UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

"Aplicación de herramientas de hacking ético para reducir el grado de vulnerabilidad en el sistema web informativo de una pyme - Piura, 2021"

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE: INGENIERO DE SISTEMAS

AUTORES:

Ipanaque Silva, Grace Beatriz (orcid.org/0000-0002-7061-0918)

Valverde Yovera, Eduardo Jordan (orcid.org/0000-0002-4948-4099)

ASESOR:

Mg. Agurto Marchan, Winner (orcid.org/0000-0002-0396-9349)

LÍNEA DE INVESTIGACIÓN:

Auditoría de sistemas y seguridad de la información

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo sostenible y adaptación al cambio climático

PIURA - PERÚ

2022

Dedicatoria

Dedicado a Dios por iluminar nuestros caminos, a nuestros padres, ya que, gracias a su gran esfuerzo, hacen posible que estemos culminando nuestros estudios superiores y al apoyo incondicional que siempre nos han brindado.

Agradecimiento

Agradecemos a nuestro asesor de tesis el Ing. Winner Agurto Marchan que gracias a sus conocimientos impartidos y lecciones estamos logrando culminar satisfactoriamente una etapa más de nuestra carrera universitaria.

ÍNDICE DE CONTENIDOS

Dedicatoria ii
Agradecimiento iii
Resumen vii
Abstract viii
I. INTRODUCCIÓN 1
II. MARCO TEÓRICO 5
III. METODOLOGÍA 20
3.1. Tipo y diseño de investigación 20
3.2. Variables y operacionalización 21
3.3. Población, muestra y muestro 22
3.4. Técnicas e instrumentos de recolección de datos 23
3.5. Procedimientos 26
3.6. Método de análisis de datos 27
3.7. Aspectos éticos 28
IV. RESULTADOS 29
V. DISCUSIÓN 36
VI. CONCLUSIONES 39
VII. RECOMENDACIONES 40
REFERENCIAS 41
ANEXOS 48

Índice de tablas

Tabla 1 - Tabla de valoración de vulnerabilidades 29
Tabla 2 – Tabla de vulnerabilidades.....29
Tabla 3 - Tabla de valoración de amenazas.....31
Tabla 4 – Tabla de amenazas.....31
Tabla 5 - Cuadro de frecuencia – Amenazas 32
Tabla 6 - Tabla de valoración de riesgos.....33
Tabla 7 - Tabla de Riesgos 33
Tabla 8 - Matriz probabilidad - impacto 35
Tabla 9 - Operacionalización de variables.....48
Tabla 10 - Matriz de consistencia.....51
Tabla 11 - Niveles y puntaje.....53
Tabla 12 - Ficha de observación 53
Tabla 13 - Matriz de criterios de vulnerabilidades 55
Tabla 14 - Matriz de criterios de amenazas.....55
Tabla 15 - Matriz de criterios de riesgos.....56

Índice de ilustraciones

Ilustración 1 - Metodología ISSAF....23
Ilustración 2 - Grafico Pre-Test Jats....30
Ilustración 3 - Grafico Post-Test Jats....30
Ilustración 4 - Grafico Pre-Test amenazas Sitio web Jats....31
Ilustración 5 - Grafico Post-Test amenazas Sitio web Jats....32
Ilustración 6 - Grafico Pre-Test riesgo Sitio web Jats....33
Ilustración 7 - Grafico Post-Test riesgo Sitio web Jats....34
Ilustración 8 - Recolección de información....56
Ilustración 9 - Recolección de información....57
Ilustración 10 - Identificación de vulnerabilidades....57
Ilustración 11 - Escaneo con Nikto....58
Ilustración 12 - Escaneo con Nessus en el Pre-Test sitio web Jats....58
Ilustración 13 - Escaneo con Nessus en el Post-Test Jats....59
Ilustración 14 - Creación del archivo example.conf....59
Ilustración 15 - Archivo de configuración nginx.conf....60
Ilustración 16 - Archivo nginx.conf....60
Ilustración 17 - Editando el archivo nginx.conf....61
Ilustración 18 - Evidencia SSL en el sitio web....61
Ilustración 19 - Datos de acceso....61
Ilustración 20 - Instrumento validado por el primer experto....62
Ilustración 21 - Instrumento validado por segundo experto....63
Ilustración 22 - Instrumento validado por el tercer experto....64
Ilustración 23 - Solicitud para recolección de datos....65
Ilustración 24 - Carta de aceptación para la recolección de información....66

Resumen

El presente trabajo de investigación tuvo como objetivo principal evaluar la reducción de vulnerabilidades en el sitio web de una pyme de matizados de Piura con la aplicación de hacking ético, haciendo uso de sus herramientas que permiten detectar, analizar y evaluar las posibles vulnerabilidades en el sitio web de una determinada empresa.

La presente investigación fue de tipo aplicada y de nivel descriptivo, dado que se van a describir las vulnerabilidades, amenazas y riesgos de un sitio web. Como población de estudio se tuvo al sitio web de la empresa, tiene un muestreo no probabilístico intencional ya que se seleccionó 1 sitio web de las pymes de Piura para aplicar las herramientas de hacking ético. Además, se aplicó la prueba test-retest, la cual consiste en aplicar la prueba reiteradas veces para verificar la confiabilidad al instrumento de recolección de datos. Como resultado de la investigación se logró reducir las vulnerabilidades de nivel bajo en un 9 % con la aplicación de las herramientas de hacking ético. Este estudio de investigación concluye que las herramientas de hacking ético ayudan a reducir considerablemente las vulnerabilidades en los sitios web, ya que permiten analizar y visualizar los errores que se presentan en un sitio web.

Palabras clave: Hacking ético, vulnerabilidades, riesgos, amenazas.

Abstract

The main objective of this research work was to evaluate the reduction of vulnerabilities on the website of a nuanced SME from Piura with the application of ethical hacking, making use of its tools that allow detecting, analyzing and evaluating possible vulnerabilities on the site. website of a certain company.

The present investigation was of an applied type and of a descriptive level, since the vulnerabilities, threats and risks of a website are going to be described. As a study population, the company's website was taken, it has an intentional non-probabilistic sampling since 1 website of the SMEs of Piura was selected to apply the ethical hacking tools. In addition, the test-retest test will be applied, which consists of applying the test repeatedly to verify the reliability of the data collection instrument. As a result of the investigation, low-level vulnerabilities were reduced by 9% with the application of ethical hacking tools. This research study concludes that ethical hacking tools help reduce website vulnerabilities considerably, as they allow us to analyze and visualize the errors that occur on a website.

Keywords: Ethical hacking, vulnerabilities, risks, threats.

I. INTRODUCCIÓN

El presente trabajo de tesis se refiere al tema de la aplicación de herramientas de hacking ético, estos son programas informáticos que ayudan analizar, detectar e identificar las posibles vulnerabilidades y riesgos que pueden existir en un determinado sitio web. Además, gracias a estas herramientas que son gratuitas se puede prevenir futuros ataques informáticos de cibercriminales.

El análisis de vulnerabilidades en los sistemas web informativos se define como la identificación de fallas o debilidades de seguridad que pueden existir, estas son actividades realizadas por profesionales del área de TI, empleando técnicas, métodos y herramientas informáticas que ayudan a la prevención de delitos informáticos, la aplicación del análisis de vulnerabilidades es de vital importancia ya que mediante ello podemos disminuir el riesgo de la integridad, disponibilidad y confidencialidad de la información de determinada empresa o persona.

Según el blog de la compañía internacional de seguridad informática Kaspersky menciona que en Latinoamérica el principal objetivo de ciberataques es a empresas. Siendo así Brasil el país con mayor número de ataques informáticos (55,97%), México (27,86%), Colombia (7,33%), Perú (5,36%), Argentina (1,87%) y Chile (1,62%). (Kaspersky 2020)

También menciona que el ámbito empresarial, Brasil lidera la lista con 56,25% de los ataques realizados en la región en los nueve primeros meses del 2020 además le sigue México (22.61%), Colombia (10,20%), Perú (4, 22%), Chile (3,27%) y Argentina (3, 25%). (Kaspersky 2020).

En la actualidad los ataques informáticos se dan en distintas empresas tanto en el sector público como en el sector privado, estos ataques pueden ser realizados a través del sitio web de la empresa, ya que se puede acceder a través de internet mediante un navegador, el sitio web es vulnerable y de alto riesgo cuando no se ha configurado correctamente. Estas negligencias permiten a los cibercriminales planificar ataques informáticos con el objetivo de introducirse y apoderarse de información valiosa de la empresa.

El 28 de enero del 2020 se publicó que el Programa de Recompensa por Vulnerabilidades de Google que en el año 2019 ha pagado más de $6,5 millones en recompensas, duplicando así lo que había pagado en el año 2018. Desde el año 2010 este gigante tecnológico ha ampliado sus Programas de Recompensa por Vulnerabilidades para cubrir áreas de productos de Google incluyendo Chrome, Android y otros. Además, se ha expandido para cubrir aplicaciones de terceros en Google Play, desde entonces esta multinacional ha pagado más de $21 millones en recompensas. (Google 2020).

También el 4 de agosto del 2020 se publicó que otro gigante tecnológico como es Microsoft ha pagado en los últimos 12 meses del periodo 2019 - 2020 $13.7 millones, esta cantidad es tres veces más de los $4.4 millones que se otorgaron en el periodo 2018-2019 en recompensas mediante sus Programas de Recompensas de Errores de Microsoft (Microsoft 2020).

En el Perú muchas empresas han sido víctimas de ataques informáticos, estas se han visto severamente afectadas, las cuales no han sabido responder a estas amenazas provocando así las actividades diarias paralizadas. Por ende, se deduce que el análisis de vulnerabilidades en los sistemas de información de las empresas peruanas es deficiente o nula. Según el portal Andina el 25.1% de ataques de ransomware (secuestro de datos) en el año 2017 fueron identificados en nuestro país, como la cifra más alta en América Latina, según explica la empresa de seguridad Eset. (Portal Andina 2018).

En la ciudad de Piura las pymes son un blanco perfecto para los cibercriminales, ya que muchas de estas entidades no realizan el análisis de vulnerabilidades en sus respectivos sistemas de información. En un estudio realizado por EY Perú indica que el 47% de las empresas del Perú tienen poca probabilidad de encontrar en corto plazo un ataque cibernético sofisticado. Las pymes que son entidades que recién están saliendo al mercado, no incorporan en su plan de operaciones el análisis de vulnerabilidades en sus sistemas de información.

En relación a lo descrito anteriormente, nace la idea general de investigar ¿Cómo la aplicación de herramientas de hacking ético ayuda a reducir el grado de vulnerabilidad en el sitio web de la pyme de matizados de Piura? Además,

como preguntas específicas ¿Cómo la implementación de hacking ético ayuda a mitigar las amenazas en el sitio web de la pyme de matizados de Piura? Y ¿Cómo la implementación de hacking ético reduce los riesgos en el sitio web de la pyme de matizados de Piura?

El trabajo de estudio se justificó socialmente ya que está orientado a las pymes de la ciudad de Piura de la cuales se pudo saber información respecto a la seguridad de sus sistemas y sitios web.

La investigación se justificó teóricamente ya que las herramientas de hacking ético permiten hacer un análisis y detección de vulnerabilidades en un determinado sitio web, además ayudan a prevenir futuros ataques informáticos de personas que se dedican al cibercrimen.

El trabajo de investigación de tesis se justificó metodológicamente porque se utilizó herramientas que permiten gestionar la bibliografía y almacenar investigaciones que nos permitieron usar como antecedentes. Además, se hizo un análisis y filtrado de cada uno de los antecedentes, también se revisó la metodología empleada en los estudios encontrados, lo que permite conceptualizar la variable de estudio “herramientas de hacking ético” en la matriz de análisis de antecedentes, esto ayuda a conocer el nivel de la investigación respecto al tema y como va evolucionado estos trabajos en el tiempo.

La tesis se justificó de forma práctica ya que se implementará las herramientas de hacking ético para demostrar la reducción de vulnerabilidades en el sitio web de la pyme de matizados de Piura.

El objetivo general de la tesis es evaluar la reducción de vulnerabilidades en el sitio web de la pyme de matizados de Piura con la aplicación de hacking ético y como objetivos específicos, mitigar las amenazas con la implementación de hacking ético en el sitio web de una pyme de matizados de Piura y analizar la reducción de riesgos con la implementación de hacking ético en el sitio web de una pyme de matizados de Piura. Dentro de esta tesis se formuló la siguiente hipótesis general, en realidad la aplicación de hacking ético reduce significativamente el grado de vulnerabilidad en el sitio web de una pyme de

matizados de Piura. Y como hipótesis específicas tenemos, la implementación de hacking ético reduce significativamente las amenazas en el sitio web de una pyme de matizados de Piura y la implementación de hacking ético reduce significativamente los riesgos en el sitio web de una pyme de matizados de Piura

II. MARCO TEÓRICO

En esta parte de la investigación se buscaron antecedentes a nivel internacional y de los cuales tenemos al autor Briones (2020), que tuvo como objetivo de su investigación aplicar hacking ético para detectar las amenazas, riesgos y vulnerabilidades en la Universidad Estatal del Sur de Manabí en el que se establece un ambiente de pruebas para evaluar el nivel de detección de vulnerabilidades. Fue un estudio de tipo experimental, además se empleó la metodología cuantitativa porque se recogieron datos estadísticos efectuados mediante encuestas; la población de estudio fue de siete mil trescientos noventa y cinco usuarios, tomando como muestra a trescientos sesenta y cinco involucrados entre docentes, personal administrativo y estudiantes, dentro de los resultados obtenidos de la investigación se determinó que un elevado porcentaje de los estudiantes que participaron en las encuestas requieren de capacitaciones relacionadas a este tema y que se necesita de mayor información sobre la aplicación de hacking ético para la detección de vulnerabilidades en la red. Por último, se concluyó que la aplicación de hacking ético determinó las respectivas vulnerabilidades que se pueden encontrar en las redes wifi dentro de la institución con la finalidad de brindar una mejor seguridad a los dispositivos tecnológicos.

Asimismo, Rojas (2018), en su tesis tuvo como objetivo de investigación aplicar Hacking Ético para examinar y evaluar la seguridad informática en la infraestructura tecnológica de la empresa Plasticaucho Industrial S.A. Fue una investigación de tipo aplicada, lo que permitió entender el estado real de la infraestructura tecnológica, asimismo se posibilita al investigador obtener competencias en seguridad informática. Este trabajo se empleó la modalidad de investigación bibliográfica buscando acomodarse en el conocimiento del investigador para el desarrollo del proyecto a través de: documentos, revistas, libros y de artículos en línea que brindan información relevante para la recolección de información. Los principales resultados de la investigación con la implementación de la herramienta Nslookup fue que se identificaron que sus servidores de correo pertenecen al servicio de Office 365 y asimismo disponen de una configuración SPF el cual permitirá el envío a través del mismo, otro resultado resaltante es que con la implementación de la herramienta llamada

Nessus se arrojaron una gran cantidad de vulnerabilidades identificadas en uno de los equipos Windows Server. Por último, se concluyó que con el análisis efectuado a la infraestructura de la empresa se reconocieron que los sistemas operativos son “Windows 7 Profesional”, asimismo se confirma que las entradas DNS del dominio fueron identificaron con un número estimado a las vulnerabilidades críticas en los equipos permitiendo la evaluación para los ataques conocidos.

Según Macías (2021) en su trabajo de investigación tuvo como objetivo de investigación realizar la aplicación de hacking ético para la determinación de amenazas, riesgos y vulnerabilidades en la red wifi de la Universidad Estatal del Sur De Manabí, este trabajo de investigación fue desarrollado bajo un enfoque cualitativo ya que, el problema requiere de una investigación interna y de total importancia además, este estudio fue de tipo aplicada porque se construyeron a base de investigaciones teóricas concretas y con una modalidad experimental ya que, se consideró la relación entre la variable independiente Hacking ético y su influencia en la red wifi para considerar sus causas y efectos; también se aplicó instrumentos de encuestas realizadas al personal administrativo de la Universidad Estatal del Sur y de los cuales como resultados en una de las preguntas de la encuesta sobre si se ha realizado alguna prueba de instrucción de hacking ético, 30 personas que corresponden al 17% del personal administrativo encuestados afirman tener conocimiento sobre la realización de la prueba de hacking ético, mientras que 146 personas que equivale al 83% no tienen conocimiento de ello, por ello se deduce que la mayoría no tiene conocimiento de esta prueba de hacking ético por lo que se resalta la importancia de aplicar y dar un poco más de información sobre este tema. Esta investigación concluye que el resultado de la prueba demuestra que el hacker obtuvo el acceso al sistema principal de la institución debido al aprovechamiento de una vulnerabilidad de software, el cual permitió conocer el nombre de usuario y su contraseña.

Oñate y Martínez (2017), tuvieron como objetivo en su trabajo de investigación mejorar la seguridad de la red inalámbrica de la universidad de Chimborazo aplicando hacking ético, esta investigación fue un estudio longitudinal puesto

que se obtienen datos en diferentes momentos durante un determinado periodo con la finalidad de examinar variaciones de tiempo, asimismo esta investigación fue un estudio de tipo aplicada ya que permitió aplicar métodos y técnicas de hacking ético con el uso de las herramientas para detectar vulnerabilidades y ataques en la red inalámbrica; el diseño de la investigación fue descriptiva puesto que se realizó un análisis sobre vulnerabilidades y riesgos que afectan la mejora de la red. En la investigación no se dispuso de población y muestra ya que se trabajó con los equipos de la red de la universidad Nacional de Chimborazo, como resultado del análisis se obtuvo: el número de dispositivos empleados por los estudiantes fueron analizados con cinco herramientas de hacking ético para comprobar si permitió mejorar la seguridad de las redes inalámbricas en la universidad estableciendo políticas de seguridad y reduciendo las vulnerabilidades detectadas en los equipos. Por último, se concluyó que las mejores herramientas de hacking ético para detectar vulnerabilidades y clasificar paquete de datos son WireShark, Sniffer, Nessus, asimismo se determinó un mayor porcentaje en vulnerabilidades las cuales fueron de nivel crítico y encontradas en la capa de aplicación y en la capa de transporte de los equipos dispuestos en la red de la universidad.

De igual modo, en la tesis de Remache (2018) tuvo como objetivo general proponer un modelo para la mitigación de vulnerabilidades informáticas en los servicios web de la Pontificia Universidad Católica del Ecuador Ambato. Ésta investigación fue de tipo aplicada ya que, se enfoca en la búsqueda del conocimiento para su respectivo desarrollo, su nivel de investigación fue exploratorio ya que, es utilizó para estudiar el problema encontrado en la universidad y, para la recolección de información se emplearon encuestas las cuales permitieron el desarrollo de la investigación asimismo se aplicó la metodología para la administración y el estudio de riesgos informáticos a base de Magerit Versión 3, la cual identifica los activos sobresalientes de la organización y la estimación que poseen. Los resultados obtenidos de las encuestas de seguridad realizada por la corporación ecuatoriana indican que el 46% de las universidades miembro no realizan ningún tipo de revisión de seguridad a sus sistemas, mientras que el 36% los evalúa una vez al año y, apenas un 18% lo hacen más de tres veces al año. Finalmente se concluye que

de los servicios analizados en el repositorio digital poseen el mayor número de vulnerabilidades, con un 165% de grado alto y 4% de grado medio, además el servicio con menor número de vulnerabilidades es el catálogo en línea, con una sola detección de alto grado, los servicios como, academics, moodle, catálogo en línea y mesa de ayuda, poseen una reducción del 100% de las detecciones de grado alto, mientras que el repositorio digital tiene una reducción del 1% de grado alto, esto se debe a que el 99% de las detecciones son relacionadas a problemas de programación.

Dentro de los antecedentes a nivel nacional tenemos al autor Bermeo (2017), que tuvo como objetivo principal en su investigación realizar la Implementación de Hacking Ético en la Empresa Complex del Perú S.A.C; para ayudar en la detección y evaluación de vulnerabilidades de Red. Fue un estudio de tipo descriptivo y de corte transversal, el tipo de investigación fue cuantitativa y como parte del diseño de investigación es no experimental. Ésta investigación tuvo una población constituida por 24 trabajadores convirtiéndose en una población muestral, los instrumentos empleados fueron las encuestas a sus trabajadores y de los cuales como resultados se lograron que el 96% de los trabajadores encuestados están insatisfechos con las circunstancias actuales en la empresa y el 100% de los encuestados revelaron una necesidad de implementación de hacking ético para mejorar la seguridad de la información y detectar ataques de red en beneficio de la empresa y en especial de su información. Por último, esta investigación concluye en formular una propuesta tecnológica de seguridad, que permita establecer políticas de comunicación oportuna y poder detectar posibles vulnerabilidades y/o penetraciones en la red de datos de la empresa Complex del Perú S.A.C – Tumbes.

Igualmente, Beltrán (2021) tuvo como objetivo principal en su investigación aplicar las técnicas empleadas de hacking ético para mejorar la seguridad de la red de telecomunicaciones de Inversiones Mayito – Agente BCP, para identificar y neutralizar las amenazas y riesgos de su red de telecomunicaciones. Fue un estudio de tipo aplicada y de diseño experimental. Esta investigación tuvo como población a la red de telecomunicaciones inalámbrica, puertos y la unidad de almacenamiento interno del CPU de empresa. Mediante lo mencionado esta

investigación obtuvo resultados que mediante la aplicación de hacking se logró reducir del 9.33 a 1.50 los ataques a la empresa. El estudio de investigación concluye que con la metodología aplicada y utilizada para la prevención de ataques a la red de comunicación en Inversiones Mayito – Agente BCP, se logra mitigar el nivel de vulnerabilidad reduciendo considerablemente los ataques cibernéticos en un 83.93%, además se logró reducir los ataques en un 83.25% en los puertos del CPU de la red principal de telecomunicaciones.

A continuación, los fundamentos teóricos que sustentan el presente estudio para definir nuestra primera variable sobre vulnerabilidades tenemos a Romero, et al. (2018) define que una vulnerabilidad es un sistema desactualizado, un sistema configurado de forma incorrecta que permite la entrada a recursos y a la información sin permisos apropiados. Así mismo de manera general define a la vulnerabilidad como un fallo en un sistema, la cual puede ser aprovechada por un ciberdelincuente provocando riesgos en la organización o en el sistema mismo (p. 41).

Físicas, son aquellas vulnerabilidades donde se indica el lugar donde se guarda la información, por ejemplo, un centro de datos o un área de cómputo, para un delincuente informático le resulta más fácil tener acceso a la información que contienen los equipos que tratan de acceder a la información por vía lógica.

Naturales, este tipo de vulnerabilidades están relacionadas con las condiciones climáticas de la naturaleza, lluvias, terremotos, inundaciones, entre otros, debido a estos fenómenos naturales siempre se debe contar con un plan de contingencia el cual, permita salvaguardar la información de la empresa, por ejemplo, realizar copias de seguridad, tener fuente de energía alterna, etc.

Hardware, estas vulnerabilidades se relacionan con los posibles desperfectos de fábrica que pueden traer algunos equipos informáticos o una incorrecta configuración de estos. Por ejemplo, desactualización de la infraestructura informática. Según Prinetto (2020) precisa que una vulnerabilidad en el hardware se denomina puerta trasera, y que no solo pueden ser desperfectos de fábrica sino también pueden ser insertadas por una persona para asegurar un acceso al sistema para su posterior uso.

Software, este tipo de vulnerabilidades está relacionado con las entradas no autorizadas a los sistemas informáticos de la empresa sin permiso del administrador de sistemas, por ejemplo, inadecuada configuración en los sistemas informáticos, instalación de programas no autorizados, los cuales podrían ser virus que infecten toda la red de la empresa. Según Jimenez (2019) define a una vulnerabilidad de software como un error en el sistema, que puede ser utilizado por un atacante para poder entrar o tener acceso de un determinado sistema informático.

Comunicación, está relacionado con el trayecto de la información, en otras palabras, es el envío de información por diferentes medios como vía satélite, cable, fibra óptica, siempre debe prevalecer la seguridad de la información enviada. El éxito del envió de información es muy importante ya que, se pueden tomar medidas en el sistema de seguridad de la información, además se debe prevenir que la información enviada sea capturada por personas mal intencionadas. También se debe evitar fallas en la comunicación ya que, éstas ponen en peligro la integridad de los datos. Según Shukla (2017) precisa que las comunicaciones se basan en redes que están conectadas por enrutadores y los puntos de acceso que permiten la conectividad y la transferencia de información.

Humanas, estas vulnerabilidades están relacionadas con los daños que puedan sufrir la información y la infraestructura tecnológica, de forma intencional o por negligencia por parte de los usuarios. Muchos ataques realizados a empresas surgen por la falta de capacitación a los usuarios de los sistemas informáticos en temas sobre la seguridad de la información dentro de la empresa.

Según la norma ISO 27001 determina que un riesgo es la unión de posibles acontecimientos en un evento de seguridad de la información, generando consecuencias como resultado.

Pérdida de datos, es el hurto de datos puede darse dentro de una organización determinada, por ejemplo, en manos de un ex empleado disconforme con la empresa o por personas mal intencionadas del exterior. Según Garba (2020) precisa que el robo de datos o robo de identidad ha sido denominado como el

delito con mayor crecimiento a nivel mundial, esta actividad tiene como objetivo robar los datos personales y confidenciales para una persona u empresa para obtener ganancias de ellas

Modificación de información, se trata sobre la intercepción y adulteración de la información sin autorización alguna, lo cual produce serios daños a la empresa ya que, al suceder este tipo de riesgos se pierde la información correcta y se puede estar trabajando con información falsa.

Denegación de servicio, son propósitos malintencionados para negar o anular el funcionamiento de un determinado sistema impidiendo que esté disponible, este tipo de riesgo se puede efectuar enviando grandes cantidades de paquetes para investigar y reconocer las inseguridades del software.

Extorsión, la extorsión es una forma de advertencia con el propósito de obtener información apropiada, esta situación se da mediante internet cuando se apoderan de información personal o información valiosa de una empresa, los ciberdelincuentes piden un cierto monto de dinero a cambio de no divulgar la información sustraída. Por eso es importante contar con protocolos de seguridad y herramientas que permitan disminuir el robo de información, por ejemplo, siempre se debe poseer un antivirus en los sistemas informáticos de la empresa.

Por último, para definir las Amenazas según Baca (2016) define que una amenaza es cualquier circunstancia que podría dar origen a que se produzca una violación de seguridad en los entornos de los sistemas, áreas o dispositivos informáticos (p. 29). Es decir, las amenazas son posibles acciones que dan lugar a que un equipo sea atacado, estas se dividen en humanas, lógicas y físicas, entre ellas tenemos; las amenazas humanas, estas amenazas están relacionadas con las personas que con o sin intención, causan daño en los sistemas de una determinada organización como son las siguientes.

Hacker, es una persona especializada en ramas de la tecnología de información, tiene conocimientos sólidos en redes computacionales, en lenguajes de programación y en sistemas operativos. Tiene los suficientes conocimientos para poder diseñar, crear y aplicar sistemas informáticos para su conveniencia. Según Abhineet (2017) precisa que un hacker es aquella persona

que burla la seguridad de un sistema informático de una determinada empresa o persona. Emplea exploits y su sólido conocimiento en el área para lograr su objetivo. Estos personajes también son expertos en temas de hardware, en lenguajes de programación, ciberseguridad y redes informáticas. Además, es una persona que está en constante aprendizaje.

Cracker, es un hacker cuya finalidad es hacer daño haciendo uso de sus sólidos conocimientos en las tecnologías de la información, el objetivo de estas personas suele estar por encima de la investigación algunos lo hacen por diversión y otros por obtener dinero. Según Maurushat (2019) precisa que un cracker es aquel individuo que tratan de entrar a sistemas informáticos sin permiso alguno. Estos pueden ser muy astutos y maliciosos, que solo buscan dañar la integridad de los sistemas informáticos.

Personal interno, son amenazas internas dentro de una organización procedente de los usuarios de los sistemas informáticos que tiene una entidad. Muchos ataques informáticos a empresas han sido éxitos, debido a la falta de conocimiento del personal interno ya que, muchas empresas no capacitan a su personal en asuntos de seguridad de la información. Otros ataques informáticos exitosos se han logrado con ayuda del personal interno de la empresa las cuales, burlan los protocolos establecidos para lograr sus objetivos malintencionados.

Exempleados, son personas que forman parte de una determinada organización y por descontento con la entidad, desean utilizar sus conocimientos y las vulnerabilidades que la empresa tiene para poder tomar represalias contra ellas. Como amenazas lógicas**,** estas amenazas están relacionadas con los programas maliciosos que existen para poder causar daño de manera intencional a los sistemas informáticos de una determinada empresa.

Exploits, según el portal de Avast (2020) define que son programas informáticos o instrucciones de código elaborados para explotar un software y causarle daños que inhabilitan su operatividad. Además, según Baloch (2107) precisa que un exploit es algo que utiliza una determinada vulnerabilidad en un

activo para ocasionar un comportamiento intencionado en un sistema informático, lo cual permitirá que el atacante tenga acceso al sistema.

Malware, según Avast (2021) define a un malware como un software malicioso, el cual se infiltra sin permisos, lo que genera daños e infecta a un computador, no solo afecta a ordenadores sino también a los dispositivos móviles mediante mensajes de textos. Por ejemplo tenemos; inyección SQL.

Inyección SQL, según Avast (2021) define que un SQL es un tipo de malware que ejecuta una porción de código directa a la base de datos para obtener información interna de la empresa.

Gusanos informáticos, según Madrigal (2019) define que son programas informáticos que tienen la posibilidad de propagarse por sí solos ya que, estos programas son diseñados para replicarse. Tiene como finalidad sobrecargar al computador y obstruir su correcto funcionamiento.

Ransomware, según Avast (2021) precisa que es un tipo de malware o programa informático malintencionado, que rapta archivos de equipos informáticos y también de dispositivos móviles. Tiene como finalidad cifrar o encriptar la información obtenida para luego pedir una cierta cantidad de dinero por el rescate, en otras palabras, podemos decir que se trata de una extorsión. También según Kok (2019) define al ransomware como un tipo de ofensiva de intrusión que tiene como finalidad pedir a cambio un rescate.

Adware, según el autor Madrigal (2019) define a un adware como un tipo de malware que consiste en someter a la víctima mostrándole publicidad no deseada, con el fin de obtener datos personales de la víctima.

Spyware o programas espía, según el portal de Avast (2021) define que es un programa informático malicioso cuyo objetivo es recopilar información de un equipo o de toda una red informática para luego enviarla al atacante, que en estos casos son mayormente los hackers. En otras palabras, se puede decir, que los programas espías son muy utilizados por los hackers ya que, les permite inspeccionar la actividad que realizan los usuarios en internet.

Troyanos, según el autor Jaiswal (2017) define a un troyano como un malware altamente dañino cuando se realiza su ejecución, es capaz de eliminar toda la información que hay en el disco duro, además tiene la particularidad de replicarse. También podemos definir a un troyano como un programa informático muy perjudicial, este se presenta como un software inofensivo y en algunos casos como un software legítimo.

Phishing, se define como una técnica de robo de información muy usada actualmente que consiste en engañar a la víctima, haciéndose pasar por buenas personas o empresas confiables y legítimas con la finalidad de obtener información delicada, por ejemplo, las cuentas bancarias, credenciales, usuario y contraseñas. Según el sitio de ESET (2021) el sector más afectado por ataques de phishing es el sector financiero ya que, se registró un 24,9% de intentos de esta modalidad durante el primer trimestre del año 2021.

Pharming, según Avast (2021) determina que Pharming es la usurpación del Sistema de Resolución de Nombres de Dominio (DNS, Domain Name System) con el objetivo de dirigir a la víctima a un sitio web falso.

Spam, según AV-TEST (2021) define al spam como correos peligrosos, además de ser muy molestos, estos se encargan de distribuir malware. También podemos decir que es una técnica muy usada ya que, se muestra como correos inofensivos pero que en realidad son altamente muy peligrosos.

Según el portal de Seguridad Informática BRM (2017) estas amenazas físicas, está orientado a encubrir amenazas que son generadas por el ser humano como por la naturaleza, además estos se encuentran instalados en los centros de cómputo de cada institución o individuo.

Incendios, son amenazas que se pueden originar por fallas en el sistema eléctrico, debido a una incorrecta instalación de los equipos eléctricos y por falta de equipos de ventilación. Por ello, se recomienda realizar una adecuada implementación del sistema eléctrico y mantener los equipos informáticos en ambientes ventilados.

Inundaciones, están relacionadas con las consecuencias que puede generar la invasión agua a los centros de cómputo por ello, se recomienda no instalar los equipos informáticos cerca de las instalaciones sanitarias.

Terremotos, son amenazas que están relacionadas con los movimientos telúricos de la naturaleza los cuales son impredecibles. Por ello, se recomienda instalar los data center en lugares de infraestructura segura.

Instalaciones eléctricas, éstas amenazas están relacionadas con las incidencias que pueden suceder por cortocircuitos y sobrecargas en las instalaciones eléctricas. Por ello se recomienda utilizar equipos para prevenir estas incidencias, tales como: estabilizador, supresores de pico.

Como segunda definición de nuestra variable sobre las herramientas de hacking ético estos son un conjunto de programas informáticos de acceso libre, los cuales permiten realizar el análisis para detectar vulnerabilidades en un determinado sistema informático, además ayudan a prevenir futuros ataques. Existen muchas herramientas de hacking ético las cuales nos pueden ayudar a examinar y evaluar las debilidades de un sistema informático, por ejemplo: Nessus, Network Security Scanner, SAINT, Nmap, Aircrack-ng, etc.

Aircrack-ng, según el sitio web de la herramienta Aircrack-ng.org (2021) describe que es un conjunto de paquetes que se utilizan para examinar la seguridad en la red Wi-Fi. Entonces podemos decir que esta herramienta nos permite desencriptar contraseñas inalámbricas de tipo WEP/WAP/WPA2, entre las funciones que tiene esta herramienta tenemos la captura de paquetes y el envío de datos a ficheros de texto para luego ser procesadas por terceros.

Nmap, según el sitio web oficial de Nmap (2021) define que es una herramienta gratuita y de código abierto empleada por millones de usuarios con la finalidad de explorar, administrar y realizar auditorías de seguridad en la red. También podemos definir que se le conoce a esta herramienta como mapeador de redes, la cual permite analizar redes de forma rápida y eficiente.

Nessus, según Carey, Criscuolo y Petruzzi describen a Nessus como un escáner de vulnerabilidades que está presente en todas partes, además es un

escáner de robusta visibilidad que se ajusta bien a las grandes redes corporativas (p, 27).

Nikto, es una herramienta gratuita que permite escanear fallas en los servidores web mediante líneas de comando, tiene como finalidad buscar archivos peligrosos, detectar fallas de configuración y desactualización de programas del servidor.

Para el desarrollo de nuestro trabajo de investigación se empleará la metodología ISSAF, según ISSAF (2006) define esta metodología como un marco estructurado para la evaluación de seguridades en los sistemas de información, esta metodología incluye fases cruciales para los procesos de análisis y evaluación de vulnerabilidades, las cuales se describen a continuación; la primera fase consiste en la recopilación de información buscar reunir una imagen completa sobre la infraestructura de tecnología de la información la cual se debe tener en cuenta para la evaluación de riesgos.

Esta metodología presenta 3 fases, cada una de estas fases tiene una secuencia de pasos específicos que son comunes para todas las organizaciones, y de las cuales se describirán a continuación.

Fase I. Planeación y preparación

Según Issaf (2006) describe que esta fase abarca pasos para intercambiar información inicial, organizar y acondicionarse para la prueba. Se firmará por un contrato de evaluación formal antes de la prueba, la cual facilitará la base para asignación y resguardo legal mutuo. Además, detallará al grupo que participará específicamente en las fechas y horas exactas para la prueba. En esta fase se realizan las siguientes actividades: se identifican a las personas que participarán en la prueba, asamblea de inicio para confirmar la importancia, el planteamiento y la metodología que se va a emplear, y pactar los casos de prueba específicos que se realizaran y las rutas de escalamiento.

Fase II. Evaluación

Esta es la fase en la que realmente se realiza la prueba de penetración, en la etapa de evaluación, se seguirá un enfoque por capas como se muestra en la

figura siguiente. Cada capa representa un mayor nivel de acceso a sus activos de información. Esta fase consiste en 9 etapas:

1. Recopilación de información: Consiste en utilizar el internet para recabar información sobre la empresa de estudio, utilizando técnicas de búsqueda (DNS / WHOIS) y métodos no técnicos (motores de búsqueda). Se debe explorar todas las vías posibles para la extracción de información, para esta etapa también se puede conseguir anuncios en periódicos y folletos de la empresa. En esta etapa es muy importante identificar las posibles vulnerabilidades e indagar más sobre ellas, para poder aplicar la herramienta correcta. Por eso esta primera etapa en la fase 2 de la metodología de ISSAF es muy importante y se debe dedicar la cantidad de tiempo necesario para poder recopilar toda la información posible.

2. Mapeo de redes: Después de recoger toda la información posible de la empresa en la primera etapa, se toma un enfoque más técnico ya que se conoce más sobre el objeto de estudio, y ahora se puede realizar una posible topología de red, para esto existen muchas herramientas que nos pueden ayudar a encontrar información sobre los hosts y la red de prueba. En esta etapa se realiza un mapeo de red en donde se incluye los puntos más vulnerables y los más importantes para entidad, esto ayudará a afirmar o descartar las posibles hipótesis que se ha generado en la primera etapa, además se identifica puntos críticos y se escanea los puestos y servicios.

3. Identificación de vulnerabilidades: Para realizar esta tercera etapa, primero se debe seleccionar los puntos específicos para probarlos, luego el evaluador realizará pruebas para encontrar puntos frágiles explotables. Estas actividades incorporan: conocer los servicios que son vulnerables, ejecutar un análisis para la búsqueda de vulnerabilidades, especificar las vulnerabilidades encontradas, ordenar las vulnerabilidades halladas y reconocer caminos de ataque.

4. Penetración: En esta etapa el evaluador, evadiendo lo protocolos de seguridad trata de tener acceso no permitido. Esta etapa consta de 5 pasos:

Encontrar código / Herramienta de prueba de concepto: Aquí debemos encontrar código de prueba, si tenemos un condigo confiable podemos usarlo sino debemos hacer las pruebas en un entorno aislado.

Desarrollar herramientas / guiones: En ciertas ocasiones será preciso los evaluadores deberán crear su propio código.

Prueba de código / herramienta de prueba de concepto: Aquí debemos individualizar el código y ensayar el código.

Use código de prueba de concepto contra el objetivo: Este código se emplea en nuestro objetivo para tener acceso no autorizado.

Verificar o refutar la existencia de vulnerabilidades: En este paso los evaluadores podrán corroborar si existen o no vulnerabilidades

Documentar los hallazgos: En este paso se explicará detalladamente los caminos explotables, las evaluaciones y las pruebas para afirmar la validez de vulnerabilidades

5. Obtener acceso y escalamiento de privilegios: En este paso se obtiene acceso a privilegios mínimos a través de distintos medios, como puede ser: encontrar password en blanco o password predeterminados, hallar servicios públicos para realizar operaciones dentro del sistema (escribir, leer y crear archivos).

6. Enumerar más: Reunir las cookies para ser utilizadas para atacar sesión y contraseñas, reconocer las rutas y las redes de prueba, analizar el tráfico de datos, obtener password encriptados para luego poder descifrar su contenido.

7. Comprometer usuarios / sitios remotos: Este paso consiste en que debemos asegurar las comunicaciones y el envío de información entre los usuarios y sitios remotos ya que, un solo en las comunicaciones puede hacer que toda la información que se envía puede ser falsificado o copiada. Por eso se recomienda que se use comunicaciones privadas como VPN.

8. Mantenimiento del acceso: Se hace uso de canales ocultos para mantener en secreto nuestra presencia en la red, se recomienda usar los túneles VPN

9. Cubriendo pistas: Se ocultan los archivos y las herramientas para no comprometer al sistema, también se debe eliminar los registros de actividades que se han realizado al sistema, ya que estos se quedan grabados en el sistema.

Fase III. Reportar, limpiar y destruir artefactos

Reporte verbal: Se informa inmediatamente sobre las pruebas que se han realizado y también de todas las vulnerabilidades que se han encontrado, para que la organización sepa y pueda tomar medidas para mejorar la seguridad en su organización.

Reporte final: Se redacta un informe detalladamente de los resultados de las pruebas, las fallas encontradas, y las recomendaciones para su posterior mejora. Este documento debe estar muy bien estructurado.

Limpieza y destrucción de artefactos: Es toda la información que se ha generado en el sistema y de la cual debe ser eliminada.

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

Tipo: La investigación fue de tipo aplicada ya que se basan en conocimientos existentes, además, el tipo de investigación tuvo como finalidad resolver un determinado problema enfocándose en la búsqueda del conocimiento para su utilización.

Según Lozada (2014) define que el objetivo de la investigación aplicada es producir conocimiento con aplicación directa, este tipo de estudio muestra un gran valor adicional por el empleo del conocimiento que deriva de la investigación básica.

Paradigma: El trabajo de investigación se basó en el paradigma positivista porque permite determinar los parámetros de una variable mediante expresiones numéricas. Ricoy (2006) define al paradigma positiva como un paradigma que defiende a la investigación que tenga como objeto comprobar una hipótesis por medios estadísticos asimismo resolver la variable por términos numerales.

Enfoque: El trabajo estudio tuvo un enfoque cuantitativo puesto que, se emplea el método de análisis y recolección de datos para poder responder y confirmar las hipótesis establecidas, según Hernández, Fernández y Baptista (2014) este enfoque cuantitativo permite definir y expresar un problema científico a partir de análisis estadísticos y mediciones numéricas asimismo, se emplea la recolección de datos para confirmar las hipótesis con la finalidad de establecer modelos de comportamiento y demostrar teorías.

El nivel del trabajo de investigación fue descriptivo ya que, permite especificar las características de un grupo, personas o de cualquier fenómeno. Según Hernández, Fernández y Baptista (2014) define a la investigación descriptiva como un estudio en donde se busca detallar propiedades y características importantes de cualquier fenómeno que se analice.

Diseño: Para el desarrollo de la tesis se aplicó el diseño pre experimental, puesto que se trata de dos mediciones sobre una sola muestra al mismo grupo de personas y objetos evaluando un antes y después de la variable

independiente. Según el autor Arias (2012), define que la investigación pre experimental es un proceso que se someterá a un objeto o grupo de individuos con determinadas condiciones lo cual, hace referencia a la variable independiente y para examinar los efectos o reacciones que se producen se relaciona a la variable dependiente.

3.2. Variables y operacionalización

V1: Vulnerabilidades:

Definición conceptual: Romero (2018) define que una vulnerabilidad es un sistema desactualizado, un sistema configurado de forma incorrecta que permite el acceso a recursos y a la información sin permisos apropiados. Así mismo de manera general define a la vulnerabilidad como un fallo en un sistema, la cual puede ser aprovechada por un ciberdelincuente provocando riesgos en la organización o en el sistema mismo (p. 41).

Definición operacional: La primera variable detectada como vulnerabilidad fue evaluada teniendo en cuenta sus dimensiones, tratando de evaluar la reducción del grado de vulnerabilidad con la aplicación de las herramientas de hacking ético.

Dimensiones:

Para la variable vulnerabilidades se estableció las siguientes dimensiones; como primera dimensión tuvimos los tipos de vulnerabilidades las cuales la identificamos como físicas, naturales, de hardware, de software, de comunicaciones y humanas; así mismo como segunda dimensión determinamos sus riesgos, entre ellas tenemos la perdida de datos, la modificación de información, las denegaciones de servicio y las extorsiones, por último, como tercera dimensión tenemos las amenazas y estas se clasifican en humanas, lógicas y físicas.

V2. Herramientas de hacking ético

Definición conceptual: Son un conjunto de programas informáticos de acceso libre, los cuales permiten realizar el análisis para detectar vulnerabilidades en un determinado sistema informático, además ayudan a prevenir futuros ataques.

Existen muchas herramientas de hacking ético las cuales nos pueden ayudar a examinar y evaluar las debilidades de un sistema informático, por ejemplo: Nessus, Network Security Scanner, SAINT, Nmap, Aircrack-ng, etc. Según Maurushat (2019) define que el hacking ético es el uso no agresivo de una determinada tecnología post de un motivo, política u otro tipo de situación, que habitualmente es legítimo y moralmente confuso.

Definición operacional: La segunda variable fue herramientas de hacking ético las cuales serán aplicadas para detectar y analizar las vulnerabilidades en los sitios web de las pequeñas y medianas empresas de la ciudad de Piura.

Dimensiones:

Para la variable herramientas de hacking ético se implementó las diversas herramientas y dentro de ellas tuvimos las siguientes: Aircrack-ng, Nmap, Nessus, Nikto, etc.

3.3. Población, muestra y muestro

Universo: En el trabajo de investigación se consideró como universo a todas las páginas web encontradas de las pymes de la ciudad de Piura.

Según el autor Carrasco (2009) señala que el universo es el conjunto de elementos, personas, objetos, sistemas, sucesos, los cuales pueden ser finitos e infinitos, asimismo la muestra de estudio tiene una estrecha relación con las variables definidas y el fragmento problemático de la realidad en la investigación.

Población: el trabajo de investigación tuvo como población de estudio al sitio web de una pyme de matizados de la ciudad de Piura, el cual permitió realizar el estudio con la finalidad de aplicar las herramientas de hacking ético y evaluar la reducción de vulnerabilidades encontradas.

Según el autor Arias (2012) define como población un conjunto finito o infinito de elementos con características comunes para las cuales serán detalladas en los resultados de la investigación.

Muestreo, para el trabajo de investigación se consideró un muestreo no probabilístico intencional ya que, se seleccionó de la población a 1 sitio web de

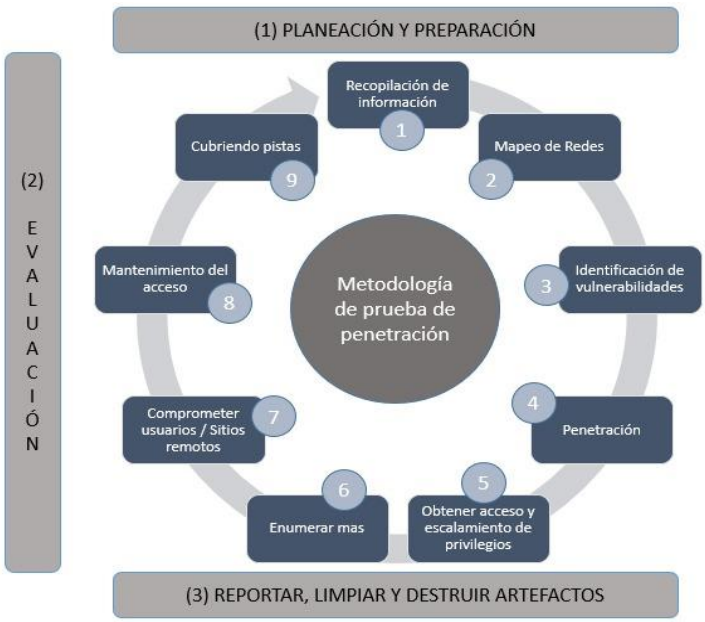
las pymes de la ciudad de Piura, según Arias (2012) define que el muestreo no probabilístico intencional es aquel que se basa en elementos con criterios y son escogidos por el investigador para el desarrollo de la investigación.

3.4. Técnicas e instrumentos de recolección de datos

En el presente trabajo de investigación se emplea de un marco estructurado llamado ISSAF (Information Systems Security Assessment Framework) que permite calificar y examinar la seguridad de los sistemas, este marco incorpora un conjunto de fases, procesos de seguridad con aportaciones complementarias para la protección del sistema respecto a las vulnerabilidades que pueden existir. Según OISSG (2006), define ISSAF como un marco estructurado que categoriza la evaluación de la seguridad del sistema de información en los diferentes dominios y detalles con criterios de evaluación, asimismo cumple con los requisitos de evaluación de seguridad de una organización y a su vez se puede utilizar como referencia para satisfacer otras necesidades de seguridad de la información.

Esta metodología presenta 3 fases, cada una de estas fases tiene una secuencia de pasos específicos que son comunes para todas las organizaciones, y de las cuales se describirán a continuación.

Ilustración 1 - Metodología ISSAF



Fuente: Sitio web Issaf

Fase I. Planeación y preparación, en esta primera fase se inicia con el intercambio de información, seguido de esto se debe llevar a cabo el planteamiento, desarrollo, preparación y ejecución de pruebas. Se determina que, para ejecutar una prueba, la metodología empleada es la misma a comparación de otras. Debido a que en esta etapa se exige en ambas partes tanto como auditor o como usuario, lo que conlleva a que se firme un acuerdo mutuo con la respectiva formalidad del caso.

Fase II. Evaluación, en esta fase se lleva a cabo las pruebas de intrusión, estos pasos que se deben seguir y ejecutar de manera cíclica hasta completarlos.

Recolección de información, en esta parte se describe de manera técnico, ya que se emplea para averiguar información de los datos, esta fase es considerada como una etapa de control auditable, permitiendo conservar la seguridad de la información.

Mapeo de red, esta parte es todo aquello que está relacionado con la red de datos y de la información, éstas son obtenidas con la recopilación, de tal manera que se puede acudir a las herramientas para contribuir con el descubrimiento de información de forma técnica y a su vez, se recopilarán las redes implicadas en la prueba de intrusión.

Identificación de vulnerabilidades, en esta parte se identifican las vulnerabilidades encontradas en los sitios web de las pequeñas y medianas empresas de la ciudad de Piura.

Penetración, en esta parte se obtiene el acceso no autorizado o también llamado ataque wifi, el cual tiene como objetivo conseguir el acceso a datos, evadiendo todas las medidas de seguridad, en efecto la intrusión es considerable porque permite buscar codificaciones disponibles, las cuales serán ejecutadas a través de pruebas con el uso de las herramientas detallando la aprobación o desaprobación de las vulnerabilidades y realizando una adecuada documentación.

Acceso y privilegios, en esta parte se accede a los dispositivos establecidos en la red, a su vez se autoriza y documenta todas las intrusiones en la

propagación de los ataques computarizados, autorizando tener un mayor alcance sobre impacto en las organizaciones que se tiene a cargo.

Enunciados adicionales, en esta parte se realiza la extracción de la información encriptada para obtener contraseñas usando la técnica sniffing o Keylogger, explorar sesiones y disponer de un nuevo mapeo.

Comprometer usuarios, para comprometer usuarios se comprueba que un escritorio remoto sea vulnerable, asimismo se muestra toda la red ya que, los elementos de autenticación son llaves importantes para la comunicación de los usuarios y de las redes corporativas.

Mantenimiento del acceso, en esta parte se permite tener privilegios en los sistemas, accediendo y manteniendo acceso a la integridad de la información en dichos sitios web.

Cubrir huellas, para cubrir huellas se detalla lo ejecutado y dentro de ellas se generan registros, asimismo con esta prueba se pueden encubrir archivos y eliminar el rastreo con la finalidad de no dejar pasar por alto estas pistas de la intrusión.

Fase III. Informe, limpieza y destrucción, en esta fase se presentan los reportes, éstos deberán ser comunicados de manera inmediata para asegurar la pervivencia de la organización.

Presentación de Informes, se encarga de presentar tres tipos de informes, los informes verbales que no son indispensables, el informe final que es vital y un informe sobre los componentes que deben ser excluidos en los sitios web.

Limpieza y Destrucción de Artefactos, para la limpieza la información que es creada y guardada en los sistemas web debe ser eliminada, para que se efectúen todos los archivos encontrados en el análisis deben ser mencionados en un informe técnico y enviados directo al personal técnico para que estos puedan ser apartados.

Instrumento: se empleó la ficha de observación como instrumento de recolección de datos. Según Abril (2008) define que la observación radica en la

captación sistemática y dirigida a entender los estados más significativos de los objetos, sucesos e individuos en un determinado contexto donde se desarrollan.

Validez: En el trabajo de investigación, la validación de la ficha de observación, fue necesario ya que, el instrumento nos permitió registrar los diferentes ataques, vulnerabilidades que son encontradas en los sitios web de las pymes de la ciudad de Piura. Y se validó por 3 expertos en seguridad informática. Según Hernández, Fernández y Baptista (2014) define que la validez es el grado en el que un instrumento mide la variable que intenta medir.

La confiabilidad, se determinó por el método del test retest. Según Chiner (2011) define al método test-retest como el procedimiento de medición de errores que resultan después de aplicar una determinada prueba en dos ocasiones en diferentes intervalos de tiempo.

3.5. Procedimientos

Se optó por una metodología como técnica de recolección de datos y determinar su validez y confiabilidad, se procedió a iniciar el trabajo de campo, el cual se le denomina procedimiento de investigación.

Antes de aplicar las fases de la metodología ISSAF, tuvimos que buscar una empresa que tenga un sitio web, donde aplicamos las herramientas de hacking ético, una vez que se seleccionó la empresa se procedió a ponerse en contacto con los dueños para que nos den autorización para aplicar las herramientas de hacking ético. Después que nos autorizan la aplicación tuvimos que seguir paso a paso la metodología ISSAF, la cual se basó en tres fases muy importantes, la primera fase consistió en llegar a un acuerdo firmado por ambas partes para poder aplicar las herramientas de hacking ético, siguiendo con la segunda fase, que consistió en la recolección de información y aplicación de las herramientas de hacking ético, es aquí donde se realizó una secuencia de 9 pasos: donde se inició con la recopilación de información, es aquí en donde hicimos uso del internet para buscar la información necesaria de la empresa, no solo podemos usar internet sino también revistas, folletos, periódicos, anuncios y todo lo relacionado a nuestro objeto de estudio, seguido se realizó el siguiente paso

llamado mapeo de redes, este paso consistió en aplicar las herramientas de hacking ético para la detección de vulnerabilidades, escaneo de puertos, mapeo de red; el tercer paso fue la identificación de vulnerabilidades la cual consistió en que el evaluador seleccionó puntos específicos de la red para realizar varias pruebas y poder identificar las vulnerabilidades y puntos débiles; el cuarto paso se llamó penetración y consistió en que el evaluador intentó conseguir acceso no permitido burlando las medidas seguridad. Siguiendo con el quinto paso, obtener acceso y escalamiento de privilegios consistió en que el evaluador afirma y documenta una posible propagación de ataque. El sexto paso fue enumerar más, este consistió en obtener los password mediante la aplicación de técnicas para descifrar datos además recopilación de cookies y direcciones de correo electrónico. Continuando con el séptimo paso comprometer usuarios / sitios remotos, consistió en las comunicaciones entre los usuarios y sitios remotos estos deben ser muy seguros, ya que un orifico en la red de comunicaciones puede exponer a toda la red completa. Por lo cual se recomienda hacer uso de VPN para una comunicación segura, el octavo paso fue mantenimiento del acceso, consistió en canales encubiertos para ocultar presencia en la red. El último paso cubriendo pistas, consistió en ocultar los archivos generados y descartar el rastreo de actividades con el objetivo de no ser registrados en el sistema y, por último, en la tercera fase se realizó las recomendaciones verbales y por escrito para que sean tomados en cuenta evitando futuros ataques y salvaguardando el sitio web.

3.6. Método de análisis de datos

Después de obtener los datos. Estos estos serán tabulados para luego procesarlos y analizarlos, dando respuesta a los objetivos de la investigación, al tratarse de un estudio descriptivo, los métodos de análisis de datos a utilizar son métodos descriptivos, los cuales permiten describir tendencias, observar situaciones, identificar niveles y estados de las variables. En este estudio se utilizó los cuadros comparativos y grafico de barras, todo esto a través del programa SPSS o el MS Excel.

3.7. Aspectos éticos

La siguiente investigación se basa en fundamentos éticos como es la probidad ya que, consiste en actuar con honestidad durante toda la investigación. Esto incluye mostrar de manera fidedigna los resultados obtenidos en la aplicación de las herramientas de hacking ético en el sitio web informativo de una pyme de Piura y prevenir modificaciones en el protocolo aprobado sin previa autorización por parte del comité de ética y la incorporación de autores que no han tenido un aporte a la investigación. Así mismo otro principio ético es la responsabilidad la cual, consiste en que los investigadores asumen las consecuencias de las acciones derivadas al proceso de investigación o productos de divulgación.

IV. RESULTADOS

Después de haber aplicado las herramientas de hacking ético se llegó a los siguientes resultados:

4.1. OG: Evaluar la reducción de vulnerabilidades en el sitio web de la pyme de matizados de Piura con la aplicación de hacking ético

Según FIRST - Forum of Incident Response and Security Teams (2015) establece el estándar CVSS v3 (Common Vulnerability Scoring System) que se utiliza para evaluar la gravedad de una vulnerabilidad, determinando el valor de criticidad en un rango 0 a 10 a partir de las métricas de puntuación base.

Tabla 1 - Tabla de valoración de vulnerabilidades

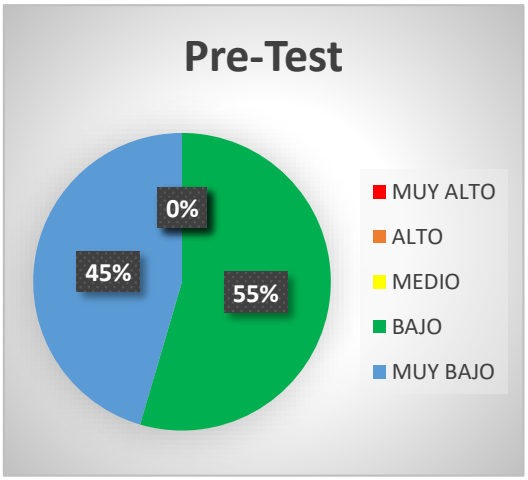
NIVELES	PUNTAJE
Muy Bajo	0.0 - 1.0
Bajo	1.1 - 3.9
Medio	4.0 - 6.9
Alto	7.0 - 8.9
Muy Alto	9.0 - 10.0

Tabla 2 – Tabla de vulnerabilidades

VULNERABILIDADES	VALORACION PRE-TEST	VALORACION POST-TEST
El encabezado X-Content-Type-Options no está configurado.	3	1
El encabezado X-XSS-Protection no está definido	3	1
El sitio usa SSL y el encabezado Expect-CT no está presente	3	1
El sitio utiliza SSL y el encabezado HTTP Strict-Transport-Security no está definido.	3	1
Not shutdown: 998 filtered tcp ports (no-responsive)	1	1
(443/tcp) open https	1	1
Enumeración de plataforma común (CPE)	1	1
Información de análisis de Nessus	1	1
Detección de servidor HTTP Nginx	1	1
Identificación del sistema operativo	1	1
Información de ruta de detección de servicio	1	1

Se realizó un Pretest para detectar e identificar las posibles vulnerabilidades que el sitio web de matizados pueda tener. Para la prueba se empleó la herramienta Nessus, la cual permitió encontrar vulnerabilidades de nivel bajo representado por el 45% y un nivel muy bajo representado por el 55%.

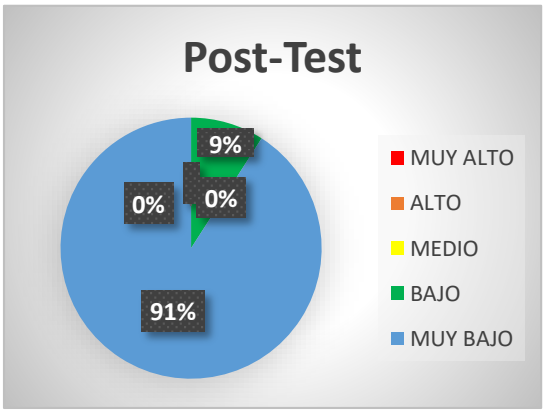
Ilustración 2 - Grafico Pre-Test Jats



Fuente: elaboración propia

Luego se aplicó una segunda prueba, previo a esta prueba se realizaron configuraciones en el servidor de la empresa de matizados para lograr reducir las vulnerabilidades encontradas, se empleó la misma herramienta Nessus que se aplicó en la primera prueba y se observó que las vulnerabilidades de nivel bajo se redujeron en un 9%.

Ilustración 3 - Grafico Post-Test Jats



Fuente: elaboración propia

4.2. OE 1: Mitigar las amenazas con la implementación de hacking ético en el sitio web de una pyme de matizados de Piura.

Según ISO 27001 establece el siguiente cuadro de valoración para evaluar la frecuencia u ocurrencia con la que puede presentarse determinando en una escala de valor. Además, dicha tabla se utiliza para la valoración de riesgos usando los mismos criterios.

Tabla 3 - Tabla de valoración de amenazas

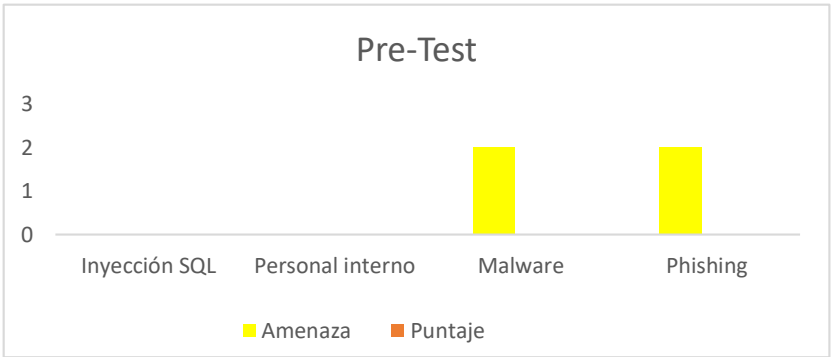
Nivel	Puntaje
Muy Baja	0
Baja	1
Media	2
Alta	3

Tabla 4 – Tabla de amenazas

AMENAZAS	VALORACION PRE-TEST	VALORACION POST-TEST
Inyección SQL	-	-
Personal interno	-	-
Malware informáticos	2	1
Phishing	2	1

Para evaluar las amenazas en el sitio web de matizados se realizó un pretest empleando la ficha de observación y tomando como referencia el cuadro de valoración de frecuencia, y mediante este se observó que el sitio web si presentó amenazas como malware informáticos y phishing con una escala de nivel medio.

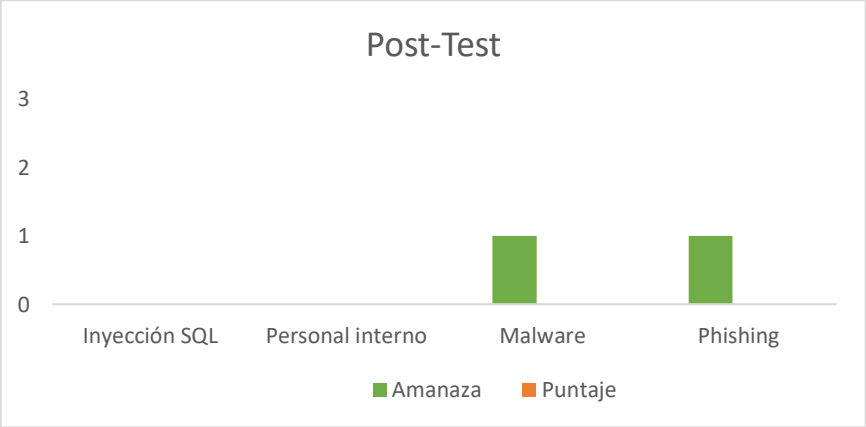
Ilustración 4 -Grafico Pre-Test amenazas Sitio web Jats



Fuente: Elaboración propia

Se aplicó un Post-Test empleando la misma ficha de observación y tomando como referencia el cuadro de valoración de frecuencia en la cual se observó que con la implementación de hacking ético se pueden mitigar los posibles ataques informáticos al sitio web de la pyme.

Ilustración 5 - Grafico Post-Test amenazas Sitio web Jats



Fuente: Elaboración propia

Tabla 5 - Cuadro de frecuencia – Amenazas

Descripción	Nivel	Descripción - Frecuencia
Muy Bajo	0	No se identifican agresores o incidentes ni hay antecedentes
Baja	1	Se identifica historial de este tipo de agresiones, así como incidentes dentro del sector o área geográfica, pero no hay incidentes registrados en nuestra organización. Se esperan posibles incidentes de forma esporádica.
Media	2	Se identifica historial de este tipo de agresiones, así como incidentes en nuestra organización. Se esperan posibles incidentes de forma periódica sin frecuencia determinada.
Alta	3	Se identifica historial de este tipo de agresiones e incidentes en nuestra organización identificándose el origen. Incidentes o eventos de esta naturaleza ocurren con frecuencia conocidos.

Fuente: ISO 27001

4.3. OE 2: Analizar la reducción de riesgos con la implementación de hacking ético en el sitio web de una pyme de matizados de Piura.

Tabla 6 - Tabla de valoración de riesgos

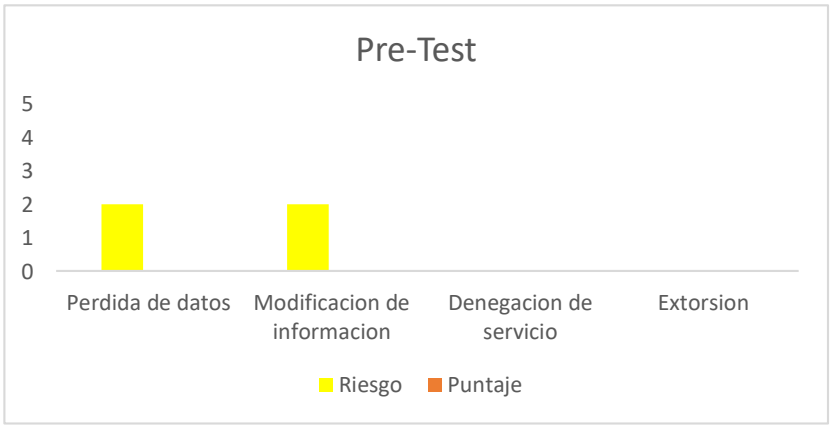
Nivel	Puntaje
Muy Baja	0
Baja	1
Media	2
Alta	3

Tabla 7 - Tabla de Riesgos

RIESGOS	VALORACION PRE-TEST	VALORACION POST-TEST
Perdida de datos	2	1
Modificaciones de información	2	0
Denegación de servicio	-	-
Extorsión	-	-

Para analizar los riesgos en el sitio web se realizó un Pretest aplicando la ficha de observación y tomando como referencia el cuadro de valoración; y se observó que se encontraron riesgos de nivel medio y bajo en el sitio web de matizados y de los cuales serán configurados para luego aplicar una segunda prueba y reducirlos.

Ilustración 6 - Grafico Pre-Test riesgo Sitio web Jats



Fuente: Elaboración propia

Después se realizó un Post-Test aplicando la misma ficha de observación y considerando el cuadro de valoración, donde se observó que se redujeron los riesgos en el sitio web de nivel medio a un nivel bajo, obteniendo permisos para realizar las respectivas configuraciones dentro del sitio web de la empresa y lograr reducirlas.

Ilustración 7 – Grafico Post-Test riesgo Sitio web Jats

Fuente: elaboración propia

Tabla 8 - Tabla de probabilidad

PROBABILIDAD	Puntaje
CASI SEGURO	5
ALTO	4
MEDIO	3
BAJO	2
RARO	1

Fuente: ISO 27001

Tabla 9 - Tabla de impacto

IMPACTO	Puntaje
MUY GRAVE	5
SEVERO	4
MEDIO	3
LEVE	2
SIN IMPACTO	1

Fuente: ISO 27001

Tabla 10 - Matriz probabilidad - impacto

Riesgo	Probabilidad	Impacto	Valor Riesgo
Perdida de datos	3	5	15
Modificaciones de información	3	3	9
Denegación de servicio	4	3	12
Extorsión	5	4	20

Fuente: Elaboración propia

V. DISCUSIÓN

En el trabajo de investigación se obtuvieron resultados los cuales demuestran que la aplicación de herramientas de hacking ético ayuda en la reducción de vulnerabilidades; estos resultados coinciden con el trabajo de investigación de Durand (2019) donde tuvo como objetivo evaluar y reducir vulnerabilidades en una empresa prestadora de servicio mediante la aplicación de las herramientas de hacking ético, gracias a estas herramientas aplicadas en la empresa de estudio se pudo evaluar la red de comunicaciones, lo que resultó que se encontraron vulnerabilidades de nivel crítico, alto y bajo, esto demostró que las herramientas de hacking ético ayudan en la detección y reducción de vulnerabilidades, en nuestro caso de estudio se aplicaron herramientas de hacking ético para detectar, analizar y reducir las vulnerabilidades de un sitio web de una pyme, debido a la aplicación de estas herramientas se pudieron encontrar vulnerabilidades de nivel medio, bajo y muy bajo; estas investigaciones se aplicaron en el sector comercial.

Además, nuestra investigación se asemeja a los resultados del estudio Remache (2018) donde su objetivo fue mitigar vulnerabilidades en los servicios web de una universidad, haciendo uso de herramientas de hacking ético pudo obtener resultados donde se observó la presencia de vulnerabilidades, riesgos y amenazas en el sitio web de la universidad. De la misma manera en nuestro trabajo de estudio mediante la aplicación de herramientas se pudo identificar y clasificar por niveles las vulnerabilidades, riesgos y amenazas encontradas en el sitio web de estudio. Estas investigaciones se han realizado en diferentes sectores; nuestro estudio se aplicó en el sector comercial, en cambio el estudio de Remache (2018) fue aplicado en el sector educativo. Con los resultados obtenidos en ambas investigaciones se demuestra que la aplicación de herramientas de hacking ético permite identificar, analizar y reducir las vulnerabilidades en sitios y servicios web de una determinada organización.

En los resultados obtenidos en nuestra investigación se demuestra que la aplicación de las herramientas de hacking ético ayuda en la identificación y reducción de riesgos en los sitios web, estos coinciden con el trabajo de estudio de Orbegoso (2021) quien tuvo como objetivo implementar un modelo para analizar las vulnerabilidades y riesgos en una empresa dedicada a prestar de servicios de gestión, aplicando herramientas de hacking ético se obtuvieron como resultados la identificación y reducción riesgos, los cuales fueron clasificados por niveles de severidad (alto, medio y bajo). Con esto se demuestra que la aplicación de herramientas de hacking ético permite reducir riesgos en un sitio web. De la misma forma en el trabajo de investigación se aplicó las herramientas de hacking ético, en donde también se identificaron riesgos, los cuales fueron evaluados por niveles (alto, medio, bajo y muy bajo), con estos resultados podemos afirmar que la aplicación herramientas de hacking permite identificar, evaluar y reducir riesgos. En ambas investigaciones se han aplicado diferentes metodologías; en nuestro trabajo estudio se aplicó la metodología ISSAF y en el trabajo de investigación de Orbegoso (2021) se aplicó la metodología OWASP con la finalidad de identificar, analizar y reducir; además estos estudios se han realizados en diferentes sectores, en el sector comercial y servicios respetivamente. Con estos resultados obtenidos en ambas investigaciones queda demostrado que las herramientas de hacking ético ayudan en la identificación, análisis y reducción de riesgos en un determinado sitio web.

Los resultados obtenidos en nuestra investigación demuestran que mediante el uso de las herramientas de hacking ético se puede reducir las amenazas en un determinado sitio web, estos resultados también guardan relación con el trabajo de estudio realizado por Briones (2020) que tuvo como objetivo detectar las amenazas, vulnerabilidades y riesgos en la red de la Universidad del Sur de Manabí aplicando las herramientas de hacking ético, se obtuvo como resultados la identificación de amenazas las cuales fueron clasificadas por escalas (alto, medio y bajo) así mismo se redujeron las amenazas encontradas en la red de la institución educativa privada. Con estos resultados se demostró que con el uso de las herramientas de hacking permiten analizar y reducir las amenazas de una determinada red de

comunicaciones. En nuestro trabajo de investigación se detectaron amenazas en el sitio web de las pymes, las cuales fueron detectadas aplicando las herramientas de hacking. Con ello se obtuvieron como resultado la identificación de amenazas las cuales fueron clasificadas por niveles (medio, bajo y muy bajo). Estos trabajos de investigación se han realizado en diferentes sectores como es en el sector educativo y sector comercial respectivamente. Con los resultados obtenidos en ambas investigaciones podemos afirmar que las herramientas de hacking ético ayudan en la identificación y reducción de amenazas en determinada red de comunicación y en los sitios web.

VI. CONCLUSIONES

- Tras el análisis realizado en el trabajo de investigación, podemos concluir que la aplicación de herramientas de hacking ético permitió disminuir las vulnerabilidades en el sitio web de la empresa de matizados de la ciudad de Piura. Para llevar a cabo dicha reducción de vulnerabilidades encontradas en el sitio web de la entidad, se tuvo que acceder al directorio y también a subdirectorios del servidor Nginx para poder crear y editar los archivos correspondientes que permitieron la configuración. Además, se concluye que estas configuraciones están basadas en la seguridad HTTP que son conocidos como encabezados de seguridad las cuales son importantes ya que permite proteger al sitio web de diversos ataques como, por ejemplo: inyecciones SQL, Protección XSS, clickjacking, etc.
- Se concluye que se logró reducir los riesgos en el sitio web de la empresa de matizados, mediante la aplicación del instrumento de recolección de datos se pudo observar la reducción de dichos riesgos ya que se realizó la una configuración en el sitio web para que una sola cuenta sea el administrador y tenga acceso global.
- Además, se concluye que las amenazas no se pueden reducir ya que son agentes externos, pero si se pueden realizar acciones para mitigar los ataques informáticos. Una de las acciones que se deben realizar es la actualización del antivirus en los equipos informáticos de la empresa, así mismo el sitio web cuenta con un certificado SSL el cual reduce las posibilidades de un ataque de Phishing.

VII. RECOMENDACIONES

- Se recomienda a los dueños o gerentes de las empresas que deberían realizar un análisis de vulnerabilidades a su sitio web periódicamente para poder saber si el sitio cuenta con la seguridad adecuada y poder detectar posibles vulnerabilidades, además así prevenir futuros ataques cibernéticos que pueden poner en riesgo la información y data sensible de la entidad.
- Se sugiere implementar protocolos de seguridad de la información en la empresa y a su vez capacitar al personal interno del área administrativa en políticas de seguridad de la información. Además, se recomienda a la empresa adquirir un antivirus para el servidor, mantener actualizados el sistema operativo de los equipos de cómputo de la entidad para reducir los riesgos y amenazas.
- Se recomienda a los futuros investigadores indagar sobre temas de seguridad de la información, aplicando técnicas y herramientas de prevención las cuales permitan realizar un mejor análisis de vulnerabilidades, riesgos y amenazas en los sitios web. Así mismo, se recomienda investigar a profundidad sobre las diferentes metodologías que existen para proteger al sitio web, hacerlo más seguro y reducir las probabilidades de sufrir un ciberataque.

REFERENCIAS

DIAZGRANADOS, Hernan, 2020.Empresas, principal objetivo de ciberataques en América Latina. En: Kaspersky blog [en línea]. Disponible en: https://latam.kaspersky.com/blog/empresas-principal-objetivo-de-ciberataques-en-america-latina/20209/ [setiembre 2020]

PABRAI, Natasha, KELLER, Jan, LIN, Jessica, HUPA, Anna y BACCHUS, Adam, 2020. Vulnerability Reward Program: 2019 Year in Review. En: Google Security Blog [en línea]. Disponible en: https://security.googleblog.com/2020/01/vulnerability-reward-program-2019-year.html [setiembre de 2020]

STALEY, Jarek, 2020. Microsoft Bug Bounty Programs Year in Review: $13.7M in Rewards. En: Msrc Blog Microsoft [en línea]. Disponible en: https://msrc-blog.microsoft.com/2020/08/04/microsoft-bug-bounty-programs-year-in-review/ [setiembre 2020]

Andina, 2018. ¿Cuáles son los ciberataques más comunes en el Perú? En: Portal Andina [en línea]. Disponible en: https://portal.andina.pe/edpespeciales/2018/ciberataques-peru/index.html [setiembre 2020]

BRIONES, Idelinda, 2020. *Aplicación de hacking ético para la determinación de amenazas, riesgos y vulnerabilidades en la red de la Universidad Estatal del Sur de Manabí.* Tesis pregrado. Ecuador: Universidad Estatal del Sur de Manabí. Disponible en: http://repositorio.unesum.edu.ec/handle/53000/2588

ROJAS, Alexander, 2018. *Hacking ético para analizar y evaluar la seguridad informática en la infraestructura de la empresa Plasticaucho industrial S.A.* Tesis pregrado. Ecuador: Universidad Técnica de Ambato. Disponible en: https://repositorio.uta.edu.ec/handle/123456789/28102

MACÍAS, Bryan, 2021. *Aplicación de hacking ético para la determinación de amenazas, riesgos y vulnerabilidades en la red wifi de la universidad estatal del sur de Manabí*. Tesis pregrado. Ecuador: Universidad Estatal del Sur de Manabí. Disponible en: http://repositorio.unesum.edu.ec/handle/53000/3062

OÑATE, O, MARTINEZ, C, 2017. *Mejoras en la seguridad de la red inalámbrica de la Universidad Nacional de Chimborazo aplicando hacking ético.* Tesis pregrado. Ecuador: *Universidad Nacional de Chimborazo*. Disponible en: http://dspace.unach.edu.ec/handle/51000/4170

REMACHE, Eduardo, 2018. *Modelo para la mitigación de vulnerabilidades informativas en los servicios web de la Pontifica Universidad Católica del Ecuador Ambato.* Tesis de maestría. Ecuador: Universidad Católica del Ecuador. Disponible en: https://repositorio.pucesa.edu.ec/handle/123456789/2474

BERMEO, Jean Carlos, 2017. *Implementación de hacking ético para la detección y evaluación de vulnerabilidades de red en la empresa Complex del Perú SAC.* Tesis pregrado. Perú: Universidad Católica los Ángeles de Chimbote. Disponible en: http://repositorio.uladech.edu.pe/handle/20.500.13032/10391

BELTRAN, Pedro, 2021. *Aplicación de Hacking ético para gestionar la prevención de ataques a la red de comunicación de inversiones Mayito – Agente BCP*. Tesis Postgrado. Perú: Universidad Cesar Vallejo. Disponible en: https://repositorio.ucv.edu.pe/handle/20.500.12692/55951

ISO 27001: 2013. Guía de implantación para la seguridad de la información. [En línea]. Disponible en: https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf

ROMERO, Martha, et al., 2018. *Introducción a la seguridad informática y el análisis de vulnerabilidades* [en línea]. 1º Ed [consulta: 13 noviembre 2021]. ISBN: 978-84-949306-14. Disponible en: https://books.google.es/books?hl=es&lr=&id=5Z9yDwAAQBAJ&oi=fnd&pg=PA29&dq=Introducci%C3%B3n+a+la+seguridad+inform%C3%A1tica+y+el+an%C3%A1lisis+de+vulnerabilidades++Romero&ots=ymvUvUh_Sy&sig=LliWhlcpk7WxYOUFQYbCujcrZzA#v=onepage&q=Introducci%C3%B3n%20a%20la%20seguridad%20inform%C3%A1tica%20y%20el%20an%C3%A1lisis%20de%20vulnerabilidades%20%20Romero&f=false

BACA, Gabriel, 2016. *Introducción a la seguridad informática* [en línea]. 1° Ed. México: Grupo Editorial Patria. ISBN: 978-607-744-471-8 Disponible en: https://books.google.es/books?hl=es&lr=&id=IhUhDgAAQBAJ&oi=fnd&pg=PP1&dq=amenaza+inform%C3%A1tica&ots=0XPA6zthKp&sig=jWHqk39i7KgR7n_CRVKmwwtZxz8#v=onepage&q=amenaza%20inform%C3%A1tica&f=false [consulta: 13 noviembre de 2021]

LATTO, Nica, 2020. Exploits: todo lo que debe saber. En: *Avast* Academia Blog [en línea]. Disponible en: https://www.avast.com/es-es/c-exploits#gref [setiembre 2021]

BELCIC, Iván, 2021. ¿Qué es el malware? En: *Avast Academy Blog* [en línea]. Disponible en: https://www.avast.com/es-es/c-malware#gref [mayo 2021]

MADRIGAL, Walter, 2019. Seguridad Informática [en línea]. Costa Rica: Universidad San Marcos. Disponible en: http://repositorio.usam.ac.cr/xmlui/handle/11506/958

SEGUIN, Patrick, 2021. Guía esencial sobre el ransomware. En: *Avast Academy Blog* [en línea]. Disponible en: https://www.avast.com/es-es/c-what-is-ransomware#gref [setiembre 2021]

HARÁN, Juan Manuel, 2021. En 2021 se registró pico histórico en la cantidad de sitios de phishing. En: *ESET Blog* [en línea]. Disponible en: https://www.welivesecurity.com/la-es/2021/06/15/2021-registro-pico-historico-cantidad-sitios-phishing/ [junio 2021]

RICOY, Carmen, 2006. Educação. Revista do Centro de Educação. *Contribución sobre los paradigmas de investigación* [en línea]. Brasil: Educacão, vol. 31, núm. 1, pp. 11-22 [consulta: noviembre 2021]. ISSN: 0101-9031. Disponible en: https://www.redalyc.org/pdf/1171/117117257002.pdf

HERNÁNDEZ, Roberto, et al., 2014. *Metodología de la Investigación* [en línea]. 6º Ed. México. ISBN: 978-1-4562-2396-0. Disponible en: http://observatorio.epacartagena.gov.co/wp-content/uploads/2017/08/metodologia-de-la-investigacion-sexta-edicion.compressed.pdf

SEGUIN, Patrick, 2021. Spyware: detección, prevención y eliminación. En: Avast Academy Blog [en línea]. Disponible en: https://www.avast.com/es-es/c-spyware#gref [setiembre de 2021]

AVAST Academy Team, 2021. Pharming. En: Avast Academy Blog [en línea]. Disponible en: https://www.avast.com/es-es/c-pharming#gref [octubre de 2021]

AV-TEST, 2021. Estadísticas de spam. En: The Independent IT-Security Institute Blog [en línea]. Disponible en: https://www.av-test.org/es/estadisticas/spam-av-test/ [noviembre de 2021]

AV-TEST, 2021. ¿Qué es la inyección SQL y cómo funciona? En: Avast Academy Blog [en línea]. Disponible en: https://www.avast.com/es-es/c-sql-injection [setiembre de 2021]

SEGURIDAD INFORMATICA BRM, 2021. Tipos de amenazas: Físicas. En: Seguridad Informática BRM Blog [en línea]. Disponible en: https://seguridadeinformaticabrm.wordpress.com/2017/02/07/tipos-de-amenazas-fisicas/ [febrero de 2017]

LOZADA, José, 2014. Investigación Aplicada: Definición, Propiedad Intelectual e Industria. Vol.3 Num1, pp (34-39). Disponible en: http://cienciamerica.uti.edu.ec/openjournal/index.php/uti/article/view/30/23

ARIAS, Fidias, 2012. *El proyecto de investigación, Introducción a la Metodología Científica.* [en línea]. 6° Edición. Caracas Venezuela: Editorial Episteme C.A. ISBN: 980-07-8529-9. Disponible en: https://www.researchgate.net/publication/301894369_EL_PROYECTO_DE_INVESTIGACION_6a_EDICION

OISSG, 2006. Information Systems Security Assessment Framework [en línea]. Draft 0.2.1. Disponible en: https://www.oissg.org/

MAURUSHAT, Alana, 2019. *Hacking Ethical* [En línea]. Canadá: Gauvin Press [consulta: 19 de noviembre 2020]. ISBN: 9780776627915. Disponible en: https://books.google.es/books?hl=es&lr=&id=PhqTDwAAQBAJ&oi=fnd&pg=PT9&dq=hacking+ethical&ots=XVPFApLFsV&sig=-VOK4-_iomF95cMtG19uOxQ2eOY#v=onepage&q=hacking%20ethical&f=false

JAISWAL, Manishaben, 2017. International Journal of Creative Research Thoughts (IJCRT). Computer viruses: principles of exertion, occurrence and awareness [online]. United States: Volume.5, Issue 4, pp.648-651. ISSN: 2320-2882. Available in: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3772376

BALOCH, Rafay, 2017. *Ethical Hacking and Penetration Testing Guide.* [En línea]. Estados Unidos: Taylor & Francis Group [Consulta: 20 de noviembre 2020]. ISBN: 9781482231625. Disponible en: https://books.google.es/books?hl=es&lr=&id=fKfNBQAAQBAJ&oi=fnd&pg=PP1&dq=hacking+ethical+&ots=SdBENf_a0P&sig=w8OfgPVwhj9nfLXgF86elYZyxh8#v=onepage&q=hacking%20ethical&f=false

JIMENEZ, Matthieu; RWEMALIKA, Renaud; PAPADAKIS, Mike; SARRO, Fererica, 2019. The importance of accounting for real-world labelling when predicting software vulnerabilities. *In Proceedings of the 27th ACM Joint Meeting 2019 on the European Software Engineering Conference and Symposium on the Fundamentals of Software Engineering.* [En línea]. Estonia: pp. 695-705. [Consulta: noviembre de 2020]. Disponle en: https://dl.acm.org/doi/pdf/10.1145/3338906.3338941

PRINETTO, Paolo, ROASCIO, Gianluca, 2020. Hardware Security, Vulnerabilities, and Attacks: AComprehensive Taxonomy. *Conference onCybersecurity tenutosi a Ancona.* [En línea]. Italian: CEUR Workshop Proceedings. Vol.2597, pp. 177-189. [Consulta: noviembre de 2020]. Disponible en: https://core.ac.uk/reader/327177450

SHUKLA, Varun; CHATURVEDI, Atul; SRIVASTAVA, Neelam, 2017. Secure Wireless Communication Protocol: To Avoid. *Communications on Applied Electronics Vulnerabilities in Shared Authentication.* [En línea]. Usa: Vol. 7. No. 6, ISSN: 23944714. Disponible en: https://www.caeaccess.org/archives/volume7/number6/shukla-2017-cae-652680.pdf

GARBA, Musa, 2020. Dark Side of IT Usage: Investigating Effectiveness of Information Security Controls Against Identity Theft Committed in Nigerian Banks. *Dutse Journal of Pure and Applied Sciences.* [En línea]. Vol. 6, No. 3. ISSN:

26353490. Disponible en: https://fud.edu.ng/journals/dujopas/2020_Vol6_3/35%20edited(1).pdf

KOK, S, 2019. Prevention of Crypto-Ransomware Using a Pre-Encryption Detection Algorithm. [En línea]. Malasya: Cumputers. [Consulta: noviembre de 2020]. Disponible en: https://www.mdpi.com/2073-431X/8/4/79

GUPTA, Aman; ANAND, Abhineet, 2017. Ethical hacking and hacking attacks. *Ethical Hacking and Hacking Attacks "International.pdf.* [En línea]. India: Ijecs, Vol. 6, pp. 40-50. [Consulta: noviembre de 2020]. ISSN: 2319-7242. Disponible en: https://d1wqtxts1xzle7.cloudfront.net/58213946/Ethical_Hacking_and_Hacking_AttacksInternational-with-cover-page-v2.pdf?Expires=1637368394&Signature=Fx6OD5edoxx3PxBQOCpXyk1JHAvcGucipg8sVjJC3roTP8PWQDqMqsM6CKbXA6E6ETcuuFxZWoUiO7XEhRu5q0Kcbgg5au-8wq~64Jes-rUPcQN649L~wqCfiNSGQ~oPkeKJ9EJPjH5WCU7ykytkdEupvm9BSXvmbNdslMc8hWoUwh-GisJ8NbA8z3G0fh2NbF6Xf2Xnb4Ezk4wHCrFSybs-UPHCX~H0e5WoUuVwA7E4g3rYn1P3q-YFx7i0EGPfFqXo2R9VHh67XwLg65dQREz9EXRvZLX-9e0VStZMUK~uVDXb3tz5lzCeH~QdI1s0rt3agUwAc4MBPWa0LbZu3A__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

Aircrack-ng [en línea]. Disponible en: https://www.aircrack-ng.org/

GORDON, Lyon, 2021. Nmap. En: Insecure.ORG [en línea]. Disponible en: https://nmap.org/book/

CAREY, Mark, et al., (s.f). *Nessus Network Auditing Second Edition* [en línea]. 2º Ed. Books Google. ISBN 13: 978-1-59749-208-9. Disponible en: https://books.google.com.pe/books?id=3OiclLcGdTgC&pg=PP1&dq=nessus+network+auditing+second+edition&hl=es&sa=X&ved=2ahUKEwj3iozPkZb0AhUdHrkGHSp9DMwQ6AF6BAgGEAI#v=onepage&q=nessus%20network%20auditing%20second%20edition&f=false

ABRIL, Víctor, 2008. *Téc*nicas e instrumentos de la investigación. Disponible en: https://www.academia.edu/6964411/T%C3%A9cnicas_e_Instrumentos_de_Investigaci%C3%B3n_Abril_Ph_D

FIRST, 2015. Forum of Incident Response and Security Teams [en línea]. Disponible en: https://www.first.org/cvss/

ANEXOS

Tabla 8 - Operacionalización de variables

Variable	Definición conceptual	Dimensión	Indicador	Nivel de medición
Vulnerabilidades	Romero (2018) define que una vulnerabilidad es un sistema desactualizado, un sistema configurado de forma incorrecta que permite la entrada a recursos y a la información sin permisos apropiados. Así mismo de manera general define a la vulnerabilidad como un fallo en un sistema, la cual puede ser aprovechada por un ciberdelincuente provocando riesgos en la	Tipos	Físicas Naturales De hardware De software De comunicación humanas	Razón
		Riesgo	Pérdida de datos Modificación de información Denegación de servicio Extorsión	Razón
		Amenazas	Humanas Hacker Cracker Personal interno Exempleados Lógicas	Razón

	organización o en el sistema mismo (p. 41).		Exploits Gusanos Malware Phishing Pharming Spam Spyware o programas espía Físicos Incendios Inundaciones Terremotos Instalaciones eléctricas	
Herramientas de hacking ético	Son un conjunto de programas informáticos de acceso libre, los cuales permiten realizar el análisis para detectar vulnerabilidades en un determinado sistema informático, además	Aircrack-ng Nmap Nessus Nikto		

	ayudan a prevenir futuros ataques.			

Fuente: Elaboración propia

Tabla 9 - Matriz de consistencia

TÍTULO	FORMULACIÓN DEL PROBLEMA	OBJETIVO GENERAL	OBJETIVO ESPECIFICO	HIPÓTESIS	VARIABLES	DIMENSIÓNES	INDICADORES	METODOLOGÍA
Aplicación de herramientas de hacking ético para reducir el grado de vulnerabilidad en el sistema web informativo de una pyme - Piura, 2021	¿Cómo la aplicación de herramientas de hacking ético ayuda a reducir el grado de vulnerabilidad en el sitio web de la pyme de matizados de Piura?	**OG:** Evaluar la reducción de vulnerabilidades en el sitio web de la pyme de matizados de Piura con la aplicación de hacking ético	**OE1:** Mitigar las amenazas con la implementación de hacking ético en el sitio web de una pyme de matizados de Piura **OE2:** Analizar la reducción de riesgos con la implementación de hacking ético en el sitio web de una pyme de matizados de Piura	**HG:** En realidad la aplicación de hacking ético reduce significativamente el grado de vulnerabilidad en el sitio web de una pyme de matizados de Piura **H_1:** La implementación de hacking ético reduce significativamente las amenazas en el sitio web de una pyme de matizados de Piura	Vulnerabilidades	Tipos	Físicas, Naturales De hardware De software De comunicación Humanas	**TIPO DE INVESTIGACIÓN:** Pre-experimental **POBLACIÓN:** El sitio web de la pyme de matizados de la ciudad de Piura **INSTRUMENTO:** Ficha de observación **TÉCNICAS:** Metodología ISSAF
						Riesgos	Perdida de datos Modificación de información Denegación de servicio, Extorsión.	
						Amenazas	**Humanas**: Hacker, Cracker, Personal interno, exempleados.	
							Lógicas: Exploits, Malware, Gusanos, Spyware,	

				H_2: La implementación de hacking ético reduce significativamente los riesgos en el sitio web de una pyme de matizados de Piura			Phishing, Pharming	
							Físicos: Incendios, inundaciones, terremotos, instalaciones eléctricas.	
					Herramientas de hacking ético	Aircrack-ng Nmap Nessus Nikto		

Fuente: Elaboración Propia

Ficha de observación

En esta ficha de observación se registrarán las vulnerabilidades de los sitios web, tomando en cuenta los criterios de evaluación, se evaluará con una escala del 0 a 10, donde 0 es la puntuación más baja y 10 la más alta.

Tabla 10 - Niveles y puntaje

NIVELES	PUNTAJE
Muy Bajo	Desde 0 hasta 1
Bajo	Desde 2 hasta 3
Medio	Desde 4 hasta 6
Alto	Desde 7 hasta 8
Muy Alto	Desde 9 hasta 10

Fuente: Elaboración propia

Tabla 11 - Ficha de observación

FICHA DE OBSERVACION 01				
Investigadores	Ipanaque Silva, Grace Beatriz Valverde Yovera, Eduardo Jordan	Tipo de Prueba	Aplicada	
Institución	Universidad Cesar Vallejo			
Dimensiones	Tipos – Riesgos - Amenazas			
Fecha				
Variable	**Técnica**			
Vulnerabilidades	Observación			
Ítem	**Preguntas**	**Valoración**	**Nivel**	**Observaciones**
Vulnerabilidades				
1	¿El sitio web presenta tipos de vulnerabilidades físicas?			
2	¿El sitio web presenta tipos de vulnerabilidad naturales?			
3	¿El sitio web presenta tipos de vulnerabilidad de hardware?			
4	¿El sitio web presenta tipos de vulnerabilidad de software?			
5	¿El sitio web presenta tipos de vulnerabilidad comunicación?			

Riesgos				
6	¿En el sitio web se exponen riesgos como la perdida de datos?			
7	¿De qué valoración se han presentado modificaciones de información en el sitio web?			
8	¿De qué nivel se presentan tipos denegación de servicio en el sitio web?			
9	¿En el sitio web se detectan tipos riesgos como la extorsión?			
Amenazas				
AMENAZAS HUMANAS				
10	¿Se detectan amenazas de hackers en el sitio web?			
11	¿Se encontraron amenazas de personal interno en el sitio web?			
AMENAZAS LÓGICAS				
12	¿Se encontraron amenazas de tipo lógicas como malware informáticos en el sitio web?			
13	¿En el sitio web se detectaron amenazas lógicas como Phishing en el sitio web?			

Fuente: Elaboración propia

Tabla 12 - Matriz de criterios de vulnerabilidades

	Muy bajo (0.0 – 1.0)	Bajo (1.1 – 3.9)	Medio (4.0 – 6.9)	Alto (7.0 – 8.9)	Muy Alto (9.0 – 10.0)
Criterios de vulnerabilidades en el sitio web	La asignación de este valor indica que es poco probable que tenga un efecto en la organización o en las personas asociadas con la organización.	La asignación de este valor indica que es probable que solo tenga un efecto adverso limitado en la organización o en las personas asociadas con la organización.	La asignación de este valor indica que es probable que tenga un efecto adverso grave en la organización o en las personas asociadas con la organización	La asignación de este valor indica que es probable que tenga un efecto adverso catastrófico en la organización o en las personas asociadas con la organización.	La asignación de este valor indica que se tiene un efecto catastrófico en la organización o en las personas asociadas

Fuente: Elaboración propia

Tabla 13 - Matriz de criterios de amenazas

	Muy bajo [0]	Bajo [1]	Medio [2]	Alto [3]
Criterios de amenazas	La asignación de este valor indica que la amenaza es mínima y se toman acciones para mejorar la seguridad.	La asignación de este valor indica que la amenaza es aceptable y para reducir los graves peligros se implementan mejoras de seguridad y mitigación.	La asignación de este valor indica que la amenaza es probable de realizar acciones perjudiciales al sitio web y se debe realizar planes para reducirlos y mitigar peligros.	La asignación de este valor indica que la amenaza es inaceptable y se implementan medidas de seguridad para mitigar y/o reducir el peligro de riesgo.

Fuente: Elaboración propia

Tabla 14 - Matriz de criterios de riesgos

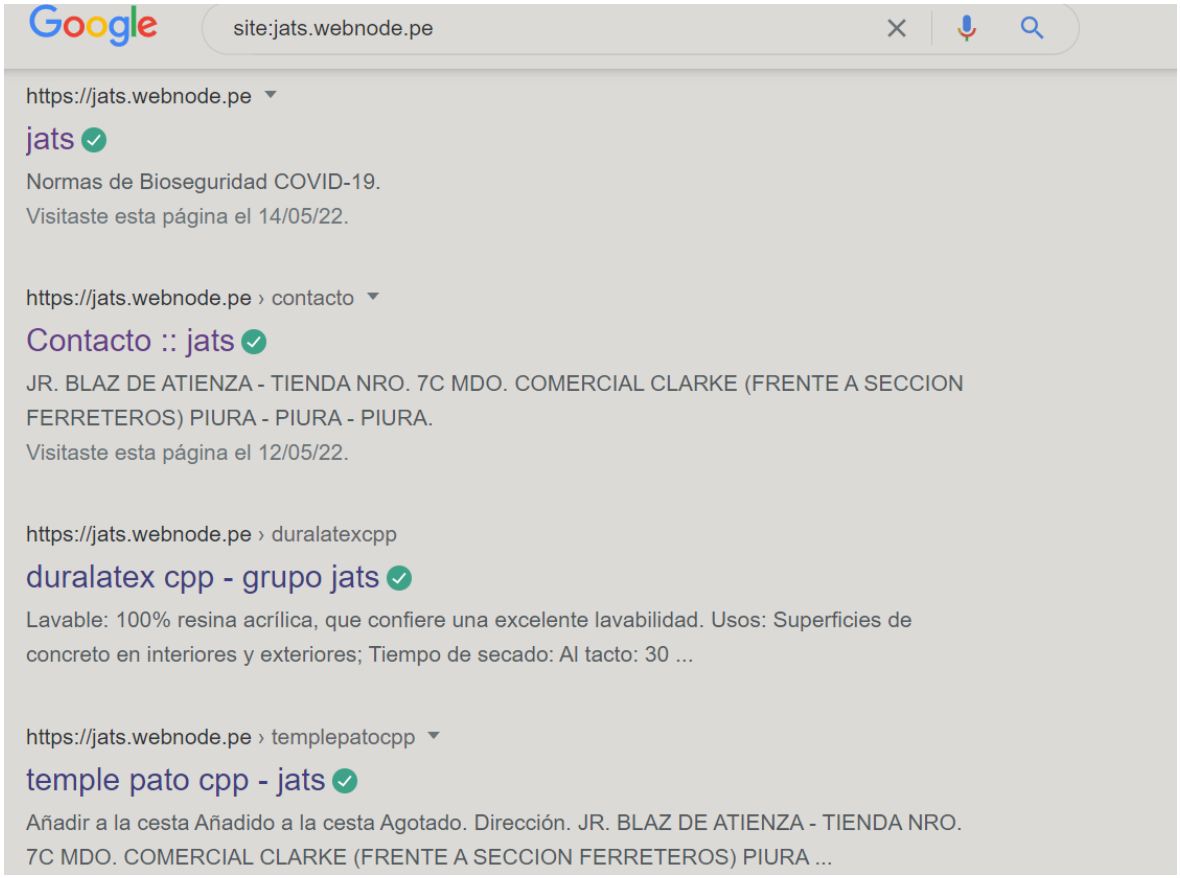
	Muy bajo [0]	Bajo [1]	Medio [2]	Alto [3]
Criterios de riesgos	La asignación de este valor indica que el riesgo es mínimo y se toman acciones para mejorar la seguridad.	La asignación de este valor indica que el riesgo es aceptable y para reducir los graves peligros se implementan mejoras de seguridad y mitigación.	La asignación de este valor indica que el riesgo es aceptable y se debe realizar planes para reducirlos y mitigar peligros.	La asignación de este valor indica que es el riesgo es inaceptable y se implementan medidas de seguridad para mitigar y/o reducir el peligro de riesgo.

Fuente: Elaboración propia

Ilustración 8 - Recolección de información

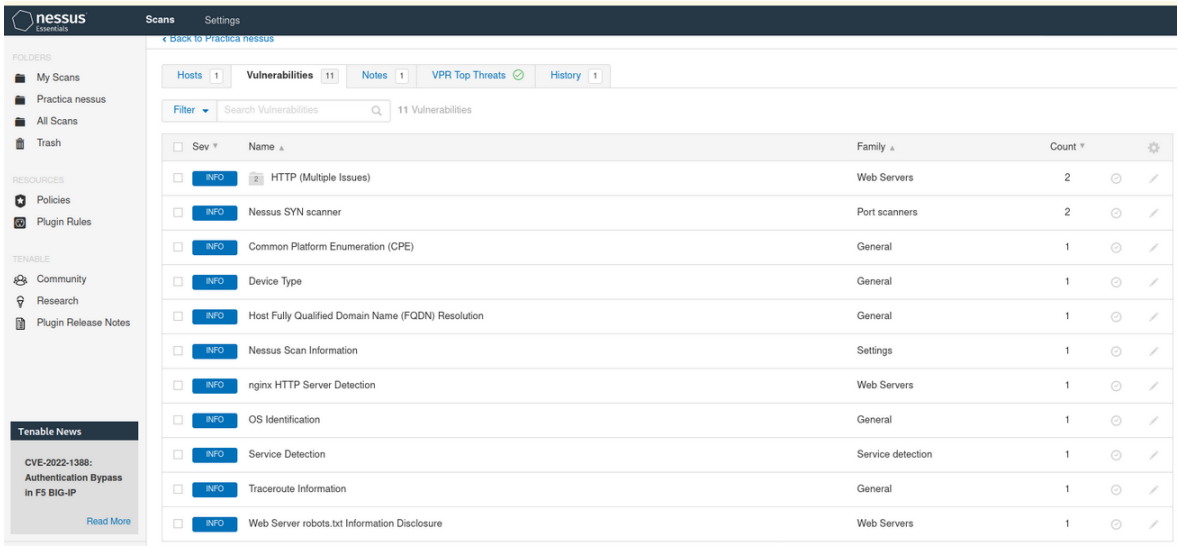
Fuente: Buscador Google

Ilustración 9 - Recolección de información



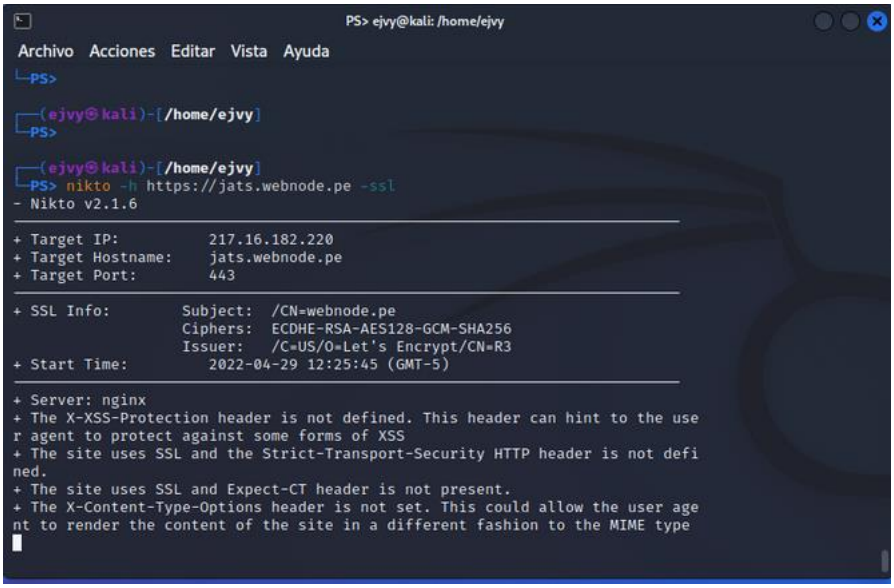
Fuente: Buscador Google

Ilustración 10 - Identificación de vulnerabilidades



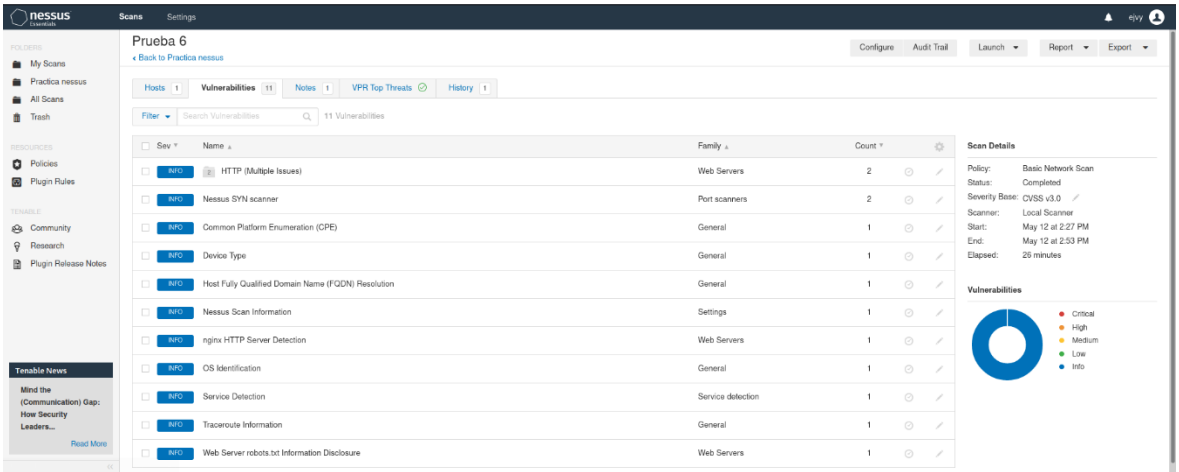
Fuente: Nessus

Ilustración 11 - Escaneo con Nikto



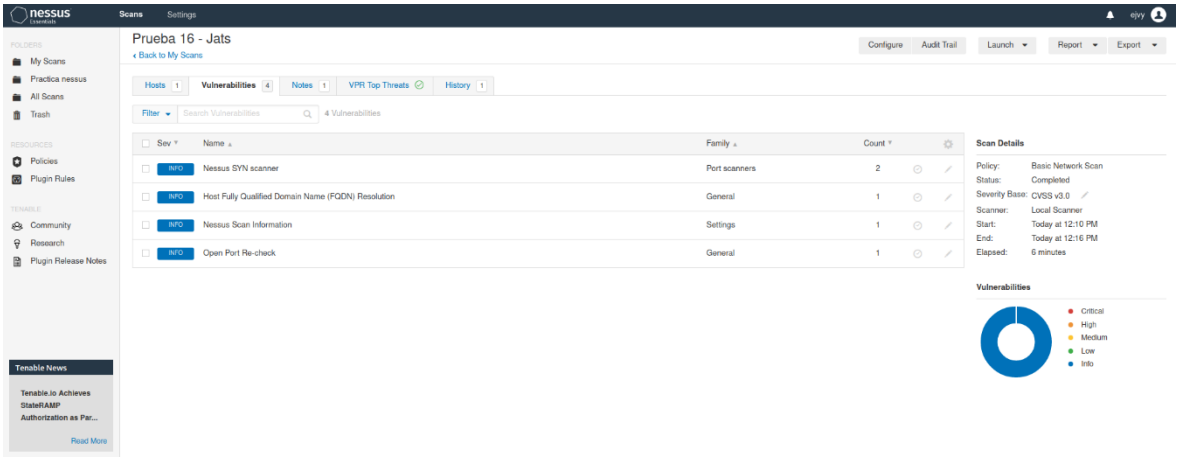
Fuente: Terminal Kali Lunux

Ilustración 12 - Escaneo con Nessus en el Pre-Test sitio web Jats



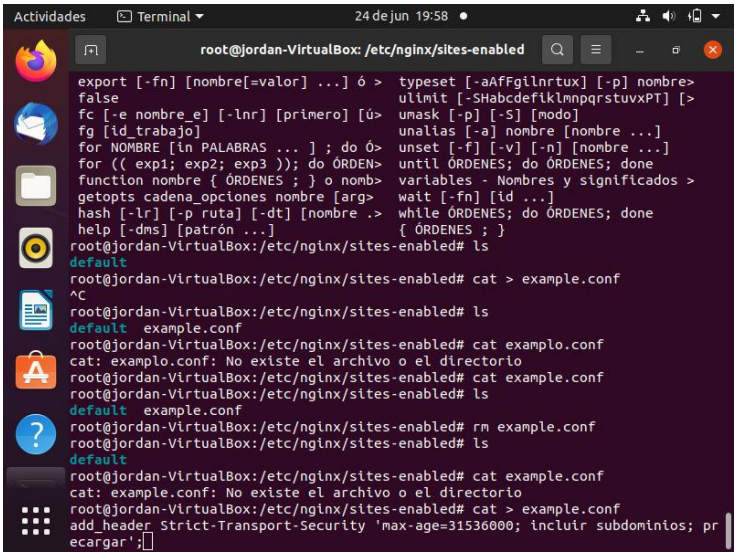
Fuente: Nessus

Ilustración 13 - Escaneo con Nessus en el Post-Test Jats



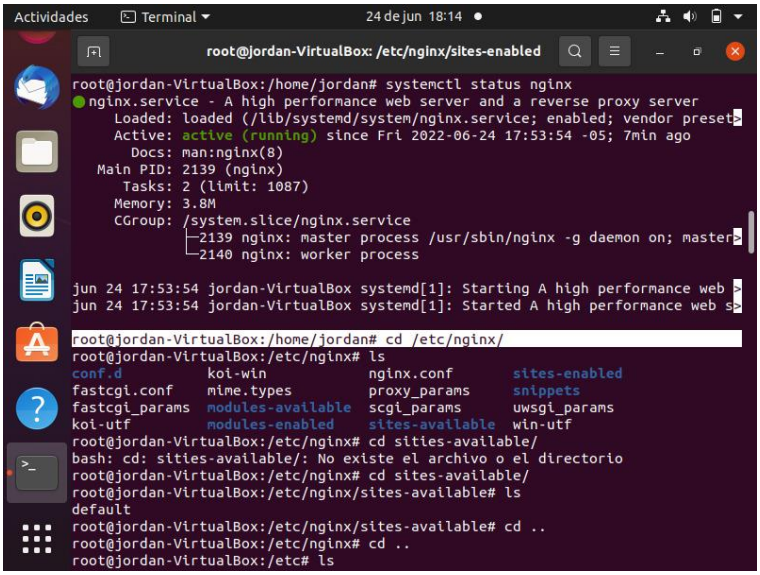
Fuente: Nessus

Ilustración 14 - Creación del archivo example.conf



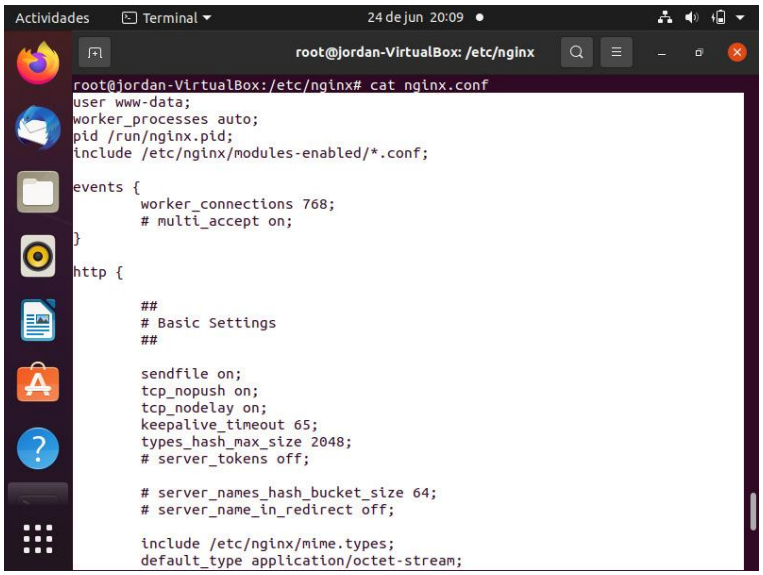
Fuente: Terminal Ubuntu

Ilustración 15 - Archivo de configuración nginx.conf



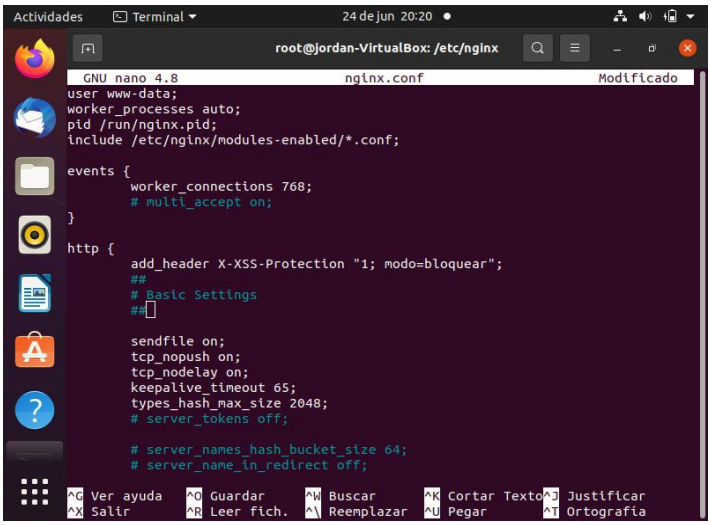
Fuente: Terminal Ubuntu

Ilustración 16 - Archivo nginx.conf



Fuente: Terminal Ubuntu

Ilustración 17 - Editando el archivo nginx.conf

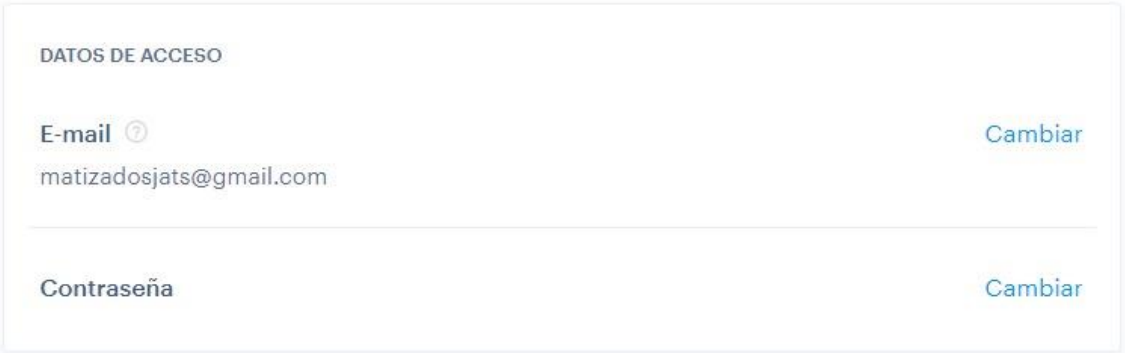


Fuente: Terminal Ubuntu

Ilustración 18 - Evidencia SSL en el sitio web

Fuente: Sitio web Jats

Ilustración 19 - Datos de acceso



Fuente: Sitio web Jats

Ilustración 20 - Instrumento validado por el primer experto

UNIVERSIDAD CÉSAR VALLEJO

CONSTANCIA DE VALIDACIÓN

Yo, **Winner Agurto Marchán**, con DNI N.° **40673760** Magister en "Ingeniería en Análisis de datos, mejora de procesos y toma de decisiones", de profesión Ingeniero de sistemas desempeñándome actualmente como Docente de Metodología de la Investigación y Cultura estadística en la Universidad César Vallejo de Piura.

Por medio de la presente hago constar que he revisado con fines de Validación de la Ficha de observación.

Luego de hacer las observaciones pertinentes, puedo formular las siguientes apreciaciones.

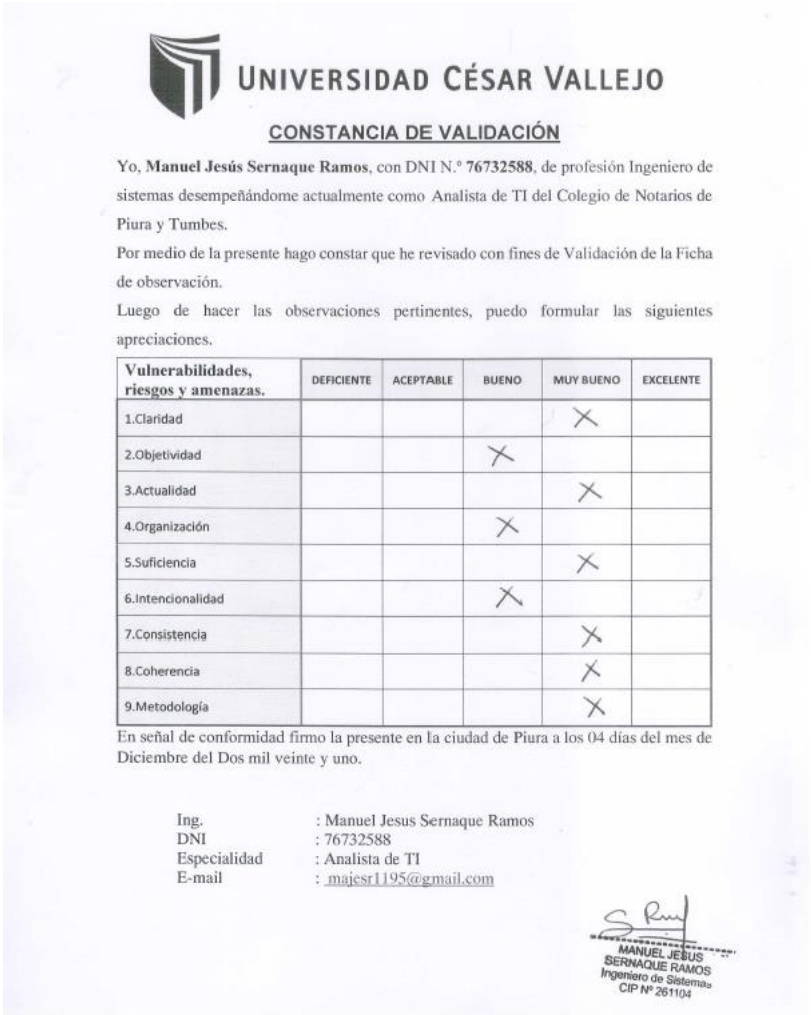
Vulnerabilidades, riesgos y amenazas.	DEFICIENTE	ACEPTABLE	BUENO	MUY BUENO	EXCELENTE
1.Claridad				X	
2.Objetividad				X	
3.Actualidad				X	
4.Organización				X	
5.Suficiencia				X	
6.Intencionalidad				X	
7.Consistencia				X	
8.Coherencia				X	
9.Metodología				X	

En señal de conformidad firmo la presente en la ciudad de Piura a los 21 dias del mes de noviembre del Dos mil veinte y uno.

Mg. Ing. : Winner Agurto Marchán
DNI : 40673760
Especialidad : Análisis de datos
E-mail : wagurtom@ucvvirtual.edu.pe

Fuente: Ficha de validación UCV

Ilustración 21 - Instrumento validado por segundo experto



UNIVERSIDAD CÉSAR VALLEJO

CONSTANCIA DE VALIDACIÓN

Yo, **Manuel Jesús Sernaque Ramos**, con DNI N.° **76732588**, de profesión Ingeniero de sistemas desempeñándome actualmente como Analista de TI del Colegio de Notarios de Piura y Tumbes.

Por medio de la presente hago constar que he revisado con fines de Validación de la Ficha de observación.

Luego de hacer las observaciones pertinentes, puedo formular las siguientes apreciaciones.

Vulnerabilidades, riesgos y amenazas.	DEFICIENTE	ACEPTABLE	BUENO	MUY BUENO	EXCELENTE
1.Claridad				X	
2.Objetividad			X		
3.Actualidad				X	
4.Organización			X		
5.Suficiencia				X	
6.Intencionalidad			X		
7.Consistencia				X	
8.Coherencia				X	
9.Metodología				X	

En señal de conformidad firmo la presente en la ciudad de Piura a los 04 días del mes de Diciembre del Dos mil veinte y uno.

Ing. : Manuel Jesus Sernaque Ramos
DNI : 76732588
Especialidad : Analista de TI
E-mail : majesr1195@gmail.com

MANUEL JESUS SERNAQUE RAMOS
Ingeniero de Sistemas
CIP N° 261104

Fuente: Ficha de validación UCV

Ilustración 22 - Instrumento validado por el tercer experto

UNIVERSIDAD CÉSAR VALLEJO

CONSTANCIA DE VALIDACIÓN

Yo, Eduardo Raul Perez Zamora con DNI N° 17639065, de profesión Ingeniero en Computación e Informática y docente en la Universidad César Vallejo de Piura.

Por medio de la presente hago constar que he revisado con fines de Validación de la Ficha de observación.

Luego de hacer las observaciones pertinentes, puedo formular las siguientes apreciaciones.

VULNERABILIDADE RIESGOS Y AMENAZAS	DEFICIENTE	ACEPTABLE	BUENO	MUY BUENO	EXCELENTE
1.Claridad				x	
2.Objetividad					x
3.Actualidad				x	
4.Organización					x
5.Suficiencia					x
6.Intencionalidad					x
7.Consistencia				x	
8.Coherencia					x
9.Metodología				x	

En señal de conformidad firmo la presente en la ciudad de Piura a los 24 días del mes de junio del Dos mil veintidós.

Mg. Ing. : PEREZ ZAMORA EDUARDO RAUL
DNI : 17639065
Especialidad : INGENIERO EN COMPUTACIÓN E INFORMÁTICA
E-mail : eduardo.perez@pucp.pe

EDUARDO RAUL PEREZ ZAMORA
INGENIERO EN COMPUTACIÓN E INFORMATICA
Reg. CIP N° 212391

Fuente: Ficha de validación UCV

Ilustración 23 - Solicitud para recolección de datos

SOLICITAMOS: Permiso para la recolección de datos

KARINA SENA SEMINARIO
Gerente de la empresa matizados JATS EIRL

Nosotros, Grace Beatriz Ipanaque Silva identificada con DNI N° 72676701 con domicilio en Av. Progreso 2015 – Campo Polo - Castilla y Eduardo Jordan Valverde Yovera identificado con DNI N° 47506765 con domicilio en Av. San Pablo Mz. A Lt: 13. A.H. Juan Velasco Alvarado Nuevo Catacaos - Catacaos, nos presentamos ante usted respetuosamente y exponemos:

Que siendo estudiantes del décimo ciclo de la escuela profesional de Ingeniería de Sistemas de la Universidad Cesar Vallejo, solicitamos ante usted nos conceda el permiso para la recolección de datos para nuestro proyecto de investigación titulado "Aplicación de herramientas de hacking ético para reducir el grado de vulnerabilidad en los sistemas web informáticos de las pymes de Piura" ya que esto es necesario para la presentación del informe final.

Por lo expuesto:

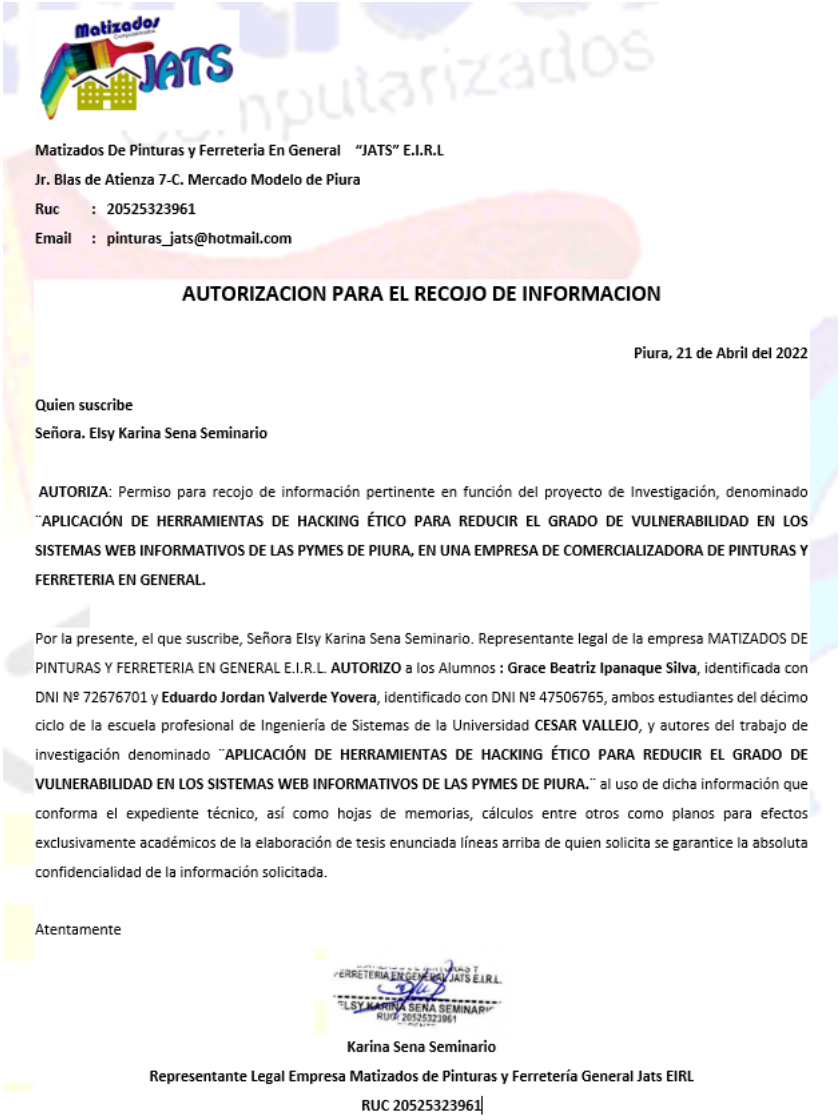
Ruego a usted acceder nuestra petición

En Piura a los 21 días del mes de abril del 2022

FIRMA DEL INVESTIGADOR Eduardo Jordan Valverde Yovera	FIRMA DEL INVESTIGADOR Grace Beatriz Ipanaque Silva	FIRMA DEL GERENTE Karina Sena Seminario
DNI: 47506765	DNI: 72676701	DNI: 41082493

Fuente: Elaboración propia

Ilustración 24 - Carta de aceptación para la recolección de información



Matizados De Pinturas y Ferreteria En General "JATS" E.I.R.L
Jr. Blas de Atienza 7-C. Mercado Modelo de Piura
Ruc : 20525323961
Email : pinturas_jats@hotmail.com

AUTORIZACION PARA EL RECOJO DE INFORMACION

Piura, 21 de Abril del 2022

Quien suscribe
Señora. Elsy Karina Sena Seminario

AUTORIZA: Permiso para recojo de información pertinente en función del proyecto de Investigación, denominado ¨**APLICACIÓN DE HERRAMIENTAS DE HACKING ÉTICO PARA REDUCIR EL GRADO DE VULNERABILIDAD EN LOS SISTEMAS WEB INFORMATIVOS DE LAS PYMES DE PIURA, EN UNA EMPRESA DE COMERCIALIZADORA DE PINTURAS Y FERRETERIA EN GENERAL.**

Por la presente, el que suscribe, Señora Elsy Karina Sena Seminario. Representante legal de la empresa MATIZADOS DE PINTURAS Y FERRETERIA EN GENERAL E.I.R.L. **AUTORIZO** a los Alumnos **: Grace Beatriz Ipanaque Silva**, identificada con DNI Nº 72676701 y **Eduardo Jordan Valverde Yovera**, identificado con DNI Nº 47506765, ambos estudiantes del décimo ciclo de la escuela profesional de Ingeniería de Sistemas de la Universidad **CESAR VALLEJO**, y autores del trabajo de investigación denominado ¨**APLICACIÓN DE HERRAMIENTAS DE HACKING ÉTICO PARA REDUCIR EL GRADO DE VULNERABILIDAD EN LOS SISTEMAS WEB INFORMATIVOS DE LAS PYMES DE PIURA.**¨ al uso de dicha información que conforma el expediente técnico, así como hojas de memorias, cálculos entre otros como planos para efectos exclusivamente académicos de la elaboración de tesis enunciada líneas arriba de quien solicita se garantice la absoluta confidencialidad de la información solicitada.

Atentamente

FERRETERIA EN GENERAL JATS E.I.R.L.
ELSY KARINA SENA SEMINARIO
RUC# 20525323961

Karina Sena Seminario
Representante Legal Empresa Matizados de Pinturas y Ferretería General Jats EIRL
RUC 20525323961

Fuente: Matizados Jats