UNIVERSIDAD NACIONAL
SANTIAGO ANTÚNEZ DE MAYOLO

FACULTAD DE CIENCIAS

ESCUELA PROFESIONAL DE
INGENIERÍA DE SISTEMAS E INFORMÁTICA

APLICACIÓN DE PENTESTING Y LA SEGURIDAD INFORMÁTICA EN LOS EQUIPOS TECNOLÓGICOS DE LA UNIVERSIDAD NACIONAL SANTIAGO ANTÚNEZ DE MAYOLO, 2022

TESIS PARA OPTAR EL TÍTULO DE:
INGENIERO DE SISTEMAS E INFORMÁTICA

PRESENTADO POR:
Bachiller Jhunior Leonel Calvo Cacha

ASESOR:
Mag. Joseph Darwin Alvarado Tolentino

HUARAZ - PERÚ
2022

Nº Registro: T170

DEDICATORIA

Dedico este proyecto a mis padres, por sus consejos, su comprensión y ayuda en todo momento. Me enseñaron a enfrentar las dificultades, sin perder la dignidad y sin rendirme en el intento. Quienes, con mucho amor, me inculcaron mis principios, mis valores y gracias a su apoyo incondicional y toda su confianza permitieron que logre culminar mi carrera profesional.

A mis hermanos, por estar siempre presente, acompañándome, brindándome su apoyo incondicional durante todo este proceso, y a toda mi familia por sus consejos, oraciones y palabras de aliento el cual me hicieron una mejor persona, y de una y otra manera me acompañaron en esta etapa aportando en mi formación personal y profesional.

Por último y no menos importante, a mis Docentes y amistades, a quienes agradezco su contribución e incondicional apoyo, son quienes han dado generosamente su tiempo y experiencia para poder desarrollarme profesionalmente.

AGRADECIMIENTO

Agradezco a Dios por ser mi guía y acompañarme con su bendición, para permitirme el haber llegado hasta este momento tan importante de mi formación profesional. A mis padres por ser el pilar fundamental y haberme apoyado pese a las adversidades e inconvenientes que se presentaron.

También quiero agradecer a la Universidad Nacional Santiago Antúnez de Mayolo, por darnos la oportunidad de estudiar, a los directivos y a nuestros docentes, por todo su esfuerzo y dedicación, quienes, con sus conocimientos, experiencias, y su motivación ha logrado fortalecer nuestros conocimientos con éxito.

De igual manera, agradezco a mi asesor de tesis por su visión crítica, por su rectitud en su profesión como docente, que gracias a sus consejos y correcciones hoy puedo culminar este trabajo.

RESUMEN

En el proyecto de investigación se realizó una introducción al tema de seguridad informática, la definición de sus principales términos, se llegó a identificar las posibles vulnerabilidades, las fases de un pentesting, se definen los principales términos de la seguridad informática. Teniendo como objetivo determinar la relación entre la aplicación del pentesting y la seguridad informática en los equipos tecnológicos en la Universidad Nacional Santiago Antúnez de Mayolo.

En el presente proyecto se hará uso de la técnica de recolección de datos mediante el cual se podrá identificar el fenómeno de estudio, detectar vulnerabilidad haciendo uso de las pruebas de OWASP, por lo cual se utilizará el enfoque cuantitativo, de acuerdo a su nivel será correlacional, debido a que se buscó la relación entre las variables de la investigación , en el presente estudio se identifica una muestra y se tiene dos variables las cuales son necesarias para identificar las vulnerabilidades, medir el nivel de riesgo y evaluar en qué medida afecta a la seguridad informática de la Universidad.

En la presente investigación se aplicara el estudio de diseño no experimental debido a que no se modifica las variables que se tiene, asimismo solo se tiene una sola muestra, se identifica vulnerabilidades a la que se encuentra expuesta la entidad y se determina la relación con la seguridad informática de la Universidad Nacional Santiago Antúnez de Mayolo.

El objetivo de la investigación es determinar la existencia de una relación directa y significativa entre la aplicación de pentesting y la seguridad informática en los equipos tecnológicos en la Universidad Nacional Santiago Antúnez de Mayolo. Se concluye que la aplicación de pentesting se relaciona significativamente con la seguridad informática con una alta correlación y un coeficiente de spearman igual a 0.779, el análisis de valor p igual a sig(bilateral)=0.000 que es menor a 0.05. Posterior a la aplicación del pentesting utilizando las pruebas de Owasp se logró identificar vulnerabilidades en la implementación del servidor Apache con un impacto global bajo de 2.750 y teniendo un nivel alto de probabilidad que es de 6.125. La vulnerabilidad basada en PHP tiene un impacto global bajo de 1.500 y un nivel medio de probabilidad que es de 5.

PALABRAS CLAVE: Pentesting, seguridad informática, vulnerabilidad.

ABSTRACT

In the research project, an introduction to the topic of computer security was made, the definition of its main terms, possible vulnerabilities were identified, the phases of a pentesting, the main terms of computer security were defined. With the objective of determining the relationship between the application of pentesting and computer security in technological equipment at the Santiago Antúnez de Mayolo National University.

In the present project, use will be made of the data collection technique through which the study phenomenon can be identified, vulnerability detected using the OWASP tests, for which the quantitative approach will be used, according to its level it will be correlational, because the relationship between the research variables was sought, in the present study a sample is identified and there are two variables which are necessary to identify vulnerabilities, measure the level of risk and evaluate to what extent it affects computer security at the University.

In the present investigation, the non-experimental design study will be applied because the variables that are not modified, likewise, there is only a single sample, vulnerabilities to which the entity is exposed are identified and the relationship with the entity is determined. computer security from the Santiago Antúnez de Mayolo National University.

The objective of the research is to determine the existence of a direct and significant relationship between the application of pentesting and computer security in technological equipment at the Santiago Antúnez de Mayolo National University. It is concluded that the application of pentesting is significantly related to computer security with a high correlation and a Spearman's coefficient equal to 0.779, the p-value analysis equal to sig(bilateral)=0.000, which is less than 0.05. After the application of the pentesting using the Owasp tests, it was possible to identify vulnerabilities in the Apache server implementation with a low global impact of 2,750 and having a high level of probability that is 6,125. The PHP-based vulnerability has a low overall impact of 1,500 and a medium probability level of 5.

KEY WORDS: Pentesting, computer security, vulnerability.

ÍNDICE GENERAL

Contenido

INDICE DE TABLAS

INDICE DE FIGURAS

INTRODUCCIÓN

1.1 Planteamiento de del problema

La universidad, en la actualidad está experimentando cambios muy drásticos, que ha movido su base de sustento de un negocio habitual, los cuales se basa en los recursos financieros, académicos y tecnológicos pasando a la nueva etapa de la virtualidad.

A lo largo de este tiempo la universidad ha venido implementando y adquiriendo diversos equipos y sistemas informáticos debido al rápido crecimiento de las tecnologías de información, servicios y equipos que permiten a la comunidad universitaria en general realizar sus trámites de forma virtual. Es por ello de vital importancia mantener y asegurarse que todos los servicios de la universidad estén funcionando correctamente.

Junto al crecimiento y desarrollo de las tecnologías también se toma en cuenta el crecimiento repentino de los ataques informáticos y tecnologías desarrolladas por parte de los crackers en estos últimos tiempos ha vuelto sensibles y vulnerables a la seguridad de la información.

En la actualidad, muchas empresas públicas y privadas no toman en consideración la seguridad informática, debido al alto costo que conlleva ello ya que no les genera ganancia a fin de año, sin embargo no se dan cuenta de la importancia que tiene la seguridad informática, por cuestiones de costo prefieren hacer uso de programas en versiones de prueba y adquisición ilegal del software, si bien es cierto estas tecnologías cumplen con su labor sin embargo no son suficientes y ponen en riesgo la información debido a que estos ya fueron manipulados previamente, es por ello que no brindan ninguna garantía, y están inmerso a posibles ataques informáticos.

Muchas organizaciones tanto nacionales como internacionales fueron víctimas de los cyberdelincuentes y las consecuencias fueron fatales, tales como pérdidas económicas, sanciones, robos de información, etc. Es por ello de vital importancia tomar mayor consideración en la utilización de técnicas de identificación de vulnerabilidades para poder protegerse ante posibles ataques informáticos debido a eso hoy en día es

importante tener un control de vulnerabilidades todo ello con el objetivo de evitar problemas a futuro y mejorar la imagen de la institución.

La universidad actualmente maneja una gran cantidad de activos de información es por ello que se ve en la necesidad de protegerlas, ante un ataque informático. Uno de los principales problemas que se afrontaría es la posible fuga de información es decir la salida no controlada de los datos, y se corre el riesgo que la información llegue a personas no autorizadas, además de ello posee servicios en funcionamiento de forma virtual, desde trámites documentarios, matrículas, clases virtuales entre otros, por lo cual la universidad tiene la obligación de velar por el correcto funcionamiento de dichos servicios.

La Universidad Nacional Santiago Antúnez de Mayolo tiene la necesidad de contar con un plan de trabajo para la aplicación de pentesting o técnicas de hacking ético para detectar vulnerabilidades, ya que al no contar con dicho plan representa un gran riesgo para la información, debido a que un cyberatacante puede aprovechar las vulnerabilidades para lograr acceder y tomar el control de los quipos informáticos de la misma manera la información puede ser interceptada, modificada y robada, esto ocasionaría un impacto negativo a la institución, como la perdida de dinero generándole multas, la perdida de la imagen institucional y de ser el caso sanciones drásticas.

El tema que se propuso hace mención a la aplicación de pentesting y la seguridad informática en los equipos tecnológicos de la Universidad Nacional Santiago Antúnez de Mayolo, el cual será de mucha ayuda para la institución ya que permitirá detectar vulnerabilidades y determinaremos la relación existente entre estos, posterior a la detección de las vulnerabilidades se brindará un listado de recomendaciones de las acciones a tomar.

1.2 Formulación del problema

1.2.1 Problema general

¿De qué manera se relaciona la aplicación de pentesting con la seguridad informática en los equipos tecnológicos de la Universidad Nacional Santiago Antúnez de Mayolo?

1.2.2 Problemas específicos

- ¿Es posible identificar la relación entre la aplicación de pentesting y la confidencialidad en la seguridad informática de los equipos tecnológicos de la institución?

- ¿Es posible conocer la relación entre la aplicación de pentesting y la integridad en la seguridad informática de los equipos tecnológicos de la institución?

- ¿Es posible analizar la relación entre la aplicación de pentesting y la disponibilidad en la seguridad informática de los equipos tecnológicos de la institución?

1.3 Objetivos de la investigación

1.3.1 Objetivos generales

Determinar la relación entre la aplicación del pentesting y la seguridad informática en los equipos tecnológicos en la Universidad Nacional Santiago Antúnez de Mayolo

1.3.2 Objetivos específicos

- Identificar la relación entre la aplicación de pentesting y la confidencialidad en la seguridad informática de los equipos tecnológicos de la institución.

- Conocer la relación entre la aplicación de pentesting y la integridad en la seguridad informática de los equipos tecnológicos de la institución.

- Analizar la relación entre la aplicación de pentesting y la disponibilidad en la seguridad informática de los equipos tecnológicos de la institución.

1.4 Justificación de la investigación

En el presente apartado se describen las razones por el cual se desarrolla el estudio con su respectiva justificación.

1.4.1 Tecnológico

En la actualidad los ataques cibernéticos están incrementando exponencialmente por lo cual es sumamente importante realizar tareas de prevención, detección de posibles fallos y tomar acciones ante ellos de ese modo salvaguardar toda información de valor de la universidad. Se debe de tomar en cuenta que si la universidad sufre un ciberataque el impacto que esto puede ocasionar son grandes pérdidas económicas de la misma forma la reputación de la entidad se vería afectada. (Margaret Lesly Palacios Gallardo, 2021, p. 17)

Toda organización maneja una gran cantidad de información para su funcionamiento diario, la Universidad Nacional Santiago Antúnez de Mayolo actualmente depende de sitios webs, sistemas internos y de los equipos informáticos para mejorar sus diferentes procesos para brindar una mejor calidad de servicio a los estudiantes; por ende, se tiene la necesidad de salvaguardar los datos personales e información sensible de los alumnos, docentes y personal administrativo de la entidad. En la actualidad toda entidad que cuente con equipos informáticos, sistemas operativos,

redes y sitios webs están propensos a ser vulnerados, en cualquier caso, trabajar con información, conlleva una serie de riesgos. Debido a lo indicado anteriormente las entidades están expuestas a posibles ataques informáticos o fuga de información; es por ellos que existen una serie de métodos y herramientas que permiten realizar un análisis conocido como test de penetración, por lo cual la Universidad Nacional Santiago Antúnez de Mayolo debe considerar la utilización del pentesting como un plan de seguridad para analizar los sistemas que soportan la gestión de la información con el fin de descubrir, explorar y corregir las debilidades detectadas en el entorno tecnológico de la universidad.

Para la aplicación del pentesting se cuenta con los equipos informáticos tecnológicos y plataformas web de la Universidad Nacional Santiago Antúnez de Mayolo, en donde se llevará a cabo el estudio para la detección de vulnerabilidades con el fin de detectar y poder prevenir posibles fallos.

1.4.2 Social

Mediante la aplicación de pentesting y la seguridad informática en los equipos tecnológicos de la Universidad Nacional Santiago Antúnez de Mayolo se tiene como fin descubrir debilidades con el objetivo de mitigar las amenazas y de ese modo reducir posibles ciberataques.

La presente se justifica socialmente pues al ser la universidad una entidad que posee equipos informáticos, sistemas de redes, datos personales que son uno de los activos más valiosos de los hackers, es por ello que la entidad es un objetivo potencial de ciberataque, debido a todo lo expuesto anteriormente un ataque informático afectaría el desarrollo normal y adecuado de la actividades de la universidad generando demoras, procesos detenidos, déficit en las plataformas virtuales, pérdida de confianza en los sistemas informáticos por parte de los alumnos y admirativos. Al realizar la prueba de penetración se logrará detectar y prevenir posibles fallos evitando de esa manera la perdida de información, daños en la infraestructura empresarial, repercusiones económicas, impactos negativos en la reputación de la entidad.

1.4.3 Económico

La aplicación del pentesting en la Universidad Nacional Santiago Antúnez de Mayolo, permitirá identificar vulnerabilidades, analizarlas y brindarles posibles soluciones con el objetivo de mitigarlas, es decir reducir esencialmente la probabilidad de que un ciberatacante pueda explotar dichas vulnerabilidades. Si la entidad sufre un ciberataque podría detener su operación, puede dejar de funcionar sus aplicativos webs, puede dejar de facturar, sufrir daños en su infraestructura tecnológica por ende los administrativos no podrían realizar sus actividades normalmente, asimismo poder solucionar los daños a consecuencia de un ciberataque sería muy costoso para la Universidad.

1.4.4 Legal

- Ley Nº 29733 “Ley de protección de datos personales”- reglamento de ley N° 29733 ley de protección de datos personales, decreto supremo N°003-2013-JUS.

- “Ley de Gobierno Digital” (Decreto Legislativo N° 1412, 2018)

- Ley N°30999 -2019 ” Ley de Ciberdefensa”

- Decreto Supremo Nº029-2021-PCM “Reglamento de la Ley de Gobierno Digital”.

MARCO TEÓRICO

2.1 Antecedentes de la investigación

En la actualidad existen investigaciones y proyectos realizados en diferentes instituciones:

2.1.1 Antecedentes Internacionales

Vera (2020) en su tesis aplicación de técnicas de pentesting para determinar vulnerabilidades en la red lan de la empresa csednet de santo domingo. Los autores identificaron como objetivo general Aplicar técnicas de pentesting para determinar vulnerabilidades en la red LAN de la empresa CSEDnet de Santo Domingo. La investigación tiene como finalidad identificar puntos débiles en la red de la organización, para lo cual hacen uso de la metodología de evaluación de vulnerabilidad de red. Durante el proyecto se realizaron diferentes pruebas tales como el sniffing permitiendo identificar vulnerabilidades tales como capturar contraseñas, cambiar nombre de usuarios y interceptar conversaciones; debido a todo ello se implementó reglas de mitigación de captura de paquetes concluyendo que el número de paquetes capturados disminuyo drásticamente, obteniendo como resultado una reducción del 98,62% de la vulnerabilidad de captura de paquetes.

Gomez (2020) En su estudio test de penetración pentesting aplicado en la empresa Megaseguridad para evaluar vulnerabilidades y fallas en el sistema de información, Universidad Nacional Abierta y a Distancia. El objetivo de la investigación es implementar experimentos de pentesting para detectar vulnerabilidades en la red de la organización. El presente estudio tiene como finalidad hacer entrega de un diagnóstico situacional de las posibles vulnerabilidades y fallas a que está expuesta su red de información. Como resultado de aplicar el pentesting se pudo identificar algunas vulnerabilidades como puertos expuestos, información de sistemas operativos. Se concluye que con el manejo de tecnología y el trabajo en red para equipos conectados a la LAN e internet inalámbrico deja una brecha abierta a un activo importante como la información digital de compañía asimismo se detectaron sistemas operativos sin

actualizaciones, deshabilitada la seguridad firewall entre otros, finalmente se hace recomendaciones para mitigar fallas y vulnerabilidades

Sánchez (2018) en su tesis implementación de pentesting para encontrar vulnerabilidades en el sistema utilizado en la compañía “dirsa” aplicando metodología de owasp tiene como objetivo general implementar un test de seguridad para identificar vulnerabilidades en el tratamiento de los datos de la empresa dirsa y busca brindar recomendaciones para poder incrementar el nivel de seguridad dentro de la organización. La investigación tiene como finalidad hacer uso de la metodología owasp de owasp para detectar posibles fallos en los equipos tecnológicos de la entidad mediante un ataque dirigido a la organización, se concluye que los fallos y vulnerabilidades son de altos a medios se debe realizar esfuerzos adecuados para mitigar el efecto de las fallas en toda la organización, la única solución es establecer políticas que incluyan la realización de auditorías y concientizar a los empleados dentro de la organización de que tan frágil es la información que se maneja. evitar ataques informáticos es previniendo su ocurrencia.

2.1.2 Antecedentes Nacionales

Mena (2019) en su tesis aplicación de pentesting y prevención de ataques a los sistemas de industrias san miguel del sur –planta Huaura. El objetivo es determinar la relación entre la aplicación de Pentesting y la prevención de ataques a los sistemas de Industrias San Miguel del Sur - Planta Huaura. El método de estudio es una investigación no experimental a nivel de investigación correlacional. Los resultados de la investigación muestran que la mayoría de los colaboradores están de acuerdo con la aplicación del pentesting para la prevención de ataques y la detección de vulnerabilidades. Se concluye que la metodología de pentesting si tiene una relación significativa con los Sistemas de Industrias San Miguel del Sur con una alta correlación con un coeficiente de Spearman igual a 0.766 el análisis de p valor o Asintótica (Bilateral) = 0.000 que es menor que 0.05.

Palacios (2021) En su tesis aplicación de pentesting en el análisis de vulnerabilidades del sistema web de gestión administrativa de la empresa

DEVHUAYRA SAC Huancayo, Universidad Continental. La investigación tiene como objetivo aplicar el pentesting para el análisis de vulnerabilidades, clasificarlas de acuerdo con el nivel de gravedad y reducir las vulnerabilidades encontradas. El método de investigación es el analítico y el método inductivo-deductivo, los resultados obtenidos en la investigación muestran que se identificaron 4 vulnerabilidades de nivel critica, 1 vulnerabilidad de nivel importante, 3 vulnerabilidades de nivel moderado y 2 de nivel bajo, finalmente los resultados posteriores a la aplicación del pentesting muestra una reducción mínima de un 16.67% del impacto de aprovechamiento de una vulnerabilidad. La conclusión del estudio realizado hace mención que la aplicación del pentesting disminuyo las vulnerabilidades del sistema web de gestión administrativa, luego de aplicado el control de seguridad redujo un 39.72% en el impacto general y un máximo de 55.66% del impacto del aprovechamiento de una vulnerabilidad.

Piñashca (2022) en su estudio evaluación técnica de hacking ético para analizar la seguridad informática de la municipalidad distrital de los olivos, Universidad Señor de Sipán. Tiene como objetivo evaluar las técnicas de hacking ético aplicada en la seguridad informática que permita identificar las vulnerabilidades en la entidad. El tipo de estudio es cuantitativo y de diseño no experimental. Posterior a la aplicación de las técnicas de hacking ético los resultados indican la existencia de diversas vulnerabilidades en la red de trabajo. Luego de obtener los resultados se llegó a la conclusión que la seguridad informática de la entidad es deficiente, dado que en su infraestructura presenta muchas falencias estando expuesto a ataques informáticos y posterior al escaneo al host la evaluación del sistema indica que el servidor esta activo.

2.1.3 Antecedentes Locales

Alvarado (2017), en su tesis análisis de las vulnerabilidades mediante el uso de phishing para mejorar la seguridad informática de los equipos de cómputo y redes de la municipalidad distrital de independencia, Huaraz 2017, Universidad Nacional "Santiago Antúnez de Mayolo", el proyecto de tesis tiene como objetivo utilizar métodos de phishing para analizar las vulnerabilidades para mejorar la seguridad informática de los equipos de cómputo y redes. El diseño empleado fue descriptivo

simple, tipo exploratorio tecnológico. El resultado de la presente tesis confirma que los peligros que amenaza en la eficacia del servicio de informática también pueden detener las actividades, se consideró ya que eran de mayor importancia por el alto nivel de riesgo que le ocasionaría al usuario. En esta investigación se concluyó que, dentro de los conceptos de phishing, se pueden encontrar muchas técnicas que son utilizadas para la ingeniería social, son bastante fáciles de usar y normalmente se aprovechan de la falta de conocimiento de los individuos, quienes sin darse cuenta conceden cualquier tipo de información a sujetos desconocido y no se da cuenta que la información que brindan puede causar pérdidas desastrosas dentro de la entidad.

2.2 Bases teóricas

2.2.1 Seguridad Informática

Uno de los activos más importantes que maneja una entidad es la información que maneja es por ello la necesidad de proteger su infraestructura tecnológica, las mismas que deben estar establecidas en un Sistema de Gestión de la Seguridad de la Información “ISO/IEC 27000”. El termino de seguridad informática es toda acción, método, medida y política para resguardar la infraestructura informática de posibles amenazas, ataques, vulnerabilidades y riesgos que puedan ocurrir. (Gascó, Romero, Ramada, y Pérez, 2017, p.7).

2.2.1.1 Vulnerabilidades Informáticas

La vulnerabilidad informática es un defecto en el diseño, ejecución, gestión de un sistema tecnológico que podría aprovecharse para comprometer los recursos del sistema de cualquier entidad. (The OWASP Fundation, 2018, p. 27).

2.2.1.2 Amenazas Informáticas

En su libro de seguridad informática define a la amenaza como cualquier ente o suceso que atente contra el correcto funcionamiento de un sistema

informático". Se hace mención a las amenazas informáticas más comunes tales como: Crackers, Sniffers, Spammers y otros, códigos maliciosos como los virus, troyanos, gusanos, spyware entre otros. (Gascó et al., 2017, p.9)

2.2.1.3 Riesgos Informáticos

El riesgo es una probabilidad de que una amenaza se haga real o concrete, como el riesgo no se puede evitar se tienen medidas de que asume una organización. Para realizar una clasificación correctamente los riesgos es necesario priorizar o clasificarlos activos y recursos de la entidad. (Gascó et al., 2017, p. 12). Por lo tanto, se tiene la necesidad de contar con un equipo dedicado a gestionar los riesgos con el objetivo principal de proteger a la organización y poder cumplir con su misión. El proceso de gestión de riesgos debe ser tratado como una función de gestión esencial de una organización. (NIST, 2002).

En la Tabla 1 se muestra el top de las 10 amenazas más importantes de la Web según OWASP.

Tabla 1

Top 10 de Vulnerabilidades OWASP.

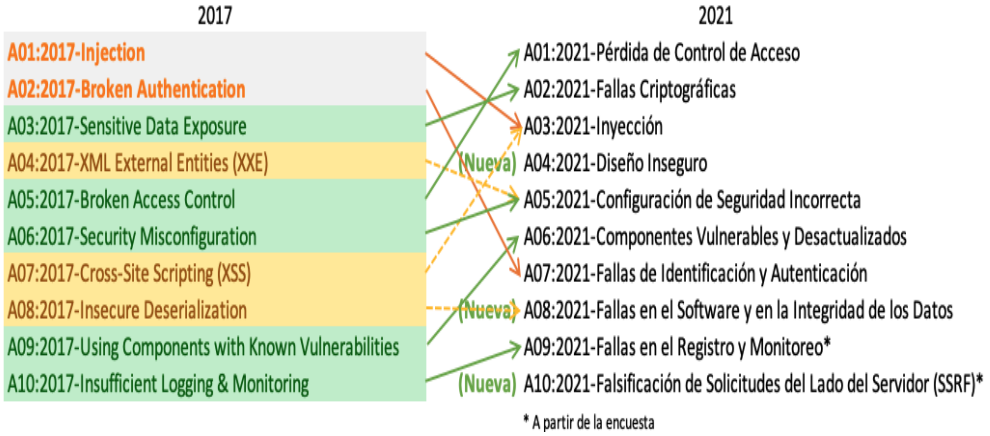
Top 10 de Vulnerabilidades OWASP.		
A1: 2021	-	Pérdida de control de acceso
A2: 2021	-	Fallas criptográficas
A3: 2021	-	Inyección
A4: 2021	-	Diseño Inseguro
A5: 2021	-	Configuración de seguridad Incorrecta
A6: 2021	-	Componentes Vulnerables y Desactualizados
A7: 2021	-	Fallas de Identificación y Autentificación
A8: 2021	-	Fallas en el software y la Integridad de Datos
A9: 2021	-	Fallas en el riesgo y monitoreo

A10: 2021	-	Falsificación de solicitudes del lado del servidor (SSRF)*

Nota. Fuente: Adaptado de The OWASP Foundation, 2021.

Figura 1

OWASP Top 10 – 2021



Nota: Cuadro comparativo del 2017 al 2021

- **A01: Pérdida de Control de Acceso:** Es el de mayor riesgo en seguridad de aplicaciones web; los datos indican que el 3,81% de las aplicaciones que se analizaron tenían una o más debilidades identificadas en el Common Weakness Enumerations (CWEs), con más de 318 mil casos en estas clases de riesgo.

- **A02: Fallas Criptográficas:** Se basa en las debilidades relacionadas con la criptografía, esta categoría continuamente trae como consecuencia la exposición de datos confidenciales.

- **A03: Inyección:** El 94% de las aplicaciones fueron analizadas con el objetivo de encontrar alguna debilidad logrando como resultado un promedio de incidencia máxima del 19% y de 3.37% de promedio. Las CWEs que tienen relación con la inyección tienen la segunda mayor cantidad de ocurrencias en aplicaciones con 274.000.

- **A04: Diseño Inseguro:** Es nueva categoría en la edición 2021, se enfoca en los riesgos que tengan relación con las fallas de diseño. Si verdaderamente se desea avanzar como industria es necesario identificar más modelos de amenaza, utilizar más patrones y principios de diseño seguro.

- **A05: Configuración de Seguridad Incorrecta**: El 90% de las aplicaciones fueron probadas con el fin de identificar vulnerabilidades de tipo configuración incorrecta, con un promedio de incidencia 4,5% y más de 208 mil ocurrencias de CWEs relacionadas con esta categoría de riesgo. Esta categoría asciende con la adopción de software altamente configurable.

2.2.1.4 Triada CID

Se define a la información como el valor de los datos, es lo que aporta conocimiento. Las guías, los datos de los alumnos, de los profesores y administrativos de la entidad, la base de datos son datos ordenados de tal forma que se transforman en información que aporta valor a la compañía. (Romero et al, 2018)

En la siguiente figura se visualiza la triada de seguridad de información (CID)

Figura 2

Los 3 pilares fundamentales

Según la Figura 2, la seguridad consta de 3 conceptos fundamentales, en este caso, si alguno de los lados se encuentra vulnerado o en riesgo se perderá seguridad o usabilidad, si alguno de los lados tiene deficiencias la entidad queda expuesta a posibles ataques informáticos.

2.2.1.5 Análisis de amenazas y vulnerabilidades

(Romero et al, 2018) según su estudio realizado plantea una definición general de que la vulnerabilidad es un fallo en un sistema que puede ser aprovechada por un atacante generando un peligro para la entidad y para el mismo sistema tecnológico. Así mismo también define la existencia de las vulnerabilidades lógicas y las físicas.

- **Vulnerabilidades lógicas:** Este tipo de vulnerabilidades son las que tienen una afectación directa con la infraestructura y el funcionamiento correcto de estos. Estas pueden ser las de configuración en el sistema operativo, las vulnerabilidades de actualización y las vulnerabilidades de desarrollo; este tipo de vulnerabilidades afectan directamente al desarrollo correcto de las operaciones de los equipos tecnológicos esto podría darse

debido a que los firewalls no están gestionados de una manera correcta, la falta de actualización de los softwares o inyecciones Sql.

- **Vulnerabilidades físicas:** Este tipo de vulnerabilidades son las que afectan directamente a la infraestructura física de la compañía por ejemplo los desastres naturales, una sísmica se podría considerar como una vulnerabilidad alta, ya que al ocurrir un desastre podría afectar gravemente a los equipos tecnológicos por ende se tendría afectación en la disponibilidad es ahí donde inician los problemas o si la compañía se encuentra ubicada en una zona que normalmente se inunda al ocurrir el desastre se podría afectar perder información por ende afecta la disponibilidad.

Identificar vulnerabilidades y estimar la gravedad de todos los riesgos es importante ya que al contar con un sistema para medir los riesgos ahorra tiempo y ayuda a que la entidad se enfoque más en riesgos mucho más serios sin que se distraiga en los riesgos o vulnerabilidades ya conocidas.

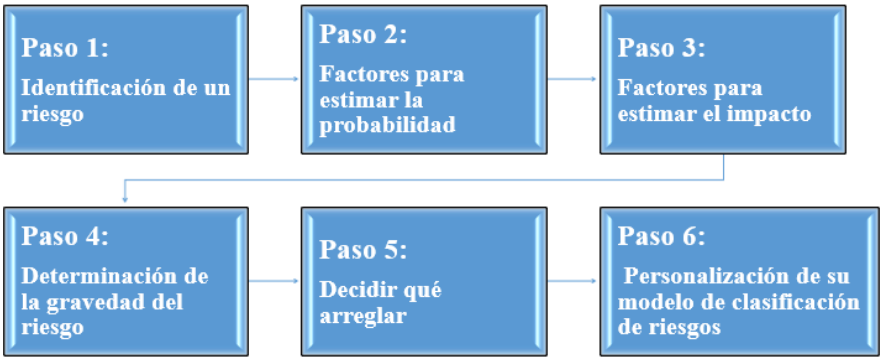
El enfoque OWASP está personalizado para la seguridad de aplicaciones, en la cual toma en cuenta factores de probabilidad y riesgo (The OWASP Fundation, 2021)

Riesgo = Probabilidad * Impacto

En la siguiente imagen se describe los pasos que se deben de seguir para identificar el nivel de riesgo para la seguridad de las aplicaciones.

Figura 3

Clasificación de riesgos



Nota. Clasificación de riesgos adaptado a The OWASP Fundation, 2021

- **Paso 1: Identificación de un riesgo**

  Para identificar un riesgo lo primero que se debe hacer es identificar un riesgo, para lo cual se debe recopilar información sobre el agente amenaza a estudiar, el ataque se utilizará, la vulnerabilidad y el impacto de un ataque exitoso en el negocio.

- **Paso 2: Factores para estimar la probabilidad**

  Consiste en un conjunto de factores que apoyan a determinar la probabilidad mediante una serie de factores siendo una de ellas relacionada con el agente de amenaza involucrado, teniendo como objetivo principal estimar la probabilidad de un ataque exitoso.

  a) Factores amenaza:

  El objetivo aquí es estimar la probabilidad de un ataque exitoso por parte de un conjunto de agentes de amenaza. Utilizar el agente de amenaza en el peor de los casos como muestra la siguiente tabla2

Tabla 2

Factores de agente de amenaza

Factores de agente de amenaza			
Nombre	**Detalle**	**habilidad**	**Puntos**
Nivel de habilidad	Capacidad técnica del grupo	Sin habilidades técnicas	1
		Algunas habilidades técnicas	3
		usuario avanzado de computadoras	5
		Conocimientos de red y programación	6
		habilidades de penetración de seguridad	9
Motivo	Motivación del grupo para encontrar y explotar una vulnerabilidad	baja o sin recompensa	1
		Posible recompensa	4
		Recompensa alta	9
Oportunidad	Recursos y oportunidades que se requieren para que este grupo encuentre y explote la vulnerabilidad	Accesos completos o recursos costosos	0
		Accesos especiales o recursos requeridos	4
		Algun acceso o recursos requeridos	7
		No se requiere accesos ni recursos	9
Tamaño	Tamaño de grupo	Desarrolladores	2
		Administradores de sistema	2
		Usuarios de la intranet	4
		Socios	5
		Usuarios autentificados	6
		Usuarios anónimos de internet	6

Nota: Adaptado de (The OWASP Fundation, 2021)

a) Factores de vulnerabilidad

Este apartado está relacionado con la vulnerabilidad encontrada, el principal objetivo aquí es estimar de que la vulnerabilidad involucrada sea identificada y explotada.

Tabla 3

Factores de vulnerabilidad

Factores de vulnerabilidad			
Nombre	**Detalle**	**habilidad**	**Puntos**
Facilidad de descubrimiento	Dificultad del grupo para descubrir una vulnerabilidad	Prácticamente imposible	1
		Difícil	3
		Fácil	7
		Herramientas disponibles	9
Facilidad de explotación	Facilidad del grupo para explotar vulnerabilidades	Teórico	1
		Difícil	3
		Fácil	5
		Herramientas disponibles	9
Conciencia	Conocimiento del grupo sobre la vulnerabilidad	Desconocido	1
		Oculto	4
		Obvio	6
		Conocimiento público	9
Detección de intrusos	Probabilidad de que se detecte un exploit	Detección activa en la aplicación	1
		Registrado y revisado	3
		Registrado sin revisión	8
		No registrado	9

Nota. Adaptado de (The OWASP Fundation, 2021).

- **Paso3: Factores para estimar el impacto**

  Para considerar el impacto de un ataque con éxito se tiene dos tipos de impacto: el impacto técnico y comercial.

a) Factores de impacto técnico:

Las áreas de mayor precaución son las de seguridad tradicionales tales como la confidencialidad, integridad, disponibilidad y responsabilidad. El objetivo principal de este impacto es medir la magnitud del impacto en el sistema si se llega a explotar la vulnerabilidad.

Tabla 4

Factores de impacto técnico

Factores de impacto técnico			
Nombre	**Detalle**	**habilidad**	**Puntos**
Pérdida de Confidencialidad	Cantidad de información a divulgarse y que tan confidencial es	Datos mínimos no confidenciales divulgados	2
		Datos críticos mínimos divulgados	6
		Extensos datos no confidenciales revelados	6
		Extensos datos críticos revelados	7
		Todos los datos divulgados	9
Pérdida de integridad	Cantidad de datos afectados	Datos mínimos ligeramente corruptos	1

	y que tan dañados están	Datos mínimos gravemente corruptos	3
		Extensos datos ligeramente corruptos	5
		Extensos datos gravemente corruptos	7
		Datos totalmente corruptos	9
Pérdida de disponibilidad	Perdida de servicio y cuan vital es	Servicios secundarios mínimos interrumpidos	1
		Servicios primarios mínimos interrumpidos	5
		Amplios servicios secundarios interrumpidos	5
		Amplios servicios primarios interrumpidos	7
		Servicios completamente perdidos	9
Pérdida de responsabilidad	Las acciones amenazantes pueden ser rastreadas	Totalmente rastreable	1
		Registrado y revisado	3
		Posiblemente rastreable	8
		Completamente anónimo	9

a) **Factores de impacto comercial:**

El riesgo empresarial es lo que justifica la inversión en solucionar los problemas de seguridad. Algunas entidades cuentan con una guía de clasificación de activos o una referencia de impacto comercial para identificar lo que es importante para su negocio y estos estándares identificados podrían ayudar a conocer que se activos o áreas se pueden proteger. Si la entidad no cuenta con una guía es necesario pedir una opinión sobre que considera importante en su

negocio. En el siguiente cuadro visualizamos los factores que son áreas comunes de muchas entidades, asimismo mencionar que estas áreas son exclusivas para una empresa relacionado con el agente amenaza, vulnerabilidad y el impacto técnico.

Tabla 5
Factores de impacto comercial

Factores de impacto comercial

Nombre	Detalle	habilidad	Puntos
Daño financiero	Daño financiero generado por un exploit	Menos que el costo de arreglar la vulnerabilidad	1
		Efecto menor en la utilidad anual	3
		Efecto significativo en la utilidad anual	7
		Bancarrota	9
Daño a la reputación	Daño a la reputación del negocio generado por un exploit	Daño mínimo	1
		Pérdida de cuentas importantes	4
		Pérdida de buena voluntad	5
		Daños a la marca	9
Incumplimiento	Nivel de exposición al incumplir	Violación menor	2
		Violación clara	5
		Violación de alto perfil	7
Violación de privacidad	Cantidad de información divulgada	Un individuo	3
		Cientos de personas	5
		Miles de personas	7
		Millones de personas	9

Nota. Adaptado de (The OWASP Fundation, 2021).

- **Paso 4: Determinar la gravedad del riesgo**

Con los datos obtenidos, se realiza la matriz de riesgos por cada vulnerabilidad previamente identificada en la cual toma en cuenta factores de probabilidad y riesgo. Como se muestra

Riesgo = Probabilidad * Impacto

Fórmula de Riesgo Aplicada al Proyecto:(The OWASP Fundation, 2021)

La estimación de probabilidad e impacto se combinan para calcular la gravedad general de este riesgo. Para ello se utilizan valores del 0 al 9 de acuerdo al nivel de impacto al negocio.

Figura 4

Niveles de probabilidad e impacto

Likelihood and Impact Levels	
0 to <3	LOW
3 to <6	MEDIUM
6 to 9	HIGH

En la siguiente imagen se explica la gravedad general de riesgo:

Figura 5

Matriz determinación de la gravedad de probabilidad por impacto.

(The OWASP Fundation, 2021)

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

2.2.2 Aplicación pentesting

2.2.2.1 Metodologías pentesting

Estas metodologías son necesarias para las compañías, el desarrollo y mantenimiento de aplicaciones web, su principal objetivo debe ser la clasificación de riesgos informáticos, basados en las amenazas y su probabilidad de ocurrencia. A continuación, mencionaremos las metodologías más conocidas de pentesting (Añazco y Ortiz, 2018)

- **OWASP Testing Guide V4:** Es un proyecto de código abierto encargado de identificar el nivel de seguridad en las aplicaciones web, OWASP se basa en crear artículos, metodologías y documentación. Las dimensiones que considera son: personas, procesos y tecnologías. OWASP Testing Guide v4 es la documentación principal.

- **Payment Card Industry Data Security Standard Penetration Testing guide:** Es una comisión conformada por las compañías más importantes de tarjetas de crédito y débito, cuentan con una guía para aquellas entidades que procesan y almacenan datos de sus clientes, la cual tiene por objetivo evitar fraudes que tengan que ver con tarjetas de pago.

- **Penetration Testing Execution Standard (PTES):** El presente estándar está diseñado con el fin de facilitar a las organizaciones y los proveedores que brindan servicios de seguridad, un lenguaje común al alcance de todos para realizar pruebas de penetración.

- **NIST 800-115:** El Instituto Nacional de Estándares y de Tecnología (NIST), es el encargado de desarrollar normas y directrices, incluidos los requisitos mínimos para proporcionar seguridad de información adecuada para todas las operaciones y activos de la agencia de los Estados Unidos de América, sin incluir los sistemas de seguridad nacional de dicho país.

- **Penetration Testing Framework de Toggmeister y Lee Lawson:** Brinda un recorrido detallado de diferentes aspectos de una prueba de pentest, asimismo hace énfasis en el uso de herramientas especiales y los comandos utilizados en cada herramienta.

- **Information Systems Security Assessment Framework (ISSAF):** Se define como marco estructurado revisado por pares que categoriza la evaluación de seguridad del sistema de información en varios dominios tales como Unix, Linux, seguridad en base de datos entre otros puntualizando criterios específicos de evaluación y prueba por cada dominio.

2.2.2.2 Etapas del Pentesting

- **Descubrimiento y enumeración:** Es la primera etapa del pentesting y una de las más importantes es por ello que se tiene la necesidad de ponerle más énfasis en esta etapa ya que es donde se recopila toda la información necesaria sobre el objetivo, trataremos de identificar que equipos tecnológicos tenemos tales como servidores web, dispositivos de red, impresoras entre otros dispositivos informáticos en los cuales se puede encontrar vulnerabilidades, también se puede identificar datos sobre los subdominios de una página web que nos sirve para realizar ataques de tipo diccionario es decir podemos identificar la información que se encuentra alojada en internet.

  Por lo indicado anteriormente la información se puede recopilar de forma activa donde el atacante siempre está en contacto con el objetivo con el propósito de reunir información y la recopilación de información de forma pasiva es cuando no es necesario que el atacante tenga comunicación con el objetivo directamente ya que este se encuentra recopilando información desde internet.

- **Análisis de vulnerabilidades:** Es el proceso de identificar deficiencias en los sistemas y aplicaciones que puedan ser explotadas por un ciberatacante, las posibles fallas podrían ser configuraciones incorrectas y diseños inseguros de la aplicación. En aquí se usa la información que se recopiló en la etapa anterior y de acuerdo con los resultados conseguidos de la búsqueda de brechas de seguridad.

  En este proceso se utilizan escáners de vulnerabilidades de red y escáners de vulnerabilidades web, dentro de los escáners de vulnerabilidades de red encontramos a la herramienta NMAP que nos permitirá escanear puertos, es decir nos ayuda a identificar que puertos o servicios se encuentran abiertos en una red. También existen otras herramientas para escanear puertos tales como Nessus,

OpenVas y Nexpose que es una potente herramienta que nos permite identificar vulnerabilidades en la base de datos.

Para los escaneos de aplicaciones web se usan herramientas como acunetix, esta nos permite detectar fallos de seguridad a través de los protocolos http y https.

Debemos tener en cuenta el ciclo de gestión de las vulnerabilidades, el cual consiste en una serie de pasos y lo utilizamos cuando vamos a hacer una evaluación completa en la compañía.

Figura 6

Ciclo de vida de la gestión de vulnerabilidades

Nota. Fuente: https://vbshield.com/gestion-de-vulnerabilidades-dibujo-en-png24/

- **Explotación:** En esta etapa el pentest realiza la explotación de una de las vulnerabilidades identificadas en la etapa anterior, es aquí donde se aplica todas las técnicas necesarias para lograr explotar una vulnerabilidad y esto se logra haciendo uso de la herramienta exploit. Según welivesecurity de la empresa eset, exploit se define como un programa o código que se aprovecha de un agujero de seguridad (vulnerabilidad) en un sistema, de forma que un atacante podría usarla en su beneficio.

  Existen varios tipos de exploit tales como exploit remoto que se puede realizar en la propia red local o basta con que el objetivo tenga acceso a internet. Exploit local se realiza estando físicamente en el objetivo a atacar y el exploit cliente que son los más comunes ya que para poder ejecutarse necesitan acción alguna del usuario como ejemplo un enlace malicioso.

- **Informe:** Esta es la etapa donde se documenta para la presentación de un informe con los resultados conseguidos durante toda las anteriores fases ejecutadas, su finalidad es darle una visión clara detallando en donde se encuentran las vulnerabilidades encontradas, asimismo se debe indicar que equipos tienen vulnerabilidad y cuales no, se debe hacer la entregar de un informe técnico, dirigido al personal TI detallando la cantidad de vulnerabilidades encontradas, números de equipos comprometidos, facilidad de explotación, indicando el nivel del riesgo y consecuencias para la organización, para finalizar brindar recomendaciones para lograr mitigar las vulnerabilidades.

2.2.2.3 Tipos de Pentest

El tipo de pentest que se desea aplicar en una compañía se determinan de acuerdo con la cantidad de información que se tiene y considerando las condiciones en que está y del tipo de información que se obtiene del objetivo a estudiar. (Romero, 2013)

- **Caja blanca:** Una de las pruebas más completas, la empresa suministra toda la información posible como, por ejemplo: cantidad de equipos, tipos de sistemas, estructura de la red, servidores, contraseñas, código fuente, documentación, entre otros, se usa con el objetivo de identificar vulnerabilidades potenciales.

  Esta prueba se basa en detectar vulnerabilidades en el sistema, así como sus códigos fuentes y configuraciones. Algunas de las técnicas mayormente usadas son: vulnerabilidades de calidad del código, vulnerabilidades de los protocolos, vulnerabilidades criptográficas y vulnerabilidades en la gestión de contraseñas.

- **Caja negra:** En este tipo de pruebas no se tiene información de los sistemas de la infraestructura, redes, software, contraseñas, entre otro, esta prueba se asemeja más a la realidad en la que se encuentran para con los atacantes y sirve para verificar el nivel de seguridad de los equipos tecnológicos.

  Una de las desventajas es la dificultad que se tienen para obtener información, se pueden pasar por desapercibidas puertas traseras o vulnerabilidades parciales. Las pruebas más comunes realizadas son, pruebas de penetración de infraestructura, penetración a aplicaciones y un ataque simulado completo utilizando tales como vulnerabilidades de tipo cross-site scripting, vulnerabilidades inyección de SQL, vulnerabilidades de desbordamiento de memoria, autenticación incompleta, entre otras.

- **Caja gris:** Es una mezcla de la caja blanca y caja gris, es decir que se tiene cierta información para realizar estas pruebas. Se usa generalmente cuando se desea identificar vulnerabilidades en puntos específicos debido a que es más rentable y nos proporciona una apreciación más real de amenazas. Las pruebas realizadas estaría la aplicación de pentesting y test de infraestructura.

2.2.2.4 Herramientas del Pentesting

VMware y Kali Linux: Las máquinas virtuales son algunas opciones que nos permiten crear un entorno de pruebas, normalmente las máquinas virtuales se usan en servidores para mantener software antiguo, así también ejecutar aplicaciones en un sistema operativo diferente al del origen. Algunas máquinas virtuales con mayor uso son VMWare Workstation, Virtual Box de Oracle y Hyper-V de Microsoft.

Por otro lado, tenemos el sistema operativo Kali Linux el cual posee herramientas orientadas a Pentesting, incluyendo aplicaciones como: Aircrak-ng, Burpsuite, Hydra, John, Maltego, Metasploit Framework, Nmap, OWASP-Zap y Wireshark, entre otros y si se requiere utilizar otras herramientas solo hay que instalar. El sistema operativo Kali Linux está basado en Debian GNU/Linux Este sistema está orientado a seguridad informática.

2.3 Definición de términos

2.3.1 Vulnerabilidad

La vulnerabilidad se define como una debilidad del sistema informático que puede ser aprovechada con el fin de causar daño. (Avenía, 2017, p. 12) Todo sistema informático corre el riesgo de estas debilidades pueden presentarse en cualquiera de los activos y su consecuencia son los impactos como efectos nocivos de un evento.

2.3.2 Exploit

Se define como una secuencia de comandos utilizados para identificar las vulnerabilidades en un sistema, con el fin de provocar un comportamiento no deseado (Incibe, 2017)

2.3.3 Ciberseguridad

Es el área relacionada con la informática la cual está encargada de la protección de activos digitales. (ISACA, 2015) ciberseguridad consiste en proteger los activos de información, mediante un control de las amenazas que ponen en riesgo la información que es gestionada por los sistemas de información (ISACA, 2015, p. 20)

2.3.4 Pentesting

Una prueba de pentest consiste en realizar un ataque simulado, controlado y autorizado contra un sistema informático con el fin de identificar vulnerabilidades, analizarlas y de ese modo poder evaluar la seguridad del sistema. Durante la simulación, se detectan las vulnerabilidades existentes en el sistema seguidamente se procede a explótalas tal cual lo haría un atacante cibernético. Esto tiene como objetivo evaluar riesgos en la organización basándose en los resultados de las pruebas realizadas y finalmente sugerir un plan de medida s correctivas a tomar (Guillen, 2017,p 5)

2.3.5 Hardware

Considera que hardware es un término usado por la informática para hacer referencia a los equipos físicos tecnológicos, también se considera como hardware las partes y los accesorios tales como los periféricos, discos, memorias. (Guevara, 2006, p 121)

2.3.6 Software

(Guevara, 2006, 122) lo define como un conjunto de programas que brindan instrucciones para que el hardware ejecute tareas, ya sea realizando cálculos, escribir textos jugar, crear simulaciones entre otros, por su parte (Garrido, 2006, p2) señala que el software es la parte lógica, al conjunto de programas y por lo tanto intangible al sistema.

2.3.7 Mitigar

Consiste en tomar un conjunto de medidas con el objetivo de disminuir la probabilidad de que una vulnerabilidad se pueda explotar, es decir implementar algún control que reduzca el riesgo.

2.3.8 Riesgo

Es la posibilidad de explotar una vulnerabilidad con el objetivo de causar daño o perdida de información, es decir un problema no es más que la posibilidad de que una amenaza se convierta en un evento real.

2.3.9 Amenaza

Es toda aquella acción que aprovecha de una vulnerabilidad con el objetivo de invadir un sistema informático, es decir consiste en la posibilidad de sufrir un ataque que tiene como resultado un impacto no deseado en un sistema.

2.3.10 Confidencialidad

Hace referencia a que la información debe ser protegida con el fin de que no sea divulgada.

La confidencialidad trata de que la información no sea revelada a usuarios no autorizados. Los atacantes tendrían acceso a la información con el objetivo de robo de contraseñas, romper sistemas de encriptación y utilizar la ingeniería social para poder obtener dicha información. (Cortes, 2016 p.1)

2.3.11 Integridad

Consiste en prevenir modificaciones no autorizadas, es decir solo podrá ser modificada por el personal autorizado, su aplicación permite mantener la información inalterada.

La integridad consiste en que la información será la misma desde su origen hasta que el cliente haga uso de la información sin alteraciones. Por lo tanto, no se manipulará en ningún instante de la transacción Cliente- Servidor. La integridad estará en riesgo a causa de los errores humanos, accidentales o intencionales (Cortes, 2016, p.1).

2.3.12 Disponibilidad

Es la capacidad de asegurar que el acceso a la información esté disponible en cualquier momento que el usuario que lo solicite. En este punto se debe asegurar que los usuarios autorizados puedan acceder a tiempo a sus recursos. Los router, DNS, Firewall, IDS, DHCP, Servidores, software son algunos dispositivos que están disponibles para el acceso de la información (Cortes,2016, p.1).

2.4 Hipótesis

2.4.1 Hipótesis general:

Existe una relación directa y significativa entre la aplicación del pentesting y la seguridad informática en los equipos tecnológicos en la Universidad Nacional Santiago Antúnez de Mayolo

2.4.2 Hipótesis especificas:

- Existe una relación directa entre la aplicación de pentesting y la confidencialidad en la seguridad informática de los equipos tecnológicos de la institución.

- Existe una relación directa entre la aplicación de pentesting y la integridad en la seguridad informática de los equipos tecnológicos de la institución.

- Existe una relación directa entre la aplicación de pentesting y la disponibilidad en la seguridad informática de los equipos tecnológicos de la institución.

2.5 Variables:

2.5.1 Variable Independiente

(Pérez, 2007) En su investigación acerca de las variables en el método científico define a la variable independiente como el motivo, o explicación de ocurrencia de otro fenómeno. Es el tipo de variable que el investigador puede manipular.

En el presente estudio la variable independiente será: aplicación del pentesting.

2.5.2 Variable dependiente

(Pérez, 2007) lo define como el fenómeno resultante, es el tipo de variable que debe explicarse. En el presente estudio la variable dependiente será: Seguridad informática

2.5.3 Operacionalización de variables:

PROBLEMA	OBJETIVO	HIPOTESIS	VARIABLES	METODOLIA
	General			**Tipo de investigación:** • **Según la intervención**: Observacional • **Según la planificación:** Prospectivo • **Según que mide**: Transversal **Nivel de investigación:** • Correlacional **Diseño de investigación:** • No experimental **Población** • Para el presente estudio se tomó como población a los trabajadores encargados de brindar soporte tecnológico a los equipos tecnológicos las cuales lo conforman 20 personas que laboran en la UNASAM.
¿De qué manera se relaciona la aplicación de pentesting con la seguridad informática en los equipos tecnológicos de la Universidad Nacional Santiago Antúnez de Mayolo?	Determinar la relación entre la aplicación del pentesting y la seguridad informática en los equipos tecnológicos en la Universidad Nacional Santiago Antúnez de Mayolo.	Existe una relación directa y significativa entre la aplicación del pentesting y la seguridad informática en los equipos tecnológicos en la Universidad Nacional Santiago Antúnez de Mayolo.	**Variable Independiente:** Aplicación de pentesting	
	Específicos			
¿Es posible identificar la relación entre la aplicación de pentesting y la confidencialidad en seguridad informática de los equipos tecnológicos de la institución?	Identificar la relación entre la aplicación de pentesting y la confidencialidad en seguridad informática de los equipos tecnológicos de la institución.	Existe una relación directa entre la aplicación de pentesting y la confidencialidad en seguridad informática de los equipos tecnológicos de la institución.	**Variable Dependiente:** Seguridad informática	
¿Es posible conocer la relación entre la aplicación de pentesting y la integridad en seguridad informática de los equipos tecnológicos de la institución?	Conocer la relación entre la aplicación de pentesting y la integridad en seguridad informática de los equipos tecnológicos de la institución.	Existe una relación directa entre la aplicación de pentesting y la integridad en seguridad informática de los equipos tecnológicos de la institución.		

¿Es posible analizar la relación entre la aplicación de pentesting y la disponibilidad en seguridad informática de los equipos tecnológicos de la institución?	Analizar la relación entre la aplicación de pentesting y la disponibilidad en seguridad informática de los equipos tecnológicos de la institución.	Existe una relación directa entre la aplicación de pentesting y la disponibilidad en la seguridad informática de los equipos tecnológicos de la institución.	**muestra:** • El tipo de muestra es poblacional, todos los encargados de brindar soporte técnico y jefe de la OGTISE. **Instrumento de recolección de datos:** • Para ambas variables se usará un cuestionario estructurado y entrevista

VARIABLE	DEFINICION CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIONES	INDICADORES	ITEM
			Recolección de información	Cantidad de información.	P01 y P02 – Encuesta 1
				Cantidad de objetivos	P03 y P04 – Encuesta 1
VARIABLE INDEPENDIENTE Aplicación de pentesting	(Guillen, 2017, p 5) Define al pentest como un ataque simulado y autorizado contra un sistema informático con el principal objetico de evaluar la seguridad del sistema.	Aplicar el pentesting para identificar vulnerabilidades y relacionarla con la seguridad informativa para ver cómo es su comportamiento cuando crecen o disminuyen las vulnerabilidades.		Cantidad de vulnerabilidades	P05 y P06 – Encuesta 1
			Análisis de vulnerabilidad	Cantidad de equipos vulnerables	P07, P08 y P09 – Encuesta 1
	(Gómez, 2006) define a la seguridad informática como una acción que impida la ejecución de operaciones	La confidencialidad, la integridad y la disponibilidad de la información son los tres pilares fundamentales que	Confidencialidad	Confidencialidad	P10,P11 y P12 – Encuesta 1

VARIABLE DEPENDIENTE Seguridad informática	no autorizadas sobre un sistema, cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, integridad y disponibilidad.	se debe proteger en la universidad para el funcionamiento correcto de los diferentes procesos y servicios que brinda la institución.	Integridad	Integridad	P13, P14 y P15– Encuesta 1
			Disponibilidad	Disponibilidad	P16 y P17 – Encuesta 1

METODOLOGÍA

3.1 Tipo de estudio

De acuerdo con su enfoque: la presente investigación la cual lleva por título aplicación de pentesting y la seguridad informática en la Universidad Nacional Santiago Antúnez de Mayolo, se utilizó el enfoque Cuantitativo, según la investigación realizada por Tamayo (2007) menciona que dicho enfoque consiste en el contraste de teorías ya existentes partiendo de sucesión de hipótesis surgidas de la misma por ello es necesario obtener una muestra representativa del objeto de estudio.

En el presente proyecto se hará uso de la técnica de recolección de datos mediante el cual se podrá identificar el fenómeno de estudio, detectar vulnerabilidad y proponer soluciones para mitigar dichos riesgos asimismo nos permitirá probar la hipótesis.

De acuerdo con su nivel: En el presente estudio es de nivel correlacional Salkind (1999, p.223) menciona que la investigación correlacional describe la relación existente entre dos o más variables. Como técnica descriptiva, la investigación correlacional es muy potente porque indica si existe relación entre las variables o identificar si poseen algo en común.

En el presente estudio se identifica una muestra y se tiene dos variables las cuales son necesarias para identificar las vulnerabilidades, medir el nivel de riesgo y evaluar en qué medida afecta a la seguridad informática de la Universidad, posteriormente proponer acciones correctivas con el objetivo de minimizar los riesgos.

Según la intervención: Es observacional (Grimes et al.,2002) definen a partir de la ausencia de intervención del investigador en el desenlace que desea evaluar, en nuestra investigación se busca describir la relación entre la aplicación del pentesting y la seguridad informática en la entidad posterior a la detección y posibles soluciones a las vulnerabilidades encontradas sin intervenir en las variables.

Según la planificación: Es prospectivo ya que según (Corona y Fonseca, 2021, p.339) indican que un estudio de casos y controles será prospectivo si el desenlace que establece corresponde al grupo de los casos o al de los controles. En la presente investigación se va a realizar el pentesting con el fin de detectar las vulnerabilidades y medir el nivel de seguridad informática de la entidad.

Según que mide: Es transversal (Hulley et al.,2013) define a un estudio transversal es la evaluación de un momento específico y determinado de tiempo, en contraposición a los estudios longitudinales que involucran el seguimiento en el tiempo. En el proyecto será un diseño no experimental debido a que se aplicará la encuesta en una sola ocasión y según la variable de interés será analítica.

3.2 El diseño de investigación

En la presente investigación se aplicó el estudio de diseño no experimental debido a no se tocó las variables que se tiene, asimismo solo se tiene una sola muestra, se identificó vulnerabilidades al que se encuentra expuesta la entidad, seguidamente se generó un informe con las acciones correctivas y se determinó la relación con la seguridad informática de la Universidad Nacional Santiago Antúnez de Mayolo.

3.3 Descripción de la unidad de análisis, población y muestra

3.3.1 Población

Para el presente estudio se tomó como población a los trabajadores encargados de brindar soporte tecnológico a los equipos tecnológicos los cuales se identificó a 20 personas que laboran en la Universidad Nacional Santiago Antúnez de Mayolo, del Distrito de Independencia, Huaraz – Ancash.

3.3.2 Muestra

En el presente proyecto de tesis, para fijar la muestra se empleó el muestreo no probabilístico el cual según (Cuesta, 2009) define al muestreo no probabilístico como la capacidad de muestreo en la que las muestras se recolectan en un proceso que no brinda a todos los individuos de la población la misma oportunidad de ser seleccionados.

En el presente proyecto se tomó como muestra áreas específicas y funcionales de la Universidad Nacional Santiago Antúnez de Mayolo.

Se considero elegir a los sujetos aplicando el muestreo no probabilístico por conveniencia debido a que la muestra fue seleccionada en función a la accesibilidad y a juicio personal del investigador.

Figura 7
Ejemplo demuestra

La cantidad de personal involucrado se puntualiza en la siguiente tabla:

Por su parte Hernández citado en Castro (2003), menciona que "si la población es menor a cincuenta (50) sujetos, la población es igual a la muestra" (p.69), por lo tanto, la muestra será de 20 trabajadores. En esta investigación se aplicó el muestreo por conveniencia del investigador, ya que es una técnica de muestreo no probabilístico y no aleatorio que nos brinda la facilidad de crear muestras de acuerdo al acceso que se tiene.

Tabla 6

Muestra identificada

Áreas	Total
Oficina General de Tecnologías de Información, Sistemas y Estadística	5
Encargados de centro de computo	14
Otras áreas	1
TOTAL	**20**

Nota: lista de encargados de dar soporte a los equipos tecnológicos

3.4 Técnicas de instrumentos de recolección de datos

3.4.1 Técnicas

En el presente se hace mención las técnicas utilizadas como instrumento de recopilación de recolección de datos para el desarrollo de la presente investigación:

- Encuesta dirigida a un conjunto de personas específicas las cuales manejan la información detallada para la investigación para lo cual se elaboró un cuestionario de preguntas.

- Entrevista dirigida a unas personas específicas que manejan la información mucho más detallada para lo cual se elaboró un conjunto de preguntas.
- Análisis de las observaciones realizadas en el proceso de recopilar información.
- Análisis de documentos, tales como libros, revistas, tesis que se emplean para el desarrollo de la presente investigación.
- Se utilizó la infometría debido a que para la investigación se hizo la búsqueda de información en base de datos, archivo digitales y web.

3.4.2 Instrumento

En el presente se mencionará a los instrumentos de recolección de datos que se aplicará al personal seleccionado de la Universidad Nacional Santiago Antúnez de Mayolo:

- **Cuestionario:** El cuestionario nos permite la recolección de información y (Garcia, 2022) lo define como un sistema coherente y ordenado de preguntas con un significado lógico, se expresa en un lenguaje sencillo y claro.

En el proyecto se realiza una serie de cuestionarios con el fin de recoger información acerca del nivel de conocimiento sobre la aplicación de pentesting y seguridad informática en la Universidad Santiago Antúnez de Mayolo.

- **Observación directa:** En el presente estudio se utilizará la técnica de observación directa debido a que se aplicará cuestionarios, asimismo se observará la conducta y proceder de los trabajadores encargados de los equipos informáticos.

3.5 Técnicas de análisis y prueba de hipótesis

Para realizar el análisis de datos se utiliza técnicas de análisis documentarios de fuentes primarias las cuales son tesis, revistas, publicaciones, guías, tesis y entre otros. Para los análisis de los datos se utilizó la validación de juicios de expertos.

Se proceso la información obtenida mediante técnicas estadísticas y teorías en la que es imprescindible el uso y soporte de las herramientas informáticas como hojas de cálculo para procesar los resultados obtenidos.

Para la prueba de hipótesis se utiliza el coeficiente de Cronbach fue descrito en 1951 por Lee J. Cronbach (15). Es un índice usado para medir la confiabilidad del tipo consistencia interna de una escala, es decir, para evaluar la magnitud en que los ítems de un instrumento están correlacionados

Tabla 7

Clasificación de los niveles de fiabilidad

Índice	Nivel de fiabilidad	Valor de Alfa de Cronbach
1	Excelente	[0.9, 1]
2	Muy bueno	[0.7, 0.9]
3	Bueno	[0.5, 0.7]
4	Regular	[0.3, 0.5]
5	Deficiente	[0, 0.3]

RESULTADOS DE LA INVESTIGACIÓN

4.1 Descripción del trabajo de campo

En el presente apartado del proyecto se describe todo el trabajo de campo que se realizó hasta la obtención de los resultados de la investigación realizada.

4.1.1 Análisis de la situación actual

4.1.1.1 Análisis del área de trabajo

La Universidad Nacional Santiago Antúnez de Mayolo cuenta con una Oficina General de Tecnologías de Información, Sistemas y Estadística el cual es la encargada de desarrollar y mantener el buen funcionamiento del sistema informático de la Unasam administrando servidores, switches, ordenadores, aplicativos webs, etc.

De la misma manera la Universidad Nacional Santiago Antúnez de Mayolo cuenta con encargados de centros de cómputos en las 11 facultades teniendo como funciones principales dar soporte a los usuarios y velar por el correcto funcionamiento de los equipos informáticos que tienen a su cargo.

También se cuenta con personal de imagen institucional las cuales se encargan de publicar información en el portal web de la institución, asi como otras áreas que cuentan con su propio personal de soporte técnico a equipos informáticos.

Para la presente investigación se consideró a todos los personales que manejan equipos tecnológicos encargados de los centros de cómputo de las facultades, el personal de la OGTISE, personal del centro de idiomas y asistentes de informática todos ellos haciendo un total de 20.

Figura 8

Áreas centros de computo

Nota. elaboración propia.

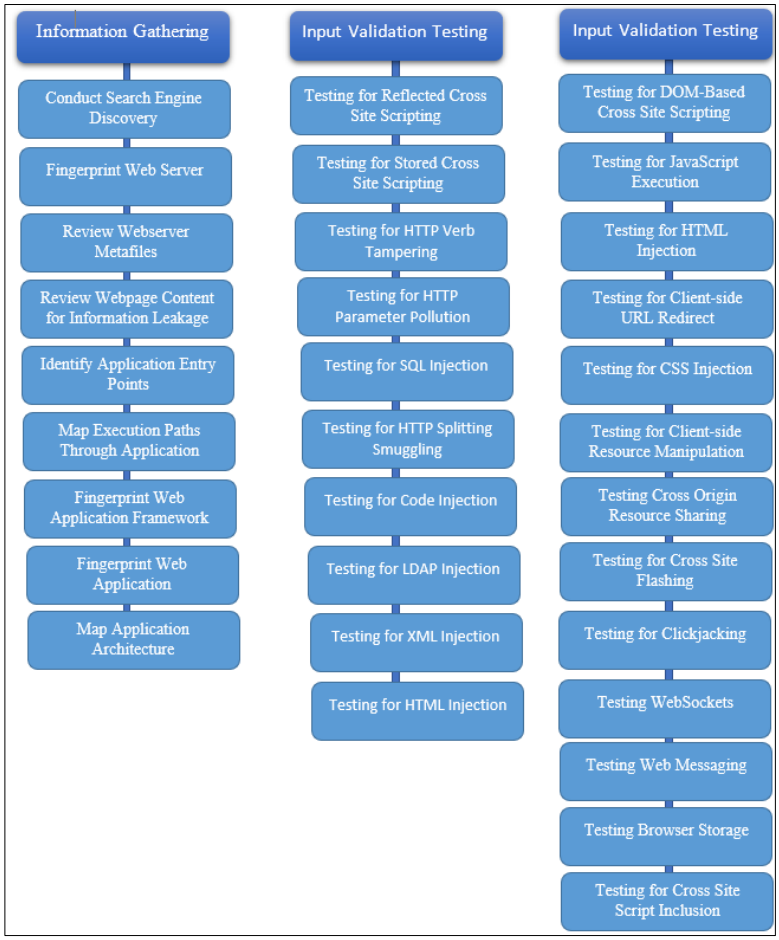
4.1.1.2 Ambiente del pentesting

Kali Linux es el sistema operativo que se utiliza para realizar las diferentes pruebas ya que está perfectamente diseñada para las necesidades profesionales en pruebas de penetración o intrusión. Se hace uso de dicho software debido a que cumple con todas las características para el desarrollo del proyecto; se cuenta con más de 600 herramientas para las pruebas de penetración, es de libre acceso, cuenta con amplio soporte, es seguro y soporta múltiplos lenguajes.

En la presente investigación se utilizó herramientas de OWASP ya que es de código abierto que se dedica a detectar y combatir las causas que hacen que un ambiente sea no seguro. En el presente proyecto se hace uso de las metodologías de Pruebas de seguridad de aplicaciones web, tales como recopilación de información, pruebas de validación de entrada y pruebas del lado del cliente. Como se muestra en la siguiente figura:

Figura 9

Herramientas OWASP



Nota. Fuente: Basado en la Metodología OWASP

4.1.2 Information Gathering

Las pruebas se realizaron las pruebas utilizando el pentesting Kali Linux en Vmware a dos aplicativos webs desarrollados por la Universidad Nacional Santiago Antúnez de Mayolo.

Los aplicativos webs dónde realizamos las pruebas son las siguientes:

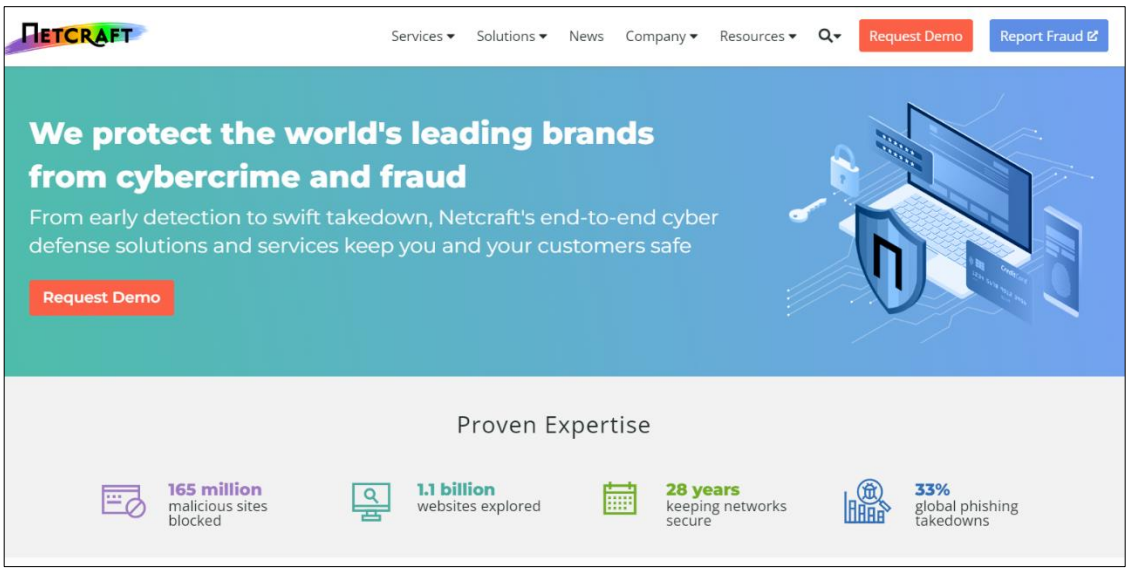
- Url 1: https://www.unasam.edu.pe/ (Portal Web)
- Url 2: http://sga.unasam.edu.pe/(SISTEMA DE GESTIÓN ACADÉMICA)

4.1.2.1 PRUEBA 1: FINGERPRINT WEB SERVER

Para realizar esta prueba se utilizó la herramienta NetCraft, que nos permitió analizar la cuota de mercado de servidores, alojamiento web e incluye la detección del tipo de servidor web y de sistema operativo. Esta herramienta es libre, como requisito es contar con un navegador web, en el buscador se ingresa al siguiente enlace: https://www.netcraft.com/ y seguidamente se ingresa la URL que se desea analizar en el buscador de NetCraft.

Figura 10

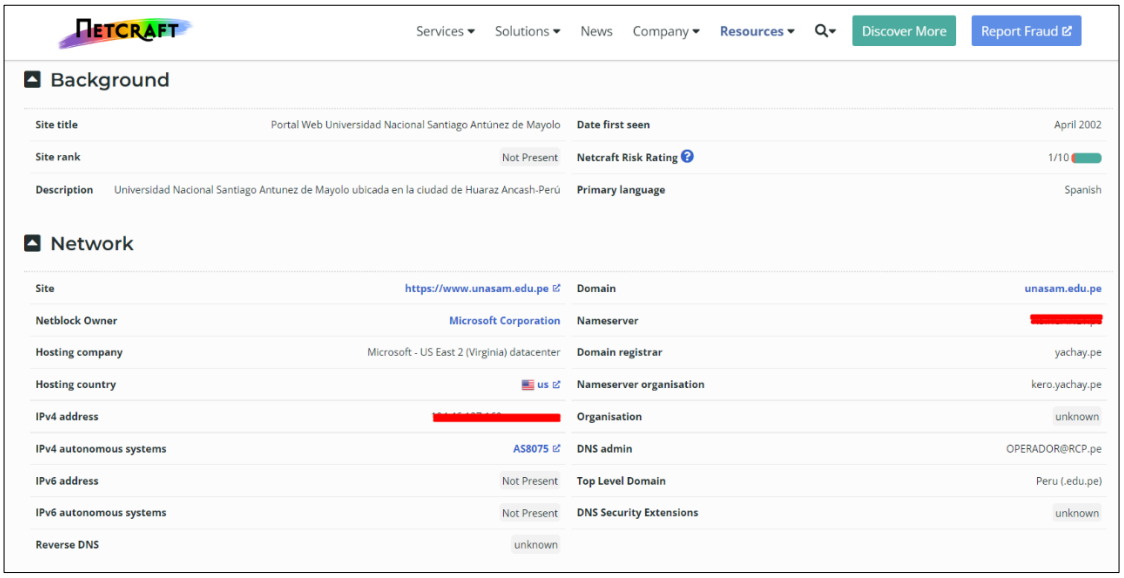
Pagina NetCraft



Pagina 1: https://www.unasam.edu.pe/

Figura 11

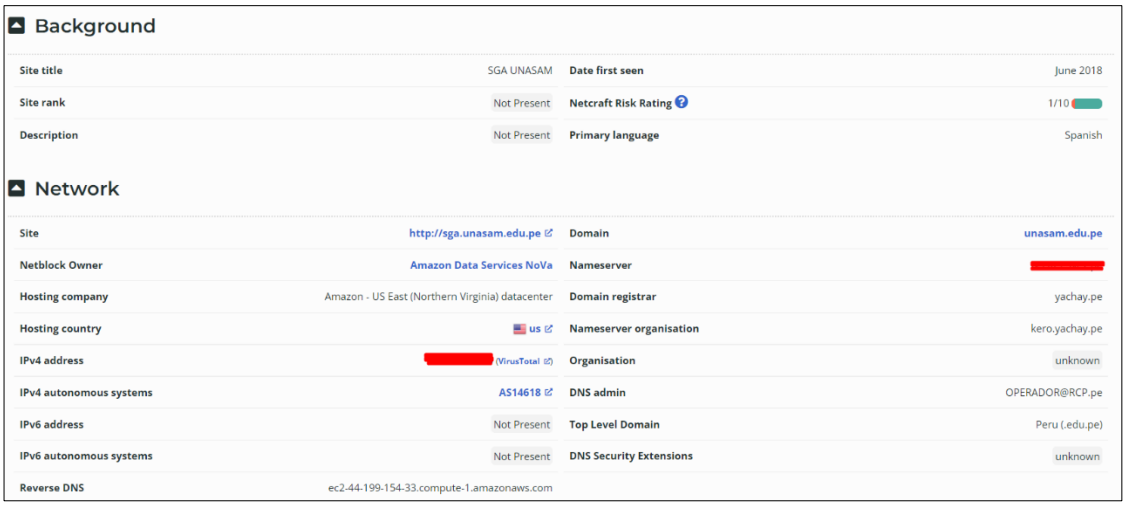
Análisis de la página1 en NetCraft



Pagina 2: http://sga.unasam.edu.pe/

Figura 12

Análisis de la página 2 en NetCraft



Resultado de las pruebas:

Tabla 8

Resultados de las pruebas en NetCraft

URL	Nombre	Resultados
https://www.unasam.edu.pe/	Propietario de bloque de red	Microsoft Corporation
	Compañía de hosting	Microsoft - US East 2 (Virginia) datacenter
	IPv4 address	[redacted]
	Nombre del servidor	[redacted]pe
	Domain	unasam.edu.pe
	OS	Linux
	Servidor Web	Apache
http://sga.unasam.edu.pe/	Propietario de bloque de red	Amazon Data Services NoVa
	Compañía de hosting	Amazon - US East (Northern Virginia) datacenter
	IPv4 address	[redacted]
	Nombre del servidor	[redacted]
	Domain	unasam.edu.pe
	OS	Linux
	Servidor Web	nginx/1.9.3 Ubuntu

4.1.2.2 PRUEBA 2: REVIEW WEBSERVER METAFILES FOR INFORMATION LEAKAGE

Para realizar esta prueba se utilizó la herramienta Whois IP, esta herramienta es libre, que nos permite detectar fugas de información de la aplicación web. Como requisito es contar con un navegador web, en el buscador de Google se ingresa al siguiente enlace: https://whois.domaintools.com/ y seguidamente se ingresa la URL a analizar en el buscador de Whois ip.

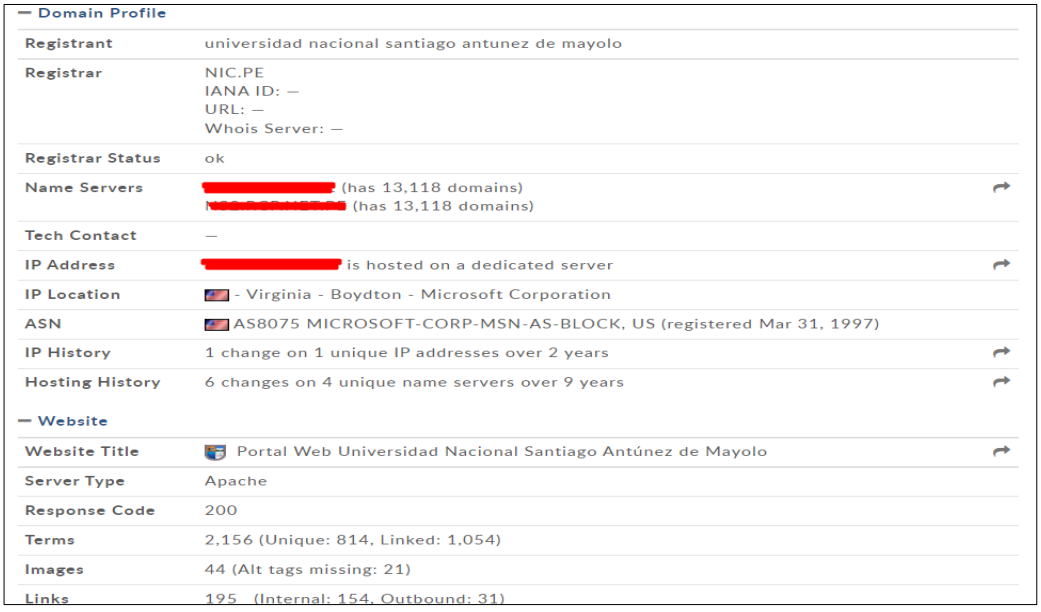
Figura 13

Página de inicio de Whois Lookup

Pagina 1: https://www.unasam.edu.pe/

Figura 14

Información Whois Lookup, página 1



Domain Profile	
Registrant	universidad nacional santiago antunez de mayolo
Registrar	NIC.PE IANA ID: – URL: – Whois Server: –
Registrar Status	ok
Name Servers	[redacted] (has 13,118 domains) [redacted] (has 13,118 domains)
Tech Contact	–
IP Address	[redacted] is hosted on a dedicated server
IP Location	- Virginia - Boydton - Microsoft Corporation
ASN	AS8075 MICROSOFT-CORP-MSN-AS-BLOCK, US (registered Mar 31, 1997)
IP History	1 change on 1 unique IP addresses over 2 years
Hosting History	6 changes on 4 unique name servers over 9 years
Website	
Website Title	Portal Web Universidad Nacional Santiago Antúnez de Mayolo
Server Type	Apache
Response Code	200
Terms	2,156 (Unique: 814, Linked: 1,054)
Images	44 (Alt tags missing: 21)
Links	195 (Internal: 154, Outbound: 31)

Resultados obtenidos:

Tabla 9

Resultados de búsqueda whois ip

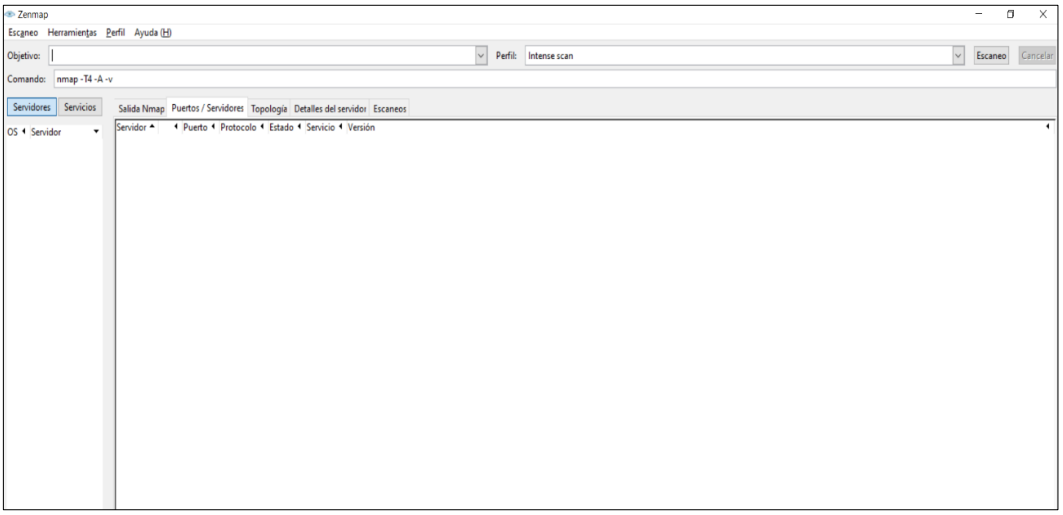
URL	Nombre	Resultados
https://www.unasam.edu.pe/	IP Location	Microsoft Corporation
	Compañía de hosting	Microsoft - US East 2 (Virginia) datacenter
	IPv4 address	[redacted]
	Nombre del servidor	[redacted]
	Domain	unasam.edu.pe
	Servidor Web	Apache

4.1.2.3 PRUEBA 3: ENUMERATE APPLICATIONS ON WEBSERVER

Para realizar esta prueba se utilizó la herramienta Zenmap para averiguar las aplicaciones instaladas en el servidor de la organización, esta herramienta es gratuita en el cual realizamos un escaneo múltiple a dominios específicos el cual nos permite conocer su topología, puertos y servidores. Como requisito es contar con un navegador web, sistema operativo Windows o Linux en el que se instala en Nmap en el cual se ingresa el dominio o la IP.

Figura 15

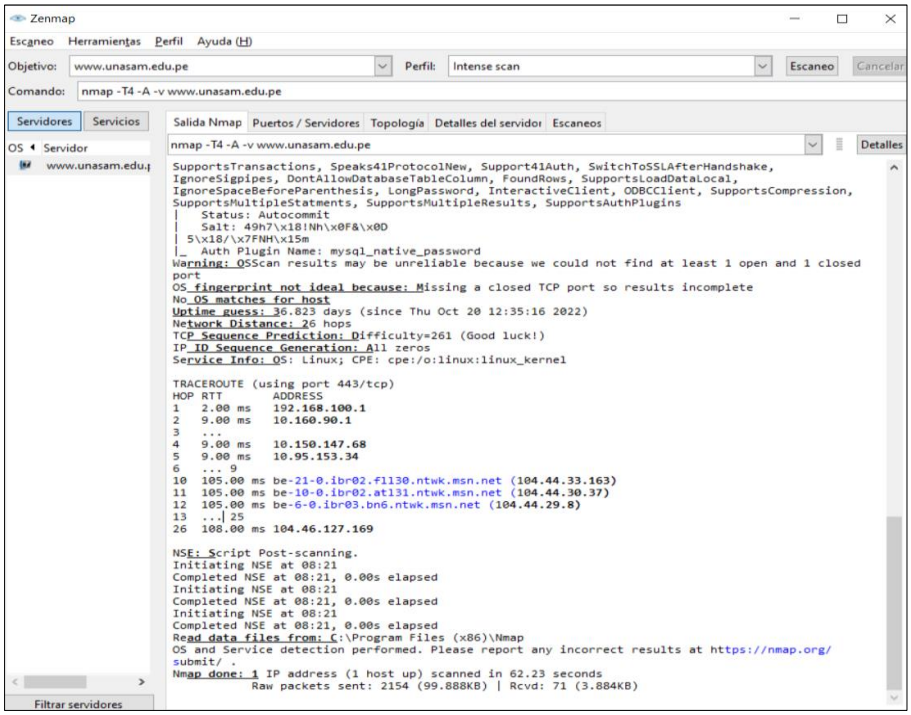
Inicio de la herramienta Zenmap



Pagina 1: https://www.unasam.edu.pe/

Figura 16

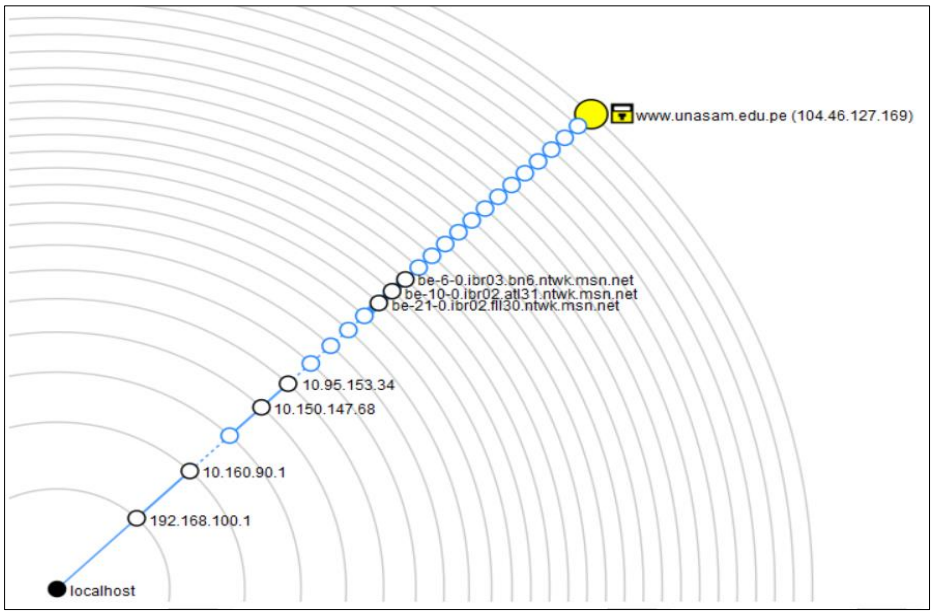
NMAP Escaneo sobre la página1.



Topología red

Figura 17

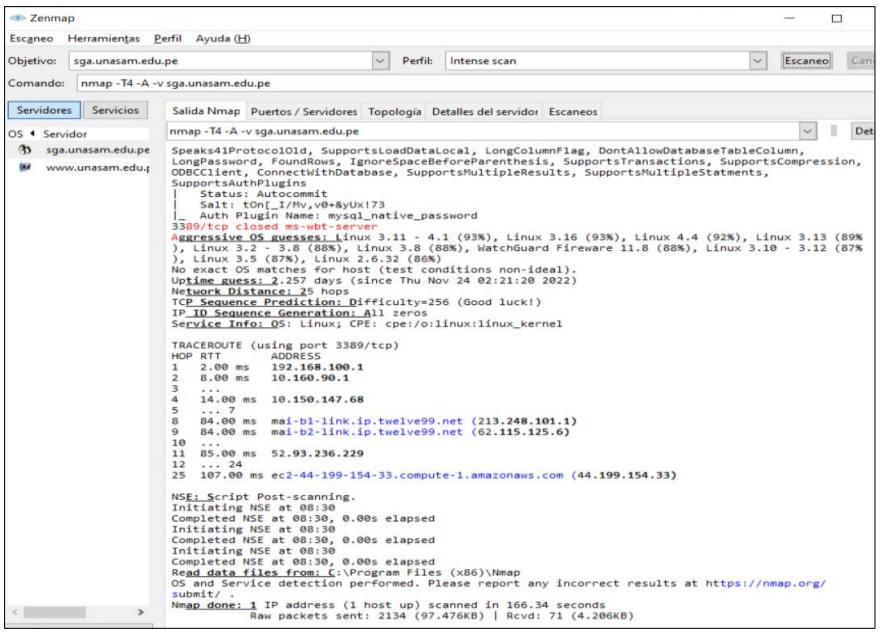
NMAP topología de saltos pagina 1.



Pagina 2: http://sga.unasam.edu.pe/

Figura 18

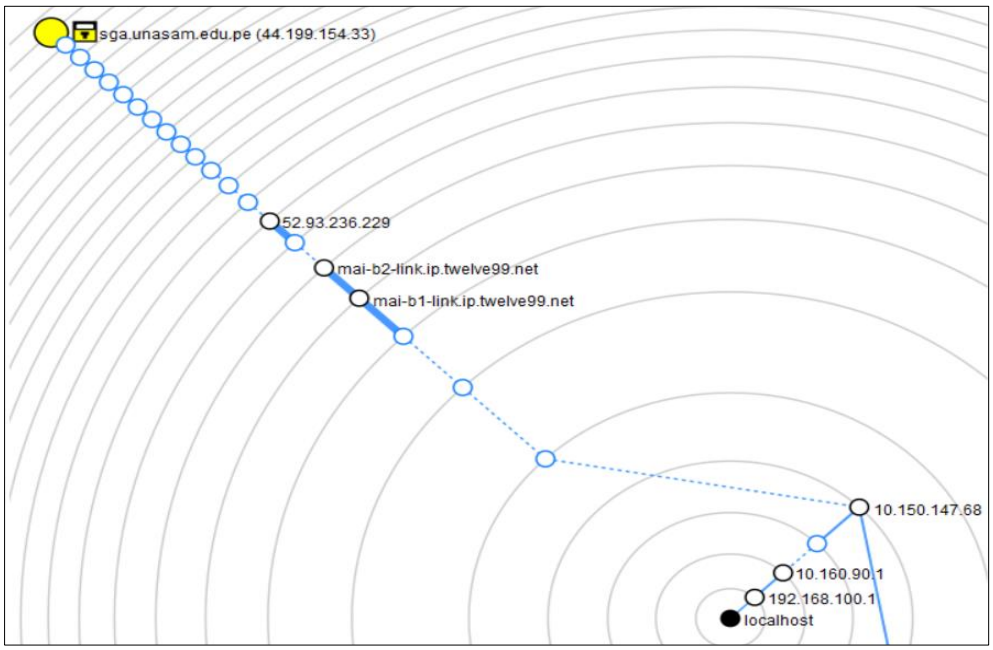
NMAP Escaneo sobre la página2.



Topología red

Figura 19

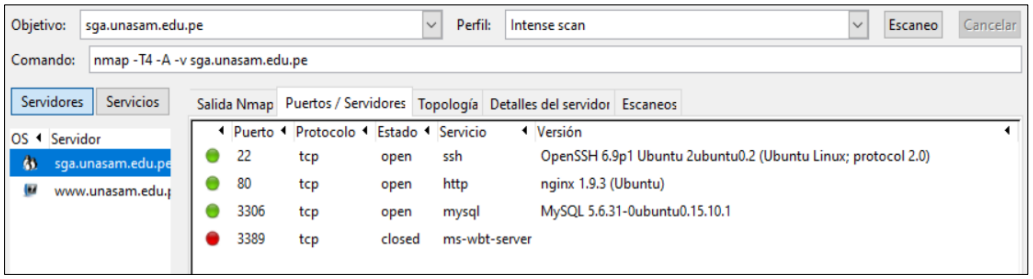
topología de saltos pagina2



Como resultado del escaneo se identificó lo siguiente:

Figura 20

Resultado de puertos abiertos.



Como se muestra en la figura se tiene abiertos los siguientes puertos:

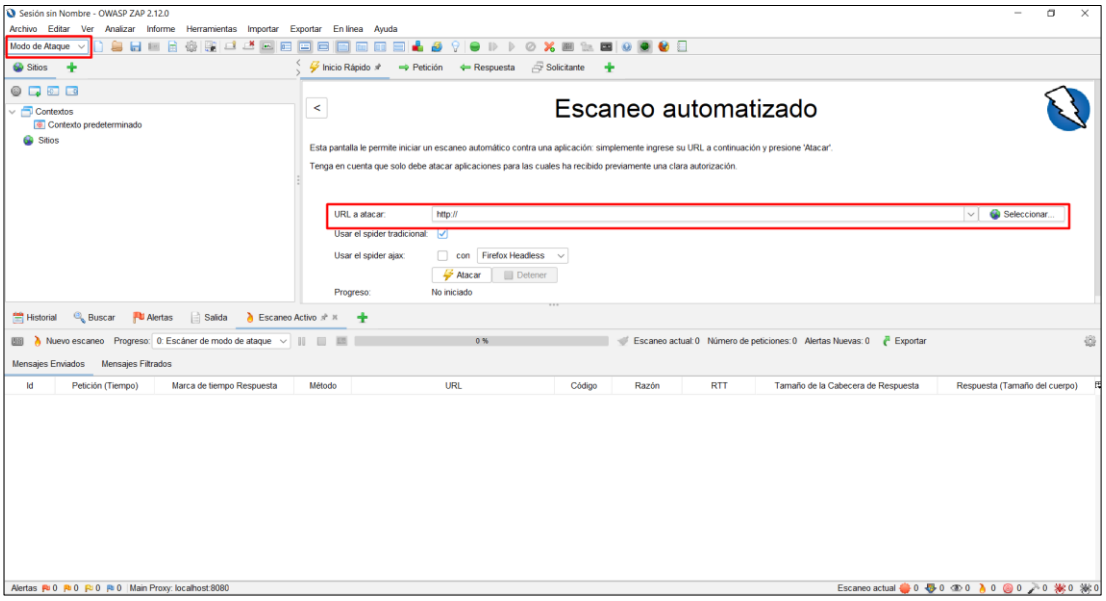
- Puerto 22 de servicio ssh y versión OpenSSH 6.9 ubuntu
- Puerto 80 servicio http y versión nginx
- Puerto 3306 servicio mysql y versión

4.1.2.4 PRUEBA 4: REVIEW WEBPAGE CONTENT FOR INFORMATION LEAKAGE

Para realizar esta prueba se utilizó la herramienta OWASP ZAP que es una herramienta para búsqueda de metadatos, código fuente en aplicaciones web, es una herramienta libre que se puede ejecutar en sistemas operativos Windows, Linux y mac. En la siguiente imagen se muestra la forma de realizar la prueba:

Figura 21

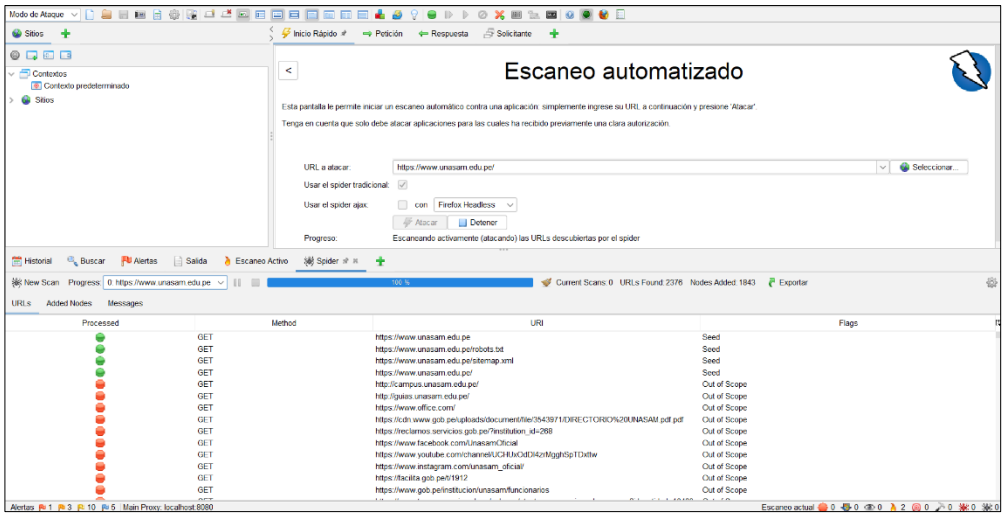
Pagina incial Zap



Pagina 1: https://www.unasam.edu.pe/

Figura 22

OWASP Zed Attack Proxy, pagina1



Como acciones adicionales se revisó el log y los falsos positivos, obteniendo como resultado:

- **Alerta: Missing Anti-clickjacking Header**(Falta el encabezado antisecuestro de clics)
- Riesgo: medio

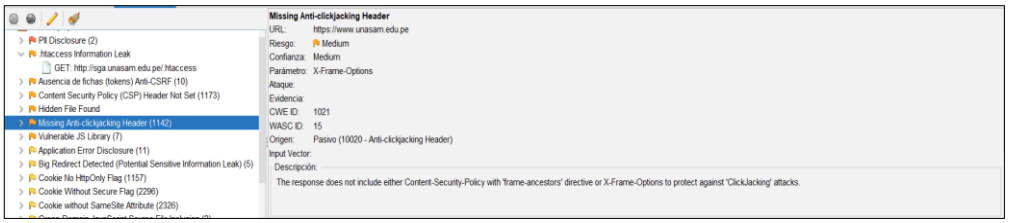
- Descripción alerta: Los navegadores web modernos admiten los encabezados HTTP Content-Security-Policy y X-Frame-Options. Asegúrese de que uno de ellos esté configurado en todas las páginas web devueltas por su sitio/aplicación.

  Si espera que la página esté enmarcada solo por páginas en su servidor (por ejemplo, es parte de un FRAMESET), querrá usar SAMEORIGIN; de lo contrario, si nunca espera que la página esté enmarcada, debe usar DENY. Alternativamente, considere implementar la directiva "frame-ancestros" de la política de seguridad de contenido.

- se encontró: Que la respuesta no incluye Content-Security-Policy con la directiva 'frame-ancestors' ni X-Frame-Options para proteger contra los ataques de 'ClickJacking' que consite en maliciosa para engañar a usuarios de Internet con el fin de que revelen información confidencial o tomar control de su ordenador cuando hacen clic en páginas web aparentemente inocentes (la alerta corresponde a un error de configuración de seguridad top 5 de las riesgos de seguridad más importantes en aplicaciones web según la Fundación OWASP)

Figura 23

Missing Anti-clickjacking Header, pagina1



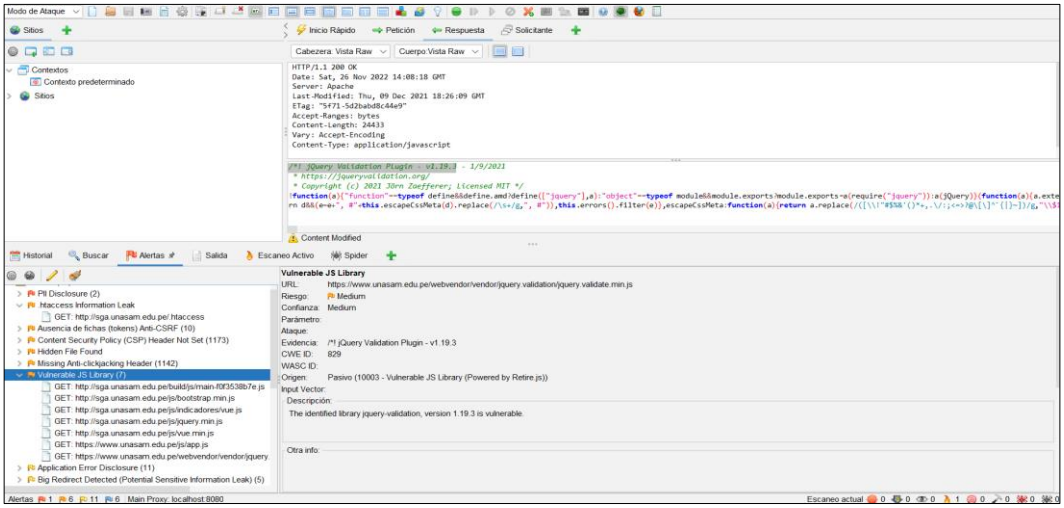
- **Alerta: Vulnerable JS Library**
- **Riesgo:** Medio

- **Descripción de la alerta:** jquery-validation, versión 1.19.3 es vulnerable debido a que la entidad podría sufrir un ataque de denegación de servicio de expresiones regulares (ReDoS), se recomienda Actualizar jquery-validationa la versión 1.19.5 o superior.

- **Se encontró:** La biblioteca identificada jquery-validation, versión 1.19.3 es vulnerable. (la alerta corresponde a una vulnerdabilidad de Componentes vulnerables y obsoletos top 6 de los riesgos de seguridad más importantes en aplicaciones web según la Fundación OWASP)

Figura 24

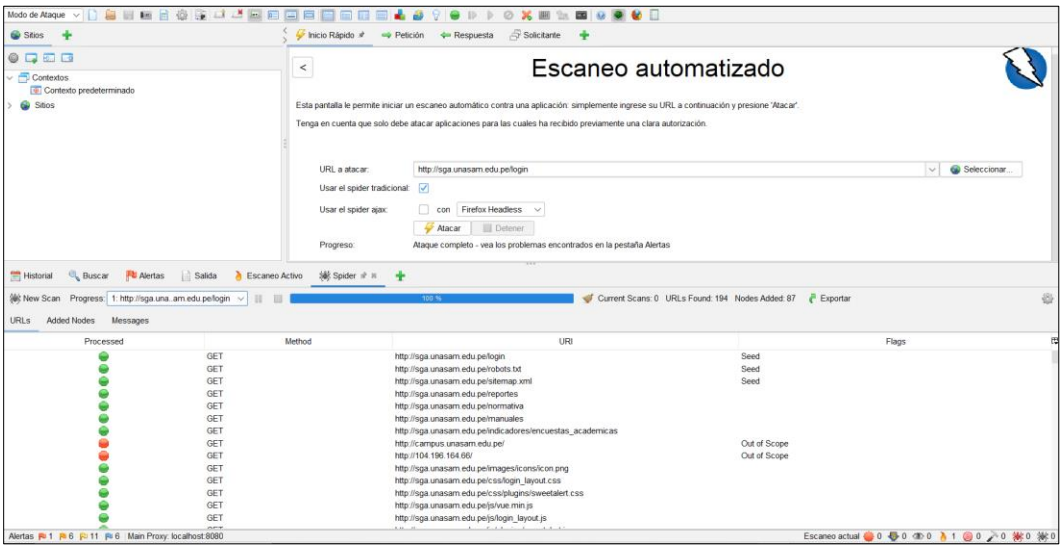
Vulnerable JS Library pagina1



Pagina 2: http://sga.unasam.edu.pe/

Figura 25

OWASP Zed Attack Proxy, pagina2



Como acciones adicionales se revisó el log y los falsos positivos, obteniendo como resultado:

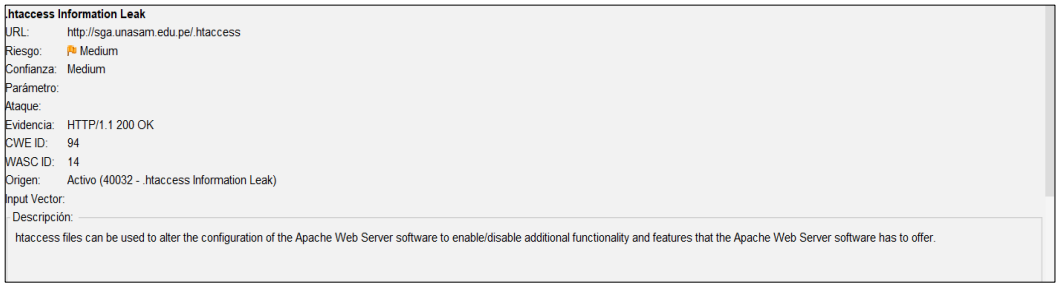
- **Alerta: .htaccess Information Leak**(Fuga de información de .htaccess)
- Riesgo: medio

- Descripción alerta: Los archivos htaccess se pueden usar para modificar la configuración del software del servidor web Apache para habilitar/deshabilitar funcionalidades y características adicionales que el software del servidor web Apache tiene para ofrecer.

- se encontró: Que .htaccess es accesible. (la alerta corresponde a una vulnerabilidad de Componentes vulnerables y obsoletos top 5 de los riesgos de seguridad más importantes en aplicaciones web según la Fundación OWASP)

Figura 26

vulnerabilidad .htaccess Information Leak, pagina2



- **Alerta: Hidden File Found**
- Riesgo: medio

- Descripción alerta: Posible filtración de información administrativa, de configuración o de credenciales que puede ser aprovechada por un individuo

malintencionado para atacar aún más el sistema o realizar esfuerzos de ingeniería social

- Se encontró: Se puede acceder a phpinfo() sin autenticación y autorización adecuadas, o limite la exposición a sistemas internos o IP de origen específicas. Lo importante aquí es que conocemos la versión de PHP. (la alerta corresponde a una vulnerabilidad de Componentes vulnerables y obsoletos top de los riesgos de seguridad más importantes en aplicaciones web según la Fundación OWASP)

Figura 27

vulnerabilidad Hidden File Found, página 2

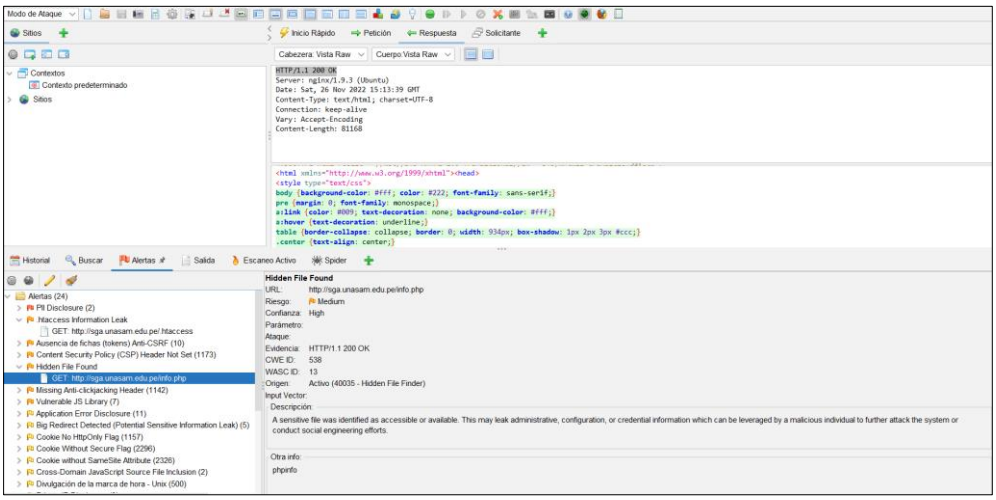
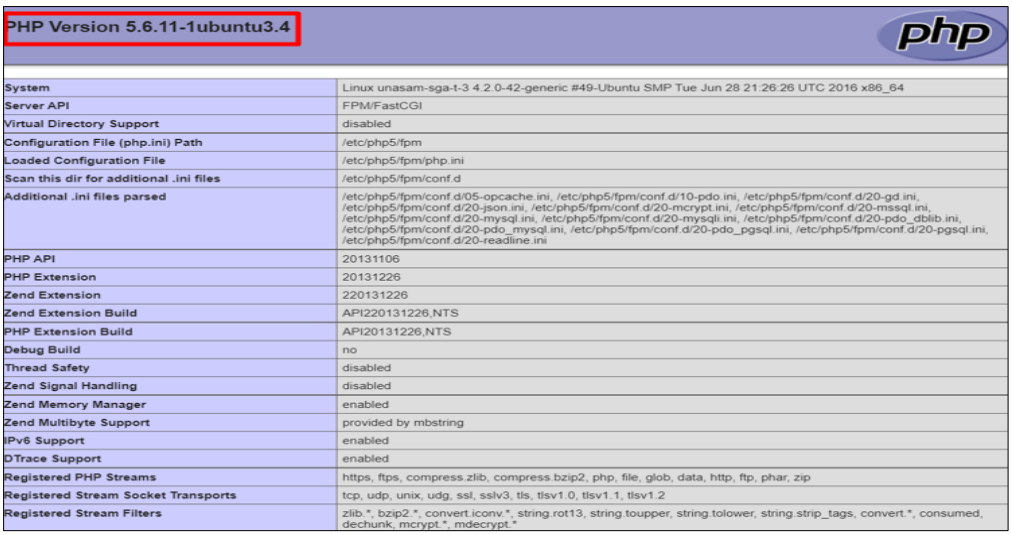


Figura 28

Dato encontrado PHP versión 5.6.11



PHP Version 5.6.11-1ubuntu3.4

System	Linux unasam-sga-t-3 4.2.0-42-generic #49-Ubuntu SMP Tue Jun 28 21:26:26 UTC 2016 x86_64
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/fpm
Loaded Configuration File	/etc/php5/fpm/php.ini
Scan this dir for additional .ini files	/etc/php5/fpm/conf.d
Additional .ini files parsed	/etc/php5/fpm/conf.d/05-opcache.ini, /etc/php5/fpm/conf.d/10-pdo.ini, /etc/php5/fpm/conf.d/20-gd.ini, /etc/php5/fpm/conf.d/20-json.ini, /etc/php5/fpm/conf.d/20-mcrypt.ini, /etc/php5/fpm/conf.d/20-mssql.ini, /etc/php5/fpm/conf.d/20-mysql.ini, /etc/php5/fpm/conf.d/20-mysqli.ini, /etc/php5/fpm/conf.d/20-pdo_dblib.ini, /etc/php5/fpm/conf.d/20-pdo_mysql.ini, /etc/php5/fpm/conf.d/20-pdo_pgsql.ini, /etc/php5/fpm/conf.d/20-pgsql.ini, /etc/php5/fpm/conf.d/20-readline.ini
PHP API	20131106
PHP Extension	20131226
Zend Extension	220131226
Zend Extension Build	API220131226,NTS
PHP Extension Build	API20131226,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	enabled
Registered PHP Streams	https, ftps, compress.zlib, compress.bzip2, php, file, glob, data, http, ftp, phar, zip
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv3, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters	zlib.*, bzip2.*, convert.iconv.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, mcrypt.*, mdecrypt.*

4.1.2.5 PRUEBA 5: IDENTIFY APPLICATION ENTRY POINTS

Mediante este método se busca Comprender cómo se forman las solicitudes y las respuestas típicas de la aplicación, para ello se utilizó la herramienta que identifica la aplicación los POST y GET, para esta prueba utilizamos la herramienta OWASP ZAP.

Pagina 1: https://www.unasam.edu.pe/

Figura 29

Puntos de entrada de la aplicación, página 1

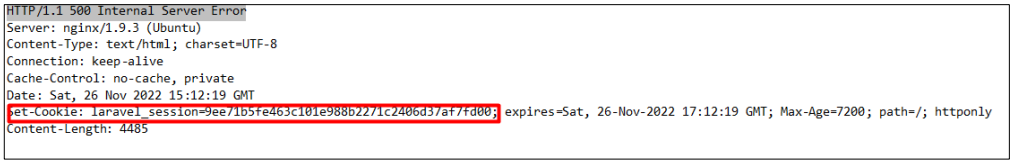
```
HTTP/1.1 500 Internal Server Error
Date: Sat, 26 Nov 2022 14:13:13 GMT
Server: Apache
Cache-Control: no-cache, private
Set-Cookie: XSRF-TOKEN=
eyJpdiI6IkE3d2ZZbHhMNlJPNzhhWFNFaEZCYkE9PSIsInZhbHV1IjoiNE5aalYxXC9IR0JTU1k3SDdva0E4OTkrdjJYzNyV1RndnoxXC9cL2xYV09CUFowTDR0d0VRTkZSakhQWnBqeVJQeSIsIm1hYyI6ImM1YWNjYTQzNGE5
Set-Cookie: appwebfec_sessionFEC=
eyJpdiI6IkFJUWlsbnFqbk5YQUpNU1pOSD1XU1E9PSIsInZhbHV1IjoiWksydFNpZnRHYjZMMnY3QVF2U3UyakdOTDlsa2k0cVE5TGZ4XC9VSXIzNFhlZWx0VmZBT3ZKSlhIQTRsMG5QXC9aIiwibWFjIjoiN2JiYzdmYTM2ZWJh
lYTQ1ZGMzNjc0YWNkZTNnZTcyMDE4OTZjYzM0YzQ3MjcyNmVjMjEzMmQ3NSJ9; expires=Sat, 26-Nov-2022 16:13:13 GMT; Max-Age=7200; path=/; httponly
<!DOCTYPE html><!--


ErrorException: gzinflate(): data error in file /var/www/appUnasam/app/Http/Controllers/PublicacionWebController.php on line 943
Stack trace:
  1. ErrorException->() /var/www/appUnasam/app/Http/Controllers/PublicacionWebController.php:943
```

Pagina 2: http://sga.unasam.edu.pe/

Figura 30

Puntos de entrada de la aplicación, pagina 2



Como resultado de ambas paginas se identifica que se visualiza la cokie, la sesión de las mismas queda comprometidas.

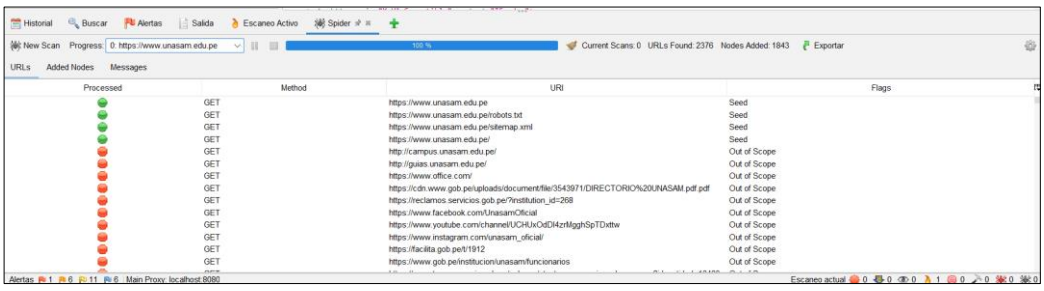
4.1.2.6 PRUEBA 6: MAP EXECUTION PATHS THROUGH APPLICATION

Para realizar esta prueba se utilizó la herramienta OWASP ZAP que es una herramienta para búsqueda de metadatos, código fuente en aplicaciones web, es una herramienta libre que se puede ejecutar en sistemas operativos Windows, Linux y mac, con esto se busca encontrar links fuera de la aplicación web. En la siguiente imagen se muestra la forma de realizar la prueba:

Pagina 1: https://www.unasam.edu.pe/

Figura 31

rutas de ejecución a través de la aplicación, pagina1

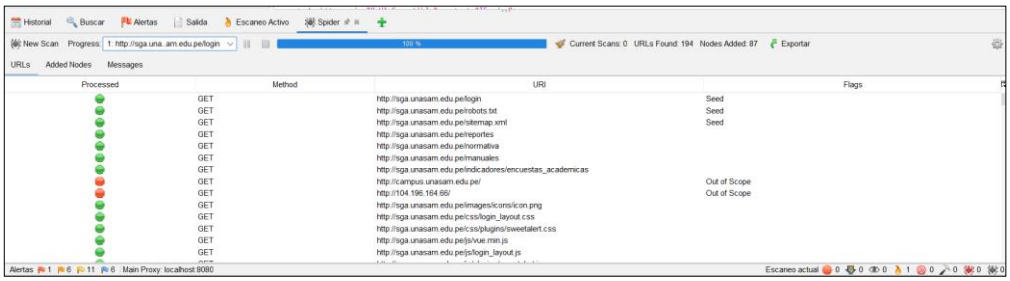


Como resultado al analizar la pagina1 se encontró 1843 links, debido a ello se concluye que no cumple con la prueba, por tal motivo se recomienda que las rutas que se muestran se puedan se ocultadas por el desarrollador

Pagina 2: http://sga.unasam.edu.pe/

Figura 32

rutas de ejecución a través de la aplicación, pagina2



Como resultado al analizar la pagina2 se encontró 87 links, debido a ello se concluye que no cumple con la prueba, por tal motivo se recomienda que las rutas que se muestran se puedan se ocultadas por el desarrollador.

4.1.2.7 PRUEBA 7: FINGERPRINT WEB APPLICATION FRAMEWORK

Para realizar esta prueba se utilizó la herramienta Wappalyzer y la consola de Kali Linux (whatweb), mediante esta prueba realizada se logró identificar los diferentes framework y tecnologías utilizadas en los sitios web.

Pagina 1: https://www.unasam.edu.pe/

Figura 33:

Listado de tecnologías con Wappalyzer, pagina1

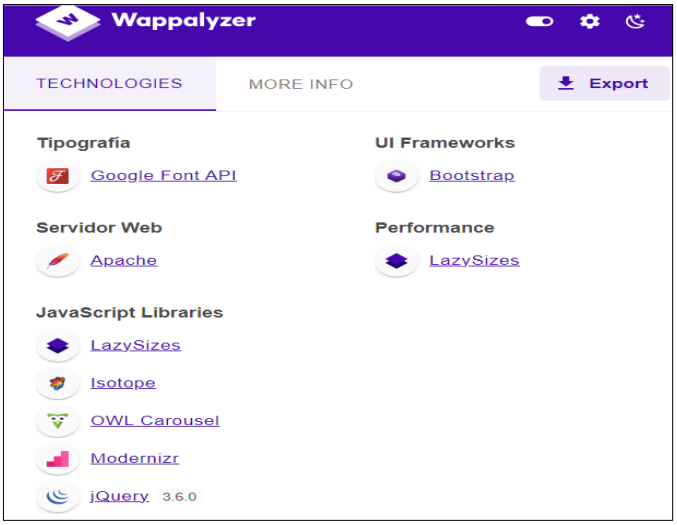


Figura 34

Listado de tecnologías con Kali linux, pagina1

Pagina 2: http://sga.unasam.edu.pe/

Figura 35

Listado de tecnologías con Wappalyzer, pagina2

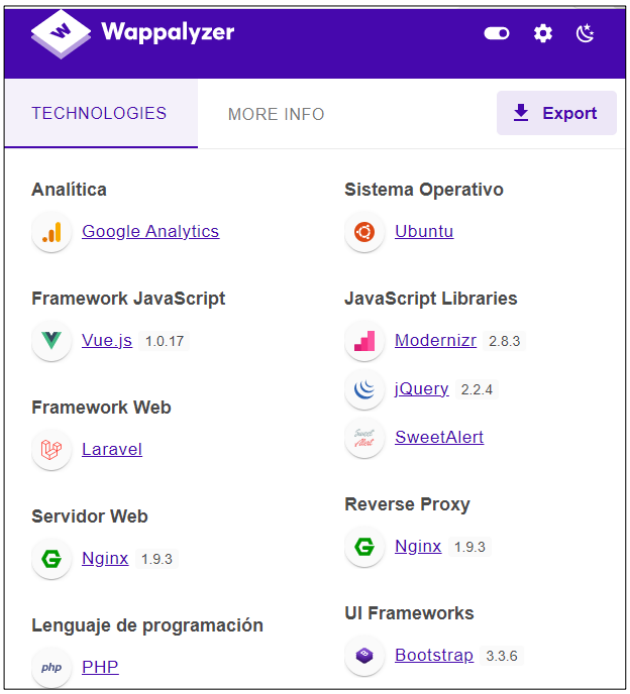
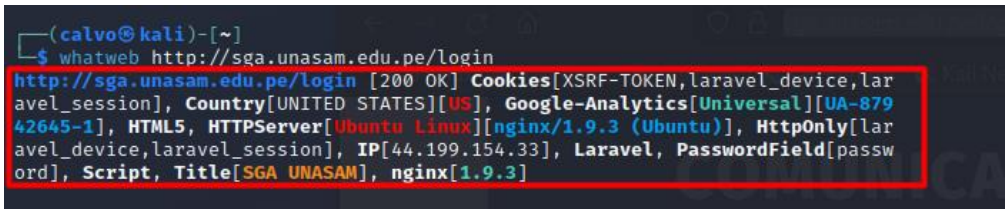


Figura 36

Listado de tecnologías con Kali linux, pagina2



Como resultado de ambos escaneos, tanto con la herramienta Wappalyzer y la consola de Kali Linux con el comando whatweb http//:urlaescaner se identificó un listado de tecnologías, pero lo importante de este análisis es la presencia de PHP, el tipo y la versión web del server tales como nginx 1.9.3 y Apache.

4.1.2.8 PRUEBA 8: FINGERPRINT WEB APPLICATION

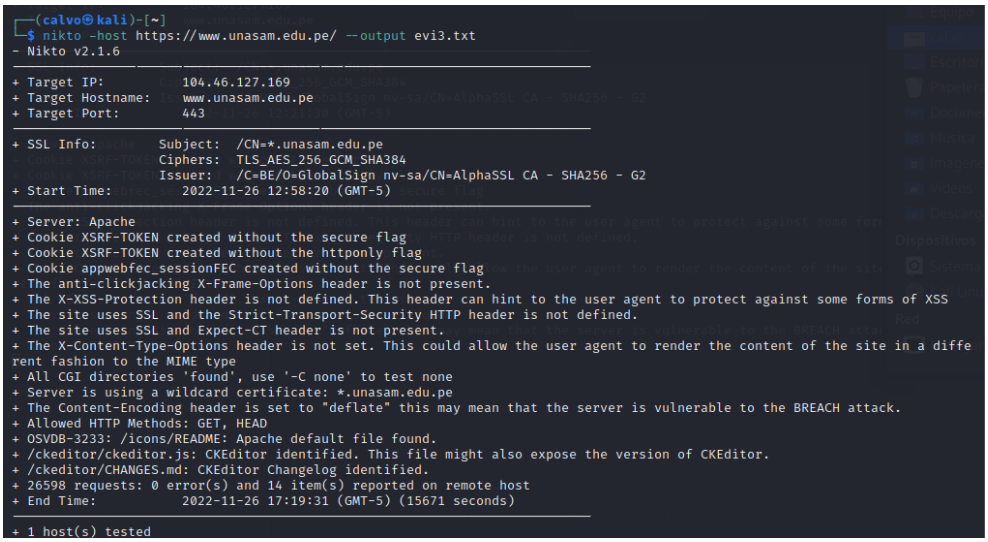
Para realizar esta prueba se utilizó la herramienta Wappalyzer y la consola de Kali Linux (Nikto), mediante esta prueba tratamos de identificar la aplicación web y las versiones para que de ese modo poder determinar las vulnerabilidades conocidas y exploit a usarse en el proceso de las pruebas. Nikto es un escáner de vulnerabilidades de servidores web.

Pagina 1: https://www.unasam.edu.pe/

Se utilizó en siguiente comando: nikto -host https://www.unasam.edu.pe/ --output pres.txt

Figura 37

Escaner de huellas dactilares, pagina1

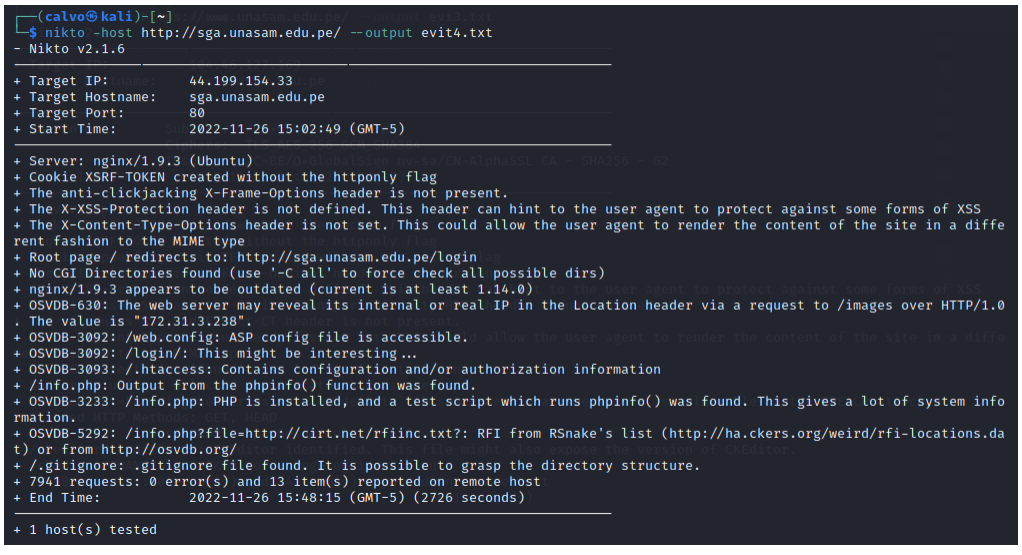


Pagina 2: http://sga.unasam.edu.pe/

Se utilizó en siguiente comando: nikto -host http://sga.unasam.edu.pe/ --output pres.txt

Figura 38

Escaner de huellas dactilares, pagina2



Al finalizar no se encontraron resultados relevantes.

4.1.3 Data test validation

Las pruebas se realizaron las pruebas utilizando el pentesting Kali Linux en Vmware a dos aplicativos webs desarrollados por la Universidad Nacional Santiago Antúnez de Mayolo.

Mediante estas pruebas se pudo conocer la existencia de las principales vulnerabilidades en las aplicaciones web tales como scripts de sitios cruzados (Cross Site Scripting XSS), inyección de SQL (SQL Injection), etc.

Los aplicativos webs dónde realizamos las pruebas son las siguientes:

- Url 1: https://www.unasam.edu.pe/ (Portal Web)
- Url 2: http://sga.unasam.edu.pe/(SISTEMA DE GESTIÓN ACADÉMICA)

4.1.3.1 PRUEBA 9: TESTING FOR REFLECTED CROSS SITE SCRIPTING

El objetivo de esta prueba fue vulnerar las distintas páginas web para que se ejecute código html o javascript afectando la sesión de los usuarios con el fin de mostrar a la víctima un contenido falso y de ese modo poder guardar información confidencial.

En la siguiente figura se inyecto en la url un script para engañar al usuario:

Figura 39

Cross Site Script esquema de ataque, pagina 2

Como resultado al realizar el ataque Cross Site Script, se concluye que ambos sitios webs no son vulnerables a Reflected XSS.

4.1.3.2 PRUEBA 10: TESTING FOR SQL INJECTION

Al realizar esta prueba se tiene como objetivo leer datos sensibles de la base de datos, insertar, editar y eliminar algún dato. Para lo cual se utilizó la herramienta Sqlmap, herramienta de pruebas de penetración de código abierto que automatiza el proceso de detección y explotación de fallas de inyección SQL en servidores de bases de datos.

La prueba consistía en enviar una consulta a la aplicación web con un código sql oculto con el fin de que la aplicación no logre detectarlo y se ejecute en la base de datos.

Para la presente prueba se utilizó la herramienta Sqlmap de kali Linux que es de código abierto el cual nos facilita el proceso ya que optimiza un ataque de inyección SQL. El ataque se realizó con la intención de obtener datos confidenciales tales como emails, direcciones, contraseñas de acceso para ello utilizaremos el comando sqlmap -u

Figura 40

Estructura de ataque inyección sql (Jaymon Security)

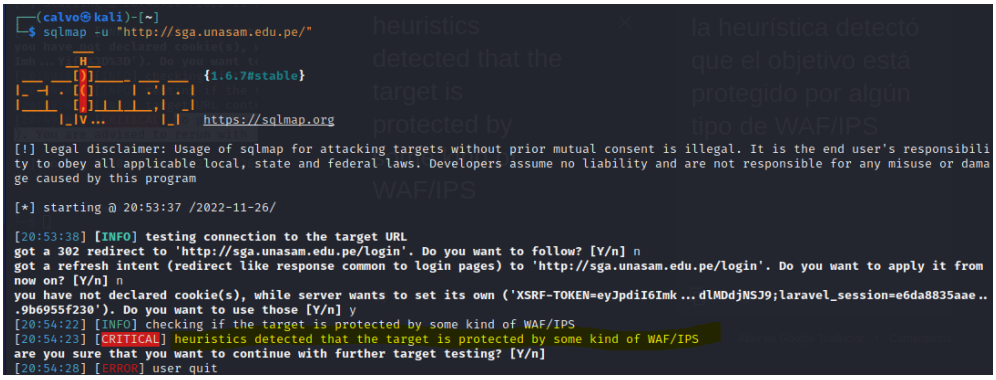
Figura 41

Inyección sql, página 1

Pagina 2: http://sga.unasam.edu.pe/

Figura 42

Inyección sql, página2



Al culminar las pruebas para ambos sitios web analizados, no se visualiza ninguna vulnerabilidad debido a que no se pudo acceder a alguna base de datos desde los sitios web, ya que posiblemente la plataforma y la base de datos no estén alojados en el mismo servidor.

4.1.3.3 PRUEBA 11: TESTING FOR HTML INJECTION

Esta prueba se realizó con el objetivo de identificar si existe algún punto de entrada y poder inyectar código HTML en la página web vulnerada. Esta vulnerabilidad puede tener como consecuencia la divulgación de información de cokies.

Para poder realizar esta prueba utilizamos cualquier navegador inyectando código manualmente.

Pagina 1: https://www.unasam.edu.pe/

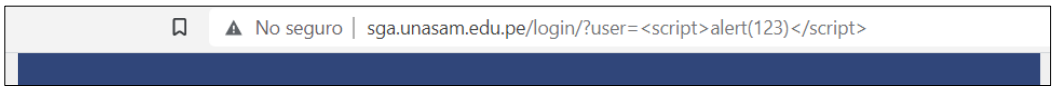
Figura 43

Inyección html, pagina2

Pagina 2: http://sga.unasam.edu.pe/

Figura 44

Inyección html, pagina2



Como resultado de la inyección de código html en ambos sitios web la prueba muestra que la inyección html fue satisfactoria debido a que al mandarle un link se muestra la nueva ruta ingresada el cual podría servir para engañar a los usuarios.

4.1.3.4 PRUEBA 12: TEST HTTP METHODS

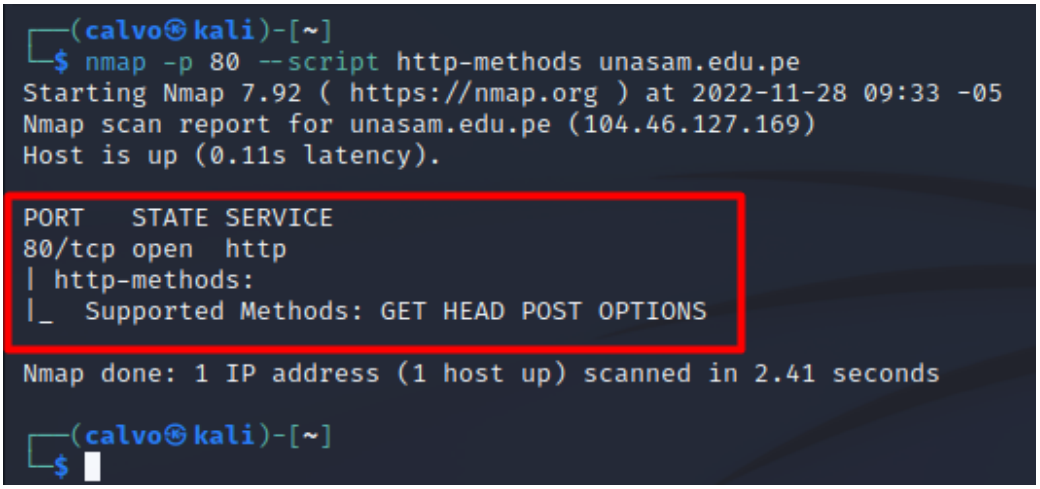
Para realizar esta prueba se busca identificar los diferentes métodos que ofrece HTTP que se están utilizando para realizar acciones en los servidores web, teniendo como objetivo identificar alguno de estos métodos que pueden ser un riesgo para las aplicaciones web ya que permiten a un atacante poder modificar cualquier documento que se encuentre guardado o alojado en el servidor web asimismo también se podría obtener información confidencial. Se utilizó la herramienta Nmap de Kali Linux, ya que nos permitirá identificar que métodos http se muestran en cada una de las páginas web analizadas.

Pagina 1: https://www.unasam.edu.pe/

Para realizar la prueba se utilizó el siguiente comando -nmap -p 80 - -script http-methods unasam.edu.pe

Figura 45

métodos http página1



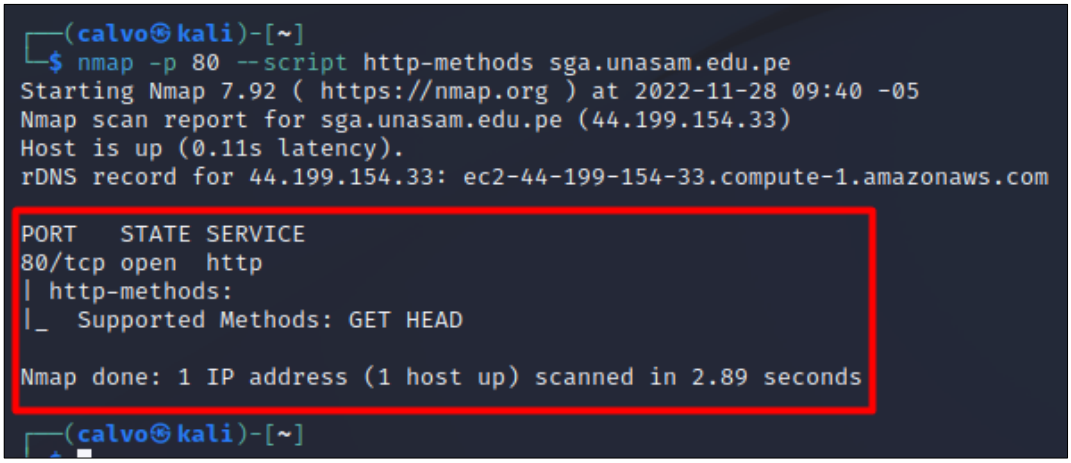
Al concluir el análisis podemos visualizar que los métodos GET, HEAD, POST Y OPTIONS no están ocultos lo cual viene siendo una falla de desarrollo, se considera como vulnerabilidad ya que mediante estos métodos se puede acceder al servidor web. Como solución se recomienda ocultar dichos métodos.

Pagina 2: http://sga.unasam.edu.pe/

Para realizar la prueba se utilizó el siguiente comando -nmap -p 80 - -script http-methods unasam.edu.pe

Figura 46

métodos http página2



Al finalizar la prueba podemos ver que los métodos GET, HEAD no están ocultos lo cual viene siendo una falla de desarrollo, se considera como vulnerabilidad ya que mediante dichos métodos se puede acceder al servidor web. Como solución se recomienda ocultar dichos métodos.

4.1.3.5 PRUEBA 13: TEST APPLICATION PLATFORM CONFIGURATION

Esta prueba se llevó a cabo con el fin de identificar si la plataforma contiene configuraciones genéricas las cuales no podrían ser adecuadas para las distintas tareas que realizan, el objetivo de esta prueba es verificar si se eliminaron los archivos predeterminados. Durante la prueba se utilizó la herramienta Reverse IP Domain chek.

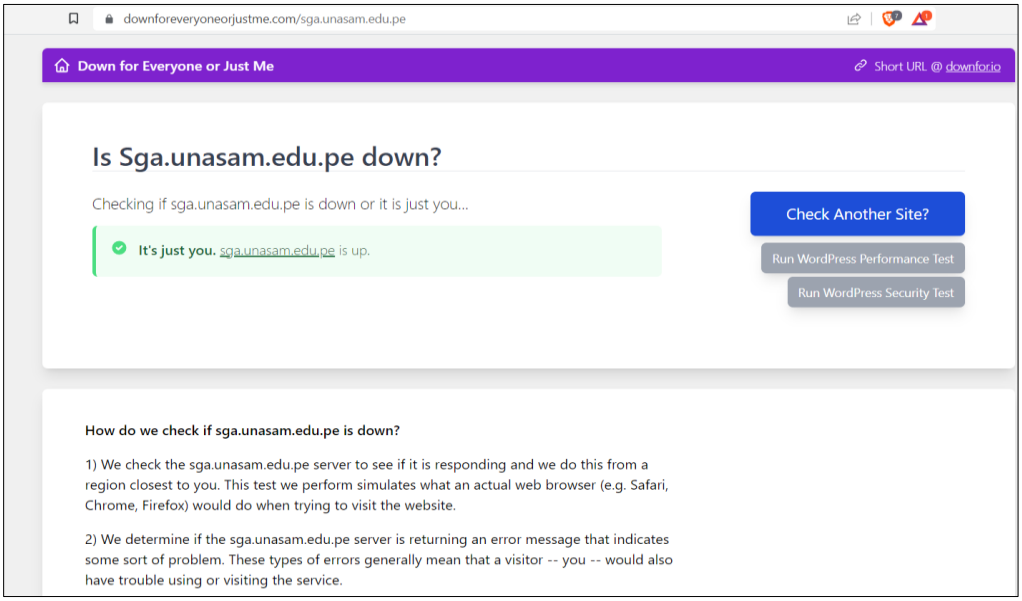
Pagina 1: https://www.unasam.edu.pe/

Figura 47

Resultados reverse IP, página1

Figura 48

Resultado de trafico, Pagina1



Para esta prueba, se encontró 1 plataforma web en el mismo dedicado como se muestra en la figura 47. Se evidencia que se realizó el ataque DDos como se muestra en la Figura 48.

Pagina 2: http://sga.unasam.edu.pe/

Figura 49

Resultados reverse IP, página1

Al finalizar la prueba se encontró 15 plataformas web con el mismo dedicado, por ende, no se pudo realizar el ataque DDos debido a que podría afectar a todos los dominios de los servidores, esta vulnerabilidad afecta a los servidores apache por lo cual podemos utilizar alguna herramienta exploit para atacar el objetivo.

4.2 Presentación resultado y prueba de hipótesis

4.2.1 Resultados de las pruebas de OWASP

Estos son las vulnerabilidades encontradas en la aplicación web, los mismos serán puntuados con respecto a la metodología de OWASP Risk Rating Methodology.

- Vulnerabilidades Apache
- Visibilidad de información de PHP

4.2.1.1 Riesgo en base a las Vulnerabilidades en Apache

Apache es un servidor web HTTP de código abierto. La gran mayoría de las vulnerabilidades solo lo pueden utilizar usuarios locales. Sin embargo, se recomienda actualizar y utilizar la última versión. Las vulnerabilidades de seguridad se documentan y publican. Se han mostrado las razones de esa calificación (Suffering and Common Exposure, 2018).

- **Factores de Amenaza:** Para explotación de las vulnerabilidades de Apache se requiere un usuario con un nivel alto de conocimiento y un nivel avanzado para que pueda utilizar herramientas que apoyen a explotar dicha vulnerabilidad. Para la explotación se puede hacer uso de un exploit que nos permita el acceso al servidor. Posteriormente hacer uso de un segundo exploit para encontrar el script requerido para ejecutarlo. El acceso a un solo recurso no es obligatorio y puede hacerlo cualquier usuario de Internet.

- **Factores de Vulnerabilidad:** Para lograr encontrar versiones y vulnerabilidades de Apache se puede hacer uso de herramientas automatizadas, sin embargo, para explotarlas es difícil porque a se requieren explotaciones sofisticadas y una investigación profunda. Estos ataques se analizan en la aplicación que aparece en el análisis.

- **Impacto Técnico:** La explotación de la vulnerabilidad no tiene un impacto significativo en la privacidad y tiene un impacto pequeño en la corrupción de datos, se puede denegar servicios básicos.

- **Impacto de negocios:** Si se llega a explotar dicha vulnerabilidad, tiene un impacto mínimo en la ganancia anual, no afecta la reputación de la empresa, y es menos daño y menos impacto en la vida personal.

Figura 50

Resumen de Probabilidad x Impacto en la aplicación web sobre Vulnerabilidades en Apache.

PROBABILIDAD								
Factores agente de amenazas					Factores de vulnerabilidad			
Habilidad	Motivo	Oportunidad	Tamaño		Facilidad de descubrimiento	Facilidad de explorar	Conciencia	Detección de intrusiones
usuario amenzado del ordenado (5)	Posible recompensa (4)	No requiere acceso o usuario (9)	Los usuarios de internet anónimos (9)		Herramientas automatizadas disponibles (9)	Dificil (3)	Conocimiento público (9)	Detección activa en la aplicación (1)
Resultado de la probablidad general: 6.125 Nivel: ALTO								
IMPACTO								
Impacto técnico					Impacto de negocio			
Perdida de confidencialidad	Perdida de integridad	Perdida de disponibilidad	Perdidad de trazabilidad del atacante		Daño financiero	Daños a la reputación	Incumplimiento	Violacción de la privacidad
Minima relación de datos no sensibles (2)	Minimo de datos seriamente corruptos (3)	Servicios primarios extensos interrumpidos (7)	Totalmente trazable (1)		Efecto menor en el beneficio anual (3)	Daño minimo (1)	Violación menor(2)	Un individuo (3)
Resultado general del impacto técnico: 3.250 Nilvel: Medio					Resultado general del impacto global: 2.250 Nivel: Bajo			
Impacto global: 2.750 Nivel: Bajo								

4.2.1.2 Riesgo en base a Vulnerabilidades de PHP

PHP (Hypertext Preprocessor) es un lenguaje de código abierto utilizado que sirva para el desarrollo web, que se puede implementar en HTML ejecutado en el lado del servidor (The PHP Group, 2018). Los efectos que se puede tener al utilizar php son:

- **Factores de Amenaza:** Al enviar información PHP representa un riesgo, principalmente si es que no se actualiza a las últimas versiones es por ello que se debe de contar con una versión actual, para poder obtener y ver esta información, no es necesario tener conocimientos avanzados, esta información no proporciona valor directo a los atacantes, es decir que para ver esta información no se requiere ningún acceso especial.

- **Factores de Vulnerabilidad:** Se detectó el info.php del servidor, la facilidad de uso de la vulnerabilidad y esta información es permitido ya que depende de la vulnerabilidad de las versiones de PHP, todo. La información sobre PHP es de libre acceso.

- **Impacto Técnico:** Esta vulnerabilidad no tiene impacto significativo con respecto a la privacidad, integridad o disponibilidad del sitio, esta información se puede encontrar.

- **Impacto de negocios:** No se tiene daño financiero, tampoco daño a la reputación, sin embargo otros podrían acceder a información confidencial en la distribución, lo que resulta en menos privacidad.

Figura 51

Resumen de Probabilidad x Impacto en la aplicación web sobre Vulnerabilidades en PHP.

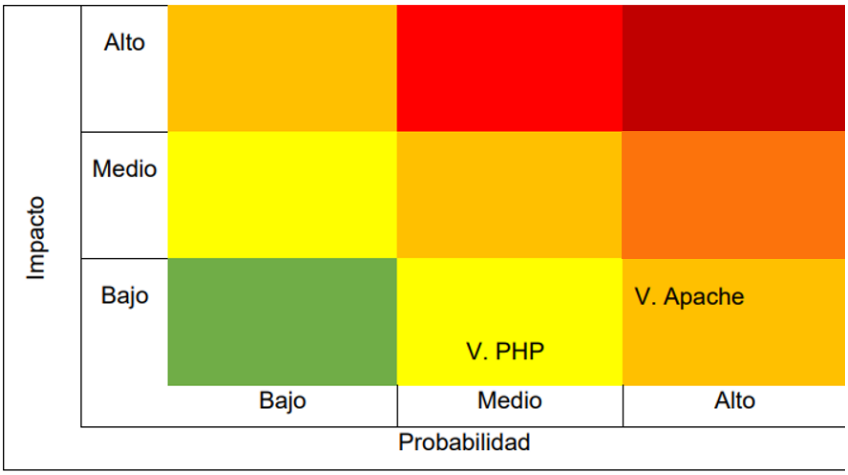
PROBABILIDAD								
Factores agente de amenazas					**Factores de vulnerabilidad**			
Habilidad	**Motivo**	**Oportunidad**	**Tamaño**		**Facilidad de descubrimiento**	**Facilidad de explorar**	**Conciencia**	**Detección de intrusiones**
Sin conocimientos técnicos (1)	Bajo o ninguna recompensa (1)	No requiere acceso o usuario (9)	Los usuarios de internet anónimos (9)		Herramientas automatizadas disponibles (9)	Tecnico (1)	Conocimiento público (9)	Detección activa en la aplicación (1)
Resultado de la probablidad general: 5				**Nivel: Medio**				
IMPACTO								
Impacto técnico					**Impacto de negocio**			
Perdida de confidencialidad	**Perdida de integridad**	**Perdida de disponibilidad**	**Perdidad de trazabilidad del atacante**		**Daño financiero**	**Daños a la reputación**	**Incumplimiento**	**Violacción de la privacidad**
Minima relación de datos no sensibles (2)	Minimo de datos seriamente corruptos (1)	Servicios secundarios minimos interrumpidos (1)	Totalmente trazable (1)		Menos que el costo de arreglar la vulnerabilidad (1)	Daño minimo (1)	Violación menor(2)	Un individuo (3)
Resultado general del impacto técnico: 1.250			**Nilvel: Bajo**		**Resultado general del impacto global: 1.750**			**Nivel: Bajo**
Impacto global: 1.500				**Nivel: Bajo**				

4.2.1.3 Matriz de Riesgos sobre Vulnerabilidades

La figura 52 muestra la matriz de Riesgos de las vulnerabilidades encontradas.

Figura 52

Matriz de Riesgos sobre vulnerabilidades



4.2.1.4 Presentación de resultado

Interpretar los resultados de una investigación, es un paso muy importante durante el proceso de ésta, porque con base en lo que arrojan se podrá identificar la relación existente entre las variables de la investigación. Para el caso de este objeto de estudio, la Universidad Nacional Santiago Antúnez de Mayolo y después de la aplicación de los instrumentos explicados en el capítulo correspondiente a Metodología y Diagnóstico se obtuvieron los siguientes resultados:

Tabla 10

Resultados de la encuesta sobre aplicación del pentesting

ESCALA/PREGUNTA	Nunca	Casi nunca	A veces	Casi siempre	Siempre
Pregunta 1	0%	20%	35%	20%	25%
Pregunta 2	0%	0%	20%	50%	30%
Pregunta 3	0%	65%	35%	0%	0%
Pregunta 4	0%	0%	0%	55%	45%
Pregunta 5	0%	10%	30%	35%	25%
Pregunta 6	0%	30%	45%	15%	10%
Pregunta 7	20%	35%	15%	25%	5%
Pregunta 8	25%	75%	0%	0%	0%
Pregunta 9	0%	5%	15%	45%	35%

Tabla 11

Resultados de la encuesta sobre seguridad informática

ESCALA/PREGUNTA	Nunca	Casi nunca	A veces	Casi siempre	Siempre
Pregunta 1	20%	15%	20%	40%	5%
Pregunta 2	5%	10%	40%	30%	15%
Pregunta 3	0%	20%	35%	20%	25%
Pregunta 4	0%	5%	40%	35%	20%
Pregunta 5	0%	15%	35%	30%	20%
Pregunta 6	0%	65%	35%	0%	0%
Pregunta 7	0%	20%	30%	35%	15%
Pregunta 8	0%	10%	10%	35%	45%

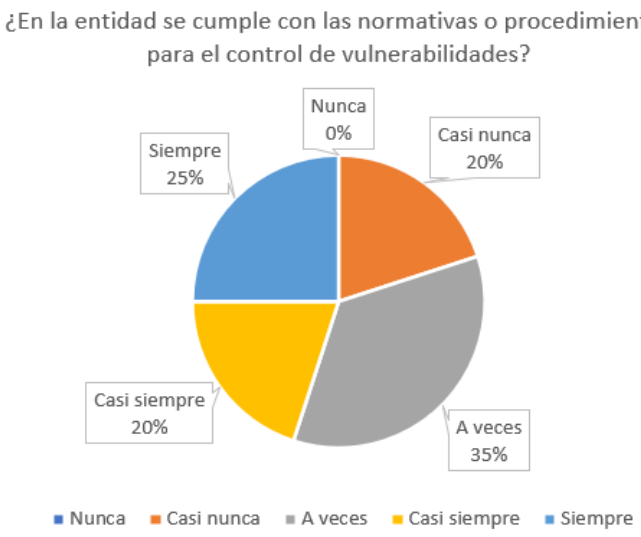
Análisis de cuestionario:

Variable 1: Aplicación de pentesting

Pregunta 1: ¿En la entidad se cumple con las normativas o procedimientos para el control de vulnerabilidades?

Figura 54

Cumplimiento de las normas para el control de vulnerabilidades

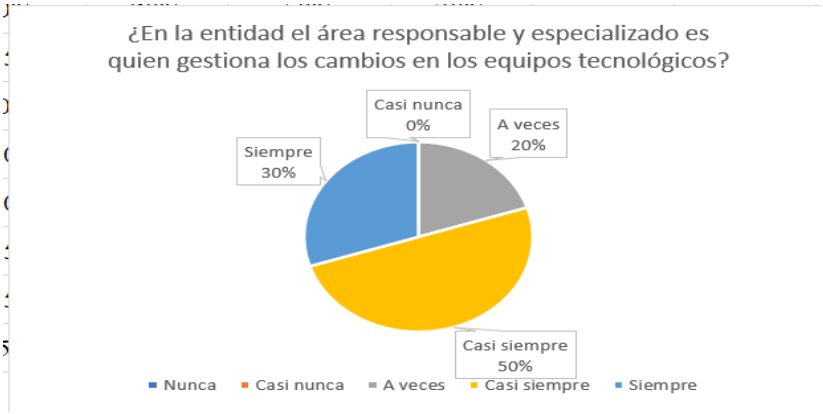


Se puede observar que del 100% de los encuestados, el 35% refieren como algo A veces, el 25 % siempre, el 20% casi siempre y el 20% casi nunca.

Pregunta 2: ¿En la entidad el área responsable y especializado es quien gestiona los cambios en los equipos tecnológicos?

Figura 55

Resultado de gestión de cambios en el equipo

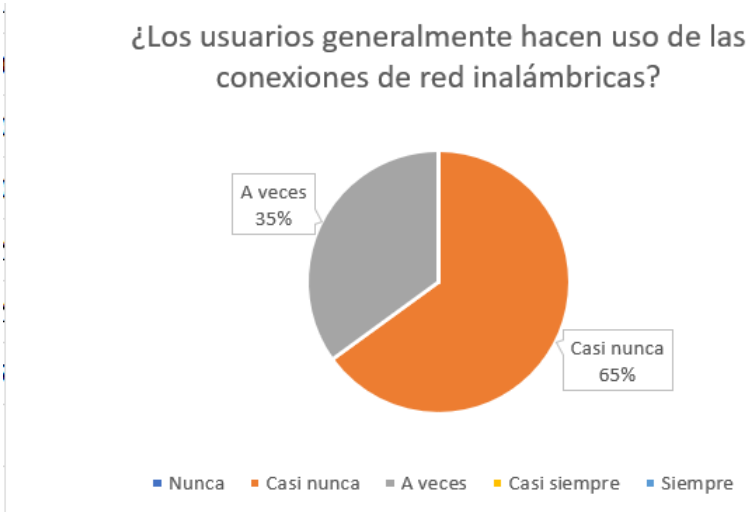


Se puede observar que del 100% de los encuestados, el 50% refieren como casi siempre, el 30 % siempre, el 20% a veces.

Pregunta 3: ¿Los usuarios generalmente hacen uso de las conexiones de red inalámbricas?

Figura 56

Resultados de conexion inalambrica

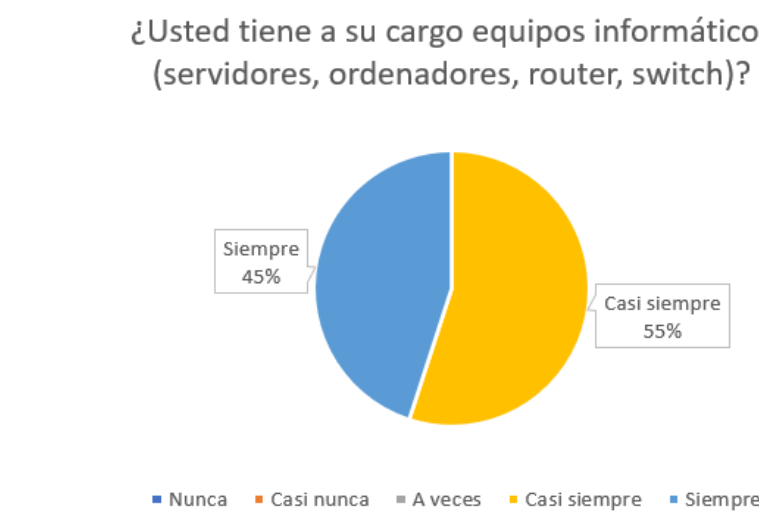


Se puede observar que del 100% de los encuestados, el 65% refieren como casi nunca, el 35 % a veces.

Pregunta 4: ¿Usted tiene a su cargo equipos informáticos (servidores, ordenadores, router, switch)?

Figura 57

Resultados de equipos informáticos

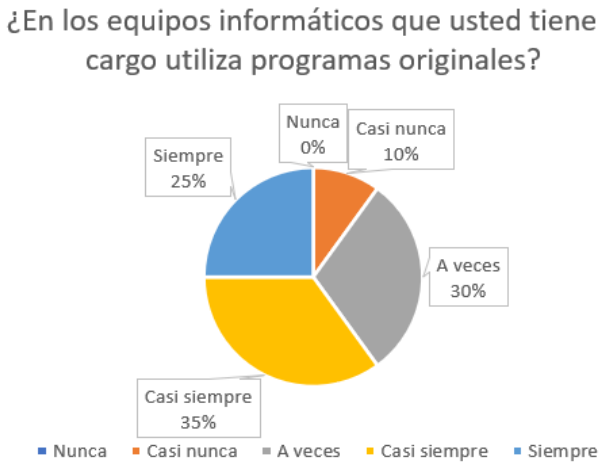


Se puede observar que del 100% de los encuestados, el 5% refieren como casi siempre, el 5 % a siempre.

Pregunta 5: ¿En los equipos informáticos que usted tiene a cargo utiliza programas originales?

Figura 58

Resultado de uso de programas originales

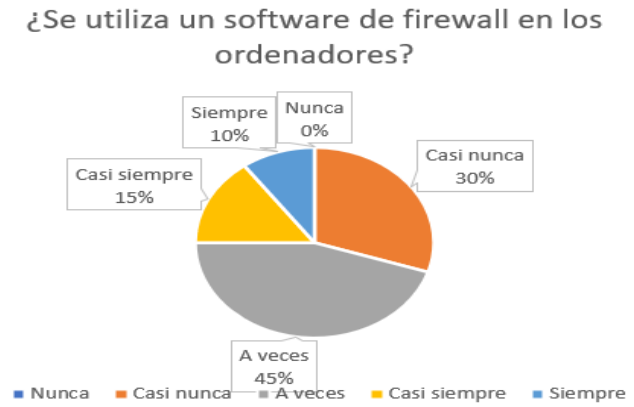


Se puede observar que del 100% de los encuestados, el 35% refieren como casi siempre, el 30 % a veces, el 25% siempre y el 10% casi nunca.

Pregunta 6: ¿Se utiliza un software de firewall en los ordenadores?

Figura 59

Resultado del uso de firewall

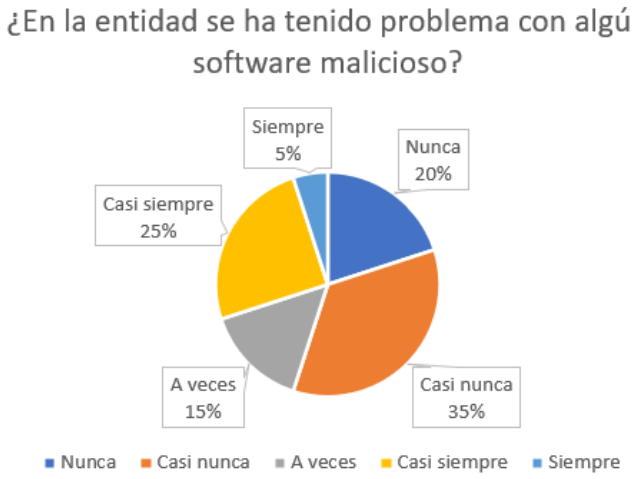


Se puede observar que del 100% de los encuestados, el 45% refieren como a veces, el 30 % casi nunca, el 15% casi siempre y el 10% siempre.

Pregunta 7: ¿En la entidad se ha tenido problema con algún software malicioso?

Figura 60

Resultado de problemas con software malisioso

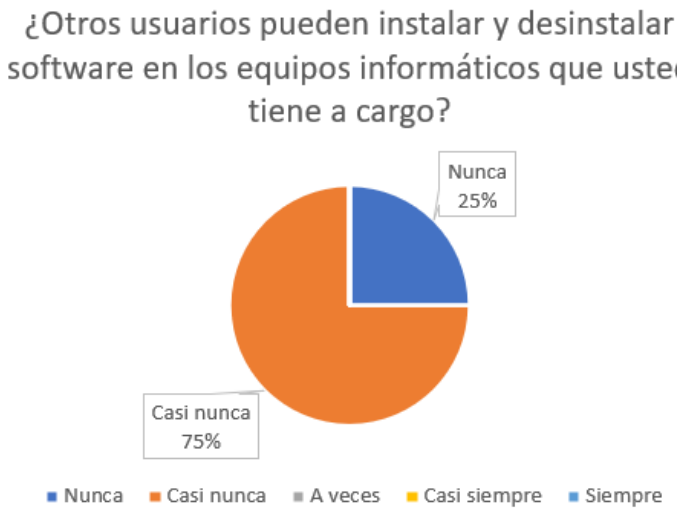


Se puede observar que del 100% de los encuestados, el 35% refieren casi nunca, el 25 % casi siempre, el 20% nunca , el 5% a veces y el 5% siempre.

Pregunta 8: ¿Otros usuarios pueden instalar y desinstalar software en los equipos informáticos que usted tiene a cargo?

Figura 61

Resultado de control de instalación de software

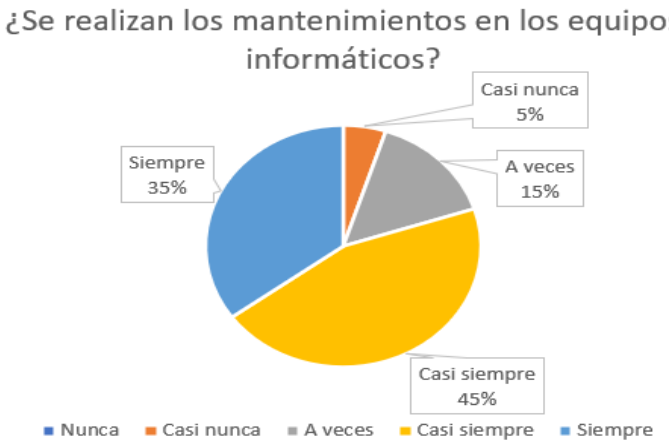


Se puede observar que del 100% de los encuestados, el 75% refieren casi nunca, y el 25% nunca.

Pregunta 9: ¿Se realizan los mantenimientos en los equipos informáticos?

Figura 62

Resultado de mantenimiento de equipos informáticos



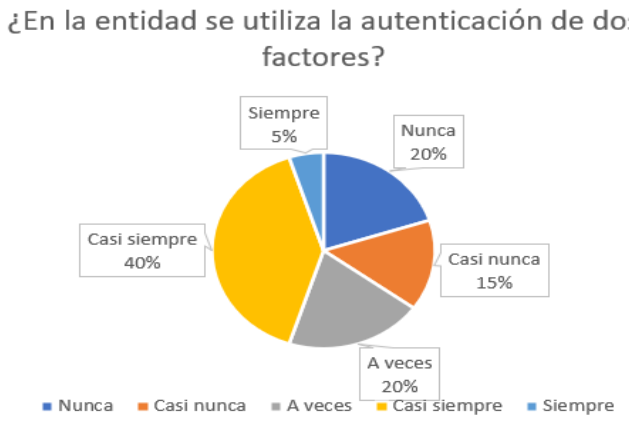
Se puede observar que del 100% de los encuestados, el 45% refieren casi siempre, el 35% siempre, 15% a veces y el 5% casi nunca.

Variable 2: Seguridad informática

Pregunta 1: ¿En la entidad se utiliza la autenticación de dos factores?

Figura 63

Resultados de la autentificación de dos factores

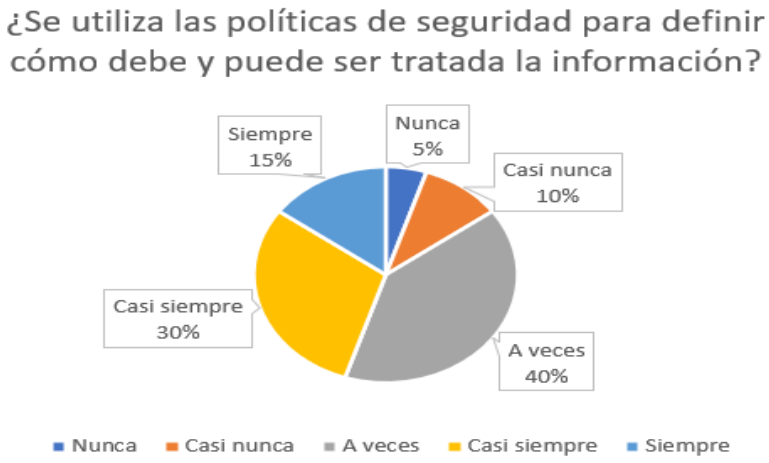


Se puede observar que del 100% de los encuestados, el 40% refieren casi siempre, el 20% a veces, 15% casi nunca, el 20% nunca y el 5% siempre

Pregunta 2: ¿Se utiliza las políticas de seguridad para definir cómo debe y puede ser tratada la información?

Figura 64

Resultados de politicas de control de información

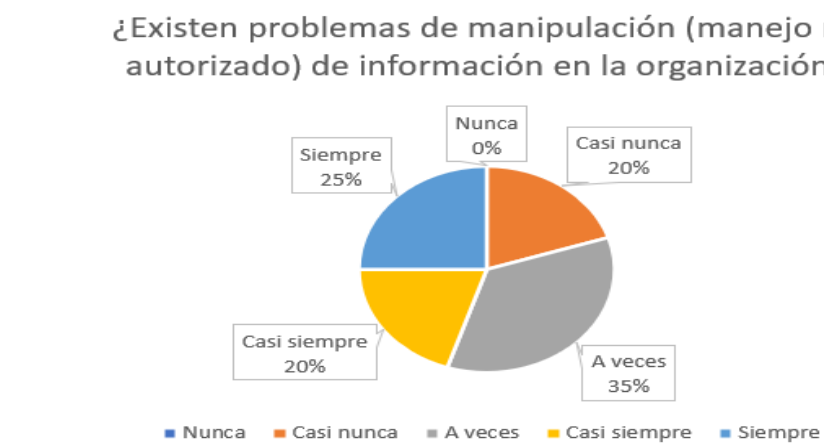


Se puede observar que del 100% de los encuestados, el 40% refieren a veces, el 30% casi siempre, 15% siempre, el 10% casi nunca y el 5% nunca.

Pregunta 3: ¿Existen problemas de manipulación (manejo no autorizado) de información en la organización?

Figura 65

Resultado de problemas de manipulación de datos

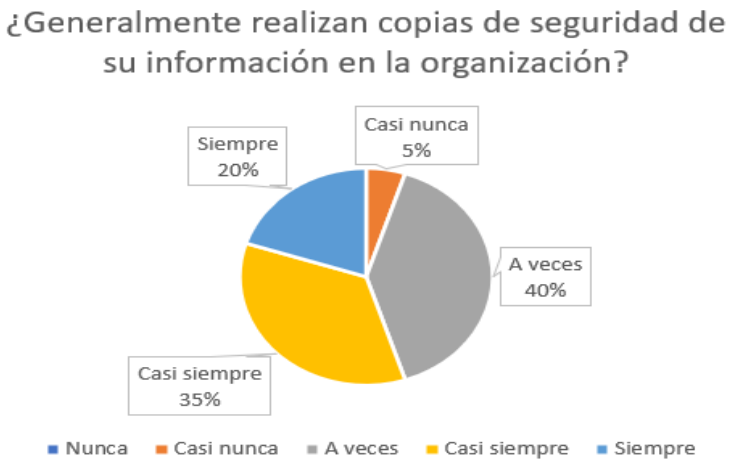


Se puede observar que del 100% de los encuestados, el 35% refieren a veces, el 25% siempre, 20% casi siempre, el 20% casi nunca y el 0% nunca.

Pregunta 4: ¿Generalmente realizan copias de seguridad de su información en la organización?

Figura 66

Resultados se realizan copias de seguridad

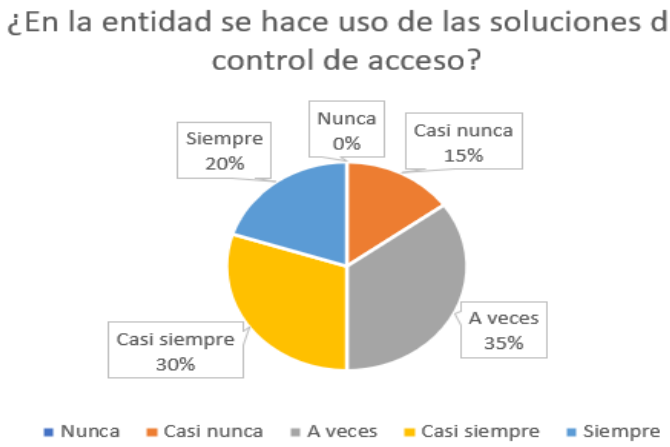


Se puede observar que del 100% de los encuestados, el 40 % refieren a veces, el 35% caso siempre, 20% siempre, el 5% casi nunca y el 0% nunca.

Pregunta 5: ¿En la entidad se hace uso de las soluciones de control de acceso?

Figura 67

Resultado de soluciones de control de acceso

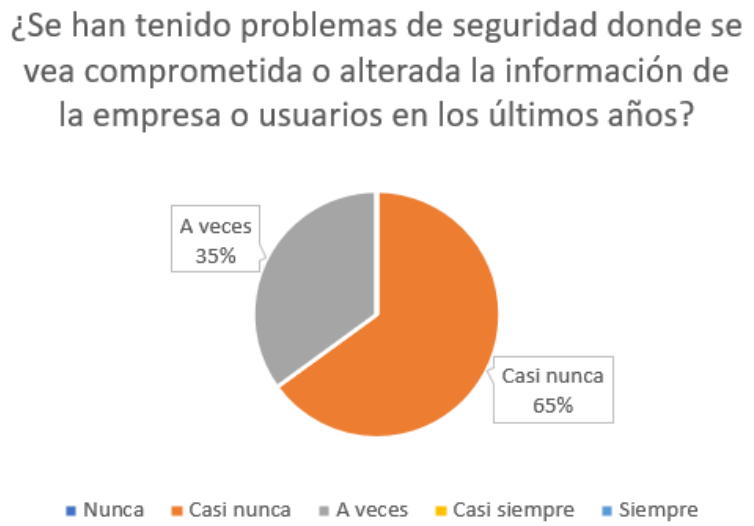


Se puede observar que del 100% de los encuestados, el 35 % refieren a veces, el 30% casi siempre, 20% siempre, el 15% casi nunca y el 0% nunca.

Pregunta 6: ¿Se han tenido problemas de seguridad donde se vea comprometida o alterada la información de la empresa o usuarios en los últimos años?

Figura 68

Resultados de problema de seguridad donde se vea comprometida la información

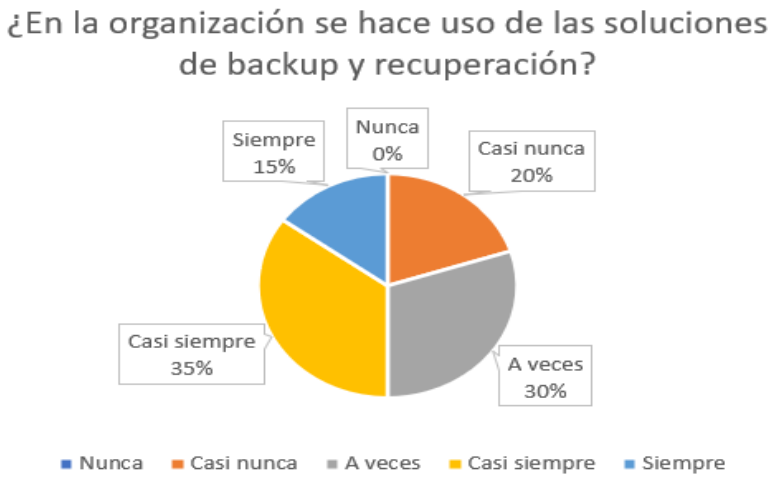


Se puede observar que del 100% de los encuestados, el 65 % refieren a casi nunca y el 35% a veces.

Pregunta 7: ¿En la organización se hace uso de las soluciones de backup y recuperación?

Figura 69

Resultados de soluciones de backup

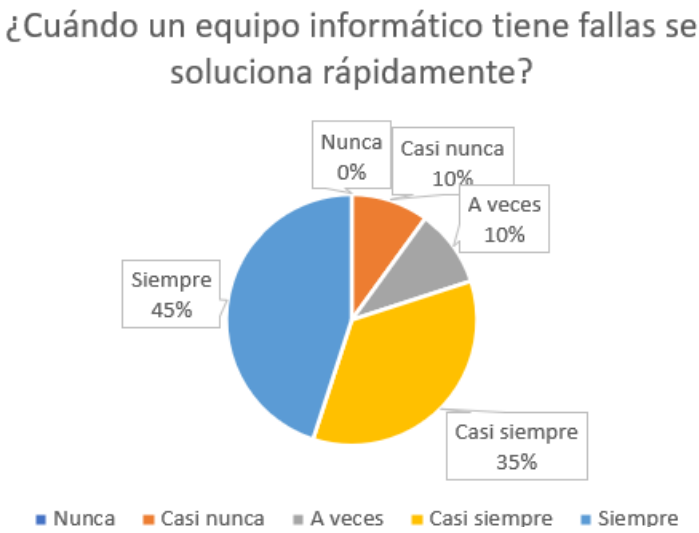


Se puede observar que del 100% de los encuestados, el 35 % refieren a casi siempre, el 30% a veces, 20% casi nunca, el 15% siempre y el 0% nunca.

Pregunta 8: ¿Cuándo un equipo informático tiene fallas se soluciona rápidamente?

Figura 70

Solucion a óallas de equipos informáticos



Se puede observar que del 100% de los encuestados, el 45 % refieren a siempre, el 35% casi siempre, 20% a veces , el 10% casi nunca y el 0% nunca

Interpretación de la entrevista:

Se realizó la entrevista al personal de la OGTISE con el fin de recabar información detallada y poder conocer el estado actual de la entidad.

- Análisis de vulnerabilidades: En la universidad nacional Santiago Antúnez de Mayolo si se realizan mantenimientos a los equipos informáticos, en los centros de cómputo se encargan de controlar los responsables de cada facultad. Actualmente no se realiza la actualización de todos los softwares instalados en los equipos informáticos debido a que la gran mayoría utilizan software craqueados. Por el contrario, lo que se realiza diariamente son los mantenimientos correctivos.

  Finalmente se comentó que la entidad no cuenta con una norma o guía en el cual nos indique como actuar ante un ataque o una posible amenaza identificada siendo la primera acción que se

realiza es acudir al área de la falla y realizar la verificación de la falla.

- Confidencialidad, disponibilidad e integridad de la información:

  En la universidad se utiliza el control de acceso, por lo cual un usuario para poder acceder a las páginas web u otros aplicativos se les tiene que brindar unas credenciales con los permisos respectivos de acuerdo a sus necesidades. Se tiene muy claro la manera de cómo tratar la información ya que existe información muy confidencial que solo pueden tener acceso el personal autorizado.

  Por otro lado, se menciona que realizan copias de seguridad a las bases de datos y a alguna otra información que se consideren importante, las soluciones a los equipos informáticos dañados se brindan diariamente sin embargo hay algunas que se quedan en cola ya que en algunos casos se necesita reemplazar alguna parte del ordenador.

En el presente apartado realizaremos un resumen de los datos ingresados al SPSS.

Tabla 12

Estadísticos de fiabilidad

Estadísticos de fiabilidad

Alfa de Cronbach	Alfa de Cronbach basada en los elementos tipificados	N de elementos
,838	,791	17

Confiabilidad: El instrumento de recolección de datos estuvo conformado por 17 ítems distribuido en la variable aplicación de pentesting y la seguridad informática. Se utiliza el coeficiente de alfa de Cronbach calculado con el SPSS es de 0.838, con lo cual se concluye que el instrumento es confiable (ver la tabla 7)

Prueba de la Hipótesis General:

a) Hipótesis estadística: El valor de coeficiente de correlación r de Spearman determina una relación lineal entre las variables ordinales o nominales; nos indica si esta relación es estadísticamente significativa.

$$Rs = 1 - \frac{6\sum_i d_i^2}{n(n-1)^2}$$

Donde:

Rs= Coeficiente de correlación de rangos de Spearman

d= Diferencia entre los rangos (X menos y)

n=Numero de datos

El valor de Spearman es Rs=0.779

b) Prueba de Hipótesis: Para ello se aplica la prueba de hipótesis de parámetro, como en toda prueba de hipótesis nula se establece que no hay relación, es decir el coeficiente de correlación es igual a 0; mientras que la hipótesis alterna debe ser diferente a 0 por lo cual se menciona que si existe una relación significativa.

PRUEBA DE HIPOTESIS GENERAL

Tabla 13

Correlación entre las variables Aplicación pentesting y la seguridad informática

Correlaciones

			Pentesting	Seguridad_informatica
Rho de Spearman	Pentesting	Coeficiente de correlación	1,000	,779**
		Sig. (bilateral)	.	,000
		N	20	20
	Seguridad_informatica	Coeficiente de correlación	,779**	1,000
		Sig. (bilateral)	,000	.
		N	20	20

**. La correlación es significativa al nivel 0,01 (bilateral).

En la tabla 13 se muestra los resultados del procesamiento que se obtuvo del SPSS, se observa que si existe una relación directa y significativa entre la aplicación de pentesting y la seguridad informática en los equipos tecnológicos en la Universidad Nacional Santiago Antúnez de Mayolo que arroja el coeficiente de spearman igual a 0.779 y con un nivel de significancia iguales a sig(bilateral)=0.000 por lo que se rechaza la hipótesis nula y se acepta la hipótesis del investigador

PRUEBA DE HIPOTESIS ESPECIFICAS:

a) Hipótesis especifica1

H_1: Existe una relación directa entre la aplicación de pentesting y la confidencialidad en la seguridad informática de los equipos tecnológicos de la institución.

H_0: No existe una relación directa entre la aplicación de pentesting y la confidencialidad en la seguridad informática de los equipos tecnológicos de la institución.

Tabla 14

Correlación entre las variables Aplicación pentesting y la confidencialidad en seguridad informática

Correlaciones

			Pentesting	Confidencialidad
Rho de Spearman	Pentesting	Coeficiente de correlación	1,000	,556*
		Sig. (bilateral)	.	,011
		N	20	20
	Confidencialidad	Coeficiente de correlación	,556*	1,000
		Sig. (bilateral)	,011	.
		N	20	20

. La correlación es significativa al nivel 0,05 (bilateral).

Resultado 1: En la tabla 14 se muestra el resultado obtenido del procesamiento con el SPSS, se observa una buena relación entre las variables que arroja el coeficiente de spearman que es igual a 0.556, el grado de relación entre la variable Aplicación pentesting y la confidencialidad de la seguridad informática, ambos sugieren que existe una relación significativa y directa con un grado de relación muy buena.

Para contrastar la hipótesis realizamos el análisis del valor sig(bilateral) es igual a 0.011 que es menor a 0.05 por lo que se rechaza la hipótesis nula y se acepta el H_1.

b) Hipótesis especifica H2

H_2: Existe una relación directa entre la aplicación de pentesting y la integridad en la seguridad informática de los equipos tecnológicos de la institución.

H_0: No existe una relación directa entre la aplicación de pentesting y la integridad en la seguridad informática de los equipos tecnológicos de la institución.

Tabla 15

Correlación entre las variables Aplicación pentesting y la integridad en seguridad informática

Correlaciones

			Pentesting	Integridad
Rho de Spearman	Pentesting	Coeficiente de correlación	1,000	,610**
		Sig. (bilateral)	.	,004
		N	20	20
	Integridad	Coeficiente de correlación	,610**	1,000
		Sig. (bilateral)	,004	.
		N	20	20

Resultado 2: En la tabla 15 se muestra el resultado obtenido del procesamiento con el SPSS, se observa una buena relación entre las variables que arroja el coeficiente de spearman que es igual a 0.610, el grado de relación entre la variable Aplicación pentesting y la Integridad de la seguridad informática, ambos sugieren que existe una relación significativa y directa con un grado de relación muy buena.

Para contrastar la hipótesis realizamos el análisis del valor sig(bilateral) es igual a 0.004 que es menor a 0.05 por lo que se rechaza la hipótesis nula y se acepta el H_2.

c) Hipótesis especifica H3

H_3: Existe una relación directa entre la aplicación de pentesting y la disponibilidad en la seguridad informática de los equipos tecnológicos de la institución.

H_0: No existe una relación directa entre la aplicación de pentesting y la disponibilidad en la seguridad informática de los equipos tecnológicos de la institución.

Tabla 16

Correlación entre las variables Aplicación pentesting y la Disponibilidad en seguridad informática

Correlaciones

			Pentesting	Disponibilidad
Rho de Spearman	Pentesting	Coeficiente de correlación	1,000	,741**
		Sig. (bilateral)	.	,000
		N	20	20
	Disponibilidad	Coeficiente de correlación	,741**	1,000
		Sig. (bilateral)	,000	.
		N	20	20

**. La correlación es significativa al nivel 0,01 (bilateral).

Resultado 3: En la tabla 16 se muestra el resultado obtenido del procesamiento con el SPSS, se observa una buena relación entre las variables que arroja el coeficiente de spearman que es igual a 0.741, el grado de relación entre la variable Aplicación pentesting y la Disponibilidad de la seguridad informática, ambos sugieren que existe una relación significativa y directa con un grado de relación muy buena.

Para contrastar la hipótesis realizamos el análisis del valor sig(bilateral) es igual a 0.000 que es menor a 0.05 por lo que se rechaza la hipótesis nula y se acepta el H_3.

POR LO TANTO: En la hipótesis general y en las tres pruebas de hipótesis especifica, se encuentra que en su totalidad se acepta la hipótesis alternativa, debido a ello se confirma la aceptación de la hipótesis principal, por lo cual podemos concluir que: si existe una relación directa y significativa entre la aplicación de pentesting y la seguridad informática en los equipos tecnológicos en la Universidad Nacional Santiago Antúnez de Mayolo.

4.3 Discusión de resultados:

Se realiza la comparación con los antecedentes de la investigación considerados en el presente proyecto de investigación, coincidiendo con los resultados obtenidos como podemos apreciar en las conclusiones de los autores de las tesis:

Vera (2020), Concluye que las técnicas de pentesting denominadas sniffing y parameter tempering que son herramientas muy sofisticadas para explotar vulnerabilidades dentro de una empresa, razón por el cual es primordial proteger la infraestructura de red de los ataques e identificar vulnerabilidades. Utilizando técnicas de sniffing se diagnosticaron vulnerabilidades tales como contraseñas y nombres de usuario, se logró interceptar correos electrónicos y espiar conversaciones.

Como solución se implementó reglas de mitigación de captura de paquetes, posterior a la implementación de dicha regla se pudo constatar que el número de paquetes capturados disminuyo de esa manera se logró dar valides a la investigación

Mena (2019) Concluyo que se tiene una relación directa y significativa entre la aplicación de pentesting y la prevención de ataques a los sistemas de industrias San Miguel del Sur-Planta Huaura, año 2019, ambas variables que proyecta el coeficiente de Spearman igual a 0.766. De la misma manera se observa que las variables configuración, variables entre la caja negra y las variables de prueba de criptografía tienen una buena correlación con la prevención de ataques a los sistemas de industrias San Miguel del Sur planta Huara - 2019.

Palacios (2021) Concluyo que la aplicación del pentesting identificar y medir las vulnerabilidades del sistema web de gestión administrativa, en el cual se identificaron 10 vulnerabilidades que ponen en riesgo a la web las cuales se clasificaron en una escala respecto a la gravedad bajo. Moderado, importante y crítico. Al aplicar la pentesting se observa que se redujo las vulnerabilidades del aplicativo web, asimismo también luego de aplicar el control de seguridad se redujo.

En la presente investigación realizada se concluye que existe una relación directa y significativa entre la aplicación de pentesting y la seguridad informática con una alta correlación entre las dos variables que arroja el coeficiente de spearman con un valor igual a 0.779, por ende, ambos sugieren que existe una relación significativa y directa con un grado de relación muy buena. Para contrastar la hipótesis se realiza el análisis de Sig (bilateral) =0.00 que es menor que 0.05 por lo que se niega la hipótesis nula y se acepta la hipótesis general alterna.

CONCLUSIONES

1. De acuerdo al resultado del estudio estadístico se puede concluir que si existe una relación directa y significativa entre la aplicación de pentesting y la seguridad informática en los equipos tecnológicos en la Universidad Nacional Santiago Antúnez de Mayolo que arroja el coeficiente de spearman igual a 0.779 y con un nivel de significancia iguales a sig(bilateral)=0.000 por lo que se rechaza la hipótesis nula y se acepta la hipótesis del investigador. Asimismo, también se realizó la aplicación del pentesting utilizando las pruebas de Owasp, mediante el cual se logró identificar vulnerabilidades en la implementación del servidor Apache con un impacto global bajo de 2.750 y teniendo un nivel alto de probabilidad que es de 6.125. La vulnerabilidad basada en PHP tiene un impacto global bajo de 1.500 y un nivel medio de probabilidad que es de 5. Por lo cual se concluye que ambas vulnerabilidades afectan a la seguridad informática de la entidad debido a que la universidad no cuenta con una normativa o procedimientos para el control de vulnerabilidades.

2. De acuerdo al resultado 1, en esta investigación se observa la relación directa que existe entre la aplicación de pentesting y la confidencialidad en seguridad informática de los equipos tecnológicos de la institución que arroja el coeficiente de spearman igual a 0.556 y con un nivel de significancia de sig(bilateral) =0.011 por lo cual se determina que si existe una relación directa, al aplicar la metodología owasp nos permitió determinar el grado de protección en la que se encuentran las aplicaciones web, al realizar las pruebas de enumerate applications on webserver review webpage y content for information leakage se pudo encontrar información tales como Ips, servers, topología red, urls, métodos post, get, softwares utilizados, que no fueron ocultados por los desarrolladores, se concluye que al aplicar el pentesting se identificó vulnerabilidades que al ser explotadas podría afectar la confidencialidad de la información.

3. De acuerdo al resultado 2, en esta investigación se concluye que existe una relación directa entre la aplicación de pentesting y la integridad en seguridad informática de los equipos tecnológicos de la institución que arroja el coeficiente de spearman igual a 0.610 y con un nivel de significancia de sig(bilateral) igual a 0.004, posterior a la aplicación de las pruebas metodologías inyección Sql, Html y código javascript nos permite determinar que no se encontraron vulnerabilidades en los servidores web por lo cual se concluye que al no encontrar vulnerabilidades las modificaciones a la información en las base de datos y las páginas web de la entidad los realizan personales autorizados.

4. De acuerdo al resultado 3, en esta investigación se pudo realizar la validez de la relación existente entre la aplicación de pentesting y la disponibilidad en la seguridad informática de los equipos tecnológicos de la institución que arroja el coeficiente de spearman igual a 0.741 con un nivel de significancia de sig(bilateral)=0.000, posterior a las pruebas de pentesting realizadas a los servidores Apache se logró identificar vulnerabilidades motivo por el cual las aplicaciones web se encuentran propensos a un posible ataque de DDos afectando la disponibilidad de la información

RECOMENDACIONES

1 Se recomiendo a la Universidad Nacional Santiago Antúnez de Mayolo contar con una guía o normativa de identificación de vulnerabilidades, todas las organizaciones deben comprender su entorno de amenazas y a los riesgos a los que se enfrentan.

2 Para iniciar con las pruebas del pentesting se recomienda utilizar Kali Linux, y para lograr realizar pruebas más sofisticadas se recomienda contar con un ambiente de pentesting auditados y pagados de acuerdo a las necesidades de la entidad.

3 Se recomienda realizar pruebas de la misma manera a los diferentes servicios web, equipos tecnológicos con la cuenta la universidad con el objetivo de identificar vulnerabilidades y comprobar el estado de su seguridad informática.

4 Se recomienda a los encargados de los equipos tecnológicos realizar los estudios para llevar a cabo la implementación de la aplicación de pentesting para prevención de ataques, al aplicar las pruebas de pentesting es importante tener un nivel de ética con el fin de que toda información encontrada que pueda afectar el funcionamiento normal de la entidad se debe informar a la entidad.

5 Al aplicar el pentesting es muy importante contar con conocimientos sobre seguridad informática, las herramientas a utilizarse y las vulnerabilidades ya que no todas pueden ser explotadas debido a que alguna de ellas podría afectar a la entidad.

REFERENCIAS BIBLIOGRÁFICAS

Aldás J. (2022). *Programa de concientización en seguridad de información para pequeñas empresas en la ciudad de puyo*. Ecuador.

Alvarado J. (2017). *Análisis de las vulnerabilidades mediante el uso de phishing para mejorar la seguridad informática de los equipos de cómputo y redes de la municipalidad distrital de independencia*, Perú.

Amiel J. (2017). *Las variables en el método científico*. Perú.

Añazco P., & Ortiz F. (2018). *Análisis de vulnerabilidades en el portal web de una institución de educación superior del ecuador mediante hacking ético*. Ecuador.

Baquero A., & Vásquez B. (2018). *Diseño y desarrollo de hacking ético aplicado a la infraestructura de red, en una empresa dedicada a la fabricación de muebles*. Ecuador.

Cardwell, K. (2019). *Construyendo un Laboratorio Virtual de Pentesting para Pruebas Avanzadas de Pentración* (3ra edicion). Birmingham.

Castro M., Moran G., Navarrete D., Cruzatty J., Mero C., Quimiz C., & Merino M. (2018). I*ntroducción a la seguridad informática y el análisis de vulnerabilidades*. Ecuador.

Corona L., & Foncesa M. (2021). *Acerca del carácter retrospectivo o prospectivo en la investigación científica*. Cuba.

Escrivá G., Romero M., Ramada J., & Onrubia R. (2017). *Seguridad informática.* Madrid: MACMILLAN IBERIA.

Gómez L. (2020). *Test de penetración pentesting aplicado en la empresa megaseguridad para evaluar vulnerabilidades y fallas en el sistema de información. Colombia.*

Gonzále J., Gallardo M., & Chávez M. (2021). *Formulación de los objetivos específicos desde el alcance correlacional en trabajos de investigación*. México: revista Científica Multidisciplinar.

Mena H. (2019). *Aplicación de pentesting y prevención de ataques a los sistemas de industrias san miguel del sur –planta huaura*. Lima.

Vera J. (2020). A*plicación de técnicas de pentesting para determinar vulnerabilidades en la red lan de la empresa csednet de santo domingo*. Ecuador.

González r., montesino r., gainza d. (2021). *Riesgos de Seguridad en Pruebas de Penetración Web.* Cuba.

Guillén L. (2017). *Introducción al Pentesting. Barcelona.* Barcelona,

https://www.researchgate.net/publication/303895876

Inoguchi A., & Macha L. (2017). *Gestión de la ciberseguridad y prevención de los ataques cibernéticos en las pymes del Perú*. Perú.

Kayat G., (2015*). Métodos y Diseños de Investigación Cuantitativa*

Martínez L., & Hernández M. (2021). *Acerca del carácter retrospectivo o prospectivo en la investigación científica*. Cuba.

Palacios L. (2021). *Aplicación de Pentesting en el análisis de vulnerabilidades del sistema web de gestión administrativa de la Empresa DEVHUAYRA SAC*. Perú.

Piñashca J. (2022). *Evaluación de técnicas de hacking ético para analizar la seguridad informática de la municipalidad distrital de los olivos*. Perú.

Romero C. (2018). *Introducción a la Seguridad Informática y el Análisis de Vulnerabilidades*. Alicante: Editorial Área de Innovación y Desarrollo,S.L.

The OWASP Foundation. (2022). Web Application Penetration Testing. Obtenido de https://www.owasp.org/index.php/Web_Application_Penetration_Testing (Consultado el 13 de agosto del 2022).

The OWASP Foundation.(2021). *Lista 2021, Qué ha cambiado en el Top 10 de 2021*. Obtenido de https://owasp.org/Top10/es/A00_2021_Introduction/ (consultado el 14 de agosto del 2022).

Valverde A. (2017). *Los riesgos de seguridad de websites y sus efectos en la gestión de información de medianas empresas de Lima Metropolitana*. Perú.

Vanegas Y. (2021). *Pentesting, ¿Porque es importante para las empresas?* Colombia.

Zafra L. (2017). *Introducción al pentesting*. España

ANEXOS

Matriz de consistencia

PROBLEMA	OBJETIVO	HIPOTESIS	VARIABLES	METODOLIA
General			**Variable Independiente:** Aplicación de la tecnología pentesting	**Tipo de investigación:** • **Según la intervención**: Observacional • **Según la planificación:** Prospectivo • **Según que mide**: Transversal **Nivel de investigación:** • Correlacional **Diseño de investigación:** • No experimental **Población y muestra:** • 4 trabajadores de la OGTISE Unasam • 16 encargados de centro de cómputo de las distintas facultades. **Instrumento de recolección de datos:** • Para ambas variables se usará un cuestionario estructurado
¿De qué manera se relaciona la aplicación de pentesting con la seguridad informática en los equipos tecnológicos de la Universidad Nacional Santiago Antúnez de Mayolo?	Determinar la relación entre la aplicación del pentesting y la seguridad informática en los equipos tecnológicos en la Universidad Nacional Santiago Antúnez de Mayolo.	Existe una relación directa y significativa entre la aplicación del pentesting y la seguridad informática en los equipos tecnológicos en la Universidad Nacional Santiago Antúnez de Mayolo.		
Específicos			**Variable Dependiente:** Seguridad informática	
¿Es posible identificar la relación entre la aplicación de pentesting y la confidencialidad en seguridad informática de los equipos tecnológicos de la institución?	Identificar la relación entre la aplicación de pentesting y la confidencialidad en seguridad informática de los equipos tecnológicos de la institución.	Existe una relación directa entre la aplicación de pentesting y la confidencialidad en seguridad informática de los equipos tecnológicos de la institución.		
¿Es posible conocer la relación entre la aplicación de pentesting y la integridad en seguridad informática de los equipos tecnológicos de la institución?	Conocer la relación entre la aplicación de pentesting y la integridad en seguridad informática de los equipos tecnológicos de la institución.	Existe una relación directa entre la aplicación de pentesting y la integridad en seguridad informática de los equipos tecnológicos de la institución.		
¿Es posible analizar la relación entre la aplicación de pentesting y la disponibilidad en seguridad informática de los equipos tecnológicos de la institución?	Analizar la relación entre la aplicación de pentesting y la disponibilidad en seguridad informática de los equipos tecnológicos de la institución.	Existe una relación directa entre la aplicación de pentesting y la disponibilidad en la seguridad informática de los equipos tecnológicos de la institución.		

Matriz de operacionalización de variables

VARIABLE	DEFINICION CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIONES	INDICADORES	ITEM
VARIABLE INDEPENDIENTE Aplicación de pentesting	(Guillen, 2017, p 5) Define al pentest como un ataque simulado y autorizado contra un sistema informático con el principal objetico de evaluar la seguridad del sistema.	Aplicar el pentesting para identificar vulnerabilidades y relacionarla con la seguridad informativa para ver cómo es su comportamiento cuando crecen o disminuyen las vulnerabilidades.	Recolección de información	Cantidad de información.	P01 y P02 – Encuesta 1
				Cantidad de objetivos	P03 y P04 – Encuesta 1
			Análisis de vulnerabilidad	Cantidad de vulnerabilidades	P05 y P06 – Encuesta 1
				Cantidad de equipos vulnerables	P07, P08 y P09 – Encuesta 1
VARIABLE DEPENDIENTE Seguridad informática	(Gómez, 2006) define a la seguridad informática como una acción que impida la ejecución de operaciones no autorizadas sobre un sistema, cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, integridad y disponibilidad.	La confidencialidad, la integridad y la disponibilidad de la información son los tres pilares fundamentales que se debe proteger en la universidad para el funcionamiento correcto de los diferentes procesos y servicios que brinda la institución.	Confidencialidad de información	Confidencialidad	P10,P11 y P12 – Encuesta 1
			Integridad de información	Integridad	P13, P14 y P15– Encuesta 1
			Disponibilidad de información	Disponibilidad	P16 y P17 – Encuesta 1

Instrumentos de recolección de datos

CUESTIONARIO

PARTE I

Escala de valoración

1	2	3	4	5
Nunca	Casi nunca	A veces	Casi siempre	Siempre

Aplicación de pentesting

N°	Item	1	2	3	4	5
1	¿En la entidad se cumple con las normativas o procedimientos para el control de vulnerabilidades?					
2	¿En la entidad el área responsable y especializado es quien gestiona los cambios en los equipos tecnológicos?					
3	¿Los usuarios generalmente hacen uso de las conexiones de red inalámbricas?					
4	¿Usted tiene a su cargo equipos informáticos (servidores, ordenadores, router, switch)?					
5	¿En los equipos informáticos que usted tiene a cargo utiliza programas originales?					
6	¿Se utiliza un software de firewall en los ordenadores?					
7	¿En la entidad se ha tenido problema con algún software malicioso?					
8	¿Otros usuarios pueden instalar y desinstalar software en los equipos informáticos que usted tiene a cargo?					
9	¿Se realizan los mantenimientos en los equipos informáticos?					

PARTE II

Escala de valoración

1	2	3	4	5
Nunca	Casi nunca	A veces	Casi siempre	Siempre

Seguridad Informática

N°	Item	1	2	3	4	5
1	¿En la entidad se utiliza la autenticación de dos factores?					
2	¿Se utiliza las políticas de seguridad para definir cómo debe y puede ser tratada la información?					
3	¿Existen problemas de manipulación (manejo no autorizado) de información en la organización?					
4	¿Generalmente realizan copias de seguridad de su información en la organización?					
5	¿En la entidad se hace uso de las soluciones de control de acceso?					
6	¿Se han tenido problemas de seguridad donde se vea comprometida o alterada la información de la empresa o usuarios en los últimos años?					
7	¿En la organización se hace uso de las soluciones de backup y recuperación?					
8	¿Cuándo un equipo informático tiene fallas se soluciona rápidamente?					

Evaluación de expertos: Se utilizó la presente evaluación para validación de los expertos del instrumento elaborado.

UNIVERSIDAD NACIONAL SANTIAGO ANTÚNEZ DE MAYOLO

FACULTAD DE CIENCIAS

ESCUELA PROFESIONAL DE INGENIERIA DE SISTEMAS E INFORMÁTICA

Huaraz 03 de noviembre del 2022

SEÑOR:

Yo, Calvo Cacha Jhunior Leonel, identificado con DNI N° 71533965, Bachiller en Ingeniería de Sistemas e Informática, me dirijo a usted con la finalidad de solicitar su valiosa colaboración en la validación de contenido de los ítems que conforman el instrumento de recolección de datos que utilizaré para recabar la información requerida en la investigación titulada "APLICACIÓN DE PENTESTING Y LA SEGURIDAD INFORMÁTICA EN LOS EQUIPOS TECNOLÓGICOS DE LA UNIVERSIDAD NACIONAL SANTIAGO ANTÚNEZ DE MAYOLO, 2022". Por lo cual, facilito la documentación pertinente:

1. Matriz de Operacionalización de Variables.
2. Matriz de Consistencia
3. Instrumento de Recolección de Datos.

Por su experiencia profesional y méritos académicos me permito para la validación de dicho instrumento.

Agradezco de antemano su valioso aporte.

Atentamente

Jhunior Leonel Calvo Cacha
DNI N°: 71533965

INFORME DE OPINIÓN DE EXPERTO

I. DATOS DEL EXPERTO

APELLIDOS Y NOMBRES:

PROFESIÓN:

GRADO ACADÉMICO:

MENCIÓN:

CENTRO LABORAL:

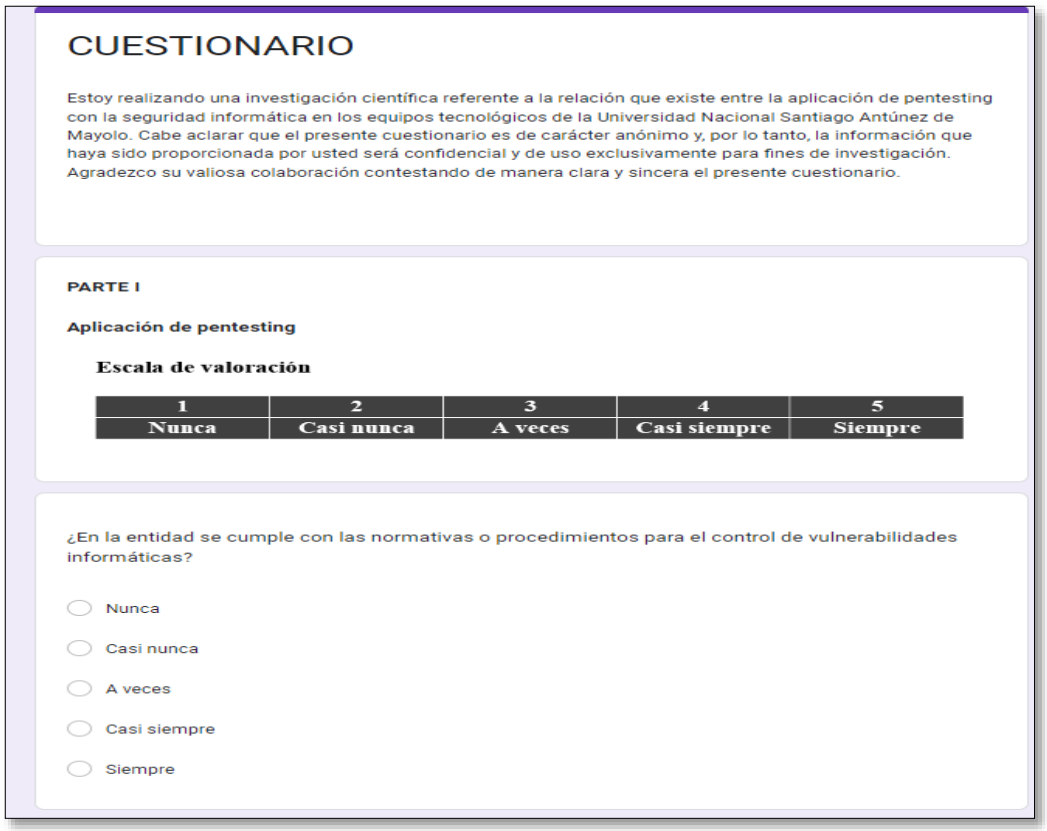
CARGO:

II. MATRIZ DE EVALUACIÓN DEL INSTRUMENTO DE RECOLECCIÓN DE DATOS

Indicador	Criterio	Deficiente 0 - 20	Regular 21 - 40	Bueno 41 - 60	Muy Bueno 61 - 80	Excelente 81 - 100
Claridad	Está formulado con un lenguaje claro.					
Objetividad	No presenta sesgo ni induce a respuestas.					
Actualidad	Está de acuerdo con los avances de la teoría, ciencia y tecnología.					
Organización	Existe una organización lógica y coherente de los ítems.					
Suficiencia	Comprende las dimensiones de la investigación en cantidad y calidad.					
Intencionalidad	Adecuado para establecer asociación.					
Consistencia	Basado en aspectos teóricos y científicos.					
Coherencia	Hay relación entre variables, dimensiones e indicadores.					
Metodología	El instrumento se relaciona con el método planteado en el proyecto.					

Huaraz, 01 de noviembre del 2022

Ejecución de la encuesta: Una vez validado el instrumento se utilizó el formulario de Google para la recolección de datos.



CUESTIONARIO

Estoy realizando una investigación científica referente a la relación que existe entre la aplicación de pentesting con la seguridad informática en los equipos tecnológicos de la Universidad Nacional Santiago Antúnez de Mayolo. Cabe aclarar que el presente cuestionario es de carácter anónimo y, por lo tanto, la información que haya sido proporcionada por usted será confidencial y de uso exclusivamente para fines de investigación. Agradezco su valiosa colaboración contestando de manera clara y sincera el presente cuestionario.

PARTE I

Aplicación de pentesting

Escala de valoración

1	2	3	4	5
Nunca	Casi nunca	A veces	Casi siempre	Siempre

¿En la entidad se cumple con las normativas o procedimientos para el control de vulnerabilidades informáticas?

- Nunca
- Casi nunca
- A veces
- Casi siempre
- Siempre

Resultados de la encuesta: Como resultado de la encuesta realizada se obtuvo los datos para el tratamiento estadístico de investigación científica.

P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16	P17
Casi siempre	Siempre	Casi nunca	Casi siempre	Casi siempre	A veces	A veces	Casi nunca	Casi siempre	Casi siempre	A veces	Casi siempre	Casi siempre	Siempre	A veces	Siempre	Casi nunca
A veces	Casi siempre	A veces	Casi siempre	Casi siempre	A veces	Casi nunca	Casi nunca	Casi siempre	Casi nunca	Nunca	A veces	Casi siempre	Casi siempre	Casi nunca	Casi siempre	Casi siempre
A veces	A veces	Casi nunca	Casi siempre	Casi nunca	Casi nunca	Casi nunca	Casi nunca	Casi nunca	Nunca	Casi nunca	A veces	Casi nunca	Casi nunca	Casi nunca	Casi nunca	Casi nunca
A veces	Casi siempre	A veces	Siempre	Siempre	A veces	Siempre	Casi nunca	Casi siempre	Nunca	A veces	A veces	Siempre	A veces	Casi nunca	Siempre	Siempre
A veces	Casi siempre	Casi nunca	Casi siempre	A veces	A veces	Casi nunca	Casi nunca	Casi siempre	A veces	Casi siempre	A veces	Casi siempre	A veces	A veces	A veces	Casi siempre
Siempre	Casi siempre	A veces	Siempre	Siempre	Siempre	Casi siempre	Casi nunca	Casi siempre	Casi siempre	Casi nunca	Siempre	Casi siempre	A veces	Casi nunca	Casi siempre	Casi siempre
Casi siempre	Siempre	Casi nunca	Casi siempre	Casi nunca	A veces	Casi nunca	Casi nunca	Casi siempre	A veces	A veces	Casi siempre	Siempre	Casi siempre	A veces	Casi siempre	Siempre
Casi siempre	Siempre	A veces	Siempre	Siempre	Casi siempre	Casi siempre	Casi nunca	Siempre	Casi siempre	Casi siempre	Casi siempre	Siempre	Siempre	Casi nunca	Casi siempre	Siempre
A veces	Casi siempre	Casi nunca	Siempre	Casi siempre	Casi siempre	A veces	Casi nunca	Siempre	Casi nunca	Casi siempre	A veces	Casi siempre	Siempre	Casi nunca	Casi siempre	A veces
Siempre	Casi siempre	Casi nunca	Casi siempre	Siempre	Siempre	Casi siempre	Casi nunca	Casi siempre	A veces	Casi siempre	Siempre	Casi siempre	Casi siempre	A veces	Casi siempre	Siempre
A veces	Casi siempre	A veces	Casi siempre	Casi siempre	Casi nunca	Nunca	Casi nunca	A veces	Nunca	A veces	A veces	Casi siempre	A veces	Casi nunca	A veces	A veces
Siempre	A veces	Casi nunca	Casi siempre	Casi siempre	A veces	A veces	Nunca	Siempre	Casi siempre	Siempre	Siempre	A veces	Casi siempre	Casi nunca	A veces	Siempre
Casi nunca	Casi siempre	Casi nunca	Casi siempre	A veces	A veces	Casi nunca	Casi nunca	Casi siempre	Casi siempre	A veces	Casi nunca	A veces	Casi siempre	A veces	A veces	Casi siempre
Casi nunca	Casi siempre	Casi nunca	Siempre	A veces	Casi nunca	Casi nunca	Casi nunca	Siempre	A veces	A veces	Casi nunca	A veces	Casi nunca	A veces	Casi nunca	Siempre
Casi nunca	A veces	Casi nunca	Siempre	Casi siempre	A veces	Nunca	Nunca	Casi siempre	Casi siempre	Casi siempre	Casi nunca	A veces	A veces	Casi nunca	Casi nunca	Siempre
A veces	Siempre	A veces	Siempre	A veces	Casi nunca	Nunca	Casi nunca	A veces	Nunca	A veces	A veces	A veces	Casi nunca	Casi nunca	A veces	Casi siempre
Siempre	Siempre	Casi nunca	Casi siempre	Siempre	Casi siempre	Casi siempre	Nunca	Siempre	Casi siempre	Siempre	Siempre	Siempre	Siempre	Casi nunca	Siempre	Casi siempre
Casi siempre	Casi siempre	A veces	Siempre	A veces	Casi nunca	Casi nunca	Casi nunca	A veces	Casi nunca	Casi siempre	Casi siempre	A veces	A veces	Casi nunca	Casi siempre	Siempre
Siempre	A veces	Casi nunca	Casi siempre	Casi siempre	A veces	Casi siempre	Nunca	Siempre	Casi siempre	Siempre	Siempre	A veces	Casi siempre	Casi nunca	A veces	Siempre
Casi nunca	Siempre	Casi nunca	Siempre	A veces	Casi nunca	Nunca	Nunca	Siempre	Siempre	A veces	Casi nunca	A veces	A veces	A veces	Casi nunca	Casi siempre

Validación de expertos

INFORME DE OPINIÓN DE EXPERTO

I. DATOS DEL EXPERTO

APELLIDOS Y NOMBRES: Miguel Angel Silva Zapata

PROFESIÓN: Ingeniero Académico

GRADO ACADÉMICO: Maestría en ciencias e ingeniería

MENCIÓN: Auditoria y seguridad informática

CENTRO LABORAL: UNASAM

CARGO: DOCENTE

II. MATRIZ DE EVALUACIÓN DEL INSTRUMENTO DE RECOLECCIÓN DE DATOS

Indicador	Criterio	Deficiente 0 - 20	Regular 21 - 40	Bueno 41 - 60	Muy Bueno 61 - 80	Excelente 81 - 100
Claridad	Está formulado con un lenguaje claro.					x
Objetividad	No presenta sesgo ni induce a respuestas.					X
Actualidad	Está de acuerdo con los avances de la teoría, ciencia y tecnología.				X	
Organización	Existe una organización lógica y coherente de los ítems.				X	
Suficiencia	Comprende las dimensiones de la investigación en cantidad y calidad.				x	x
Intencionalidad	Adecuado para establecer asociación.					x
Consistencia	Basado en aspectos teóricos y científicos.					X
Coherencia	Hay relación entre variables, dimensiones e indicadores.					X
Metodología	El instrumento se relaciona con el método planteado en el proyecto.					x

Huaraz, 03 de noviembre del 2022

Ing. Miguel Angel Silva Zapata
N° de DNI:03664700

INFORME DE OPINIÓN DE EXPERTO

I. DATOS DEL EXPERTO

APELLIDOS Y NOMBRES: Mendoza López Angel D.

PROFESIÓN: Ciencias Físicas Y Matemáticas

GRADO ACADÉMICO: Doctor

MENCIÓN: Salud publica

CENTRO LABORAL: UNASAM

CARGO: Dir. Departamento

II. MATRIZ DE EVALUACIÓN DEL INSTRUMENTO DE RECOLECCIÓN DE DATOS

Indicador	Criterio	Deficiente 0 - 20	Regular 21 - 40	Bueno 41 - 60	Muy Bueno 61 - 80	Excelente 81 - 100
Claridad	Está formulado con un lenguaje claro.					x
Objetividad	No presenta sesgo ni induce a respuestas.					X
Actualidad	Está de acuerdo con los avances de la teoría, ciencia y tecnología.				X	
Organización	Existe una organización lógica y coherente de los ítems.					x
Suficiencia	Comprende las dimensiones de la investigación en cantidad y calidad.				X	
Intencionalidad	Adecuado para establecer asociación.				X	x
Consistencia	Basado en aspectos teóricos y científicos.					X
Coherencia	Hay relación entre variables, dimensiones e indicadores.					X
Metodología	El instrumento se relaciona con el método planteado en el proyecto.				X	

Huaraz, 03 de noviembre del 2022

Dr. Ángel Mendoza López
N° de DNI: 17824554

INFORME DE OPINIÓN DE EXPERTO

I. DATOS DEL EXPERTO

APELLIDOS Y NOMBRES: Maldonado Leyva Hugo Walter

PROFESIÓN: Lic. Estadística e Informática

GRADO ACADÉMICO: Maestro

MENCIÓN: Gerencia de proyectos y programas sociales

CENTRO LABORAL: UNASAM

CARGO: Docente

II. MATRIZ DE EVALUACIÓN DEL INSTRUMENTO DE RECOLECCIÓN DE DATOS

Indicador	Criterio	Deficiente 0 - 20	Regular 21 - 40	Bueno 41 - 60	Muy Bueno 61 - 80	Excelente 81 - 100
Claridad	Está formulado con un lenguaje claro.				X	
Objetividad	No presenta sesgo ni induce a respuestas.					x
Actualidad	Está de acuerdo con los avances de la teoría, ciencia y tecnología.				x	
Organización	Existe una organización lógica y coherente de los ítems.				X	
Suficiencia	Comprende las dimensiones de la investigación en cantidad y calidad.					x
Intencionalidad	Adecuado para establecer asociación.				X	x
Consistencia	Basado en aspectos teóricos y científicos.					x
Coherencia	Hay relación entre variables, dimensiones e indicadores.					X
Metodología	El instrumento se relaciona con el método planteado en el proyecto.				X	

Huaraz, 03 de noviembre del 2022

Lic. Maldonado Leyva Hugo Walter
N° de DNI: 31659531

Evidencia de encuesta y entrevista:

UNIVERSIDAD NACIONAL
SANTIAGO ANTÚNEZ DE MAYOLO

FACULTAD DE CIENCIAS

ESCUELA PROFESIONAL DE INGENIERIA DE SISTEMAS E INFORMÁTICA

ENTREVISTA AL PERSONAL DE LA OGTISE

Pentesting y seguridad informática

Análisis de vulnerabilidades

Pregunta 1:

¿En la entidad se realizan mantenimientos a los equipos informáticos y cada cuanto tiempo lo hacen, en el mantenimiento que realizan también consideran la actualización de los softwares o la migración a las últimas versiones?

Pregunta 2:

¿La entidad cuenta con una guía, normativas o procedimientos para actuar frente a una amenaza y cuál es el primer movimiento que ustedes realizan tras recibir una alerta sobre amenazas o una vulnerabilidad informática?

Confidencialidad, Disponibilidad e Integridad

Pregunta 3:

¿En la entidad se hace uso de control de acceso y que tipos de soluciones utilizan, se hacen uso de políticas de seguridad para definir como debe y puede ser tratada la información?

Pregunta 4:

¿En la entidad se hace uso de las soluciones de backup o recuperación de datos, cuando un equipo informático de la entidad tiene fallas se soluciona rápidamente?