Src Port: 52581, Dst Port: 1433, Seq: 0, Len: 0

Figura 13 Filtrado de Flujo TCP Stream 80

tcp.stream eq 128

No.	Time	Source	Destination	Protocol	Length	Info
2932	141.710177	8.36.80.212	192.168.1.8	TCP	1502	80 → 52597 [PSH, ACK] Seq=18825 Ack=140 Win=20440 Len=1448 [TCP segment of a reassembled PDU]
2933	141.710177	8.36.80.212	192.168.1.8	TCP	1502	80 → 52597 [PSH, ACK] Seq=20273 Ack=140 Win=20440 Len=1448 [TCP segment of a reassembled PDU]
2934	141.710191	192.168.1.8	8.36.80.212	TCP	54	52597 → 80 [ACK] Seq=140 Ack=21721 Win=262656 Len=0
2935	141.710389	8.36.80.212	192.168.1.8	TCP	1502	80 → 52597 [PSH, ACK] Seq=21721 Ack=140 Win=20440 Len=1448 [TCP segment of a reassembled PDU]
2936	141.710389	8.36.80.212	192.168.1.8	TCP	1502	80 → 52597 [PSH, ACK] Seq=23169 Ack=140 Win=20440 Len=1448 [TCP segment of a reassembled PDU]
2937	141.710403	192.168.1.8	8.36.80.212	TCP	54	52597 → 80 [ACK] Seq=140 Ack=24617 Win=262656 Len=0
2938	141.710604	8.36.80.212	192.168.1.8	TCP	1502	80 → 52597 [PSH, ACK] Seq=24617 Ack=140 Win=20440 Len=1448 [TCP segment of a reassembled PDU]
2939	141.710604	8.36.80.212	192.168.1.8	TCP	1502	80 → 52597 [PSH, ACK] Seq=26065 Ack=140 Win=20440 Len=1448 [TCP segment of a reassembled PDU]
2940	141.710604	8.36.80.212	192.168.1.8	TCP	1502	80 → 52597 [PSH, ACK] Seq=27513 Ack=140 Win=20440 Len=1448 [TCP segment of a reassembled PDU]
2941	141.710604	8.36.80.212	192.168.1.8	TCP	1502	80 → 52597 [PSH, ACK] Seq=28961 Ack=140 Win=20440 Len=1448 [TCP segment of a reassembled PDU]
2942	141.710604	8.36.80.212	192.168.1.8	TCP	1502	80 → 52597 [PSH, ACK] Seq=30409 Ack=140 Win=20440 Len=1448 [TCP segment of a reassembled PDU]
2943	141.710621	192.168.1.8	8.36.80.212	TCP	54	52597 → 80 [ACK] Seq=140 Ack=31857 Win=262656 Len=0
2944	141.710630	8.36.80.212	192.168.1.8	TCP	1502	80 → 52597 [PSH, ACK] Seq=31857 Ack=140 Win=20440 Len=1448 [TCP segment of a reassembled PDU]
2945	141.710630	8.36.80.212	192.168.1.8	TCP	1502	80 → 52597 [PSH, ACK] Seq=33305 Ack=140 Win=20440 Len=1448 [TCP segment of a reassembled PDU]
2946	141.710641	192.168.1.8	8.36.80.212	TCP	54	52597 → 80 [ACK] Seq=140 Ack=34753 Win=262656 Len=0
2947	141.710830	8.36.80.212	192.168.1.8	TCP	1502	80 → 52597 [PSH, ACK] Seq=34753 Ack=140 Win=20440 Len=1448 [TCP segment of a reassembled PDU]
2948	141.760889	192.168.1.8	8.36.80.212	TCP	54	52597 → 80 [ACK] Seq=140 Ack=36201 Win=261120 Len=0
2951	141.884750	8.36.80.212	192.168.1.8	TCP	1502	80 → 52597 [PSH, ACK] Seq=36201 Ack=140 Win=20440 Len=1448 [TCP segment of a reassembled PDU]
2952	141.885069	8.36.80.212	192.168.1.8	TCP	1502	80 → 52597 [PSH, ACK] Seq=37649 Ack=140 Win=20440 Len=1448 [TCP segment of a reassembled PDU]
2953	141.885069	8.36.80.212	192.168.1.8	TCP	1502	80 → 52597 [PSH, ACK] Seq=39097 Ack=140 Win=20440 Len=1448 [TCP segment of a reassembled PDU]
2954	141.885081	192.168.1.8	8.36.80.212	TCP	54	52597 → 80 [ACK] Seq=140 Ack=40545 Win=262656 Len=0
2955	141.885280	8.36.80.212	192.168.1.8	TCP	1502	80 → 52597 [PSH, ACK] Seq=40545 Ack=140 Win=20440 Len=1448 [TCP segment of a reassembled PDU]
2956	141.885280	8.36.80.212	192.168.1.8	TCP	1502	80 → 52597 [PSH, ACK] Seq=41993 Ack=140 Win=20440 Len=1448 [TCP segment of a reassembled PDU]
2957	141.885280	8.36.80.212	192.168.1.8	TCP	1502	80 → 52597 [PSH, ACK] Seq=43441 Ack=140 Win=20440 Len=1448 [TCP segment of a reassembled PDU]
2958	141.885291	192.168.1.8	8.36.80.212	TCP	54	52597 → 80 [ACK] Seq=140 Ack=44889 Win=262656 Len=0
2959	141.885578	8.36.80.212	192.168.1.8	TCP	1502	80 → 52597 [PSH, ACK] Seq=44889 Ack=140 Win=20440 Len=1448 [TCP segment of a reassembled PDU]

```
> Frame 2959: 1502 bytes on wire (12016 bits), 1502 bytes captured (12016 bits) on interface \Device\NPF_{8A546A8B-440D-425A-BE81-756BF9688FE8}, id 0
> Ethernet II, Src: HonHaiPr_dd:83:9f (18:4f:32:dd:83:9f), Dst: ASUSTekC_5c:e7:ac (24:4b:fe:5c:e7:ac)
> Internet Protocol Version 4, Src: 8.36.80.212, Dst: 192.168.1.8
> Transmission Control Protocol, Src Port: 80, Dst Port: 52597, Seq: 44889, Ack: 140, Len: 1448
```

Figura 14 Filtrado de Flujo TCP Stream 128

3.1.2. Análisis de IP Servidor y Puertos de Servidor con NMAP

Del análisis que se realizó con WireShark obtuvimos la ip de un servidor de Pale Consultores, este servidor probablemente sea el que valida los datos de Login del Sistema IFacturacion por lo que en la Figura 15 se muestra los servicios y la versión de los servicios que corren en la ip obtenida, como podemos ver los servicios que corren en el servidor usan en su totalidad tecnología de Microsoft.

```
root@kali:/home/kali# nmap -sS -sV -O 184.168.152.2
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-11 11:44 EDT
Nmap scan report for p3nw8shg275.shr.prod.phx3.secureserver.net (184.168.1
52.2)
Host is up (0.13s latency).
Not shown: 994 filtered ports
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     Microsoft ftpd
80/tcp   open  http    Microsoft IIS httpd 7.0
443/tcp  open  https?
1027/tcp open  msrpc   Microsoft Windows RPC
1028/tcp open  msrpc   Microsoft Windows RPC
1029/tcp open  msrpc   Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at lea
st 1 open and 1 closed port
Device type: general purpose|specialized
Running: Microsoft Windows XP|7|2012, VMware Player
OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_7 cpe:/o
:microsoft:windows_server_2012 cpe:/a:vmware:player
OS details: Microsoft Windows XP SP3, Microsoft Windows XP SP3 or Windows
7 or Windows Server 2012, VMware Player virtual NAT device
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at
 https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 158.65 seconds
```

Figura 15 Analisis de Puerto y Servicios de la IP de un servidor de Pale Consultores

Se uso Nmap también para poder saber si es que existe un firewall o alguna tecnología que filtre puertos, la opción -sN de Nmap nos permite saber si existen paquetes filtrados, como podemos observar en la Figura 16 nos da el resultado: “are open | filtered” esto significa que no se tuvo una respuesta por parte de la ip proporcionada.

```
root@kali:/home/kali# nmap -sN 184.168.152.2
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-14 15:00 EDT
Nmap scan report for p3nw8shg275.shr.prod.phx3.secureserver.net (184.168.1
52.2)
Host is up (0.00022s latency).
All 1000 scanned ports on p3nw8shg275.shr.prod.phx3.secureserver.net (184.
168.152.2) are open|filtered
```

Figura 16 Analisis de respuesta de paquetes ACK opción -sN en busca de puertos expuestos

Para descartar posibles puertos filtrados por un firewall usamos el comando de -sA que nos permitirá conocer las reglas que estén establecidas por fuera del firewall en la Figura 17 podemos ver el resultado es “unfiltered” esto significa que efectivamente se tiene un ACK de respuesta, pero no se sabe si tienen puertos abiertos o cerrados, por lo que podemos deducir que existe una tecnología o firewall que nos impide el acceso a esta información.

```
root@kali:/home/kali# nmap -sA 184.168.152.2
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-14 16:05 EDT
Nmap scan report for p3nw8shg275.shr.prod.phx3.secureserver.net (184.168.152.2)
Host is up (0.000035s latency).
All 1000 scanned ports on p3nw8shg275.shr.prod.phx3.secureserver.net (184.168.15
2.2) are unfiltered

Nmap done: 1 IP address (1 host up) scanned in 0.73 seconds
```

Figura 17 Analisis de respuesta de paquetes ACK opción -sA en busca de puertos expuestos

De los análisis hechos con anterioridad podemos encontrar el nombre del dominio que pertenece esa ip por lo que será el siguiente objetivo de análisis.

3.1.3. Analisis del dominio Encontrado dentro del servidor

Del análisis anterior se obtuvo el nombre de un dominio asociado al servidor, por lo que se usó la página web de **urlscan.io** para obtener información relacionada al dominio, en la Figura 18 podemos observar que el dominio fue comprado de GoDaddy y es un dominio alojado en Nueva York.

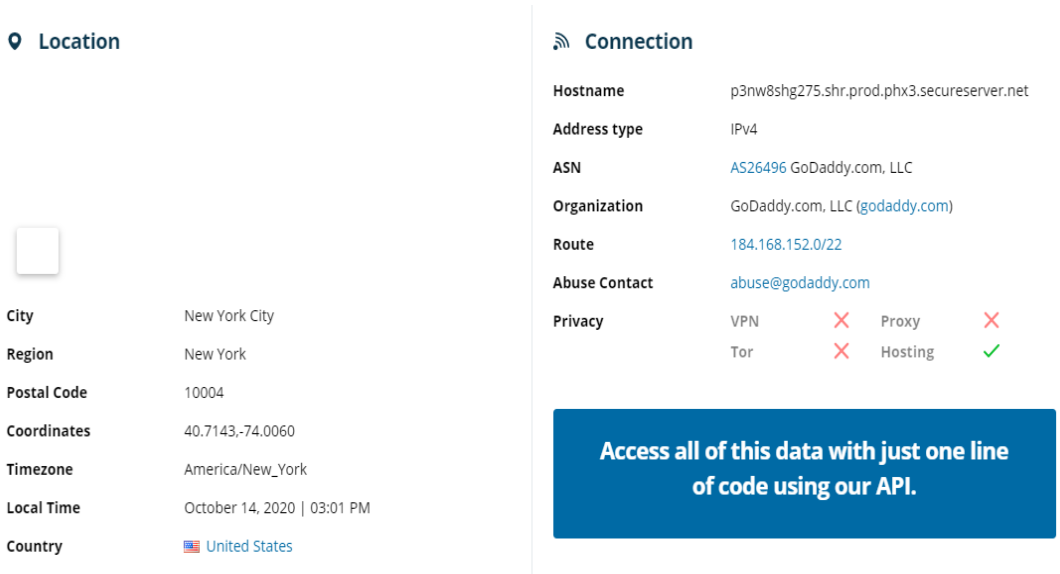


Figura 18 Análisis de Nombre de Dominio hecho en urlscan.io

3.1.4. Búsqueda del Código Fuente del Sistema IFacturacion

Para poder encontrar el código fuente del sistema IFacturacion, se optó por abrir la ubicación directamente del icono generado como muestran las Figura 19, como se observa en la Figura 20 no se pudo acceder al código de esta manera, por lo que se intentó generar un código de error en el sistema para ver si de esta manera se podía obtener alguna ruta relacionada al sistema, como se puede observar en la Figura 21 el código de error me muestra la ubicación del código fuente del sistema, en la Figura 22 se muestra un error generado por una funcionalidad del sistema mientras que en la Figura 23 se muestra un error con la base de datos asignada donde además nos muestra el nombre de usuario asignado.

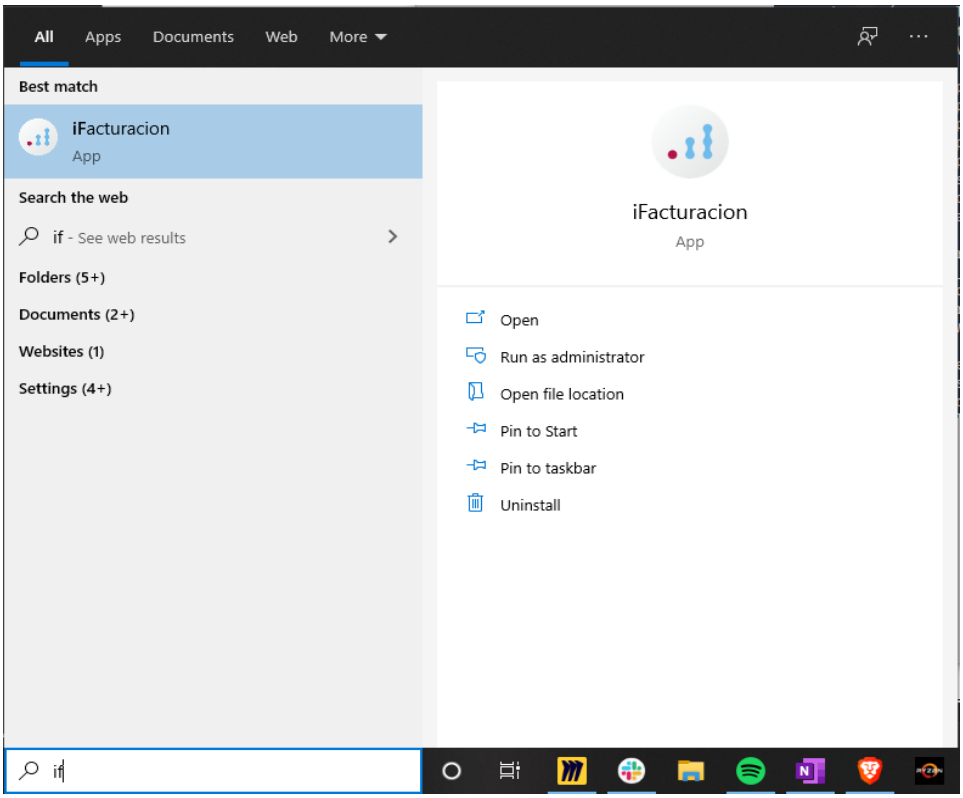


Figura 19 Buscar localización del Código Fuente mediante menú de inicio de Windows 10

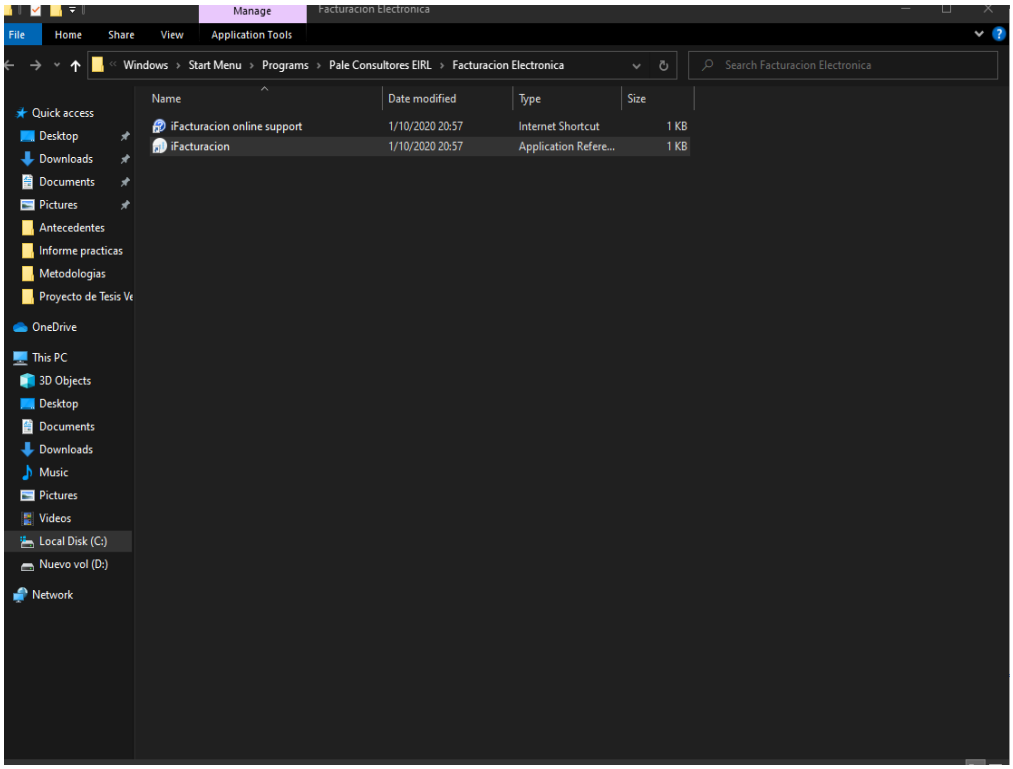


Figura 20 Ruta de archivos encontrada tras buscar en la barra de inicio de Windows 10

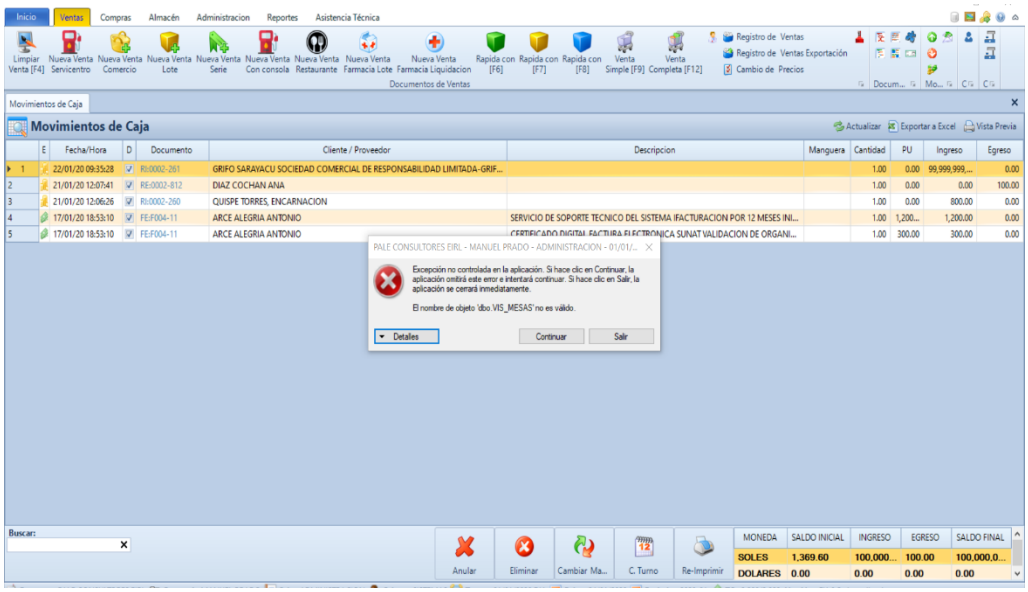


Figura 21 Error generado al hacer clic en la Viñeta de Nueva Venta Restaurante

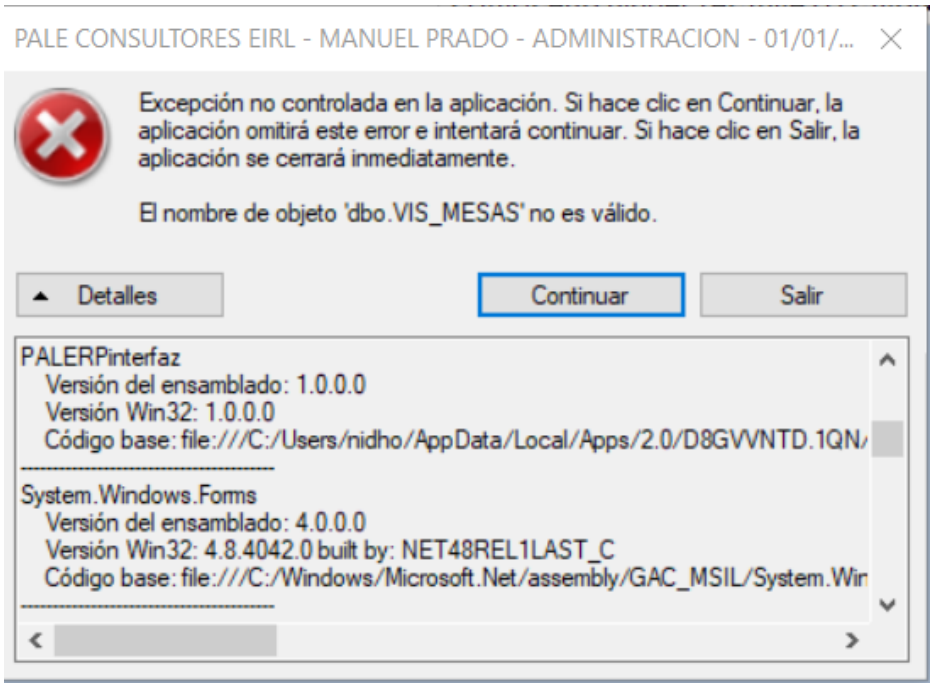


Figura 22 Detalle del error Generado en la Viñeta Nueva Venta Restaurante

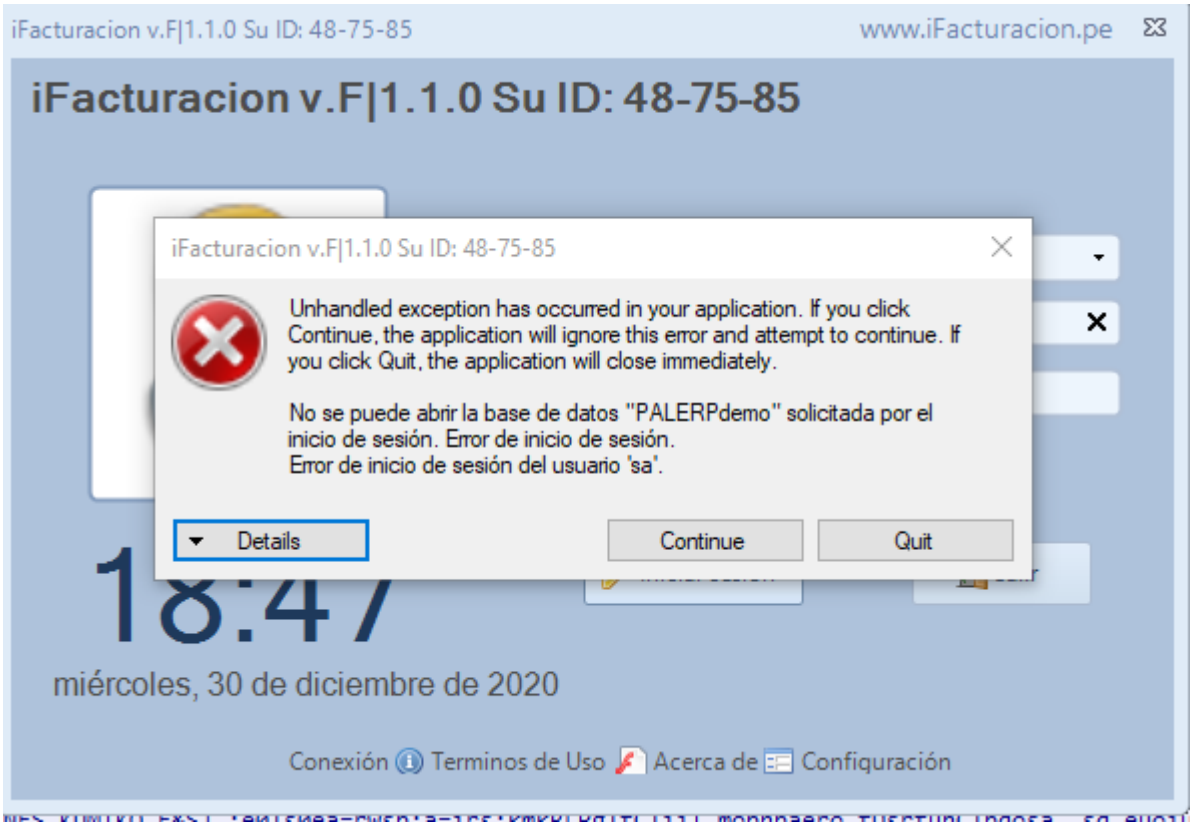


Figura 23 Error al acceder a la base de Datos asignada

3.2. Fase 2 – Identificar Fuentes de Amenaza y Eventos de Amenaza

3.2.1. Fuentes de Amenaza

Se debe de tener una lista de posibles fuentes de amenaza para el sistema de IFacturacion, para ello NIST SP 800-30 nos provee una lista de Fuentes de amenazas (ver Anexo 1) de la cual se identificaron las fuentes de amenaza en la Tabla 1, para la valorización de la capacidad, intensión y focalización se usó el Anexo 2,3,4 respectivamente, se listaron las fuentes de amenazas adversariales, las cuales están relacionados directamente con las fuentes de amenaza a los que esté involucrado uno o varios adversarios, el identificador FAA-N° por sus siglas representan Fuente de Amenaza Adversarial, en la Tabla 2 se listan las fuentes de amenaza no adversariales para los valores del rango de efectos se usó la valoración del Anexo 5, estas amenazas son todas las demás que no están relacionados con uno o más adversarios, los identificadores FANA-N° significa por sus siglas Fuente de Amenaza no Adversarial.

Tabla 1 Identificación de Fuentes de Amenaza Adversarial

Identificador	Tipo de Fuente de Amenaza	En Alcance	Capacidad	Intensión	Focalización
FAA-01	Insider	Si	Moderada	Alta	Alto
FAA-02	Trusted Insider	Si	Alta	Alta	Alto
FAA-03	Cliente	Si	Moderada	Muy Baja	Muy Bajo

Fuente: NIST SP 800-30 – Identification of Adversarial Threat Sources

Tabla 2 Identificación de Fuentes de Amenaza no Adversarial

Identificador	Tipo de Fuente de Amenaza	En Alcance	Rango de Efectos
FANA-01	Usuario	Si	**Bajo**
FANA-02	Usuario o Administrador privilegiado	Si	**Bajo**
FANA-03	Almacenamiento	Si	**Alto**

FANA-04	Procesamiento	Si	**Alto**
FANA-05	Comunicaciones	Si	**Moderado**
FANA-06	Incendio	No	**Alto**
FANA-07	Terremoto	No	**Alto**
FANA-08	Corte de suministro eléctrico	No	**Alto**
FANA-08	Corte de Telecomunicaciones	No	**Bajo**

Fuente: NIST SP 800-30 – Identification of non-Adversarial Threat Sources

3.2.2. Identificar Eventos de Amenaza

Para clasificar la relevancia de los eventos de amenaza identificados NIST SP 800-30 provee una clasificación de valores como se observa en el Anexo 6, en este punto se tuvo una reunión con el administrador de IFacturacion en la cual se le mostro los eventos de amenaza identificados y junto con él se procedió a darle la relevancia a los eventos de amenaza, en el caso del valor N/A se consideró en el caso de que el evento de amenaza no haya sido identificado o descubierto en IFacturacion, sin embargo se tomara en cuenta de todas maneras ya que las vulnerabilidades pueden estar relacionados con estos eventos de amenaza.

Al terminar de evaluar e identificar las fuentes de amenaza la metodologia nos indica que cada fuente de amenaza tiene que estar relacionado a un evento de amenaza, dicho evento puede ser generado por una fuente de amenaza o por varias a la vez, por lo que se hizo la

Tabla 3 de eventos de amenaza no adversariales, la clasificación está hecha por la caracterización TTPs (Tactics, Techniques, and Procedures), la Tabla 4 se identificaron los eventos de amenaza adversariales, con la fuente de amenaza que podría dar inicio al evento de amenaza enumerado, las siglas de la identificación de los eventos de amenaza adversariales serán EAA mientras que de las no adversariales será EANA seguidos de la correspondiente numeración, la relevancia de los eventos de amenaza adversariales como de los no adversariales fueron validadas con el administrador del sistema.

Tabla 3 Identificacion de Eventos de Amenaza no Adversariales

Identificador	Evento de Amenaza	Fuente de Amenaza	Relevancia
EANA-01	Configuración incorrecta de privilegios	Usuario/Administrador Privilegiados	N/A
EANA-02	Terremoto en la localización del servidor principal	Terremoto	Esperado
EANA-03	Introduccion de vulnerabilidades en productos de software	Usuario	N/A
EANA-04	Error en el disco duro del servidor principal	Almacenamiento	Esperado

Fuente: NIST SP 800-30 Identification of Threat Events

Tabla 4 Identificacion de Eventos de Amenaza Adversariales

Identificador	Fuente de información del Evento de Amenaza	Fuente de Amenaza	Relevancia
EAA-01	Realizar reconocimiento y vigilancia de la organización	Insider/Trusted Insider	Posible
EAA-02	Realizar un reconocimiento interno dirigido por programa maligno		Posible
EAA-03	Crear ataques específicamente basados en el entorno de la tecnología implementada.		Posible

EAA-04	Enviar programa maligno modificado al sistema de información.		Posible
EAA-05	Enviar programa maligno dirigida a controlar sistemas internos o exfiltración de datos		Predicho
EAA-06	Instalar sniffers persistentes y enfocados en el sistema de información o la red conectada al mismo		Posible
EAA-07	Insertar programa maligno no dirigido en software descargable y/o en productos comerciales de información y tecnología		Predicho
EAA-08	Explotar vulnerabilidades en el sistema de información		N/A
EAA-09	Comprometer software critico de la organización		N/A
EAA-10	Conducir una autentificación por fuerza bruta		N/A
EAA-11	Causar destrucción /deterioro del sistema de información crítico, componentes y funciones.		N/A
EAA-12	Explotar información insegura o incompleta en múltiples ambientes		N/A
EAA-13	Configuración incorrecta de privilegios		N/A
EAA-14	Introduccion de vulnerabilidades en los productos de software		N/A

EAA-15	Conducir ataque usando puertos, protocolos y servicios		N/A
EAA-16	Conducir modificación de trafico de red externo (man in the middle)		N/A
EAA-17	Derrame de información sensible	Cliente	N/A
EAA-18	Obtener acceso no autorizado		N/A
EAA-19	Obtener información por oportunamente escarbar información en los sistemas de información		N/A

Fuente: NIST SP 800-30 Identification of Threat Events

3.3. Fase 3 - Identificar Vulnerabilidades y Condiciones Predispuestas

En esta etapa se usó la adaptación de las metodologías como se describe a continuación: para la identificación de vulnerabilidades se usó el Pentesting Standard, como punto de partida se usó los datos obtenidos de la Fase 2, al realizar la recolección de información se encontró múltiples posibles vulnerabilidades por lo que se continuo por eso camino siguiendo las pautas dadas por la metodologia de Pentesting Standard, una vez identificadas las vulnerabilidades, se le asigno una severidad que está basada en el Anexo 7 de la metodologia NIST SP 800-30, para la identificación de condiciones predispuestas se usó el Anexo 8. Las condiciones predispuestas son condiciones que pueden afectar a las vulnerabilidades encontradas de manera positiva o negativa para el impacto que representen siguiendo el flujo de NIST SP 800-30.

3.3.1. Realizar el análisis de Vulnerabilidades

3.3.1.1. Vulnerabilidades FTP

En este punto se usaron las credenciales obtenidas en la Fase 2, primero se hizo la prueba en el Shell de Kali Linux como se muestra en la Figura 24 podemos observar que si bien se mostraban las rutas no se podía acceder a las mismas ya que estaba bloqueada la navegación a otros directorios, debido a que se la conexión se hacía en modo de data ASCII, la cual no recibía una respuesta y no permitía la navegación.

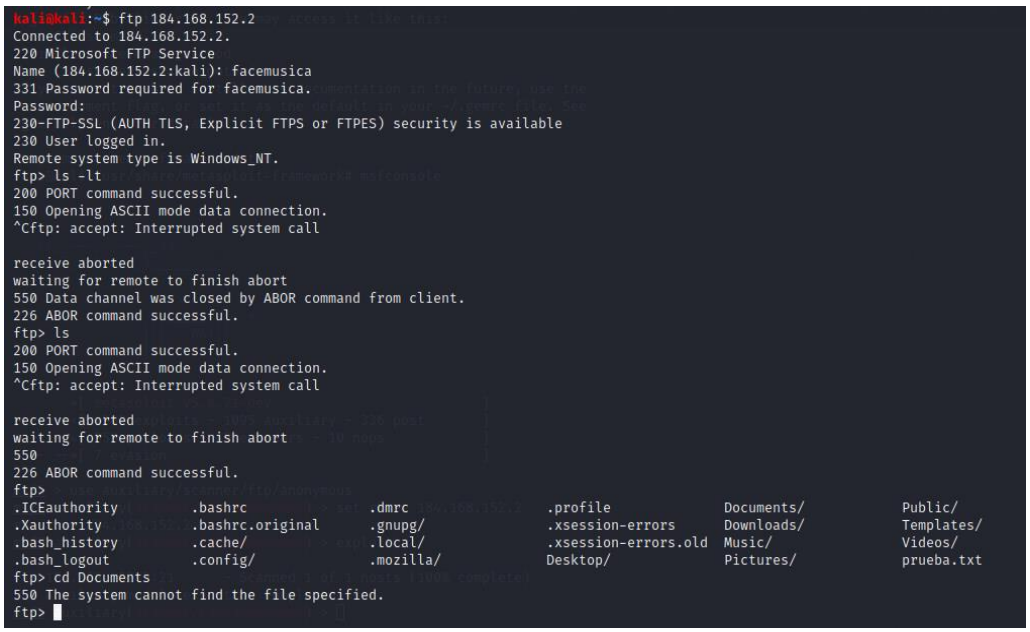


Figura 24 Intento de Acceso a FTP vía Shell de Kali Linux
Fuente: Elaboración Propia

Por lo que se accedió vía navegador web al servicio para tratar de acceder a las rutas de las carpetas como se observa en la Figura 25, si se pudo observar las rutas y los archivos que contiene el servidor ftp, además se pudo descargar una copia de seguridad de una base de datos, deducir que el usuario obtenido tiene permisos suficientes para dichos procesos.

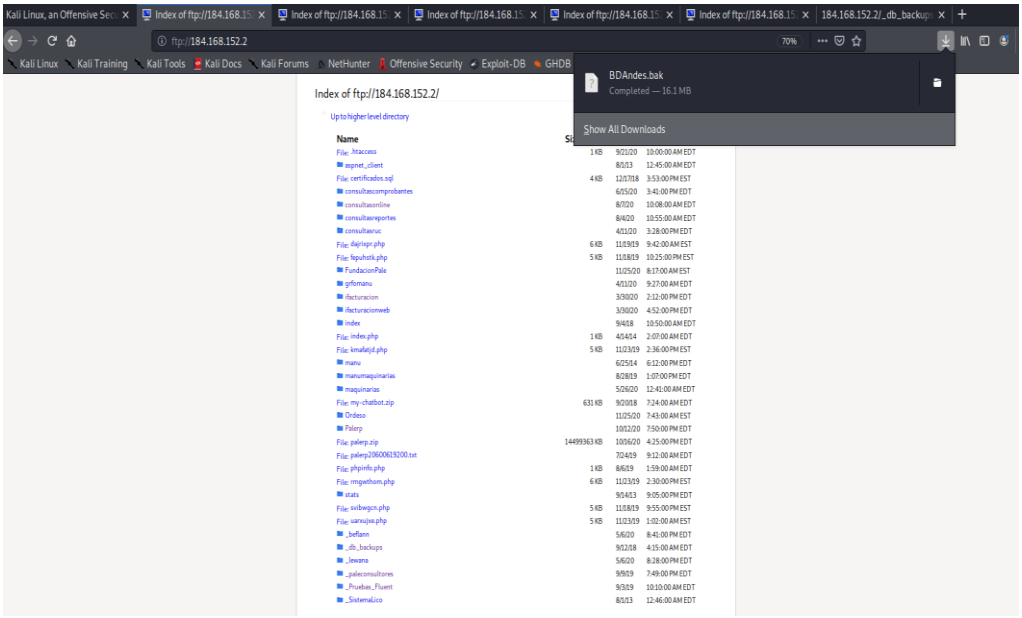


Figura 25 Acceso al servidor FTP vía Navegador Web

Sin embargo, por web no se pudo subir archivos de ningún tipo así que probé por medio del software FileZilla como se observa en la

Figura 26, por medio de FileZilla también se accedió al servicio ftp, usando FileZilla si se pudo subir archivos al servidor ftp, FileZilla además nos permite ver exactamente lo que contienen los archivos siendo que por vía web el acceso visual a estos era limitado, FileZilla tampoco puede comprobar que el servidor tenga una certificación TLS por lo que la conversación no se encuentra cifrada de ninguna manera.

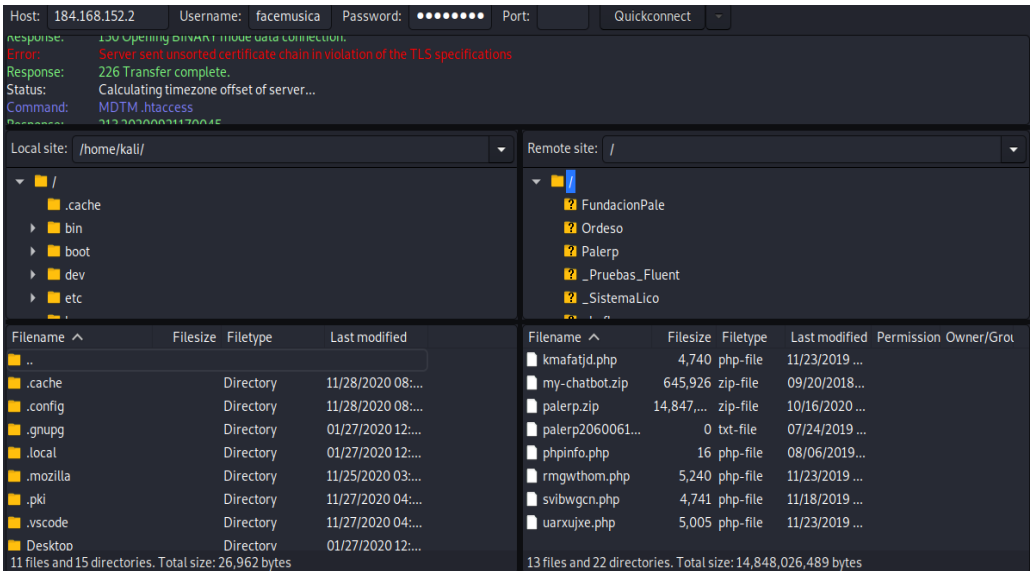


Figura 26 Acceso al Servidor mediante FileZilla

Siguiendo la recolección de información se tendría que comprobar el protocolo HTTP y HTTPS, pero dado que el sistema es desktop y la propuesta está centrada en encontrar vulnerabilidades en el sistema no se evaluara dichos protocolos, lo mismo sucede con el dominio asociado al servidor FTP, por lo que se procedió a analizar el código fuente del sistema.

3.3.1.2. Vulnerabilidades de Flujo TCP Stream

En la recolección de información se encontró un flujo TCP Stream, las vulnerabilidades que se encontraron son principalmente de que los datos no están complementa encriptados o la encriptación permite la lectura parcial de los paquetes, siguiendo el flujo se empezó por el TCP Stream 65, que contiene la Cadena de Conexión encriptada, como se observa en la Figura 27 existe un patrón que se repite por cada usuario, por lo cual puedo interpretar que esos caracteres que se repiten son la cadena de conexión encriptada por SQL Server.

En la Figura 29 se muestra que la versión de SQL usada es Microsoft SQL 2008 versión 8.0.0.0.4096, teniendo la versión de SQL Server usada se buscó en la base de datos CVE y NVD posibles vulnerabilidades asociadas a esta versión, pero no se encontró ninguna que se aplique a este caso.

Figura 27 Cadena de Conexión Encriptada

Continuando con el flujo, en el TCP Stream 79 se encontró los datos que los módulos del sistema usan, los datos en este segmento del flujo pertenecen a todos los módulos del sistema y por los datos vistos parecen ser los nombres clave, jerarquías y relaciones entre los módulos del sistema, una parte de estos datos se observan en la Figura 28.

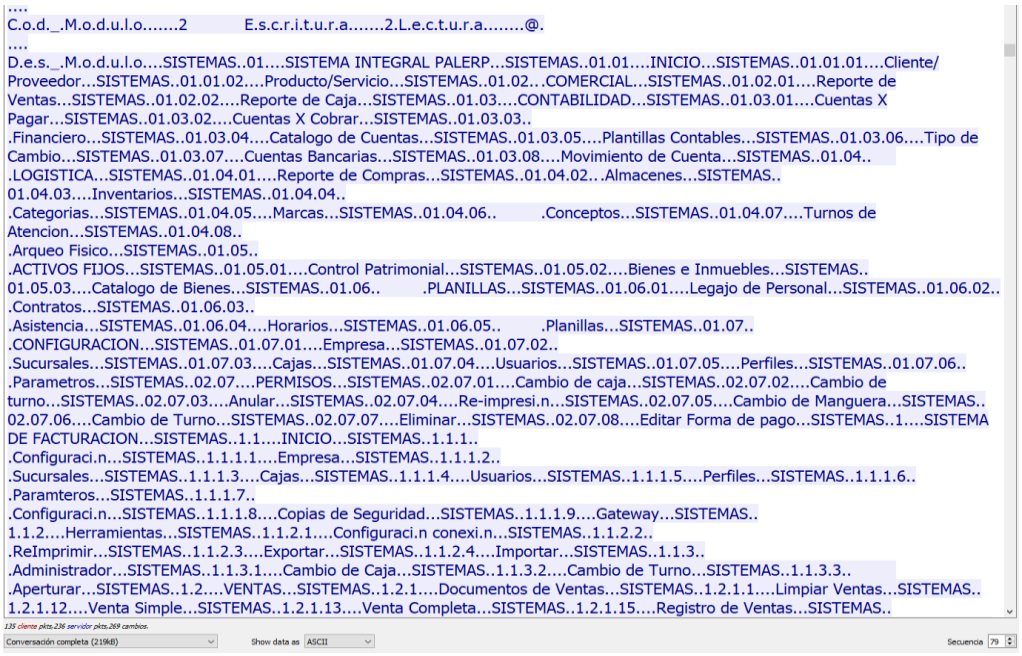


Figura 28 Nombres Clave, jerarquías y relaciones entre los módulos

En el flujo TCP Stream 80 se encontró la versión de la base de Datos SQL Server, como se observa en la Figura 29, se muestran otro tipo de datos que parecen ser los parámetros y esquemas que se usan para cada Cliente de la empresa en el sistema, siendo esta información confidencial del sistema, sin embargo, no se encontró información adicional.

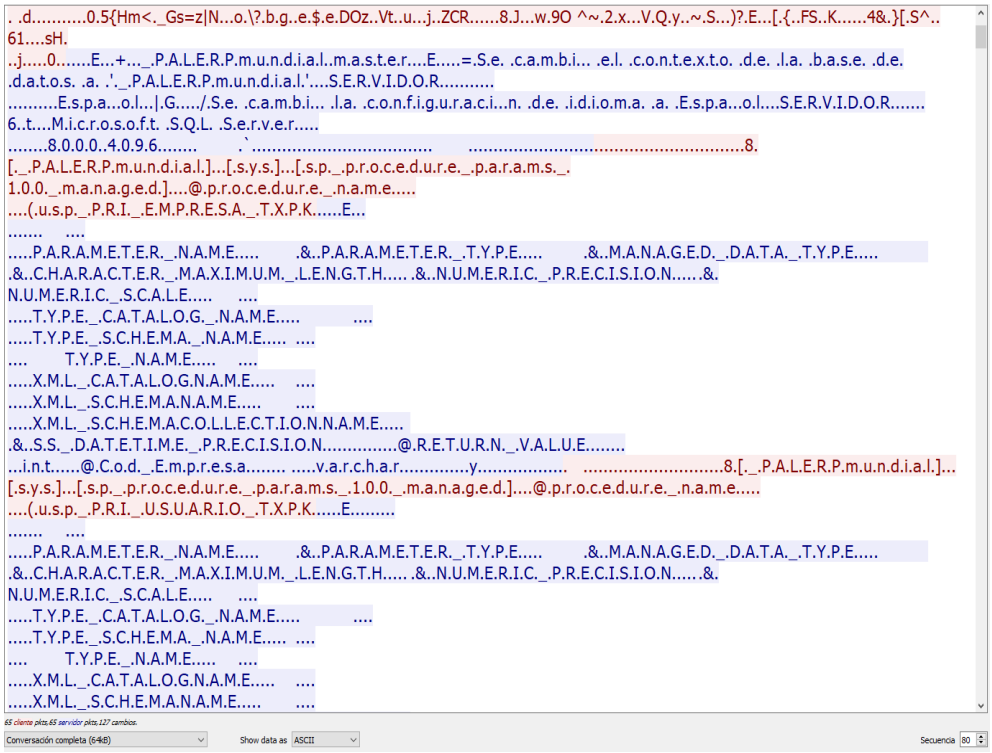


Figura 29 Palabras Clave de los parámetros por cliente y versión del servidor SQL Server

Todos estos datos fueron capturados con el protocolo TDS (Tabular data Stream) los siguientes dos flujos de TCP se encuentran totalmente encriptados u ofuscados lo que impide su lectura, por lo que la información a analizar es menor, como es el caso del TCP Stream 128, solo se puede observar la versión del servidor nginx, la última vez que fue actualizado y el estado de la conexión todos estos datos se encuentran en la Figura 30.

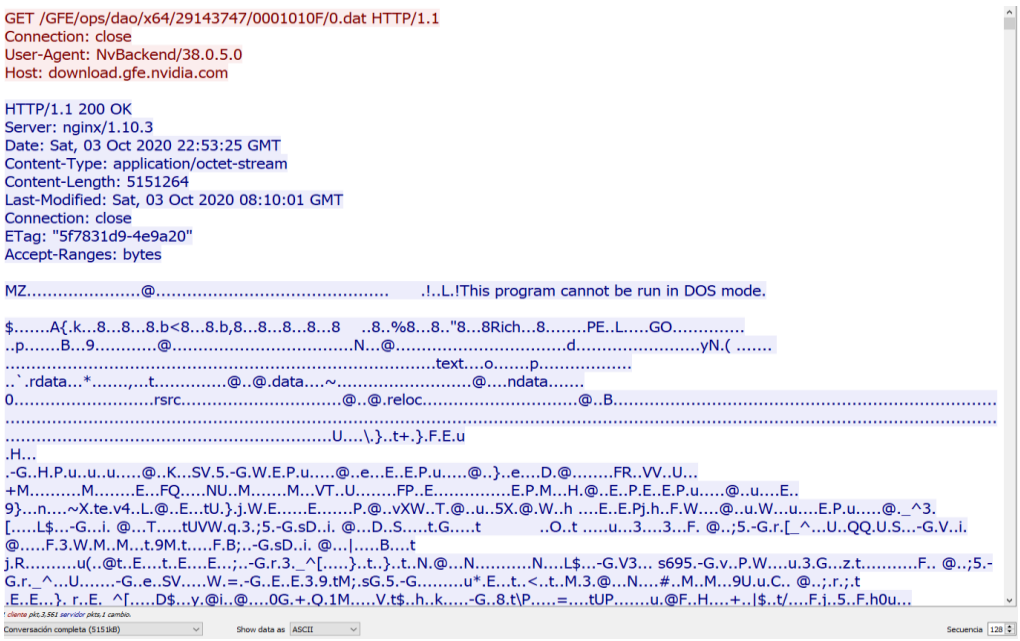


Figura 30 Datos del Servidor Nginx

3.3.1.3. Vulnerabilidades Código Fuente

Se uso justDecompile para descompilar el código, el software no asegura que el código extraído sea exactamente igual al código originalmente, por lo que el código extraído puede no ser el código exacto del sistema. Se descompilo 10 de los archivos .dll, el criterio de selección de los archivos es el nombre de estos, con el objetivo de encontrar el que contenga la cadena de conexión a la base de datos, en la Figura 31 podemos observar el nombre de los archivos seleccionados.

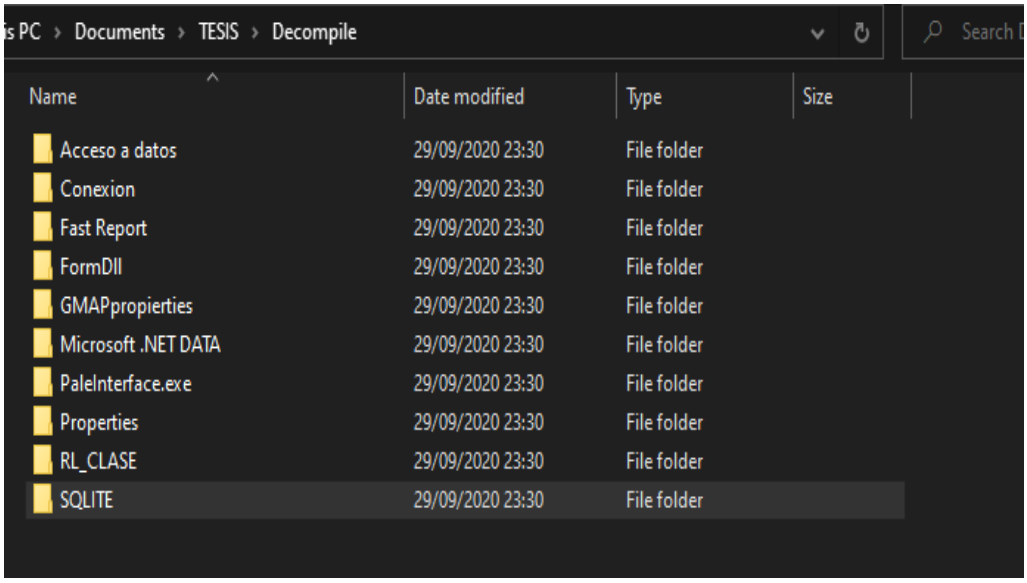


Figura 31 Carpetas de Código fuente Seleccionadas

Al realizar una inspección de las carpetas, se encontró una carpeta denominada PaleInterface.exe, el archivo de extensión .dll contenía un pedazo de código que parece ofuscar la cadena de conexión por lo que se hizo un seguimiento a la clase COfuscar en la que se encontró la manera en la que se usa en el sistema la clase COfuscar como se muestra en la Figura 32, en la carpeta se encuentra un fragmento de código llamado RL_CLASE, en el que se encuentran los algoritmos de ofuscar y desofuscar como se muestra en la Figura 33.

```
78                  else
79                  {
80                      @default.Servidor = entrada1.tbEntrada.Text;
81                  }
82              }
83              IU_Activacion uActivacion = new IU_Activacion();
84              if (upper != @default.Serie.Replace("-", ""))
85              {
86                  if (uActivacion.ShowDialog() != DialogResult.OK)
87                  {
88                      flag = false;
89                      return flag;
90                  }
91                  else
92                  {
93                      @default.IdRegistro = uActivacion.IdRegistro;
94                      @default.Serie = uActivacion.Serie;
95                  }
96              }
97              Settings.Default.BDMaster = ConfigurationManager.ConnectionStrings["BDMaster"];
98              Settings.Default.BDConexion = ConfigurationManager.ConnectionStrings["BDConexion"];
99              IAccesoDatos accesoDato = new AccesoDatos();
100             COfuscar cOfuscar = new COfuscar();
101             if (Settings.Default.BDConexion.ConnectionString != "")
102             {
103                 accesoDato.CadenaConexion = cOfuscar.US(Settings.Default.BDConexion.ConnectionString);
104                 IU_POS.EsMaster = false;
105             }
106             else
107             {
108                 accesoDato.CadenaConexion = cOfuscar.US(Settings.Default.BDMaster.ConnectionString);
109                 IU_POS.EsMaster = true;
110             }
111             accesoDato.CadenaConexion = string.Format(accesoDato.CadenaConexion, @default.Servidor);
112             accesoDato.NombreProveedor = Settings.Default.BDMaster.ProviderName;
113             CEntidad.AccesoDatos = accesoDato;
114             @default.Save();
115             flag = true;
116         }
117         else
118         {
119             if (@default.IdEmpresa == "")
```

Figura 32 Segmento de Código de para cOfuscar la cadena de conexión

```
1 referencia
public string ObfuscateString(string sInput)
{
    string str = "";
    int i = 0;
    int length = 0;
    length = sInput.Length;
    for (i = length; i >= 1; i += -2)
    {
        str = string.Concat(str, Strings.Mid(sInput, i, 1));
    }
    for (i = length - 1; i >= 1; i += -2)
    {
        str = string.Concat(str, Strings.Mid(sInput, i, 1));
    }
    return str;
}

0 referencias
public string OS(string sInput)
{
    return this.ObfuscateString(sInput);
}

1 referencia
public string UnObfuscateString(string sInput)
{
    string str = "";
    int i = 0;
    int length = 0;
    int num = 0;
    int num1 = 0;
    length = sInput.Length;
    num1 = length % 2;
    num = length / 2;
    for (i = num + num1; i >= 1; i += -1)
    {
        if (num1 == 0)
        {
            str = string.Concat(str, Strings.Mid(sInput, i + num, 1));
        }
        str = string.Concat(str, Strings.Mid(sInput, i, 1));
        if (num1 == 1 & i != 1)
        {
            str = string.Concat(str, Strings.Mid(sInput, i + num, 1));
        }
    }
    return str;
}

0 referencias
public string US(string sInput)
{
    return this.UnObfuscateString(sInput);
}
```

Figura 33 Algoritmo de Ofuscación y Desofuscación

Para observar la cadena de conexión ofuscada se siguió el flujo del algoritmo de ofuscación con la cadena de texto “BDMaster” y “BDConexion” como entrada de la función lo cual dio como resultado la cadena de texto “rtaDesMB” y “nieoDoxnCB” respectivamente, en el Anexo 18 se especifica el flujo que seguí para obtener la cadena texto siendo que puede llegar ser un posible parámetro de la cadena de conexión, para poder realizar una conexión de prueba

en SQL, sin embargo, no encontré una ip o un nombre de servidor para la conexión de la base de datos SQL.

En la

Figura 34 se puede observar el fragmento de código AccesoDato en el cual se declara la Cadena Conexión, sin embargo, parece estar asociado a otra clase por lo que seguí con el flujo a la clase DBConexion como se muestra en la Figura 35.

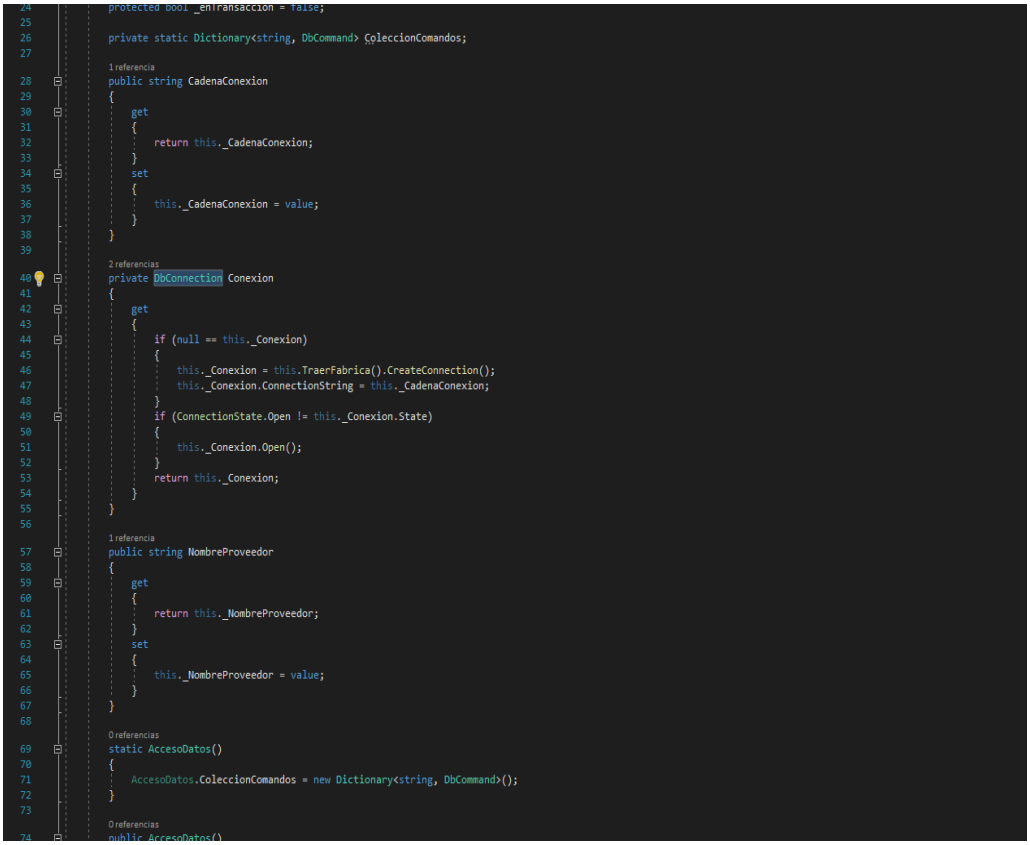


Figura 34 Fragmento de Código donde se encuentra la Cadena de conexión

```
#region ensamblado System.Data, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089
// C:\Windows\Microsoft.NET\Framework\v2.0.50727\System.Data.dll
#endregion

using System.ComponentModel;

namespace System.Data.Common
{
    public abstract class DbConnection : Component, IDbConnection, IDisposable
    {
        protected DbConnection();

        [Browsable(false)]
        public abstract string ServerVersion { get; }
        [ResCategoryAttribute("DataCategory_Data")]
        public abstract string DataSource { get; }
        [ResCategoryAttribute("DataCategory_Data")]
        public abstract string Database { get; }
        [ResCategoryAttribute("DataCategory_Data")]
        public virtual int ConnectionTimeout { get; }
        [DefaultValue("")]
        [RecommendedAsConfigurable(true)]
        [RefreshProperties(RefreshProperties.All)]
        [ResCategoryAttribute("DataCategory_Data")]
        public abstract string ConnectionString { get; set; }
        [Browsable(false)]
        [ResDescriptionAttribute("DbConnection_State")]
        public abstract ConnectionState State { get; }
        protected virtual DbProviderFactory DbProviderFactory { get; }

        [ResCategoryAttribute("DataCategory_StateChange")]
        [ResDescriptionAttribute("DbConnection_StateChange")]
        public event StateChangeEventHandler StateChange;

        public DbTransaction BeginTransaction(IsolationLevel isolationLevel);
        public DbTransaction BeginTransaction();
        public abstract void ChangeDatabase(string databaseName);
        public abstract void Close();
        public DbCommand CreateCommand();
        public virtual void EnlistTransaction(System.Transactions.Transaction transaction);
        public virtual DataTable GetSchema();
        public virtual DataTable GetSchema(string collectionName, string[] restrictionValues);
        public virtual DataTable GetSchema(string collectionName);
        public abstract void Open();
        protected abstract DbTransaction BeginDbTransaction(IsolationLevel isolationLevel);
        protected abstract DbCommand CreateDbCommand();
        protected virtual void OnStateChange(StateChangeEventArgs stateChange);
    }
}
```

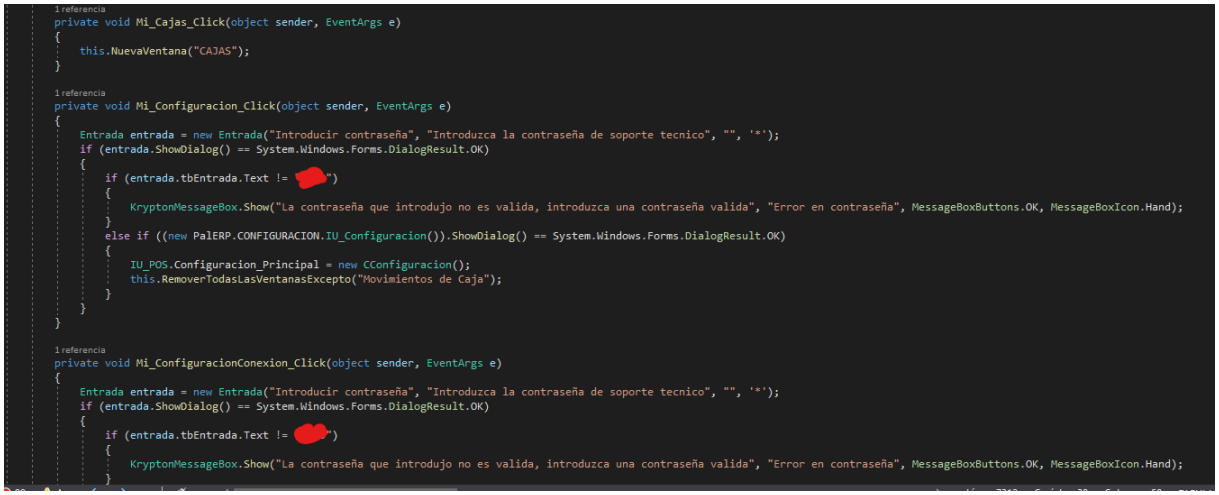
Figura 35 Fragmento de Código de DBConecction

En la Figura 36 podemos observar la manera en la que se establece el default Servidor, aquí es donde se esperaba encontrar la ip del servidor SQL, sin embargo, se encontró una variable Entrada que está asociada a una cadena de texto de la cual podemos deducir que la ip o nombre del servidor de SQL se ingresa al momento de instalación del sistema, por lo que es imposible encontrar la ip o el nombre del servidor del código fuente directamente.

```
Settings @default = Settings.Default;
string upper = Utilitario.GenerarHashMD5(@default.IdRegistro);
upper = upper.Substring(0, 25).ToUpper();
if (!Program.VerificarConexionURL("www.google.com"))
{
    if (@default.IdEmpresa == "")
    {
        Entrada entrada = new Entrada("Pale Consultores EIRL", "Ingrese el RUC de la empresa:", "");
        if (entrada.ShowDialog() != DialogResult.OK)
        {
            flag = false;
            return flag;
        }
        else if ((entrada.tbEntrada.Text.Length != 11 ? true : decimal.Parse(entrada.tbEntrada.Text) < decimal.Zero))
        {
            KryptonMessageBox.Show("El RUC ingresado es Incorrecto. \nGRACIAS IFACTURACION", Principal.aTitulo, MessageBoxButtons.OK, MessageBoxIcon.Hand);
            flag = false;
            return flag;
        }
        else
        {
            @default.IdEmpresa = entrada.tbEntrada.Text;
        }
    }
    if (@default.Servidor == "")
    {
        Entrada entrada1 = new Entrada("Pale Consultores EIRL", string.Concat("Ingrese la IP o Nombre del Servidor para ", str2, ":"), "");
        if (entrada1.ShowDialog() != DialogResult.OK)
        {
            flag = false;
            return flag;
        }
        else
        {
            @default.Servidor = entrada1.tbEntrada.Text;
        }
    }
    IU_Activacion uActivacion = new IU_Activacion();
    if (upper != @default.Serie.Replace("-", ""))
    {
        if (uActivacion.ShowDialog() != DialogResult.OK)
        {
            flag = false;
```

Figura 36 Fragmento de Código que Solicita la cadena de conexión

Continuando con la búsqueda de vulnerabilidades, en la Interfaz IU_POS.Designer se encontró un fragmento de código en el que se encontró la contraseña de soporte técnico que es usada en el sistema para acceder a la base de datos, como se observa en la Figura 37.



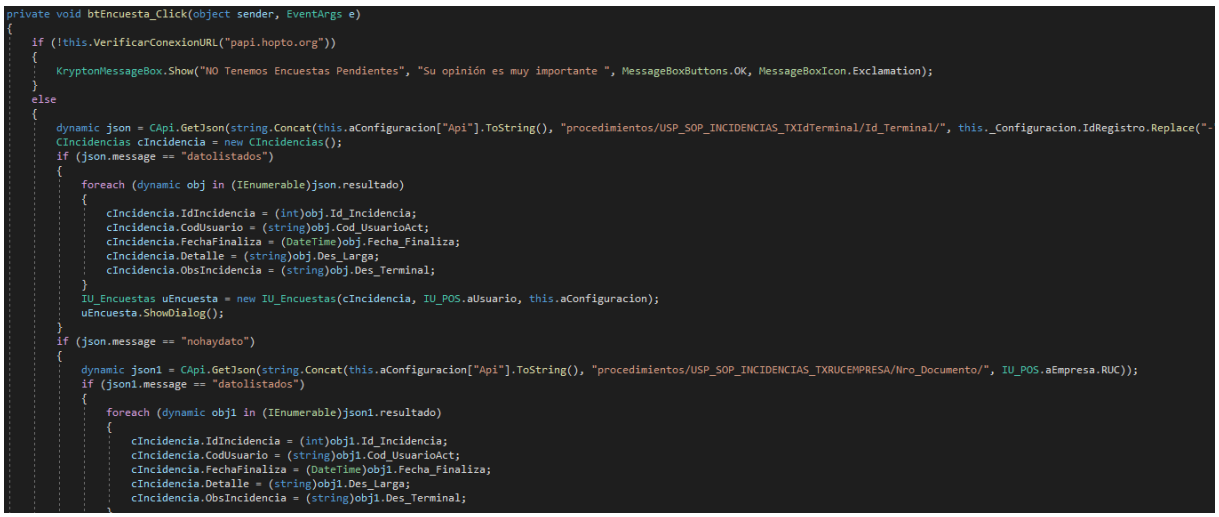
```
1 referencia
private void Mi_Cajas_Click(object sender, EventArgs e)
{
    this.NuevaVentana("CAJAS");
}

1 referencia
private void Mi_Configuracion_Click(object sender, EventArgs e)
{
    Entrada entrada = new Entrada("Introducir contraseña", "Introduzca la contraseña de soporte tecnico", "", '*');
    if (entrada.ShowDialog() == System.Windows.Forms.DialogResult.OK)
    {
        if (entrada.tbEntrada.Text != [redacted])
        {
            KryptonMessageBox.Show("La contraseña que introdujo no es valida, introduzca una contraseña valida", "Error en contraseña", MessageBoxButtons.OK, MessageBoxIcon.Hand);
        }
        else if ((new PalERP.CONFIGURACION.IU_Configuracion()).ShowDialog() == System.Windows.Forms.DialogResult.OK)
        {
            IU_POS.Configuracion_Principal = new CConfiguracion();
            this.RemoverTodasLasVentanasExcepto("Movimientos de Caja");
        }
    }
}

1 referencia
private void Mi_ConfiguracionConexion_Click(object sender, EventArgs e)
{
    Entrada entrada = new Entrada("Introducir contraseña", "Introduzca la contraseña de soporte tecnico", "", '*');
    if (entrada.ShowDialog() == System.Windows.Forms.DialogResult.OK)
    {
        if (entrada.tbEntrada.Text != [redacted])
        {
            KryptonMessageBox.Show("La contraseña que introdujo no es valida, introduzca una contraseña valida", "Error en contraseña", MessageBoxButtons.OK, MessageBoxIcon.Hand);
        }
```

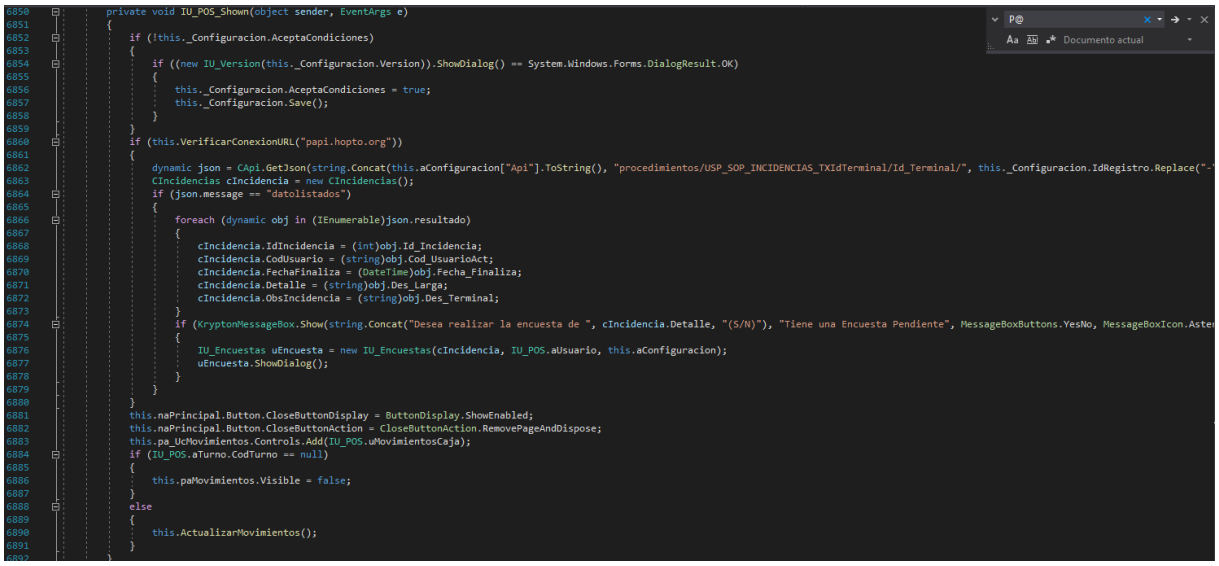
Figura 37 Fragmento de Código de Interfaz donde se Observa Contraseña Soporte Técnico

En la interfaz de IU_POS.Designer se encontró también una dirección web que fue desarrollada en express y que contiene una API para realizar encuestas a los clientes como se observa en la Figura 38 y la Figura 39 se encuentra la dirección exacta de la consulta API, también se puede observar los datos que se listan en las encuestas que realizan.



```
private void btEncuesta_Click(object sender, EventArgs e)
{
    if (!this.VerificarConexionURL("papi.hopto.org"))
    {
        KryptonMessageBox.Show("NO Tenemos Encuestas Pendientes", "Su opinión es muy importante ", MessageBoxButtons.OK, MessageBoxIcon.Exclamation);
    }
    else
    {
        dynamic json = CApi.GetJson(string.Concat(this.aConfiguracion["Api"].ToString(), "procedimientos/USP_SOP_INCIDENCIAS_TXIdTerminal/Id_Terminal/", this._Configuracion.IdRegistro.Replace("-
        CIncidencias cIncidencia = new CIncidencias();
        if (json.message == "datolistados")
        {
            foreach (dynamic obj in (IEnumerable)json.resultado)
            {
                cIncidencia.IdIncidencia = (int)obj.Id_Incidencia;
                cIncidencia.CodUsuario = (string)obj.Cod_UsuarioAct;
                cIncidencia.FechaFinaliza = (DateTime)obj.Fecha_Finaliza;
                cIncidencia.Detalle = (string)obj.Des_Larga;
                cIncidencia.ObsIncidencia = (string)obj.Des_Terminal;
            }
            IU_Encuestas uEncuesta = new IU_Encuestas(cIncidencia, IU_POS.aUsuario, this.aConfiguracion);
            uEncuesta.ShowDialog();
        }
        if (json.message == "nohaydato")
        {
            dynamic json1 = CApi.GetJson(string.Concat(this.aConfiguracion["Api"].ToString(), "procedimientos/USP_SOP_INCIDENCIAS_TXRUCEMPRESA/Nro_Documento/", IU_POS.aEmpresa.RUC));
            if (json1.message == "datolistados")
            {
                foreach (dynamic obj1 in (IEnumerable)json1.resultado)
                {
                    cIncidencia.IdIncidencia = (int)obj1.Id_Incidencia;
                    cIncidencia.CodUsuario = (string)obj1.Cod_UsuarioAct;
                    cIncidencia.FechaFinaliza = (DateTime)obj1.Fecha_Finaliza;
                    cIncidencia.Detalle = (string)obj1.Des_Larga;
                    cIncidencia.ObsIncidencia = (string)obj1.Des_Terminal;
```

Figura 38 Fragmento de Código que muestra la consulta a un API de encuestas



```
private void IU_POS_Shown(object sender, EventArgs e)
{
    if (!this._Configuracion.AceptaCondiciones)
    {
        if ((new IU_Version(this._Configuracion.Version)).ShowDialog() == System.Windows.Forms.DialogResult.OK)
        {
            this._Configuracion.AceptaCondiciones = true;
            this._Configuracion.Save();
        }
    }
    if (this.VerificarConexionURL("papi.hopto.org"))
    {
        dynamic json = CApi.GetJson(string.Concat(this.aConfiguracion["Api"].ToString(), "procedimientos/USP_SOP_INCIDENCIAS_TXIdTerminal/Id_Terminal/", this._Configuracion.IdRegistro.Replace("-
        CIncidencias cIncidencia = new CIncidencias();
        if (json.message == "datolistados")
        {
            foreach (dynamic obj in (IEnumerable)json.resultado)
            {
                cIncidencia.IdIncidencia = (int)obj.Id_Incidencia;
                cIncidencia.CodUsuario = (string)obj.Cod_UsuarioAct;
                cIncidencia.FechaFinaliza = (DateTime)obj.Fecha_Finaliza;
                cIncidencia.Detalle = (string)obj.Des_Larga;
                cIncidencia.ObsIncidencia = (string)obj.Des_Terminal;
            }
            if (KryptonMessageBox.Show(string.Concat("Desea realizar la encuesta de ", cIncidencia.Detalle, "(S/N)"), "Tiene una Encuesta Pendiente", MessageBoxButtons.YesNo, MessageBoxIcon.Aster
            {
                IU_Encuestas uEncuesta = new IU_Encuestas(cIncidencia, IU_POS.aUsuario, this.aConfiguracion);
                uEncuesta.ShowDialog();
            }
        }
    }
    this.naPrincipal.Button.CloseButtonDisplay = ButtonDisplay.ShowEnabled;
    this.naPrincipal.Button.CloseButtonAction = CloseButtonAction.RemovePageAndDispose;
    this.pa_UcMovimientos.Controls.Add(IU_POS.uMovimientosCaja);
    if (IU_POS.aTurno.CodTurno == null)
    {
        this.paMovimientos.Visible = false;
    }
    else
    {
        this.ActualizarMovimientos();
    }
}
```

Figura 39 Fragmento de Código donde se observa el formato de llamado al API de Encuestas

En la Tabla 5 se listaron las vulnerabilidades encontradas previamente, se les dará una valoración siguiendo el Anexo 7, además se tomó en consideración la opinión del administrador, por lo que en una reunión virtual se revisó cada uno de estos puntos con él. El identificador V y la secuencia de numero correspondiente a la vulnerabilidad, siendo la sigla V una abreviación de Vulnerabilidad, las vulnerabilidades identificadas pueden estar compuestas de más de una vulnerabilidad identificada en la etapa previa.

Tabla 5 Identificacion de Vulnerabilidades

Identificador	Vulnerabilidad Identificada	Severidad de la Vulnerabilidad
V01	Acceso con usuario y contraseña a servidor FTP	Alta
V02	Código Descompilable sin alterar los datos del código fuente original	Moderado
V03	Contraseña de Soporte Técnico Expuesta	Moderado
V04	Flujo TCP con encriptado parcial	Moderado
V05	Algoritmo de ofuscación de datos expuesto	Moderado
V06	Acceso a la dirección de Consulta de una API	Bajo

Fuente: NIST SP 800-30 – Identification of Vulnerabilities

3.3.2. Condiciones Predispuestas

Las Condiciones predispuestas son condiciones que afectan ya sea para incrementar o reducir la probabilidad de un evento de amenaza que haya sido iniciado resulte en un impacto adverso, la Metodologia de NIST SP 800-30 provee de taxonomías para las condiciones predispuestas la cual se observa en el Anexo 8, en la Tabla 6 se realizara la identificación de condiciones Predispuestas, con el identificador de CP con la secuencia numérica que corresponda, siendo las siglas CP una abreviación de Condiciones Predispuestas, mientras que la omnipresencia de las condiciones predispuesta son calificadas basándose en la tabla provista por NIST SP 800-30 como se ve en el Anexo 9, se ha usado el tier 3 de NIST SP 800-30 referente a sistemas de información.

Tabla 6 Identificacion de Condiciones Predispuestas

Identificador	Fuente de información sobre condiciones predispuestas	La omnipresencia de la condición
CP01	Cambio en las Políticas de Acceso a la información del Sistema	Alto
CP02	Migración de Tecnología del Sistema	Alto
CP03	Cambio de Personal Esencial para el mantenimiento del Sistema	Moderado
CP04	Mala Configuración o Ausencia de un Firewall	Bajo

Fuente: NIST-SP 800-30 – Identification of Predisposing Conditions

3.4. Fase 4 - Determinar Probabilidad

En esta fase se determinará la probabilidad de que un evento de amenaza se inicie, ocurra o resulte en impacto adverso para ello se usó las escalas de evaluación provistas por NIST SP 800-30, en los Anexos 10,11, y 12 se encuentran respectivamente las escalas de evaluación usadas.

En el Anexo 13 se encuentra la escala de evaluación de la probabilidad general la cual es el resultante de la probabilidad de que un evento de amenaza se inicie u ocurra y de que resulte en impacto adverso, se tomara en cuenta la guía de NIST SP 800-30 y también la o las vulnerabilidades a las que están asociados los eventos de amenaza.

En la Tabla 7 y Tabla 8 se determinó la probabilidad de que un evento de amenaza se inicie tanto adversarial como no adversarial respectivamente, en la Tabla 9 se indicó el impacto adverso que representaría si el evento de amenaza se inicia u ocurre, en la Tabla 10 se indicó la semejanza general que es el resultado de juntar la probabilidad de inicio y el impacto adverso que representa cada evento de amenaza siguiendo el criterio del anexo 12.

Tabla 7 Probabilidad de que un evento de amenaza adversarial se inicie

Identificador Evento de Amenaza	Evento de Amenaza	Probabilidad de Inicio
EAA-01	Realizar reconocimiento y vigilancia de la organización	Alto
EAA-02	Realizar un reconocimiento interno dirigido por programa maligno	Moderado
EAA-03	Crear ataques específicamente basados en el entorno de la tecnología implementada.	Alto
EAA-04	Enviar programa maligno modificado al sistema de información.	Moderado
EAA-05	Enviar programa maligno dirigido a controlar sistemas internos o exfiltración de datos	Bajo
EAA-06	Instalar sniffers persistentes y enfocados en el sistema de información o la red conectada al mismo	Alto
EAA-07	Insertar programa maligno no dirigido en software descargable y/o en	Bajo

	productos comerciales de información y tecnología	
EAA-08	Explotar vulnerabilidades en el sistema de información	Alto
EAA-09	Comprometer software critico de la organización	Bajo
EAA-10	Conducir una autentificación por fuerza bruta	Alto
EAA-11	Causar destrucción /deterioro del sistema de información crítico, componentes y funciones.	Moderado
EAA-12	Explotar información insegura o incompleta en múltiples ambientes	Moderado
EAA-13	Configuración incorrecta de privilegios	Muy Bajo
EAA-14	Introduccion de vulnerabilidades en los productos de software	Bajo
EAA-15	Conducir ataque usando puertos, protocolos y servicios	Muy Alto
EAA-16	Conducir modificación de trafico de red externo (man in the middle)	Moderado
EAA-17	Derrame de información sensible	Moderado
EAA-18	Obtener acceso no autorizado	Moderado
EAA-19	Obtener información por oportunamente escarbar información en los sistemas de información	Alto

Fuente: NIST-SP 800-30 – Likelihood of threat event occurrence (Adversarial)

Tabla 8 Probabilidad de que un evento de amenaza no adversarial ocurra

Identificador del Evento de Amenaza	Evento de Amenaza	Probabilidad de Inicio
EANA-01	Configuración incorrecta de privilegios	Bajo
EANA-02	Terremoto en la localización del servidor principal	Muy Bajo
EANA-03	Introduccion de vulnerabilidades en productos de software	Bajo
EANA-04	Error en el disco duro del servidor principal	Bajo

Fuente: NIST-SP 800-30 – Likelihood of threat event occurrence (non-Adversarial)

Tabla 9 Probabilidad de que un evento de amenaza resulte en un impacto Adverso

Identificador Evento de Amenaza	Evento de Amenaza	Probabilidad de Impacto Adverso
EAA-01	Realizar reconocimiento y vigilancia de la organización	Bajo
EAA-02	Realizar un reconocimiento interno dirigido por programa maligno	Bajo
EAA-03	Crear ataques específicamente basados en el entorno de la tecnología implementada.	Moderado
EAA-04	Enviar programa maligno modificado al sistema de información.	Moderado

EAA-05	Enviar programa maligno dirigida a controlar sistemas internos o exfiltración de datos	Alto
EAA-06	Instalar sniffers persistentes y enfocados en el sistema de información o la red conectada al mismo	Alto
EAA-07	Insertar programa maligno no dirigido en software descargable y/o en productos comerciales de información y tecnología	Bajo
EAA-08	Explotar vulnerabilidades en el sistema de información	Alto
EAA-09	Comprometer software critico de la organización	Moderado
EAA-10	Conducir una autentificación por fuerza bruta	Bajo
EAA-11	Causar destrucción /deterioro del sistema de información crítico, componentes y funciones.	Alto
EAA-12	Explotar información insegura o incompleta en múltiples ambientes	Moderado
EAA-13	Configuración incorrecta de privilegios	Moderado
EAA-14	Introduccion de vulnerabilidades en los productos de software	Alto
EAA-15	Conducir ataque usando puertos, protocolos y servicios	Moderado
EAA-16	Conducir modificación de trafico de red externo (man in the middle)	Moderado
EAA-17	Derrame de información sensible	Moderado
EAA-18	Obtener acceso no autorizado	Moderado
EAA-19	Obtener información por oportunamente escarbar información en los sistemas de información	Moderado

EANA-01	Configuración incorrecta de privilegios	Bajo
EANA-02	Terremoto en la localización del servidor principal	Bajo
EANA-03	Introduccion de vulnerabilidades en productos de software	Bajo
EANA-04	Error en el disco duro del servidor principal	Bajo

Fuente: NIST-SP 800-30 – Likelihood of threat event resulting in Adverse Impact)

Tabla 10 Semejanza General

Identificador Evento de Amenaza	Evento de Amenaza	Probabilidad de Impacto Adverso
EAA-01	Realizar reconocimiento y vigilancia de la organización	Bajo
EAA-02	Realizar un reconocimiento interno dirigido por programa maligno	Bajo
EAA-03	Crear ataques específicamente basados en el entorno de la tecnología implementada.	Moderado
EAA-04	Enviar programa maligno modificado al sistema de información.	Moderado
EAA-05	Enviar programa maligno dirigida a controlar sistemas internos o exfiltración de datos	Moderado
EAA-06	Instalar sniffers persistentes y enfocados en el sistema de información o la red conectada al mismo	Muy Alto
EAA-07	Insertar programa maligno no dirigido en software descargable y/o en productos comerciales de información y tecnología	Bajo

EAA-08	Explotar vulnerabilidades en el sistema de información	Alto
EAA-09	Comprometer software critico de la organización	Moderado
EAA-10	Conducir una autentificación por fuerza bruta	Moderado
EAA-11	Causar destrucción /deterioro del sistema de información crítico, componentes y funciones.	Moderado
EAA-12	Explotar información insegura o incompleta en múltiples ambientes	Moderado
EAA-13	Configuración incorrecta de privilegios	Muy Bajo
EAA-14	Introduccion de vulnerabilidades en los productos de software	Moderado
EAA-15	Conducir ataque usando puertos, protocolos y servicios	Alto
EAA-16	Conducir modificación de trafico de red externo (man in the middle)	Moderado
EAA-17	Derrame de información sensible	Moderado
EAA-18	Obtener acceso no autorizado	Moderado
EAA-19	Obtener información por oportunamente escarbar información en los sistemas de información	Moderado
EANA-01	Configuración incorrecta de privilegios	Bajo
EANA-02	Terremoto en la localización del servidor principal	Muy Bajo
EANA-03	Introduccion de vulnerabilidades en productos de software	Bajo
EANA-04	Error en el disco duro del servidor principal	Bajo

Fuente: NIST-SP 800-30 – Overall Likelihood

3.5. Fase 5 - Determinar Impacto

En esta fase se determinara el impacto que representa cada evento de amenaza basándonos en las pautas que da NIST SP 800-30, se ha medido teniendo en cuenta el impacto máximo, en la Tabla 11 se encuentra organizado por el tipo de impacto, Identificador de Evento de amenaza y Activo Afectado por Impacto, los impactos han sido extraídos del Anexo 14, los impactos se han identificado relacionándolos con los eventos de amenaza, es decir que cada evento de amenaza se relacionó con el respectivo impacto que podría tener, en el Anexo 15 se describe la escala de evaluación de los impactos y una descripción detallada de valor de impacto máximo, que será usada posteriormente en la Tabla 11.

Tabla 11 Nivel de Impacto

Tipo de Impacto	Identificador Evento de Amenaza	Activo Afectado por Impacto	Evento de Amenaza	Impacto Máximo
Daño a los Activos	EAA-01	Daño o perdida en instalaciones físicas de la empresa	Realizar reconocimiento y vigilancia de la organización	Muy Bajo
	EAA-02	Daño o perdida de Activos de información	Realizar un reconocimiento interno dirigido por programa maligno	Muy Bajo
	EAA-03	Perdida de propiedad Intelectual	Crear ataques específicamente basados en el entorno de la tecnología implementada.	Moderado
	EAA-04	Daño o perdida de Activos de información	Enviar programa maligno modificado al	Moderado

			sistema de información.	
	EAA-05	Daño o perdida de Activos de información	Enviar programa maligno dirigida a controlar sistemas internos o exfiltración de datos	Moderado
	EAA-06	Daño o perdida de Activos de información	Instalar sniffers persistentes y enfocados en el sistema de información o la red conectada al mismo	Moderado
	EAA-07	Daño o perdida de Activos de información	Insertar programa maligno no dirigido en software descargable y/o en productos comerciales de información y tecnología	Alta
	EAA-08	Daño o perdida de Activos de información	Explotar vulnerabilidades en el sistema de información	Alta
	EAA-09	Daño o perdida de Activos de información	Comprometer software critico de la organización	Alta

	EAA-10	Daño o perdida de Activos de información	Conducir una autentificación por fuerza bruta	Moderada
	EAA-11	Daño o perdida de Activos de información	Causar destrucción /deterioro del sistema de información crítico, componentes y funciones.	Bajo
	EAA-12	Daño o perdida de Activos de información	Explotar información insegura o incompleta	Moderado
	EAA-13	Daño o perdida de Activos de información	Configuración incorrecta de privilegios	Moderado
	EAA-14	Daño o perdida de Activos de información	Introduccion de vulnerabilidades en los productos de software	Moderado
	EAA-15	Daño o perdida en instalaciones físicas de la empresa	Conducir ataque usando puertos, protocolos y servicios	Moderado
	EAA-16	Daño o perdida de Activos de información	Conducir modificación de trafico de red externo	Moderado
	EANA-02	Daño o perdida de Activos de información	Terremoto en la localización del servidor principal	Bajo

	EANA-03	Daño o perdida de Activos de información	Introduccion de vulnerabilidades en productos de software	Bajo
	EANA-04	Daño o perdida de Activos de información	Error en el disco duro del servidor principal	Bajo
Daño a Otras Organización o Individuos	EAA-17	Daño a la confiabilidad en las relaciones	Derrame de información sensible	Moderado
	EAA-18	Daño a la confiabilidad en las relaciones	Obtener acceso no autorizado	Alto
	EAA-19	Daño a la confiabilidad en las relaciones	Obtener información por oportunamente escarbar en los sistemas de información	Moderado
	EANA-01	Daño a la confiabilidad en las relaciones	Configuración incorrecta de privilegios	Moderado

Fuente: NIST-SP 800-30 – Identification of Adverse Impacts

3.6. Fase 6 - Identificar riesgos basado en los eventos de amenaza.

Esta es la etapa final en la que se usó la metodologia NIST SP 800-30 por lo que se determinó el nivel de riesgo basándose en la combinación de la probabilidad de que el evento de amenaza ocurra y resulte en un impacto adverso, se usó los valores en la Tabla 10 Semejanza General con el nivel de impacto en la Tabla 11 Nivel de Impacto, el criterio para combinar los valores de ambas tablas está en el Anexo 16, una vez obtenidos los valores se evaluara por segunda vez con los criterios del Anexo 17.

Tabla 12 Nivel de Riesgo

Identificador Evento de Amenaza	Evento de Amenaza	Nivel de Riesgo
EAA-01	Realizar reconocimiento y vigilancia de la organización	Muy Bajo
EAA-02	Realizar un reconocimiento interno dirigido por programa maligno	Muy Bajo
EAA-03	Crear ataques específicamente basados en el entorno de la tecnología implementada.	Bajo
EAA-04	Enviar programa maligno modificado al sistema de información.	Moderado
EAA-05	Enviar programa maligno dirigida a controlar sistemas internos o exfiltración de datos	Moderado
EAA-06	Instalar sniffers persistentes y enfocados en el sistema de información o la red conectada al mismo	Moderado
EAA-07	Insertar programa maligno no dirigido en software descargable y/o en productos comerciales de información y tecnología	Bajo
EAA-08	Explotar vulnerabilidades en el sistema de información	Moderado
EAA-09	Comprometer software critico de la organización	Moderado
EAA-10	Conducir una autentificación por fuerza bruta	Moderado
EAA-11	Causar destrucción /deterioro del sistema de información crítico, componentes y funciones.	Bajo

EAA-12	Explotar información insegura o incompleta en múltiples ambientes	Moderado
EAA-13	Configuración incorrecta de privilegios	Muy Bajo
EAA-14	Introduccion de vulnerabilidades en los productos de software	Moderado
EAA-15	Conducir ataque usando puertos, protocolos y servicios	Moderado
EAA-16	Conducir modificación de trafico de red externo (man in the middle)	Moderado
EAA-17	Derrame de información sensible	Moderado
EAA-18	Obtener acceso no autorizado	Moderado
EAA-19	Obtener información por oportunamente escarbar información en los sistemas de información	Moderado
EANA-01	Configuración incorrecta de privilegios	Moderado
EANA-02	Terremoto en la localización del servidor principal	Moderado
EANA-03	Introduccion de vulnerabilidades en productos de software	Moderado
EANA-04	Error en el disco duro del servidor principal	Moderado

Fuente: NIST SP 800-30 - Level of Risk (Combination of Likehood and Impact)

3.7. Fase 7 - Elaborar reporte de la evaluación de riesgos.

Para esta fase de la propuesta se hizo dos tablas resumen, una adversarial y otra no adversarial, en esta tabla los eventos de amenaza están relacionados a una o más vulnerabilidades u condiciones predispuestas, en la Tabla 13 se especificó de que tabla se compondrá la información de los elementos de la tabla resumen.

Tabla 13 Descripción de Tabla Resumen

Columna	Cabecera	Contenido
1	Evento de Amenaza	Tabla 4 Identificacion de Eventos de Amenaza Adversariales, Tabla 3 Identificacion de Eventos de Amenaza no Adversariales
2	Fuente de Amenaza	Tabla 1 Identificación de Fuentes de Amenaza Adversarial, Tabla 2 Identificación de Fuentes de Amenaza no Adversarial
3	Capacidad	Tabla 1 Identificación de Fuentes de Amenaza Adversarial
4	Intención	Tabla 1 Identificación de Fuentes de Amenaza Adversarial
5	Objetivo	Tabla 1 Identificación de Fuentes de Amenaza Adversarial
6	Relevancia	Tabla 4 Identificacion de Eventos de Amenaza Adversariales
7	Probabilidad de inicio de ataque	Tabla 7 Probabilidad de que un evento de amenaza adversarial se inicie, Tabla 8 Probabilidad de que un evento de amenaza no adversarial ocurra
8	Vulnerabilidades y Condiciones Predispuestas	Tabla 5 Identificacion de Vulnerabilidades
9	Severidad y Omnipresencia	Tabla 6 Identificacion de Condiciones Predispuestas**¡Error! No se encuentra el origen de la referencia.**
10	Probabilidad de ataque exitoso	Tabla 9 Probabilidad de que un evento de amenaza resulte en un impacto Adverso
11	Probabilidad general	Tabla 10 Semejanza General
12	Nivel de impacto	Tabla 11 Nivel de Impacto
13	Riesgo	Tabla 12 Nivel de Riesgo

A continuación, en la Tabla 14 Riesgo Adversarial se tomaron los datos de referencia según la Tabla 13 Descripción de Tabla Resumen, en la que se especifica de que tablas se extraen los valores, así como la columna a la que pertenece cada uno.

Tabla 14 Riesgo Adversarial

1	2	3	4	5	6	7	8	9	10	11	12	13
Evento de Amenaza	Fuentes de Amenaza	Características de Fuentes de Amenaza			Relevancia	Probabilidad de inicialización de Ataque	Vulnerabilidad y Condiciones Predispuestas	Severidad y Omnipresencia	Probabilidad de Ataque Exitoso	Probabilidad General	Nivel de Impacto	Riesgo
		Capacidad	Intención	Objetivo								
EAA-01	Insider/Trusted Insider	Muy Baja	Alta	Alta	Posible	Alta	V04	Moderado	Bajo	Bajo	Muy Bajo	Muy Bajo
EAA-02					Posible	Moderado	V04	Moderado	Bajo	Bajo	Muy Bajo	Muy Bajo
EAA-03					Posible	Alta	V02, V05, V06	Muy Alta, Moderado	Moderado	Moderado	Bajo	Bajo
EAA-04					Posible	Moderado	V01, V04	Muy Alta, Moderado	Moderado	Moderado	Moderado	Moderado
EAA-05					Predicho	Baja	V01, V02	Muy Alta	Alto	Moderado	Moderado	Moderado
EAA-06					Posible	Muy Alta	V01, V04	Muy Alta, Moderado	Alto	Muy Alto	Moderado	Moderado

EAA-07					Predicho	Baja	V06, CP02, CP04	Bajo, Alta	Bajo	Bajo	Alta	Bajo
EAA-08					N/A	Alta	V01, V02, V06	Muy Alta	Alto	Alto	Moderada	Moderado
EAA-09					N/A	Baja	V02, V03, V05	Muy Alta, Moderado	Moderado	Moderado	Alta	Moderado
EAA-10					N/A	Alta	V04	Moderado	Bajo	Moderado	Moderada	Moderado
EAA-11					N/A	Moderado	V01, V03, CP04	Muy Alta, Alta	Alto	Bajo	Bajo	Bajo
EAA-12					N/A	Moderado	V01, V04, V05	Muy Alta, Moderado	Moderado	Moderado	Moderado	Moderado
EAA-13					N/A	Muy Baja	CP03, CP04, CP01	Alta	Moderado	Muy Bajo	Moderado	Muy Bajo
EAA-14					N/A	Baja	V01	Muy Alta	Alto	Moderado	Moderado	Moderado
EAA-15					N/A	Muy Alta	V04, CP04	Moderada, Alta	Moderado	Alto	Moderado	Moderado

EAA-16					N/A	Moderado	VP04, CP04	Moderada, Alta	Moderado	Moderado	Moderado	Moderado
EAA-17	Cliente	Moderado	Muy Baja	Muy Baja	N/A	Moderado	V01	Muy Alta, Moderado	Moderado	Moderado	Moderado	Moderado
EAA-18					N/A	Moderado	CP01, CP03, V03	Alta, Muy Alta	Moderado	Moderado	Alto	Moderado
EAA-19					N/A	Alta	V05, V06	Moderado, Baja	Moderado	Moderado	Moderado	Moderado

Fuente: NIST SP 800-30 – Template Adversarial Risk

Tabla 15 Riesgo no Adversarial

1	2	3	4	5	6	7	8	9	10	11
Evento de Amenaza	Fuentes de Amenaza	Rango de Efectos	Relevancia	Probabilidad de Evento de Ocurrencia	Vulnerabilidad y Condiciones Predispuestas	Severidad y Omnipresencia	Probabilidad de Ataque Exitoso	Probabilidad General	Nivel de Impacto	Riesgo
EANA-01	Usuario/Administrador Privilegiados	Bajo	N/A	Alta	CP03	Alto	Bajo	Bajo	Moderado	Bajo
EANA-02	Terremoto	Alto	Esperado	Moderado	-	Moderado	Bajo	Muy Bajo	Bajo	Bajo
EANA-03	Usuario	Bajo	N/A	Alta	V01, CP01	Muy Alto, Alto	Bajo	Bajo	Moderado	Bajo
EANA-04	Almacenamiento	Moderado	Esperado	Moderado	CP02, CP04	Alto, Alto	Bajo	Bajo	Bajo	Bajo

Fuente: NIST SP 800-30 – Template Non-Adversarial Risk

3.8. Fase 8 - Generar Propuesta de Mitigación de Riesgos

Para la última etapa se propondrán mitigaciones a las vulnerabilidades encontradas aplicando los controles de seguridad de la NTP-ISO/IEC 27001:2008, para cada control se incluirá el objetivo del control y el o los controles asociados a la vulnerabilidad.

3.8.1. Acceso con Usuario y Contraseña a servidor FTP

Severidad: Alto

<table>
<tr><td colspan="4">A.9.4 Control de acceso a sistema y aplicación</td></tr>
<tr><td colspan="4">Objetivo: Informar el acceso no autorizado a los sistemas y aplicaciones.</td></tr>
<tr><td rowspan="2">A.9.4.3.</td><td rowspan="2">Sistema de gestión de contraseñas</td><td>Control</td><td>Mitigación Propuesta</td></tr>
<tr><td>Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad.</td><td>Revisar lineamientos para la creación de una contraseña segura (ver anexo 19)</td></tr>
<tr><td colspan="4">A.14.1 Requisitos de seguridad de los sistemas de información</td></tr>
<tr><td colspan="4">Objetivo: Avalar que la seguridad de la información es una parte de los sistemas de información mediante el ciclo de vida completo.</td></tr>
<tr><td rowspan="2">A.14.1.1</td><td rowspan="2">Protección de transacciones en servicios de aplicación</td><td>Control</td><td>Mitigación Propuesta</td></tr>
<tr><td>La información implicada en los servicios de aplicación debe ser protegidos para prevenir transmisión incompleta, ruteo incorrecto, alteración no autorizada de mensajes, divulgación no autorizada.</td><td>Encriptar con un certificado ssl el protocolo FTP (ver anexo 20).</td></tr>
</table>

3.8.2. Código Descompilable sin alterar los datos del código fuente original.

Severidad: Moderado

A.9.4 Control de acceso a sistema y aplicación			
Objetivo: Informar sobre el acceso no autorizado a los sistemas y aplicaciones.			
A.9.4.5	Control de acceso al código fuente de los programas	Control	Mitigación Propuesta
		El acceso al código fuente de los programas debe ser restringido	Usar un ofuscador como puede ser dotfuscator.

3.8.3. Contraseña de Soporte Técnico Expuesta

Severidad: Moderado

A.9.4 Control de acceso a sistema y aplicación			
Objetivo: Informar sobre el acceso no autorizado a los sistemas y aplicaciones.			
A.9.4.1	Restricción de acceso a la información	Control	Mitigación Propuesta
		El acceso a la información y las funciones del sistema de aplicación debe ser restringido.	Restringir el acceso a la interfaz de soporte técnico.
A.9.4.3.	Sistema de gestión de contraseñas	Control	Mitigación Propuesta
		Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad.	Revisar lineamientos para la creación de una contraseña segura (ver anexo 19)
A.14.2 Seguridad en los procesos de Desarrollo y Soporte			
Objetivo: Informar sobre el acceso no autorizado a los sistemas y aplicaciones.			
A.14.2.1	Política de desarrollo seguro	Control	Mitigación Propuesta
		Pautas para el progreso de software y sistemas deben ser establecidas.	Asignar reglas en el desarrollo para evitar contraseñas expuestas en código.

3.8.4. Flujo TCP con encriptado parcial

Severidad: Moderado

A.10.1 Controles Criptográficos			
Objetivo: Asegurar el uso apropiado y efectivo de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información.			
A.10.1.1	Política sobre el uso de controles criptográficos	Control	Mitigación Propuesta
		Se debe fortalecer e implementar la política de uso de controles criptográficos para proteger la información.	Definir políticas para el uso de controles criptográficos.
A.10.1.2	Gestión de claves	Control	Mitigación Propuesta
		Se debe fortalecer e implementar la política de uso de controles criptográficos para proteger la información.	Establecer una política sobre el tiempo de vida de las claves criptográficas

3.8.5. Algoritmo de ofuscación de datos expuesto y Acceso a la dirección de Consulta de una API

Severidad: Bajo

A.14.2 Seguridad en los procesos de Desarrollo y Soporte			
Objetivo: Informar sobre el acceso no autorizado a los sistemas y aplicaciones.			
A.14.2.1	Política de desarrollo seguro	Control	Mitigación Propuesta
		Pautas para el progreso de software y sistemas deben ser establecidas.	Asignar reglas en el desarrollo para evitar la exposición de las rutas consultadas por el sistema.

CAPITULO 4 - Resultados

4.1. Comprobación de la prospectiva

Se espera que esta propuesta de mitigación y evaluación de riesgos basados en NIST SP 800-30 y Pentesting standard pueda ser usada para tomar decisiones de negocio sobre el sistema de IFacturacion y de esa manera ayudar a mejorar el sistema.

Para realizar la evaluación de riesgos primero se hizo una recolección de información usando diferentes herramientas con el objetivo de detectar posibles vulnerabilidades, y posibles entradas a los activos del sistema de información, esta recolección de información marcara el camino de la propuesta, ya que las vulnerabilidades se identificarán basado en esta recolección.

Una vez terminada la recolección de información, se identificó las fuentes de amenaza basado en la metodologia NIST SP 800-30. Seguidamente se buscó las vulnerabilidades usando la metodologia de Pentesting Standard mientras que las condiciones predispuestas se identificaron usando la mitología de NIST SP 800-30, las escalas para medir los resultados son Muy Alto, Alto, Moderado, Bajo, Muy Bajo, para continuar con la metodología NIST SP 800-30 emparejaron los eventos de amenaza con las vulnerabilidades identificadas, cada evento de amenaza tiene una probabilidad de inicio, impacto, vulnerabilidades y su riesgo estimado. Finalmente, para la propuesta de mitigaciones se usó el NTP ISO/IEC 27001:2008, por lo que se asignaron controles del ISO a cada vulnerabilidad y una mitigación relacionada a cada control.

De acuerdo con las recomendaciones a las que llegaron en el antecedente de “DISEÑO DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION BASADO EN LA NORMA ISO/IEC 27001:2013 PARA LA MUNICIPALIDAD DISTRITAL DE EL AGUSTINO” – Tesis de pregrado de la Universidad Peruana de Ciencias Aplicadas – Lima. Dice, “Se recomienda revisar la metodología de gestión de riesgos para evaluar su efectividad y realizar mejoras en su implementación.”
Se coincide con la recomendación que da el investigador en el antecedente, de revisar metodologías de gestión de riesgos.
Mientras que con el antecedente “DISEÑO DE UN MODEOL DE SEGURIDAD DE LA INFORMACION, BASDO EN OSSTMv3, NIST SP 800-30 E ISO 27001, PARA

CENTROS DE EDUCACION: CASO DE ESTUDIO UNIVERSIDAD REGIONAL AUTONOMA DE LOS ANDES, EXTENSION TULCAN" – Tesis Maestría de la Universidad Internacional SEK – Ecuador. Dice "Se recomiendan los modelos de seguridad OSSTMMv3 y NIST 800-30 porque son más flexibles y se pueden personalizar según las necesidades de la organización, a diferencia de la ISO 27001, que es estricta y requiere certificación para esta norma. Por ello se recomienda que esto se haga desde la matriz y no solo desde la extensión de la universidad".

Se coincide con la conclusión a la que llega la investigadora de en el antecedente anteriormente mencionado, ya que efectivamente NIST SP 800-30 es una metodologia flexible e integrable con otras como es el caso del Pentesting Standart por lo que las metodologías propuestas tendrán un impacto significativo y positivo en la evaluación de riesgos, mientras que la NTP ISO/IEC 2701:2014 tendrá impacto positivo y significativo en la propuesta de mitigación de riesgos.

Poe lo que se puede concluir que presente tesis tendrá impacto positivo y significativo para la toma de decisiones en los procesos de negocio relacionados con el sistema de IFacturacion de la empresa Pale Consultores.

4.2. Cumplimiento de objetivos

El desarrollo de la investigación propone mitigaciones a los riesgos en el sistema IFacturacion de la empresa Pale Consultores, basado en NIST SP 800-30. El proceso de recolección de información, identificación vulnerabilidades y mitigación fue basado en la metodología Pentesting Standard.

Para la recolección de información se usó el Pentesting Standard, en el que se usaron herramientas sugeridas por la metodologia como por ejemplo WireShark y Nmap, siendo el sistema desarrollado en un entorno de escritorio no se pudo hacer uso de muchas de las herramientas sugeridas por Pentesting Standard ya que están orientados a entornos Web, a su vez se identificó los eventos de amenaza y fuentes de amenaza basado en la metodologia de NIST SP800-30.

Basado en la recolección de información se hizo una identificación de vulnerabilidades, en su mayoría las vulnerabilidades encontradas están relacionado al código fuente y a los puertos que usa el sistema de IFacturacion, como se mencionó

anteriormente el hecho de que sea en un entorno desktop dificulta el uso de herramientas prefabricadas para el análisis de vulnerabilidades.

Se aplico el Tier 3 de NIST SP800-30 el cual está orientado a sistemas de información, para el riesgo que representa cada evento de amenaza, dicho riesgo fue definido basado en el impacto que representa cada uno y la probabilidad general, la probabilidad general es el resultado de la probabilidad de que el evento de amenaza se inició y la probabilidad de que el evento de amenaza resulte en un impacto adverso, la escala de valoración para la probabilidad, el impacto y el riesgo es Muy Alto, Alto, Moderado, Bajo, Muy Bajo.
Se aplico la tabla desarrollada en NIST SP 800-30 para el reporte de evaluación de riesgos, donde se muestran los resultados de la investigación por cada evento de amenaza identificado tanto de amenazas adversariales como no adversariales.

La propuesta de mitigación se basó en las vulnerabilidades identificadas previamente ya que los riesgos asociados a los eventos de amenaza están directamente relacionados a las vulnerabilidades que pueden generar un impacto en el sistema. La propuesta de mitigaciones se hizo usando los controles del NTP ISO/IEC 27001:2008 para cada vulnerabilidad identificada, además se hizo una propuesta de mitigación para control.

De acuerdo con los lineamientos y tablas ofrecidas por NIST SP800-30 y Pentesting Standard, se logró evaluar los riesgos, más el apoyo de los controles de NTP ISO/IEC 27001 se logró proponer mitigaciones a las vulnerabilidades identificadas.

4.3. Contribuciones(impacto)

La información es el activo más importante que tiene toda empresa, sin embargo, cuando un sistema de información tiene vulnerabilidades explotables, es cuando se tiene que tomar una decisión de negocio relacionado a sus activos de información, por lo que saber los riesgos que representan las vulnerabilidades es muy importante, debido a que con esta información se puede saber si mitigar las vulnerabilidades, reducirlas o aceptarlas.

Por lo que se espera que la empresa Pale Consultores sea consciente de las vulnerabilidades en el sistema IFacturacion, para que pueda tomar una decisión de manera eficiente y efectiva en caso de sufrir un ataque informático relacionado a IFacturacion.

Glosario

Firewall: Dispositivo que puede ser físico o lógico que permite bloquear el tráfico de red no autorizado y permite el paso del tráfico de red autorizado a través de reglas y normas.

Sniffers: Aplicaciones de software en la mayoría de los casos que se encargan de capturar y analizar los paquetes que se encuentren en la comunicación entre dispositivos.

Man in the Middle: Es un ataque que permite al perpetrador posicionarse en el medio de una comunicación entre un usuario y una aplicación.

TTPs (Tactics, Techniques and Procedures): Son patrones de actividades o métodos asociados con un actor de amenaza especifico o un grupo de actores de amenaza.

Ofuscar: Sirve para hacer que una parte del código o todo el código inentendible o difícil de entender, en su mayoría son software.

Desofuscar: Es la acción contraria a Ofuscar, es decir que a través de credenciales especificas se revierte la ofuscación.

API (Application Programming Interfaces): Son un conjunto de definiciones y protocolos que permiten la integración de dos o más aplicaciones.

TDS (Tabular Data Stream): Es un protocolo de capa de aplicación usado para transferir información entre un servidor de base de datos y el cliente.

Exploit: Son software o secuencias de comandos que aprovechan una vulnerabilidad para provocar un comportamiento no previsto en un software, hardware o dispositivos electrónicos.

Conclusiones

1. Las Metodologías NIST SP 800-30 y Pentesting Standard pueden ser usadas conjuntamente debido a la flexibilidad que te otorga la metodologia de Pentesting Standard.

2. El uso de la metodologia de Pentesting Standard para la recolección de información es altamente efectivo permitiendo al investigador buscar la información por todos los métodos posibles sin ningún tipo de restricción excepto lo pactado con la empresa.

3. La metodología de Pentesting Standard ayuda de manera eficiente a realizar el análisis de vulnerabilidades debido a las pautas otorgadas por la metodologia sirven para tener en consideración herramientas y protocolos en los que se suelen encontrar vulnerabilidades, sin embargo, la mayoría de las herramientas están orientadas a entorno web por lo que en un entorno de aplicación de escritorio dificulta el uso de dichas herramientas.

4. NIST SP 800-30 provee las herramientas necesarias para identificar riesgos basados en los eventos de amenaza que se hayan identificado previamente, además de ello provee tablas guía que permiten encajar los eventos de amenaza con el riesgo que representan lo más cercano a la realidad del caso de estudio.

5. El cuadro de resumen provisto por NIST SP 800-30 ayuda a resumir los resultados permitiendo de esta manera una mejor visualización de los resultados de la investigación, además permite evaluar el impacto que representa cada evento de amenaza de manera fácil.

6. Las mitigaciones propuestas están orientadas a las vulnerabilidades encontradas, en su mayoría las vulnerabilidades encontradas fueron relacionadas al código fuente y a los puertos comunes, por lo que se pudo encontrar rápidamente documentación relacionada a las vulnerabilidades, esto facilito en gran medida las mitigaciones propuestas debido que se ajustaron con más flexibilidad a los controles de la NTP ISO IEC 27001:2008.

Recomendaciones

1. Se recomienda realizar un Pentesting al Sistema de IFacturacion por lo menos una vez cada trimestre.

2. Se recomienda Aplicar la Metodología de NIST SP 800-30 para identificar los riesgos de Tier 1 de la metodologia que están orientados a los procesos de negocio de Pale Consultores.

3. Se recomienda la implementación de la propuesta de mitigación de riesgos en el sistema de IFacturacion de la empresa Pale Consultores usando las metodologías NIST SP 800-30 y Pentesting Standard.

4. Debido al uso exitoso de ambas metodologías se recomienda el uso de estas para futuras investigaciones, que requieran un Pentesting de por medio.

Referencias Bibliograficas

Alonso Cebrian Jose Maria. (n.d.). *Un informático en el lado del mal*. Retrieved 2 April 2020, from https://www.elladodelmal.com/

Barker, E. B. (2016). *Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms* (NIST SP 800-175B; p. NIST SP 800-175B). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-175B

Behera, C. K., & Bhaskari, D. L. (2015). Different Obfuscation Techniques for Code Protection. *Procedia Computer Science*, *70*, 757–763. https://doi.org/10.1016/j.procs.2015.10.114

Bishop, M. (n.d.). *Vulnerabilities Analysis*. 14.

Blakley, B., Systems, T., McDermott, E., MorganChase, J. P., & Geer, D. (n.d.). *Information Security is Information Risk Management*. 8.

Comision de Normalizacion y de Fiscalizacion de Barreras Comerciales No Arancelarias-INDECOPI. (n.d.). *Kupdf.net_ntp-iso-iec-27001-2014.pdf*.

CVE - Common Vulnerabilities and Exposures (CVE). (n.d.). Retrieved 2 April 2020, from https://cve.mitre.org/

CWE - Common Weakness Enumeration. (n.d.). Retrieved 2 April 2020, from https://cwe.mitre.org/

DS-066-2011-PCM.pdf. (n.d.).

Estado de la seguridad en las empresas de Perú | WeLiveSecurity. (n.d.). Retrieved 22 May 2020, from https://www.welivesecurity.com/la-es/infographics/estado-seguridad-empresas-peru/

Factura Electrónica—¿Qué es la factura electrónica? (n.d.). Retrieved 9 June 2021, from https://www.facturae.gob.es/factura-electronica/Paginas/factura-electronica.aspx

Friedman, J., & Bouchard, M. (2015). *Definitive guide to cyber threat intelligence: Using*

knowledge about adversaries to win the war against targeted attacks.

Grassi, P. A., Fenton, J. L., Newton, E. M., Perlner, R. A., Regenscheid, A. R., Burr, W. E., Richer, J. P., Lefkovitz, N. B., Danker, J. M., Choong, Y.-Y., Greene, K. K., & Theofanos, M. F. (2017). *Digital identity guidelines: Authentication and lifecycle management* (NIST SP 800-63b; p. NIST SP 800-63b). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-63b

Gutierrez Salazar Pablo. (2019). *Hackers White Book how become a profesional hacker* (WhiteSuit Hacking, 2019).

Inspector Pablo Alonso. (2019). *Delitos Contra la Confidenciabilidad Integridad y Disponibilidad de los datos y sistema Informaticos*. BIT. http://ccoomadrid.com/comunes/recursos/99922/doc28596_Seguridad_informatica.pdf

Instituto Superior Tecnológico Sistemas del Sur. (2020). *TEMA_1_INTRODUCCION_A_LA_SEGURIDAD_INFORMATICA.pdf*.

Joint Task Force Transformation Initiative. (2012). *Guide for conducting risk assessments* (NIST SP 800-30r1; 0 ed., p. NIST SP 800-30r1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-30r1

Mitos sobre malware #5: Exploit es lo mismo que malware | WeLiveSecurity. (n.d.). Retrieved 31 March 2020, from https://www.welivesecurity.com/la-es/2014/08/05/mitos-sobre-malware-5-exploit-es-malware/

NVD - Home. (n.d.). Retrieved 2 April 2020, from https://nvd.nist.gov/

Pérez Andrés, G., Gisbert Soler, V., & Pérez Bernabeu, E. (2017). REINGENIERÍA DE PROCESOS. *3C Empresa: Investigación y pensamiento crítico*, *6*(5), 81–91. https://doi.org/10.17993/3cemp.2017.especial.81-91

Pomerantz Jeffrey. (2015). *Metadata* (The MIT Press). Mit Press books.

¿Qué Sistema de Gestión de Seguridad de la Información ISO 27001? (n.d.). Retrieved 9 June

2021, from https://www.isotools.org/2016/07/07/sistema-gestion-seguridad-la-informacion-basado-la-norma-iso-27001/

Rahim, R. (2017). *MAN-IN-THE-MIDDLE-ATTACK PREVENTION USING INTERLOCK PROTOCOL METHOD* [Preprint]. INA-Rxiv. https://doi.org/10.31227/osf.io/8txn7

Romero Castro, M. I., Figueroa Morán, G. L., Vera Navarrete, D. S., Álava Cruzatty, J. E., Parrales Anzúles, G. R., Álava Mero, C. J., Murillo Quimiz, Á. L., & Castillo Merino, M. A. (2018). *Introducción a la seguridad informática y el análisis de vulnerabilidades* (1st ed.). Editorial Científica 3Ciencias. https://doi.org/10.17993/IngyTec.2018.46

¿Sabes qué es un exploit y cómo funciona? | WeLiveSecurity. (n.d.). Retrieved 31 March 2020, from https://www.welivesecurity.com/la-es/2014/10/09/exploits-que-son-como-funcionan/

¿Seguridad informática o seguridad de la información? (n.d.). Retrieved 2 April 2020, from https://www.pmg-ssi.com/2017/01/seguridad-de-la-informacion/

Sheikhpour, R., & Modiri, N. (2012). An approach to map COBIT processes to ISO/IEC 27001 information security management controls. *International Journal of Security and Its Applications*, *6*, 13–28.

Tanenbaum, A. S., Wetherall, D. J., & Vidal Romero Elizondo, A. (2016). *Redes de computadoras*. https://elibro.net/ereader/elibrodemo/37871

The PTES Team. (2017). *The Penetration Testing Execution Standard Documentation*.

Universidad Peruana de Ciencias Aplicadas (UPC), & Monteza Mera, L. O. (2019). *Diseño de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001:2013 para la Municipalidad Distrital de El Agustino* [Pregrado, Universidad Peruana de Ciencias Aplicadas (UPC)]. https://doi.org/10.19083/tesis/652121

Zafra, J. L. G. (n.d.). *Introducción al pentesting*. 66.

Anexos

Anexo 1 - Taxonomía de Fuentes de Amenaza

Tabla 16 Fuentes de Amenaza

Tipo de Fuente de Amenaza	Descripción	Características

ADVERSARIAL
- Individual
  - Independiente
  - Insider
  - Trusted Insider
  - Privileged Insider
- Grupo
  - Ad hoc
  - Establecido
- Organización
  - Competidor
  - Proveedor
  - Socios
  - Cliente
- Estado-Nación
	Individuos, grupos, organizaciones, o estados que buscan explotar los recursos cibernéticos de la organización.	Capacidad, Intención, Orientación

ACCIDENTAL - Usuario - Usuario Privilegiado/Administrador	Errores realizados por individuos ejecutando las responsabilidades diarias.	Rango de Efectos

ESTRUCTURAL
- Tecnología de la Informacion
  - Almacenamiento
  - Procesamiento
  - Comunicaciones
  - Pantalla
  - Sensor
  - Controladores
- Controles Ambientales
  - Temperatura/Controles de humedad
  - Fuente de Poder
- Software
  - Sistema Operativo
  - Redes
  - Propósito general de la aplicación
  - Misión específica de la aplicación
	Fallas de equipos, controles ambientales o software debido al envejecimiento, el agotamiento de los recursos u otras circunstancias que exceden las expectativas de funcionamiento.	Rango de Efectos

Ambiental - Desastre Natural o causo por humanos - Fuego.	Desastres naturales y fallas de infraestructuras críticas en la organización, pero que están fuera de control de la organización.	Rango de Efectos

- Tsunami/Inundación. - Tornado/Tormenta. - Huracán. - Terremoto. - Bombardeo. - Invasión. - Evento Natural Inusual - Falla/Corte Infraestructural - Telecomunicaciones - Energía Eléctrica	Nota: Los desastres naturales y provocados por el hombre también pueden caracterizados en términos de su gravedad y / o duración. Sin embargo, debido a que la fuente de amenaza y el evento de amenaza están fuertemente identificados, la gravedad y la duración pueden ser incluido en la descripción del evento de amenaza (por ejemplo, Un huracán de categoría 5 causa grandes daños a las instalaciones que albergan sistemas de misión crítica, lo que sistemas no disponibles).	

Fuente: NIST SP 800-30 – Taxonomy of Threat Sources

Anexo 2 – Escala de Evaluación Característica de Capacidad Adversarial

Tabla 17 Escala de Evaluación - Característica de Capacidad Adversarial

Valores Cualitativos	Descripción
Muy Alto	El adversario tiene un nivel sofisticado de pericia, por lo que puede generar oportunidades para apoyar múltiples ataques efectivos, continuos y coordinados.
Alto	El adversario tiene un nivel sofisticado de pericia, con muchos recursos y oportunidades para apoyar múltiples ataques efectivos y coordinados.
Moderado	El adversario tiene un nivel sofisticado de pericia, con muchos recursos y oportunidades para apoyar múltiples ataques efectivos y coordinados.
Bajo	El adversario tiene recursos, pericia, y oportunidades limitadas para apoyar un ataque efectivo.
Muy Bajo	El adversario tiene recursos, pericia, y oportunidades muy limitadas para apoyar un ataque efectivo.

Fuente: NIST SP 800-30 – Assessment Scale – Characteristic of Adversary Capability

Anexo 3 - Escala de Evaluación Característica de Intención Adversarial

Tabla 18 Escala de Evaluación Característica de Intención Adversarial

Valores Cualitativos	Descripción
Muy Alto	El adversario busca desmejorar, obstaculizar gravemente o destruir una misión central o función comercial, programa o empresa explotando una presencia en los sistemas de información o la infraestructura de la organización.
Alto	El adversario busca desmejorar / impedir aspectos críticos de una misión o función comercial, programa o empresa central, o colocarse en una posición para hacerlo en el futuro, manteniendo una presencia en los sistemas de información o la infraestructura de la organización.
Moderado	El adversario busca lograr o modificar información crítica o sensible específica o usurpar / interrumpir los recursos cibernéticos de la organización estableciendo un punto de apoyo en los sistemas de información o la infraestructura de la organización.
Bajo	El adversario busca rápidamente obtener información crítica o sensible o usurpar / interrumpir los recursos cibernéticos de la organización, y lo hace sin preocuparse por la detección / divulgación de ataques de técnicas comerciales.
Muy Bajo	El adversario busca usurpar, interrumpir o desfigurar los recursos cibernéticos de la organización, y lo hace sin preocuparse por la detección de ataques o la divulgación de técnicas comerciales.

Fuente: NIST SP 800-30 – Assessment Scale – Characteristic of Adversary Intent

Anexo 4 - Escala de Evaluación Característica de Focalización Adversarial

Tabla 19 Escala de Evaluación Característica de Focalización Adversarial

Valores Cualitativos	Descripción
Muy Alto	El adversario analiza la información obtenida a través del reconocimiento y ataque para apuntar a una organización, empresa, programa, misión o función comercial específica, información objetivo, recursos, líneas de disponibilidad, funciones específicas de alto valor o tareas específicas; un empleado o puesto en particular; Soporte para proveedores/proveedores de infraestructura; u organizaciones asociadas
Alto	Los competidores analizan la información obtenida a través de la encuesta para enfocarse en una organización, empresa, programa, tarea o función comercial de manera continua, o información objetivo, recursos, nivel de suministro o una función importante o de alto valor.
Moderado	Los competidores analizan la información disponible públicamente para apuntar a organizaciones de alto valor o programas.
Bajo	El adversario utiliza información disponible públicamente para apuntar a una clase de organizaciones o información de alto valor y busca objetivos de oportunidad dentro de esa clase.
Muy Bajo	El adversario puede o no apuntar a organizaciones o clases de organizaciones específicas.

Fuente: NIST SP 800-30 – Assessment Scale – Characteristic of Adversary Targeting

Anexo 5 - Escala de Evaluación Rango de efectos para Fuentes de Amenaza no adversarial

Tabla 20 Escala de Evaluación Rango de efectos para Fuentes de Amenaza no adversarial

Valores Cualitativos	Descripción
Muy Alto	Los efectos de un error, accidente o acto natural son drásticos e involucran la mayoría de los recursos cibernéticos del Nivel 3: sistemas de información.
Alto	Los efectos de un error, accidente o acto natural son drásticos e involucran la mayoría de los recursos cibernéticos del Nivel 3: sistemas de información.
Moderado	Los efectos de un error, accidente o acto natural son drásticos e involucran la mayoría de los recursos cibernéticos del Nivel 3: sistemas de información.
Bajo	Los efectos de un error, accidente o acto natural son drásticos e involucran la mayoría de los recursos cibernéticos del Nivel 3: sistemas de información.
Muy Bajo	Los efectos de un error, accidente o acto natural son drásticos e involucran la mayoría de los recursos cibernéticos del Nivel 3 sistemas de información.

Fuente: NIST SP 800-30 – Assessment Scale – Range of Effects for Non-Adversarial Threat Source

Anexo 6 - Relevancia de Eventos de Amenaza

Tabla 21 Relevancia de Eventos de Amenaza

Valor	Descripción
Confirmado	El evento de amenaza ha sido visto por la organización
Esperado	El evento de amenaza ha sido visto por los compañeros de la organización
Anticipado	El evento de amenaza ha sido reportado por una fuente confiable
Predicho	El evento de amenaza ha sido predicho por una fuente confiable
Posible	El evento de amenaza ha sido descrito por alguna fuente creíble
N/A	El evento de amenaza no es aplicable.

Fuente: NIST SP 800-30 – Assessment Scale – Range of Effects for Non-Adversarial Threat Sources

Anexo 7 - Severidad de Vulnerabilidades

Tabla 22 Severidad de Vulnerabilidades

Valores Cualitativos	Descripción
Muy Alta	La vulnerabilidad está expuesta y explotable, y la explotación puede resultar en impactos severos. Controles de seguridad o remedios no están implementados ni planeados; o no hay medida identificada para remediar la vulnerabilidad.
Alta	La vulnerabilidad es una preocupación importante, en función de cuán vulnerable es la vulnerabilidad, cuán fácilmente puede explotarse y/o la gravedad de los efectos potenciales de su explotación. Control de Seguridad está planeado, pero no implementado, existen controles de compensación que son mínimamente efectivos.
Moderado	La vulnerabilidad es una preocupación importante, en función de cuán vulnerable es la vulnerabilidad, cuán fácilmente puede explotarse y/o la gravedad de los efectos potenciales de su explotación. Control de seguridad o remediación está parcialmente implementado y algo efectivo.
Baja	La vulnerabilidad es de preocupación baja, pero la efectividad del remedio puede ser mejorado. Control de seguridad u otro remedio está completamente implementado y algo efectivo.
Muy Baja	La vulnerabilidad no es preocupante. Control de seguridad u otro remedio está completamente implementado, evaluado y efectivo.

Fuente: NIST SP 800-30 – Assessment Scale Vulnerability Severity

Anexo 8 – Taxonomía de Condiciones Predispuestas

Tipos de Condiciones Predispuestas	Descripción
RELACIONADA A LA INFORMACION - Seguridad de la información clasificada Nacionalmente - Compartimientos - Informacion no clasificada Controlada - Informacion Identificable Personal - Programa de Acceso Especial - Determinado por Acuerdo - NOFORN - Propiedad	Necesita manejar la información (a medida que se crea, transmite, almacena, procesa y / o muestra) de una manera específica, debido a su sensibilidad (o falta de sensibilidad), requisitos legales o reglamentarios y / o acuerdos contractuales u otros acuerdos organizativos.
TECNICA - Arquitectura - Cumplimiento de la norma técnica. - Uso de productos específicos o línea de productos. - Soluciones y / o enfoques para la colaboración basada en el usuario y el intercambio de información. - Asignación de funciones de seguridad específicas a controles comunes. - Funcional - Múltiples usuarios de Red - Ser unico / sin red - Restricción de Funcionalidades	Necesita usar tecnología de maneras especificas
OPERACIONAL / AMBIENTAL - Movilidad - Sitio Arreglado - Semi móvil - Basado en tierra, aerotransportado, basado en el mar, basado en el espacio - Móvil - Población acceso físico o lógico a los componentes de los sistemas de información. - Tamaño de Población - Investigación de antecedentes de la población	Capacidad para confiar en los controles físicos, de procedimiento y de personal proporcionados por el entorno operativo.

Anexo 9 – Omnipresencia de Condiciones Predispuestas

Tabla 23 Omnipresencia de Condiciones Predispuestas

Valores Cualitativos	Descripción
Muy Alta	Aplica a todos los módulos del sistema de información.
Alta	Aplica a casi todos los módulos del sistema de información.
Moderado	Aplica a varios de los módulos del sistema de información.
Baja	Aplica a algunos de los módulos del sistema de información.
Muy baja	Aplica a pocos de los módulos del sistema de información.

Fuente: NIST SP 800-30 – Assessment Scale – Pervasiveness of Predisposing Conditions

Anexo 10 – Probabilidad de que un evento de amenaza se inicie (Adversarial)

Para la valoración de cada uno de los eventos de amenaza, se tomaron en cuenta los datos recolectados en las etapas de análisis de vulnerabilidades y la etapa de recolección de información.

Tabla 24 Criterio de evento de amenaza se inicie (Adversarial)

Evento de amenaza	Etapa que apoyo la valoración
Realizar reconocimiento y vigilancia de la organización	Se uso la información de las Figura 8, Figura 9, Figura 10, Figura 11, Figura 12, Figura 13, Figura 14 para la valoración.
Realizar un reconocimiento interno dirigido por programa maligno	*Se uso la información de la* Figura 26 Figura 26 Acceso al Servidor mediante FileZilla para la valoración.
Crear ataques específicamente basados en el entorno de la tecnología implementada.	En la fase de recolección de información se identificó la tecnología, siendo Kali Linux el sistema operativo que se usó para las pruebas.
Enviar programa maligno modificado al sistema de información.	*Se uso la información de la* Figura 26 Figura 26 Acceso al Servidor mediante FileZilla para la valoración.
Enviar programa maligno dirigido a controlar sistemas internos o exfiltración de datos	*Se uso la información de la* Figura 26

	Figura 26 Acceso al Servidor mediante FileZilla para la valoración.
Instalar sniffers persistentes y enfocados en el sistema de información o la red conectada al mismo	Se uso la información de las Figura 8, Figura 9, Figura 10, Figura 11, Figura 12, Figura 13, Figura 14 para la valoración.
Insertar programa maligno no dirigido en software descargable y/o en productos comerciales de información y tecnología	*Se uso la información de la* Figura 26 Figura 26 Acceso al Servidor mediante FileZilla para la valoración.
Explotar vulnerabilidades en el sistema de información	Se uso la información de Tabla 5 Identificacion de Vulnerabilidades para la valoración.
Comprometer software critico de la organización	Se uso la información Figura 35 Fragmento de Código de DBConecction, Figura 36 Fragmento de Código que Solicita la cadena de conexión para la valoración.
Conducir una autentificación por fuerza bruta	Debido a que el sistema de información no tiene límites de intentos se podría autenticar mediante fuerza bruta.
Causar destrucción /deterioro del sistema de información crítico, componentes y funciones.	En la recolección de información y en el análisis de vulnerabilidades, no hay vulnerabilidades o eventos que apunten a este por lo que se tomó la valoración más baja.
Explotar información insegura o incompleta en múltiples ambientes	Se uso la información de Figura 37 Fragmento de Código de Interfaz donde se Observa Contraseña Soporte Técnico para la valoración.
Configuración incorrecta de privilegios	En la recolección y análisis de vulnerabilidades no se encontró información relacionada a esto, además de que en la entrevista con el administrador indico que no hay registros de que haya pasado, por lo que se tomó la valoración más baja.
Introduccion de vulnerabilidades en los productos de software	*Se uso la información de la* Figura 26 Figura 26 Acceso al Servidor mediante FileZilla para la valoración.
Conducir ataque usando puertos, protocolos y servicios	Se uso la información Figura 15 Analisis de Puerto y Servicios de la IP de un servidor de Pale Consultores para la valoración.
Conducir modificación de trafico de red externo (man in the middle)	En la recolección y análisis de vulnerabilidades no se encontró información relacionada a esto, por lo que se tomó la valoración más baja.

Derrame de información sensible	Se uso la información de Figura 37 Fragmento de Código de Interfaz donde se Observa Contraseña Soporte Técnico para la valoración.
Obtener acceso no autorizado	En la recolección y análisis de vulnerabilidades no se encontró información relacionada a esto, además de que en la entrevista con el administrador indico que no hay registros de que haya pasado, por lo que se tomó la valoración más baja.
Obtener información por oportunamente escarbar información en los sistemas de información	Se uso la información de Figura 37 Fragmento de Código de Interfaz donde se Observa Contraseña Soporte Técnico para la valoración.

Tabla 25 Probabilidad de que un evento de amenaza se inicie (Adversarial)

Valores Cualitativos	Descripción
Muy Alta	Es casi seguro que el adversario inicie un evento de amenaza.
Alta	Es altamente probable que el adversario inicie un evento de amenaza.
Moderado	Es algo probable que el adversario inicie un evento de amenaza.
Baja	Es improbable que el adversario iniciara un evento de amenaza.
Muy baja	Es altamente improbable que el adversario iniciara un evento de amenaza.

Fuente: NIST SP 800-30 – Assessment Scale – Likelihood of threat event initiation (Adversarial)

Anexo 11 – Probabilidad de que un evento de amenaza ocurra (no-adversarial)

La información que se usó para esta tabla fue extraída de la entrevista hecha con el administrador del sistema.

Tabla 26 Probabilidad de que un evento de amenaza ocurra(no-adversarial)

Valores Cualitativos	Descripción
Muy Alta	Error, Accidente, o acto de la naturaleza es casi seguro que ocurra, o que ocurra más de 100 veces en un año.
Alta	Error, Accidente, o acto de la naturaleza es altamente probable que ocurra, o que ocurra entre10 - 100 veces en un año.
Moderado	Error, Accidente, o acto de la naturaleza es algo probable que ocurra, o que ocurra entre 1 - 10 veces en un año.
Baja	Error, Accidente, o acto de la naturaleza es improbable que ocurra, o que ocurra menos de una vez por año, pero más de una vez en 10 años.
Muy baja	Error, Accidente, o acto de la naturaleza es altamente improbable que ocurra, o que ocurra menos de una vez cada 10 años.

Fuente: NIST SP 800-30– Assessment Scale – Likelihood of threat event occurrence (non-Adversarial)

Anexo 12 – Probabilidad de que un evento de amenaza resulte en un impacto adverso

Para determinar el impacto adverso de los eventos de amenaza, se hizo una reunión con el administrador del sistema, para que con él se pueda determinar el impacto esperado en caso ocurran los eventos de amenaza.

Tabla 27 Probabilidad de que un evento de amenaza resulte en un impacto adverso

Valores Cualitativos	Descripción
Muy Alta	Si el evento de amenaza es iniciado u ocurre, es casi seguro que tenga impactos adversos.
Alta	Si el evento de amenaza es iniciado u ocurre, es altamente probable que tenga impactos adversos.
Moderado	Si el evento de amenaza es iniciado u ocurre, es algo probable que tenga impactos adversos.
Baja	Si el evento de amenaza es iniciado u ocurre, es improbable que tenga impactos adversos.
Muy baja	Si el evento de amenaza es iniciado u ocurre, es altamente improbable que tenga impactos adversos.

Fuente: NIST SP 800-30 – Assessment Scale – Likelihood of threat event resulting in Adverse Impact

Anexo 13 – Probabilidad General

La tabla de probabilidad general es el resultado de la intersección de los valores de probabilidad de que un evento de amenaza resulte en impactos adversos y probabilidad de que un evento de amenaza se inicie u ocurra como se observa en la Tabla 28 Probabilidad General

Tabla 28 Probabilidad General

Probabilidad de que un evento de amenaza se inicie u ocurra	Probabilidad de que un evento de Amenaza Resulte en impactos Adversos				
	Muy Bajo	Bajo	Moderado	Alta	Muy Alta
Muy Alta	Bajo	Moderado	Alta	Muy Alta	Muy Alta
Alta	Bajo	Moderado	Moderado	Alta	Muy Alta
Moderado	Bajo	Bajo	Moderado	Moderado	Alta
Baja	Muy Bajo	Bajo	Bajo	Moderado	Moderado
Muy Baja	Muy Bajo	Muy Bajo	Bajo	Bajo	Bajo

Fuente: NIST SP 800-30 – Assessment Scale – Overall Likelihood

Anexo 14 – Ejemplos de Impacto Adverso

En la Tabla 29 Ejemplos Impactos Adversos se observa los ejemplos provistos por NIST SP 800-30, como una guía de los posibles impactos adversos.

Tabla 29 Ejemplos Impactos Adversos

Tipo de Impacto	Impacto
Daño a las operaciones	- Incapacidad para realizar misiones / funciones comerciales actuales. - De manera suficientemente oportuna. - Con suficiente confianza y / o corrección. - Dentro de las limitaciones de recursos planificadas. - Incapacidad o capacidad limitada para realizar misiones / funciones comerciales en el futuro. - Incapacidad para restaurar misiones / funciones comerciales. - De manera suficientemente oportuna. - Con suficiente confianza y / o corrección. - Dentro de las limitaciones de recursos planificadas. - Daños (por ejemplo, costos financieros, sanciones) debido al incumplimiento. - Con leyes o regulaciones aplicables. - Con requisitos contractuales u otros requisitos en otros acuerdos vinculantes (por ejemplo, responsabilidad). - Costos financieros directos. - Daños relacionales. - Daño a las relaciones de confianza. - Daño a la imagen o reputación.
Daño a los activos	- Daño o perdida a las instalaciones físicas. - Daño o perdida a los sistemas de información o redes. - Daño o pedida a los sistemas de información o suministros. - Daño o perdida de activos de información. - Perdida de propiedad intelectual.
Daño a individuos	- Lesión o muerte. - Maltrato físico o psicológico. - El robo de identidad. - Pérdida de información de identificación personal. - Daño a la imagen o reputación.
Daño a otras organizaciones	- Daños (por ejemplo, costos financieros, sanciones) debido al incumplimiento. - Con leyes o regulaciones aplicables. - Con requisitos contractuales u otros requisitos en otros acuerdos vinculantes. - Costos financieros directos. - Daños relacionales. - Daño a las relaciones de confianza. - Daño a la reputación (y por tanto a las relaciones de confianza futuras o potenciales).
Daño a la nación	- Daño o incapacitación de un sector de infraestructura crítica.

	- Pérdida de la continuidad de las operaciones del gobierno. - Daños relacionales. - Daño a las relaciones de confianza con otros gobiernos o con entidades no gubernamentales. - Daño a la reputación nacional (y por tanto a las relaciones de confianza futuras o potenciales). - Daño a la capacidad actual o futura para lograr los objetivos nacionales. - Daño a la seguridad nacional.

Fuente: NIST SP 800-30 – Examples of Adverse Impacts

Anexo 15 – Impacto de eventos de amenaza

Así como en el Anexo 12 se trabajó juntamente con el administrador del sistema, para poder determinar el impacto que representarían los eventos de amenaza en el sistema, siguiendo la escala de la Tabla 30 Impacto de eventos de amenaza.

Tabla 30 Impacto de eventos de amenaza

Valores Cualitativos	Descripción
Muy Alta	El evento de amenaza puede tener efectos adversos catastróficos en los activos del sistema.
Alta	El evento de amenaza puede tener efectos adversos severos o catastróficos en los activos del sistema.
Moderado	El evento de amenaza puede tener efectos adversos serios en los activos del sistema.
Baja	El evento de amenaza puede tener efectos adversos limitados en los activos del sistema.
Muy Baja	El evento de amenaza puede tener efectos adversos despreciables en los activos del sistema.

Fuente: NIST SP 800-30 – Assessment Scale – Impacto f Threat Events

Anexo 16 – Nivel de Riesgo (Combinación de probabilidad de que un evento de amenaza ocurra y resulte en un impacto y el nivel de impacto)

Tabla 31 Nivel de Riesgo

Probabilidad (Evento de Amenaza Ocurre y resulta en impacto adverso)	Nivel de Impacto				
	Muy Bajo	Bajo	Moderado	Alta	Muy Alta
Muy Alta	Muy Bajo	Bajo	Moderado	Alta	Muy Alta
Alta	Muy Bajo	Bajo	Moderado	Alta	Muy Alta
Moderado	Muy Bajo	Bajo	Moderado	Moderado	Alta
Baja	Muy Bajo	Bajo	Bajo	Bajo	Moderado
Muy Baja	Muy Bajo	Muy Bajo	Muy Bajo	Bajo	Bajo

Fuente: NIST SP 800-30 – Assessment Scale – Level of Risk (Combination of likehood and impact)

Anexo 17 – Nivel de Riesgo

Tabla 32 Nivel de Riesgo

Valores Cualitativos	Descripción
Muy Alta	El evento de amenaza puede tener efectos adversos catastróficos en los activos del sistema.
Alta	El evento de amenaza puede tener efectos adversos severos o catastróficos en los activos del sistema.
Moderado	El evento de amenaza puede tener efectos adversos serios en los activos del sistema.
Baja	El evento de amenaza puede tener efectos adversos limitados en los activos del sistema.
Muy Baja	El evento de amenaza puede tener efectos adversos despreciables en los activos del sistema.

Fuente: NIST SP 800-30 – Assessment Scale – Level of Risk

Anexo 18 – Flujo Algoritmo de Ofuscación y Desofuscación

Para obtener la cadena de conexión ofuscada se separó en otra aplicación de C# las funciones que cumplen con la lógica de ofuscación y des ofuscación como se observa en la Figura 40 Función de Ofuscación separada en otro programa, mientras que en la Figura 41 Resultado de la Ofuscación de cadenas de texto, se observa el resultado obtenido por las funciones de ofuscación.

```
3 referencias
public class Foo {
    2 referencias
    public static string ObfuscateString(string sInput)
    {
        string str = "";
        int i = 0;
        int length = 0;
        length = sInput.Length;
        for (i = length; i >= 1; i += -2)
        {
            str = string.Concat(str, Strings.Mid(sInput, i, 1));
        }
        for (i = length - 1; i >= 1; i += -2)
        {
            str = string.Concat(str, Strings.Mid(sInput, i, 1));
        }
        return str;
    }
    1 referencia
    public static string UnObfuscateString(string sInput)
    {
        string str = "";
        int i = 0;
        int length = 0;
        int num = 0;
        int num1 = 0;
        length = sInput.Length;
        num1 = length % 2;
        num = length / 2;
        for (i = num +num1; i >= 1; i += -1)
        {
            if (num1 == 0)
            {
                str = string.Concat(str, Strings.Mid(sInput, i + num, 1));
            }
            str = string.Concat(str, Strings.Mid(sInput, i, 1));
            if(num1 == 1 & i != 1)
            {
                str = string.Concat(str, Strings.Mid(sInput, i + num, 1));
            }
        }

        return str;
    }
}
0 referencias
class Program
{
    0 referencias
    static void Main(string[] args)
    {
        string ofuscado = Foo.ObfuscateString("BDMaster");
        string ofuscadoC = Foo.ObfuscateString("BDConexion");
        string desofuscado = Foo.UnObfuscateString(ofuscado);
        Console.WriteLine(ofuscado);
        Console.WriteLine(ofuscadoC);
    }
}
```

Figura 40 Función de Ofuscación separada en otro programa

```
Cadena BDMaster ofuscada: rtaDesMB
Cadena BDConexion ofuscada: nieoDoxnCB

D:\ConsoleApp1\bin\Debug\net5.0\ConsoleApp1.exe (proceso 21220) se cerró con el código 0.
Para cerrar automáticamente la consola cuando se detiene la depuración, habilite Herramientas →Opciones →Depuración →
Cerrar la consola automáticamente al detenerse la depuración.
Presione cualquier tecla para cerrar esta ventana. . .
```

Figura 41 Resultado de la Ofuscación de cadenas de texto

Al tener estos datos, se podría intentar conectarse a la base de datos, sin embargo como se observa en la Figura 36 Fragmento de Código que Solicita la cadena de conexión que se compone de dos parámetros, la ip o nombre del servidor y el nombre de la base de datos a conectarse, con el resultado obtenido podemos interpretar que es el nombre de la base de datos pero en el caso del nombre o ip del servidor se intuye por las variables y el mensaje de texto que el nombre de servidor o la ip para conectarse, se ingresa manualmente por lo que se imposibilita la conexión a la base de datos.

En la Figura 42 Intento de conexión con SQL Server, se puede observar que se intento acceder a la base de datos con la IP encontrada y el nombre del servidor, intente con todas las combinaciones obtenidas previamente, pero como se esperaba no hubo una conexión exitosa.

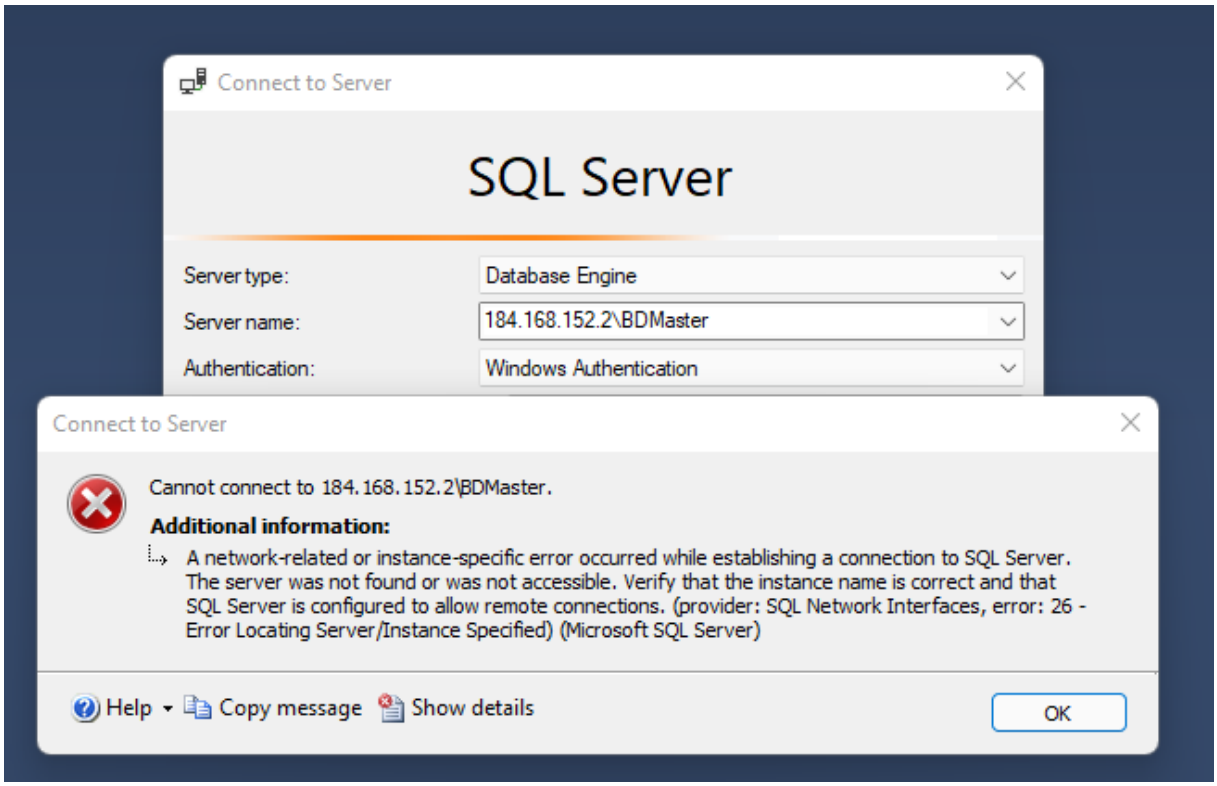


Figura 42 Intento de conexión con SQL Server

Anexo 19 – NIST SP 800-63B - Digital Identity Guidelines

NIST SP 800-63B provee recomendaciones en los procesos de autentificación, usa varios Niveles de Aseguramiento de Autentificación (AALs). También provee recomendaciones en el ciclo de vida de las autentificaciones, incluyendo perdida, revocación o robo. Se extrajeron las recomendaciones que NIST da para la creación, autentificación y almacenamientos de contraseñas.

A. Lineamientos para la creación de una Contraseñas Nueva

La seguridad de contraseñas empieza con la creación de contraseñas. Sin embargo, no es solo la responsabilidad de los usuarios para asegurar una buena contraseña, es necesario que el sistema se asegura que las contraseñas son lo suficientemente fuertes.

a. Largo > Complejidad

La sabiduría convencional dice que mientras más compleja es una contraseña es más segura, pero realmente el largo de la contraseña es más importante, debido a que una contraseña larga es, más difícil de robarle desencriptándola, como se observa en la Figura 43 Complejidad de Contraseña.

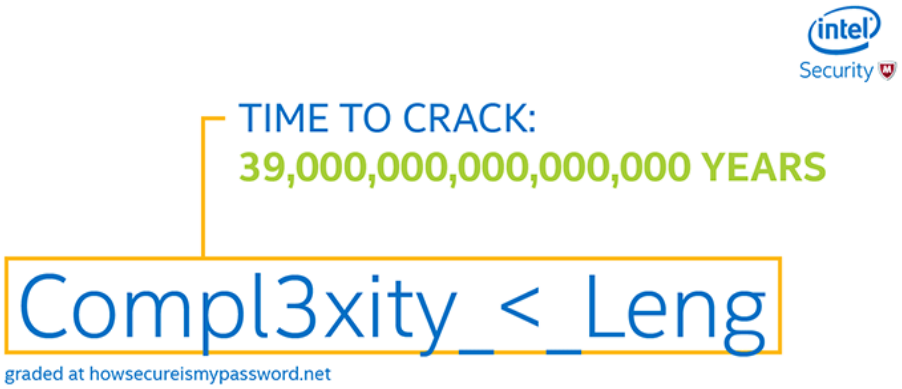


Figura 43 Complejidad de Contraseña

Adicionalmente NIST recomienda que las no se reúsen contraseñas para diferentes cuentas, además de que los añadir valores como “1” o “!” al inicio o al final no asegura nada, debido a que la mayoría de los hackers ya saben este patrón. Por lo que no es recomendable forzar a los usuarios a crear contraseñas más complejas, es mejor sugerir crear contraseñas largas.

b. Eliminar Reinicio Periódicos

Muchas compañías piden a sus usuarios que cambian sus contraseñas cada poco mes, pensado de que si alguna persona obtuvo tu contraseña pronto será bloqueada, sin embargo, cambios frecuentes de contraseña es peor.

Es suficientemente difícil para un usuario recordar una buena contraseña por año, hay varias personas que tienen que recordar varias contraseñas, por lo que cambiarlas en cortos periodos de tiempo provoca que los patrones de las siguientes contraseñas sean predecibles o reemplazar letras con símbolos parecidos como $ en vez de S.

B. Lineamientos de Autentificación de Contraseñas

La forma en la que un usuario se autentica puede tener un impacto masivo en todo lo relacionado con la seguridad de la contraseña (incluida la creación de contraseñas). Para esto NIST recomienda los siguientes puntos referido a las contraseñas.

a. Habilitar "Mostrar Contraseñas mientras Escribes"

Los errores tipográficos al escribir una contraseña son comunes, al convertirse en asteriscos todos los caracteres escritos, es difícil saber dónde se equivocaron. Por esta razón la mayoría de los usuarios elige contraseñas más cortas que es menos probable equivocarse, especialmente en sitios que tienen pocos intentos para la autentificación.

Por lo que NIST recomienda que se muestre la contraseña durante la escritura, ya que es mucho más probable que se ingresen contraseñas largas al primer intento.

b. Permitir "Pegar" en las contraseñas

Si las contraseñas son más fáciles de ingresar, los usuarios probablemente escogerán contraseñas más complejas y largas como primera opción. En estos casos es que la función de pegar contraseñas es ventajosa. Esto es importante considerando la cantidad de contraseñas que una persona tiene que memorizar y como los usuarios usan herramientas para administrarlas todas.

c. Utilizar la protección de Contraseña Infringida

Los lineamientos ofrecidos por NIST requieren que cada contraseña sea revisada contra una "lista negra" que incluye palabras de diccionario, palabras repetitivas o secuenciales, contraseñas comúnmente usadas, u otras palabras y patrones que los cibercriminales probablemente adivinen.

d. No usar "Contraseña sugerida"

Algunas aplicaciones tratan de ayudar a sus usuarios ofreciendo palabras clave o requiriendo que respondan una contraseña similar.

Sin embargo, hoy en dia que la información personal de las personas está en las redes sociales, se puede usar ingeniería social para que las respuestas a esas preguntas sean fáciles de adivinar, haciendo que sea fácil robar las cuentas de los usuarios, por esto NIST prohíbe el uso de estas.

e. Limitar Intentos de Contraseñas

NIST habla especialmente de este punto ya que la manera más común de adivinar contraseñas es a través de ataques de fuerza bruta, por lo que limitar los intentos de inicio de sesión.

f. Usar múltiples factores de Autenticación

NIST sugiere el uso de Multi-factor authentication (MFA), también conocida como two-factor authentication(2FA) el cual requiere que el usuario demuestre al menos dos de las siguientes confirmaciones:

- "Algo que tú sabes" (como una contraseña)
- "Algo que tú tienes" (como un teléfono)
- "Algo que tú eres" (como huellas digitales)

Anexo 20 – Comprobación de Propuesta de Mitigación FTP

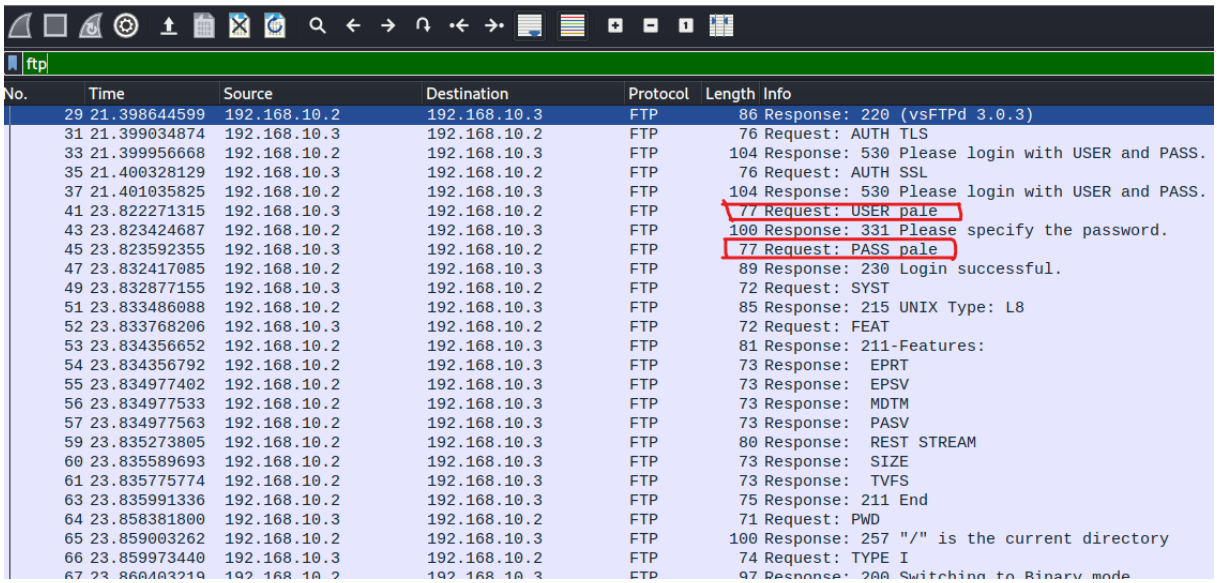
Para comprobar que la mitigación propuesta sea efectiva se hizo un escenario de pruebas con dos máquinas virtuales, Ubuntu Sever con dirección ip 192.168.10.2/24 y Kali Linux con la dirección ip 192.168.10.3/24, la máquina virtual de Ubuntu Server es en la que se alojó y configuro el servidor FTP, en el que uso una configuración básica para el funcionamiento del servidor como se observa en la

Figura 44 Configuración FTP, con esta configuración se busca simular la configuración actual del servidor FTP al que consulta IFacturacion, mientras que la maquina Kali Linux se usara para acceder al servidor a través de FileZilla y realizar la captura de paquetes con WireShark.

```
# READ THIS: This example file is NOT an exhaustive list of vsftpd options.
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
# capabilities.
# Run standalone?  vsftpd can run either from an inetd or as a standalone
# daemon started from an initscript.
listen=NO
#
# This directive enables listening on IPv6 sockets. By default, listening
# on the IPv6 "any" address (::) will accept connections from both IPv6
# and IPv4 clients. It is not necessary to listen on *both* IPv4 and IPv6
# sockets. If you want that (perhaps because you want to listen on specific
# addresses) then you must run two copies of vsftpd with two configuration
# files.
listen_ipv6=YES
#
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=NO
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
# Activate directory messages - messages given to remote users when they
# go into a certain directory.
dirmessage_enable=YES
use_localtime=YES
# Activate logging of uploads/downloads.
xferlog_enable=YES
# Make sure PORT transfer connections originate from port 20 (ftp-data).
connect_from_port_20=YES
allow_writeable_chroot=YES
chroot_local_user=YES
#chroot_list_enable=YES
# (default follows)
                                                              17,1          Top
```

Figura 44 Configuración FTP

Como se demuestra en el primer escaneo realizado con WireShark luego de levantar el servidor FTP con las configuraciones básicas, tanto el usuario como la contraseña con la que se accedió al servidor FTP fueron capturadas por el programa como se observa en Figura 45 Exposición de Usuario y Contraseña, por lo que se simulo de manera correcta la exposición del usuario y la contraseña en el servidor FTP.



ftp

No.	Time	Source	Destination	Protocol	Length	Info
29	21.398644599	192.168.10.2	192.168.10.3	FTP	86	Response: 220 (vsFTPd 3.0.3)
31	21.399034874	192.168.10.3	192.168.10.2	FTP	76	Request: AUTH TLS
33	21.399956668	192.168.10.2	192.168.10.3	FTP	104	Response: 530 Please login with USER and PASS.
35	21.400328129	192.168.10.3	192.168.10.2	FTP	76	Request: AUTH SSL
37	21.401035825	192.168.10.2	192.168.10.3	FTP	104	Response: 530 Please login with USER and PASS.
41	23.822271315	192.168.10.3	192.168.10.2	FTP	77	Request: USER pale
43	23.823424687	192.168.10.2	192.168.10.3	FTP	100	Response: 331 Please specify the password.
45	23.823592355	192.168.10.3	192.168.10.2	FTP	77	Request: PASS pale
47	23.832417085	192.168.10.2	192.168.10.3	FTP	89	Response: 230 Login successful.
49	23.832877155	192.168.10.3	192.168.10.2	FTP	72	Request: SYST
51	23.833486088	192.168.10.2	192.168.10.3	FTP	85	Response: 215 UNIX Type: L8
52	23.833768206	192.168.10.3	192.168.10.2	FTP	72	Request: FEAT
53	23.834356652	192.168.10.2	192.168.10.3	FTP	81	Response: 211-Features:
54	23.834356792	192.168.10.2	192.168.10.3	FTP	73	Response: EPRT
55	23.834977402	192.168.10.2	192.168.10.3	FTP	73	Response: EPSV
56	23.834977533	192.168.10.2	192.168.10.3	FTP	73	Response: MDTM
57	23.834977563	192.168.10.2	192.168.10.3	FTP	73	Response: PASV
59	23.835273805	192.168.10.2	192.168.10.3	FTP	80	Response: REST STREAM
60	23.835589693	192.168.10.2	192.168.10.3	FTP	73	Response: SIZE
61	23.835775774	192.168.10.2	192.168.10.3	FTP	73	Response: TVFS
63	23.835991336	192.168.10.2	192.168.10.3	FTP	75	Response: 211 End
64	23.858381800	192.168.10.3	192.168.10.2	FTP	71	Request: PWD
65	23.859003262	192.168.10.2	192.168.10.3	FTP	100	Response: 257 "/" is the current directory
66	23.859973440	192.168.10.3	192.168.10.2	FTP	74	Request: TYPE I
67	23.860403219	192.168.10.2	192.168.10.3	FTP	97	Response: 200 Switching to Binary mode

Figura 45 Exposición de Usuario y Contraseña

Para la mitigación como se sugirió se usó openssl, se generó certificado ssl con el siguiente comando: ***openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout etc/ssl/certificates/vsftpd.pem -out /etc/ssl/certificates/vsftpd.pem***, una vez generada la llave sll se configuro el servidor con la llave ssl creada como se observa en la Figura 46 Configuración SSL en el Servidor FTP.

```
# default to avoid remote users being able to cause excessive I/O on large
# sites. However, some broken FTP clients such as "ncftp" and "mirror" assume
# the presence of the "-R" option, so there is a strong case for enabling it.
#ls_recurse_enable=YES
#
# Customization
#
# Some of vsftpd's settings don't fit the filesystem layout by
# default.
#
# This option should be the name of a directory which is empty.  Also, the
# directory should not be writable by the ftp user. This directory is used
# as a secure chroot() jail at times vsftpd does not require filesystem
# access.
secure_chroot_dir=/var/run/vsftpd/empty
#
# This string is the name of the PAM service vsftpd will use.
pam_service_name=vsftpd
#
# This option specifies the location of the RSA certificate to use for SSL
# encrypted connections.
rsa_cert_file=/etc/ssl/certificates/vsftpd.pem
rsa_private_key_file=/etc/ssl/certificates/vsftpd.pem
ssl_enable=YES
allow_anon_ssl=NO
force_local_data_ssl=YES
force_local_logins_ssl=YES
ssl_tlsv1=YES
ssl_sslv2=NO
ssl_sslv3=NO
require_ssl_reuse=NO
ssl_ciphers=HIGH

#
# Uncomment this to indicate that vsftpd use a utf8 filesystem.
#utf8_filesystem=YES
                                                              164,1         Bot
```

Figura 46 Configuración SSL en el Servidor FTP

Una vez reiniciado el servicio FTP de Ubuntu Server se procedió a capturar los paquetes como se hizo antes, y efectivamente la certificación SSL funciono lo cual se nota al intentar ingresar a FileZilla nuevamente, pero con la certificación activada como se ve en la Figura 47 Certificación SSL al acceder al servidor FTP por medio de FileZilla.

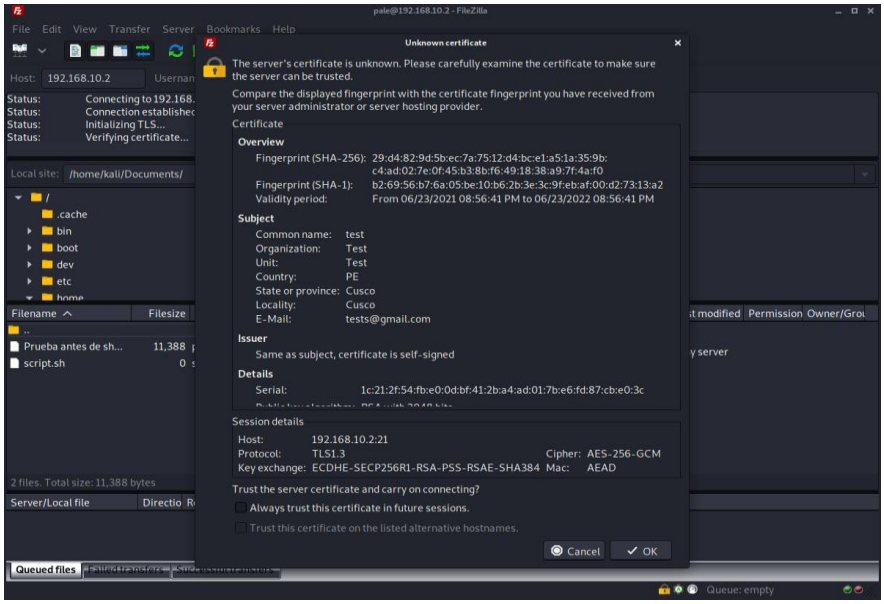


Figura 47 Certificación SSL al acceder al servidor FTP por medio de FileZilla

Al acceder a WireShark se comprueba que efectivamente ya no se visualiza la contraseña ni el usuario del servidor FTP como se ve en la Figura 48 Trafico capturado por WireShark encriptado.

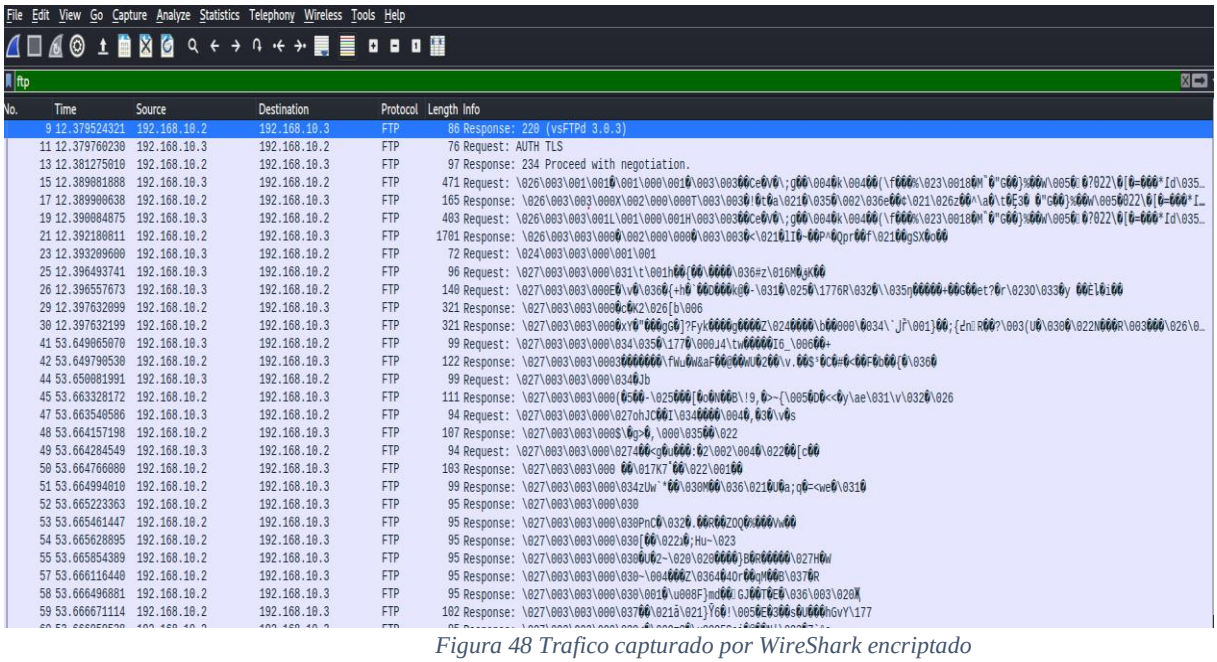


Figura 48 Trafico capturado por WireShark encriptado