UTMACH

FACULTAD DE INGENIERÍA CIVIL

CARRERA DE INGENIERÍA DE SISTEMAS

EVALUACIÓN DE RIESGOS INFORMÁTICOS EN GRUPO GUERRERO PORTILLA BASADO EN LOS PRINCIPIOS DE LA METODOLOGÍA OSSTMM

ASENCIO VEGA JOFFRE WLADIMIR
INGENIERO DE SISTEMAS

MACHALA
2022

UTMACH

FACULTAD DE INGENIERÍA CIVIL

CARRERA DE INGENIERÍA DE SISTEMAS

EVALUACIÓN DE RIESGOS INFORMÁTICOS EN GRUPO GUERRERO PORTILLA BASADO EN LOS PRINCIPIOS DE LA METODOLOGÍA OSSTMM

ASENCIO VEGA JOFFRE WLADIMIR
INGENIERO DE SISTEMAS

MACHALA
2022

UTMACH

FACULTAD DE INGENIERÍA CIVIL

CARRERA DE INGENIERÍA DE SISTEMAS

TRABAJO TITULACIÓN
PROPUESTAS TECNOLÓGICAS

EVALUACIÓN DE RIESGOS INFORMÁTICOS EN GRUPO GUERRERO PORTILLA BASADO EN LOS PRINCIPIOS DE LA METODOLOGÍA OSSTMM

ASENCIO VEGA JOFFRE WLADIMIR
INGENIERO DE SISTEMAS

CARTUCHE CALVA JOFFRE JEORWIN

MACHALA, 27 DE SEPTIEMBRE DE 2022

MACHALA
2022

tesis

INFORME DE ORIGINALIDAD

7%	7%	0%	2%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	www.produccioncientificaluz.org Fuente de Internet	1%
2	cedigec.fca.unam.mx Fuente de Internet	<1%
3	Submitted to Universidad Cesar Vallejo Trabajo del estudiante	<1%
4	www.theibfr.com Fuente de Internet	<1%
5	Submitted to Universidad Nacional Abierta y a Distancia, UNAD,UNAD Trabajo del estudiante	<1%
6	bibdigital.epn.edu.ec Fuente de Internet	<1%
7	repository.unad.edu.co Fuente de Internet	<1%
8	vsip.info Fuente de Internet	<1%
9	novasinergia.unach.edu.ec Fuente de Internet	

CLÁUSULA DE CESIÓN DE DERECHO DE PUBLICACIÓN EN EL REPOSITORIO DIGITAL INSTITUCIONAL

El que suscribe, ASENCIO VEGA JOFFRE WLADIMIR, en calidad de autor del siguiente trabajo escrito titulado EVALUACIÓN DE RIESGOS INFORMÁTICOS EN GRUPO GUERRERO PORTILLA BASADO EN LOS PRINCIPIOS DE LA METODOLOGÍA OSSTMM, otorga a la Universidad Técnica de Machala, de forma gratuita y no exclusiva, los derechos de reproducción, distribución y comunicación pública de la obra, que constituye un trabajo de autoría propia, sobre la cual tiene potestad para otorgar los derechos contenidos en esta licencia.

El autor declara que el contenido que se publicará es de carácter académico y se enmarca en las dispociones definidas por la Universidad Técnica de Machala.

Se autoriza a transformar la obra, únicamente cuando sea necesario, y a realizar las adaptaciones pertinentes para permitir su preservación, distribución y publicación en el Repositorio Digital Institucional de la Universidad Técnica de Machala.

El autor como garante de la autoría de la obra y en relación a la misma, declara que la universidad se encuentra libre de todo tipo de responsabilidad sobre el contenido de la obra y que asume la responsabilidad frente a cualquier reclamo o demanda por parte de terceros de manera exclusiva.

Aceptando esta licencia, se cede a la Universidad Técnica de Machala el derecho exclusivo de archivar, reproducir, convertir, comunicar y/o distribuir la obra mundialmente en formato electrónico y digital a través de su Repositorio Digital Institucional, siempre y cuando no se lo haga para obtener beneficio económico.

Machala, 27 de septiembre de 2022

ASENCIO VEGA JOFFRE WLADIMIR
0706427598

DEDICATORIA

El actual trabajo va dedicado con mucho esmero a cada integrante de mi familia, a quienes están y a los que por factores del destino ya no, cada uno de ellos que son un pilar importante en mi formación como profesional, quienes con buenos valores, principios y costumbres han inculcado en la persona que hoy soy.

Dedicar a los colegas y compañeros que este trayecto me ha brindado, porque han demostrado que la camaradería y el trabajo en equipo puede llevar a realizar cosas extraordinarias.

A cada uno de los docentes que, con sus conocimientos han sido luz y guía en todos estos años, quienes se han vuelto amigos y de la manera más amena nos han brindado cátedra e impartido conocimientos.

Joffre Wladimir Asencio Vega

AGRADECIMIENTO

Es oportuno agradecer a cada persona que ha sido parte de este proceso, que de alguna manera u otra ha sido parte de este logro, compañeros, docentes, amistades, colegas que nos deja y forma la Universidad Técnica de Machala, un sin número de personas que de forma directa o indirecta hacen esto posible.

Un rotundo agradecimiento al Ingeniero Joffre Cartuche Calva por la dedicación, entrega y compromiso en cada una de las interrogantes y necesidades que se presentaban para la elaboración de este trabajo.

Joffre Wladimir Asencio Vega

RESUMEN

Actualmente la seguridad a nivel de redes informáticas en pequeñas y medianas empresas, no se les brinda el interés o atención necesaria como correspondería para salvaguardar su información y tráfico de datos, es por esto que han surgido diversos inconvenientes a nivel de seguridad correspondiente a infraestructura de red y lo que con ellas conllevan, sean estas las comunicaciones entre dispositivos, el manejo de información, el enlace entre un sistema servidor y los puntos de uso etc. Manejar planes de contingencia o mejora ha demostrado ser un método preventivo y correctivo a la vez para optimizar y proteger infraestructuras de redes empresariales, independientemente del tamaño geográfico en el cual se establezca.

En base a estos casos, es oportuno que se realizar una evaluación, estudio o análisis correspondiente a los puntos necesarios que manejan dichas infraestructuras con la finalidad de encontrar puntos de quiebre por los cuales podría verse afectada la institución, es por eso que el presente trabajo tiene como punto principal, realizar una evaluación a la infraestructura de red de Grupo Guerrero Portilla con la finalidad de analizar y determinar posibles riesgos informáticos a nivel de estructura de red basándose en los principios de la metodología OSSTMM, para con los resultados de dicho análisis desarrollar un plan de mejora, optimización, prevención o contingencia con la finalidad de establecer un fortalecimiento de dicha intranet.

Es de suma importancia mencionar que la red de una empresa u organización es primordial para que ella pueda funcionar de maneras óptimas ya que de la fiabilidad de los datos e información que reciban los usuarios y todos los involucrados directa e indirectamente con la institución depende de que la misma se encuentre en las mejores condiciones posibles, es por ello que brindar un buen sistema de infraestructura de red es una inversión necesaria.

Es por ende, que la presente propuesta tecnológica titulada Evaluación de Riesgos Informáticos en Grupo Guerrero Portilla basado en los Principios de la metodología OSSTMM (Manual de la Metodología Abierta de Testeo de Seguridad) se enfoca en la recolección de datos mediante herramientas de

monitoreo, testeo y análisis tales como PRTG Network Monitor, Advanced IP Scanner, Winbox, para con ello involucrar los resultados en base a los puntos que propone la metodología; siendo Seguridad de la Información, Seguridad de los Procesos, Seguridad en las Tecnologías de Internet, Seguridad en las Comunicaciones, Seguridad Inalámbrica y Seguridad Física; abarcando cada uno de ellos en los subpuntos que tengan concordancia con la necesidad y caso de estudio que posea la empresa.

El alcance de este trabajo es analizar los datos recolectados con las diversas herramientas y con ello evaluar la situación en la cual se encuentra la empresa, mediante los resultados, determinar por rangos de importancia o gravedad los puntos de quiebre en los cuales se debe reforzar la seguridad mediante un plan de mejora o contingencia enfocado directamente a la necesidad presentada siguiendo los principios más relevantes de la metodología OSSTMM. Siendo así, se simuló la intranet existente, a la par de mantener un monitoreo, testeo y sondeo de la infraestructura con enfoque a los dispositivos más relevantes dentro de la institución, recolectando información sobre el comportamiento que tomaba la misma, se emparejó dicha información con los principios de la metodología según correspondían y con ello se establecieron las propuestas de optimización de seguridad que es la finalidad del prototipo.

Realizado el plan de contingencia, optimización o mejora; se llevó a cabo la evaluación de factibilidad haciendo uso de cinco de las siete fases de análisis que propone la Norma ISO 27001 para la Gestión de la Seguridad de la Información (Identificación de Activos de Información, Identificación de Vulnerabilidades, Identificación de Amenazas, Identificación de Riesgos y Plan de Tratamiento del Riesgo), concluyendo como óptima y oportuna la generación del ya mencionado plan para mantener y/o reforzar la seguridad a nivel de infraestructura de red.

Palabras clave: Seguridad, fiabilidad, Infraestructura de Red, OSSTMM, Riesgos Informáticos.

ABSTRACT

Currently, security at the level of computer networks in small and medium-sized companies is not given the necessary interest or attention as it should be to safeguard their information and data traffic, which is why various inconveniences have arisen at the level of security corresponding to infrastructure of network and what they entail, whether these are communications between devices, information management, the link between a server system and points of use, etc. Managing contingency or improvement plans has proven to be a preventive and corrective method at the same time to optimize and protect business network infrastructures, regardless of the geographical size in which it is established.

Based on these cases, it is appropriate to carry out an evaluation, study or analysis corresponding to the necessary points that manage said infrastructures in order to find breaking points by which the institution could be affected, that is why the present work Its main point is to carry out an evaluation of the network infrastructure of Grupo Guerrero Portilla in order to analyze and determine possible computer risks at the network structure level based on the principles of the OSSTMM methodology, in order to develop the results of said analysis. an improvement, optimization, prevention or contingency plan in order to establish a strengthening of said intranet.

It is very important to mention that the network of a company or organization is essential for it to function optimally, since the reliability of the data and information received by users and all those directly and indirectly involved with the institution depends on the fact that it is in the best possible conditions, which is why providing a good network infrastructure system is a necessary investment.

It is therefore that the present technological proposal entitled Evaluation of Computer Risks in Grupo Guerrero Portilla based on the Principles of the OSSTMM methodology (Manual of the Open Methodology of Security Testing) focuses on data collection through monitoring tools, testing and analyzes such as PRTG Network Monitor, Advanced IP Scanner, Winbox, in order to include

the results based on the points proposed by the methodology; being Information Security, Process Security, Internet Technology Security, Communications Security, Wireless Security and Physical Security; covering each one of them in the subpoints that are consistent with the need and case study that the company has.

The scope of this work is to analyze the data collected with the various tools and thereby evaluate the situation in which the company is, through the results, determine by ranges of importance or severity the breaking points in which the company should be reinforced. security through an improvement or contingency plan focused directly on the need presented following the most relevant principles of the OSSTMM methodology. Thus, the existing intranet was simulated, while maintaining a monitoring, testing and polling of the infrastructure with a focus on the most relevant devices within the institution, collecting information on the behavior that it took, said information was matched with the principles of the methodology as they corresponded and with it the security optimization proposals were established, which is the purpose of the prototype.

The contingency, optimization or improvement plan has been carried out; The feasibility evaluation was carried out using five of the seven phases of analysis proposed by the ISO 27001 Standard for Information Security Management (Identification of Information Assets, Identification of Vulnerabilities, Identification of Threats, Identification of Risks and Risk Treatment Plan), concluding as optimal and timely the generation of the aforementioned plan to maintain and/or reinforce security at the network infrastructure level.

Keywords: Security, reliability, network infrastructure, OSSTMM, computer risks.

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

GLOSARIO

OSSTMM: Manual de Metodología Abierta de Testeo de Seguridad.

Testeo: Acción de realizar pruebas, correspondiente al funcionamiento de un sistema establecido.

Infraestructura de Red: Refiérase al diseño físico del sistema de conectividad, cableada e inalámbrica que conectan diversos puntos de red desde un sistema distribuidor de comunicación.

Riesgo: Es la probabilidad o posibilidad de que se ejecute un suceso que conlleve un contratiempo, pérdida o incidente.

Amenaza: Es el instrumento, individuo, acto o acción que podría inicializar o ser posible causa de un riesgo.

Vulnerabilidad: Considerado un punto de quiebre o de posible suceso de un riesgo ante alguna amenaza.

Plan de Contingencia: Es la documentación o guía planteada y estructurada con la finalidad de evitar, prever, reducir o eliminar riesgos, amenazas y vulnerabilidades existentes.

INTRODUCCIÓN

En la actualidad, se ha incrementado los ataques a nivel informático, afectando con ello a pequeñas y grandes empresas, de igual manera como a organizaciones; lo que ha ocasionado que exista mayor demanda en el requerimiento de sistemas de detección de intrusos y monitoreo de la red interna que manejan dichas organizaciones[1].

Además, la correcta comunicación dentro de una institución a nivel de puntos de red o periféricos, es la base esencial para el óptimo funcionamiento y operación de la misma. Precisamente siendo Grupo Guerrero Portilla quien presenta problemáticas físicas y sistemáticas a nivel de infraestructura de red, sabiendo además que los riesgos informáticos son amenazas y vulnerabilidades que afectan en todos los aspectos a los usuarios como empresas, y las consecuencias pueden ser muy graves conforme a la relación que existe con la información que se está manejando[2].

Los principios de la Metodología OSSTMM (Manual de la Metodología Abierta de Testeo de Seguridad) se caracterizan por evaluar diversos puntos de vista y parámetros a nivel de estructuras de red[3], lo que brinda un amplio campo de evaluación para obtener resultados, mismos resultados que otorgan datos que permiten optar por decisiones de optimización a nivel de seguridad, logrando con ello un robustecimiento de dicha seguridad en infraestructuras de red.

El siguiente trabajo está direccionado al análisis de vulnerabilidades o riesgos informáticos que existan dentro de la infraestructura de red de Grupo Guerrero Portilla tomando como base los Principios de la Metodología OSSTMM. Dentro del presente documento se encuentra una segmentación apropiada por capítulos, los cuales abarcan puntos esenciales para el desarrollo del proyecto.

Capítulo 1: Se enfoca directamente en un análisis de sistema actual con respecto a las necesidades que se pueden presentar en empresas o instituciones a nivel de mantener o mejorar la seguridad de su intranet.

Capítulo 2: En este capítulo se da parte de conocimiento al desarrollo del prototipo como tal, basándose en la metodología propuesta, brindar un

apartado teórico el cual será base para la aplicación de ejecución y evaluación de pruebas o análisis de datos que comprenden al prototipo.

Capítulo 3: En este capítulo se registran las evidencias, resultados, valoraciones y puestas en marcha de la propuesta que se brinda al prototipo, además de las conclusiones y recomendaciones que se otorgan al finalizar.

1. CAPÍTULO I. DIAGNÓSTICO DE NECESIDADES Y REQUERIMIENTOS

1.1. Ámbito de Aplicación: descripción del contexto y hechos de interés

Es notorio que, la tecnología y los dispositivos electrónicos Smart se encuentran en auge conforme a la vanguardia, se ha hecho habitual el uso de datos en diferentes lugares; sean en empresas como en cuentas bancarias o a su vez en dispositivos de uso personal[4], hay que tener en cuenta que el manejo de información desde cualquier dispositivo electrónico tiende a ser vulnerable al momento de no tomar ciertas precauciones que reduzcan la probabilidad que sufran un ultrajamiento o sabotaje de la misma.

Es muy importante recalcar que así como la tecnología avanza, así mismo se generan o se crean nuevas alternativas de acceder de manera fraudulenta, ilegal y anti ética a la información que los usuarios tales como entidades públicas o privadas, entidades gubernamentales, comerciales, de logística y finalmente el usuario final como propietario de un dispositivo en el cual almacena la más mínima información, sea esta personal o abierta que sea de suma importancia, por lo que de igual manera se ha ido evolucionando en la recopilación de metodologías o procesos que minimicen el margen de vulnerabilidad que posee cada dirección de información.

Sabiendo que los riesgos informáticos son amenazas y vulnerabilidades que afectan en todos los aspectos a los usuarios como empresas, y las consecuencias pueden ser muy graves conforme a la relación que existe con la información que se está manejando[2].

La seguridad que posea un sistema informático depende de varios factores, uno de ellos es el correcto análisis o evaluación de riesgos que existan dentro de una sociedad, infraestructura, departamento o equipo, independientemente de cuál sea la finalidad o actividades que realicen cada uno de ellos, hay que salvaguardar la información que en ellos se registre, haciéndolo de esta forma, convirtiéndolo en una solución o corrección preventiva.

En la actualidad, la seguridad informática se encuentra en apogeo por los diversos y variados ataques cibernéticos que existen a bases de datos, en base a estos sucesos, casos y necesidades de prevención se implementará en este

trabajo una evaluación de riesgos basándose en los principios de la metodología OSSTMM, con ayuda de herramientas que permitan plasmar resultados y evidencia de dicha valoración.

El alcance de este proyecto es segmentar por cada principio, los errores existentes dentro de la empresa y plantear optimas soluciones para con ello elevar el nivel de seguridad para la información y la comunicación entre los diversos puntos interconectados en red.

1.2. Establecimiento de requerimientos

Para la inicialización de la evaluación es necesarios saber el enfoque de cada uno de los principios con respecto a la infraestructura que posee la empresa, con el fin de dirigir el punto de atención a las zonas con mayor vulnerabilidad con respecto a sufrir algún riesgo.

El proyecto se encuentra distribuido de la siguiente manera:

- Segmentación de Principios, etapa que será considerada como la fase de inicio, en la cual se deberá evaluar con uso de herramientas visuales y software según la dependencia de cada uno de dichos principios.
- Recolección de Información, se establece como la etapa de mayor importancia, en ella se registrará los datos que se obtengan según la demanda que requiere cada principio.
- Análisis de Resultados, una vez concluida la etapa de recolección, se procede a analizar dicha información para con ello determinar los puntos de riesgo que posee la empresa.
- Planteamiento de Propuesta, etapa considerada como final, basado en los resultados se planteará la opción más óptima para la cual mitigar o reducir los riesgos que han sido detectados mediante la evaluación.

1.3. Justificación de requerimiento a satisfacer

Al hablar de Infraestructura de Red, es referirse a diversos puntos conectados entre sí. Mediante la intermediación de un dispositivo comunicador, sea un switch o un router, la comunicación y accesibilidad existente entre cada uno de los equipos y dispositivos que se encuentran relacionados dentro de una misma red, permitiendo la transferencia de archivos, comunicación y vinculación de trabajo.

La seguridad dentro de una infraestructura de red, o en otras palabras entre los equipos y/o dispositivos que se encuentren interconectados entre sí, es un tema que es de suma importancia a nivel que se encuentra comprometida la información que por dicho medio transita o se genera.

De allí nace la necesidad para la empresa el recopilar los riesgos existentes, para con ello reducirlos o mitigarlos, brindando con ello una satisfacción tanto personal, como una seguridad laboral que será una base para nuevas comunicaciones en distintos puntos que proyecte establecerse en un determinado tiempo.

Lo que se propone en el siguiente proyecto es, en realizar una evaluación basada en los principios de la Metodología OSSTMM (Manual de la Metodología Abierta de Testeo de Seguridad), para con ello determinar riesgos existentes dentro de la empresa y por ende mitigar o generar un plan de contingencia en caso de un ataque. La metodología propone análisis en los siguientes puntos: Seguridad de la Información, Seguridad de los Procesos, Seguridad en las Tecnologías de Internet, Seguridad en las Comunicaciones, Seguridad Inalámbrica y Seguridad Física.

Conociendo que cada uno de los puntos previamente mencionados abarcan sus propios subpuntos de análisis, con el fin de determinar y generar un resultado que permita incrementar la seguridad dentro de los datos hacia la empresa.

2. CAPÍTULO II. DESARROLLO DEL PROTOTIPO

2.1. Definición del prototipo tecnológico

El sistema que se utiliza para la evaluación de la infraestructura de red y sus apéndices, se caracteriza en la resolución y notificación de eventos en tiempo real y programado mediante el sondeo y monitoreo de cada uno de los dispositivos que se encuentren conectados entre sí mediante un sistema de red compartido, utilizando herramientas y software dedicado que se empelan para realizar dichas tareas, mismas que permiten fundamentar y sostener conclusiones a través de la evaluación de dichos resúmenes brindados.

La siguiente propuesta tiene como propósito el brindar una solución o plan de contingencia en el cual se manejen algunos puntos que permitan fortalecer la seguridad orientada al sistema de red de la empresa, para con ello generar un entorno en el cual la comunicación, manejo de datos y acceso a red e internet sea en su mayoría o totalidad, netamente seguro.

La fundamentación analítica se basa explícitamente en los principios de la metodología OSSTMM, los cuales se caracterizan para determinar la toma de y recolección de datos y con establecer los diversos parámetros que sean necesarios para la determinación de las variables de estudio pertinentes para con obtener el resultante óptimo que supla la necesidad existente a nivel de estructura de red. En la **Figura 1** se presenta la estructura metodológica general que se propone con respecto a su funcionalidad.

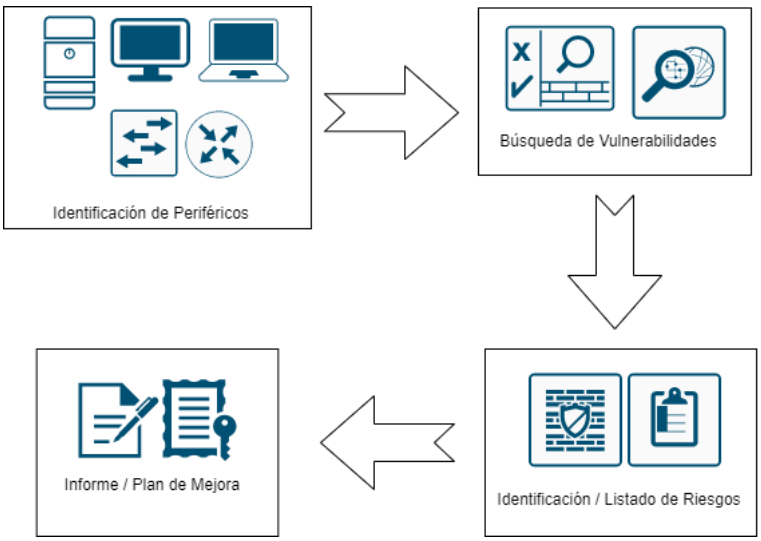


Figura 1. Arquitectura del Prototipo

2.2. Fundamentación teórica del prototipo.

La fundamentación teórica del prototipo planteado se encuentra segmentado en los parámetros de bases informativas como descripción de los puntos fundamentales que se debe conocer para el desarrollo del mismo, posterior a ello se conceptualizan las técnicas de análisis, donde se considera la sección puntual respecto a la metodología que conlleva la implementación del prototipo. Dicha segmentación se puede apreciar en la **Figura 2.**

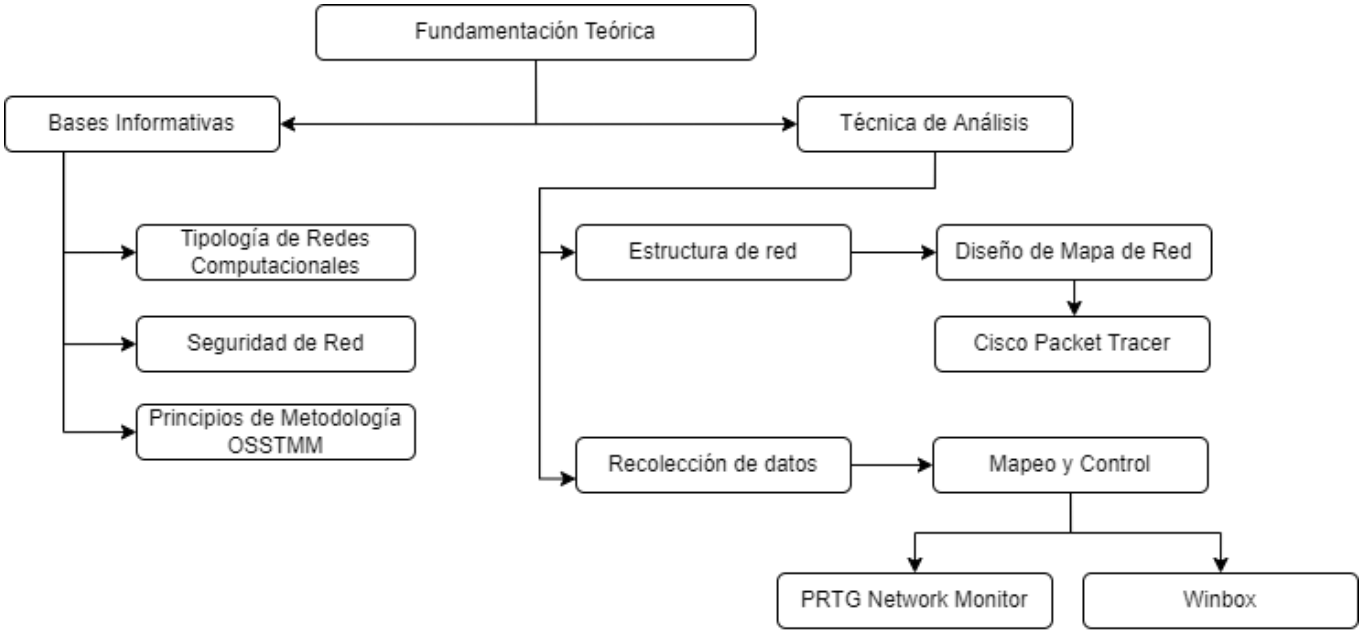


Figura 2. Mapa mental de la Fundamentación Teórica del Prototipo

2.2.1 Tipología de Redes Computacionales

2.2.1.1 Redes de Área Local – Local Área Networks (LAN)

Son aquellas que se encuentran conformadas a partir de dos o más equipos computadores, que se caracterizan por estar conectados entre sí, mediante el compartimiento de un espacio físico en común; sean estos domicilios, instituciones u organizaciones públicas o privadas[5].

Una de las caracterizas de las redes de área local, es que la comunicación que existe es netamente mediante cableado interconectado entre conmutadores, switchs y/o Routers que mediante protocolo permiten que dichos equipos logren comunicarse entre sí[6].

2.2.1.2 Redes de Área Amplia – Wide Área Networks (WAN)

Considerada un tipo de red que maneja conecta diversos dispositivos independientemente de su funcionalidad, pudiendo ser estos switchs y routers, servidores de Streaming y sobre todo clientes receptores, comunicándolos con diferentes tipos de vínculo, obteniendo una tecnología redundante con respecto a enlaces[7].

En la mayoría de los casos, las redes de área amplia son propias o pertenecientes a una organización o institución, mismas que al gestionarse de manera no pública; genera que las compañías proveedoras de internet utilicen este tipo de redes para interconectar a sectores corporativos y usuarios entre sí y el servicio de navegación en internet[8].

Una de las características relevantes de esta tipología de red en determinados entornos, es que permite obtener parámetros a niveles radioeléctricos o de radiocomunicación por las cuales mediante un adaptador se logren registrar, almacenar, analizar y visualizar las medidas que se capten, para con ello obtener datos estadísticos[9]. A nivel de seguridad una red WLAN es considerado un sistema de transferencia de datos e información mediante propiedades inalámbricas maleables o flexibles que se desplazan mediante señales de ondas electromagnética[10].

2.2.2 Seguridad de Red

Hoy en día las diversas organizaciones o instituciones poseen una diversa cantidad de bienes o activos sean estos: infraestructura, muebles, equipos de computación y comunicación, maquinarias y vehículos, entre otros. No obstante; en la mayoría de los casos se deja de lado al más importante a nivel organizacional, como es la información[11].

Existen vulnerabilidades a nivel informático, que dejan expuestas o ponen en riesgo la seguridad de uno o vario sistemas, permitiendo con ello que se pueda presentar ataques que comprometan la accesibilidad, confiabilidad e integridad de la información contenida, lo que hace una necesidad la acción de identificar, mitigar y resolver dichas amenazas[12].

Fortalecer la seguridad que debe poseer las redes digitales empresariales, comprende una necesidad a un nivel alto, ya que ello garantiza la integridad y usabilidad de los datos y los recursos digitales que posee la institución, compañía o empresa[13] .

2.2.2.1 Firewall

Es considerable que los accidentes a nivel de ciberseguridad en diferentes infraestructuras de red o de servicios de internet se han ido albergando de manera desmesurada, para lo cual es sumamente necesario lograr reconocer las vulnerabilidades y los puntos de acceso que requieran de protección inmediata[14]**.**

Los cortafuegos, significado al español de firewall; son sistemas de seguridad que vigilan el tráfico existente dentro de una red a través de reglas previamente establecidas. Un buen cortafuegos posee características principales como la de brindar soluciones que restrinjan el acceso de dispositivos o periféricos que no se encuentren autorizados, dando acceso únicamente a los que competen, brindar la opción de cifrar y revertir el cifrado del tráfico de datos, brindar asistencia, soporte y resguardo ante posibles ataques; bloqueando en primera línea, impidiendo de que pasen hacia el interior de la infraestructura[15].

2.2.2.2 Norma ISO 27001

Considerada una norma de margen internacional que se encarga de permitir parámetros como el aseguramiento, la confidencialidad e integridad de datos e información, así mismo de los sistemas que gestionan el proceso de los mismos[16]. Una de las características más relevantes de la norma es la estructura metodológica para el análisis de la seguridad de la información segmentándose en la Identificación de Activos de Información, Identificación de Vulnerabilidades, Identificación de Amenazas, Identificación de Requisitos Legales, Identificación de Riesgos, Cálculo del Riesgo y en Plan de Tratamiento de Riesgos en el cual se determina la opción más óptima para la seguridad de la información, resolviendo la problemática de los riesgos encontrados mediante las fases de Reducir, Evitar, Transferir, Aceptar.

2.2.3 Principios de Metodología OSSTMM

2.2.3.1 Seguridad de la Información

La seguridad de la Información, llamada además como seguridad cibernética, es considerada una extensión importante del área de la informática; dividida en dos enfoques principales: la seguridad lógica y la seguridad física; para ambos la prioridad será la seguridad de los activos, sean estos datos, software, etc.[4].

Se comprende como seguridad informática al consenso o existencia de normativas, metodologías, parámetros o estatutos de procesos que son considerados para la protección y cuidado de periféricos que contengan información[3].

2.2.3.2 Seguridad de los Procesos

El manejo de información dentro de una organización es una responsabilidad que comprende delicadeza y dedicación, considerando que los equipos en los cuales se almacene la misma deben trabajar en óptimas condiciones, así mismo el talento humano que maneje y administra dicha información de mantener una posición de confianza, pudiendo ser un empleado con trascendencia o un familiar. Módulo en el cual se evalúan los métodos que se emplean para la obtención de la información y a los involucrados en la obtención y administración de la misma[17].

2.2.3.3 Seguridad en las Tecnologías de Internet

La seguridad que posee las tecnologías de internet, no debes ser explícitamente similares a las que poseen la diversidad de redes de computadores, como comúnmente se considera, cabe recalcar que varios dispositivos son limitados, lo que implica que la evaluación o valoración de dicha seguridad sea limitada y con ello el uso de mecanismos los cuales solo incrementan el número de interacciones, agravando las lecturas[18].

Es conocido que las tecnologías de internet conforme han corrido los años, ha brindado facilidades y atajos a los usuarios, considerando al mayor beneficio al

tiempo de búsqueda y respuesta que brinda al momento de solventar interrogantes, también determinado como un sistema de comunicaciones entre redes[19].

Experimentando las necesidades del módulo, es considerable la valoración de las tecnologías de internet dividida en algunos parámetros tales como:

- Logística y Controles
- Exploración de Red
- Enrutamiento
- Testeo de Control de Acceso
- Testeo de Medidas de Contingencia
- Descifrado de Contraseñas

El internet como medio de comunicación, es capaz de lograr la conectividad entre millones de individuos a nivel global, suprimiendo todo tipo impedimentos que puedan existir, de igual manera al ser un medio de comunicación, también comprende ser un medio por el cual estar vulnerable y correr riesgos informáticos[20].

2.2.3.4 Seguridad en las Comunicaciones

Las comunicaciones existentes dentro de una organización son de máxima prioridad, ya que ella depende el correcto entendimiento del mensaje que se transmite por los medios establecidos y con ello evitar la sobrecarga que pueden tener las líneas de comunicación, teniendo alternativas como la transferencia de datos inalámbricos que se puede generar bastante provecho para generar una un alivio de carga para el resto de medios[21].

Al implementar tecnologías de información y comunicación en los sistemas de análisis, seguridad, control, supervisión y protección en las infraestructuras, se generan puntos de quiebre informáticamente hablando, lo cual deja expuesto a recibir ataques[22]. Además hay que tener en cuenta que conforme la vanguardia en tecnologías de comunicación aumenta, mayor debe ser la seguridad o medios a emplear para determinar una óptima emisión y recepción de datos e información, para la cual existen o se han generado medios tales

como Inteligencia artificial, aplicaciones inteligentes, tecnología de Telefonía IP, mejorando el servicio de comunicación tanto pata el emisor como para el receptor, además de la fiabilidad que brinda utilizar dichos medios[23].

2.2.3.5 Seguridad Inalámbrica

Los diversos protocolos que brindan soporte a la seguridad inalámbrica, con el tiempo van quedando obsoletos, por lo cual es oportuno mantener un control de revisión en diferentes puntos de acceso que puedan ser vulnerables a intromisión de terceros no deseados[24], unos de los mencionados de análisis pueden ser:

- Verificación de Redes Inalámbricas
- Verificación de Dispositivos de Vigilancia Inalámbricos
- Verificación de Sistemas Infrarrojos.

La variedad en grandes requerimientos de acceso por medios inalámbricos, los protocolos de seguridad y de espacio de almacenamiento que se requiere en la actualidad en el medio social, publico y empresarial, conlleva siempre el mantener la búsqueda de tecnologías innovadoras y potenciales que brinden soluciones a las problemáticas de este medio[25].

2.2.3.6 Seguridad Física

Al referirse a seguridad física, se especifica el enfoque existente en el entorno en los cuales se encuentra la infraestructura de red, teniendo en cuenta esto los diversos puntos evaluación que se consideran dentro del módulo.

2.2.4 Estructura de Red

2.2.4.1 Diseño de Mapa de Red

El diseño de un mapa de red corresponde a modelar de manera gráfica como se encuentra distribuido cada uno de los periféricos informáticos a lo largo de un perímetro o ubicación física y la forma o el medio en la que estos se interconectan, dicho diseño ayuda a conocer el estado de la red, incluyendo dispositivos dedicados tales como de interconexión, puertos de datos, equipos de cómputo, entre otros[26].

Como característica principal del diseño de una estructura de red es que permite conocer y analizar el funcionamiento y comportamiento que posee la misma con respecto a la transmisión de datos entre diversos periféricos[27].

2.2.4.1.1 Cisco Packet Tracer

Es una herramienta que permite realizar configuraciones de dispositivos simulando en tiempo real, la cual brinda soporte de análisis y verificación de recorridos de paquetes dentro de una red establecida mediante la creación de conexiones básicas entre varios periféricos, sean estos: routers, switchs, equipos de usuario final, entre otros[28].

2.2.5 Recolección de datos

2.2.5.1 Mapeo y Control

Al hablar de mapeo y control de una intranet o de la estructura establecida de una red dentro de una organización, institución o empresa, se considera la evaluación y análisis de diferentes variables que permitan llegar a conclusiones en base a los resultados obtenidos.

2.2.5.1.1 PRTG Network Monitor

Es una herramienta de monitoreo de infraestructura de red que permite analizar e identificar diversas problemáticas ante anormalidades y circunstancias informáticas, sean en redes de estructura inalámbrica o no, mediante la recolección de datos a través de sondas de monitoreo[29].

Una de las características principales de la herramienta es que supervisa toda infraestructura de tecnología compatible tales como Servidores SNMP, contadores de rendimientos de Windows, certificados de cifrado de internet de software libre, solicitudes de HTTP, testeo y ping, acceso a reportes en bases de datos y muchas funcionalidades más[30].

2.2.5.1.2 Winbox

Una herramienta de software desarrollada para administración de dispositivos de Mikrotik, misma que posee una interfaz entendible, que permite la administración y configuración del sistema de red basado en la web, por lo cual no es necesaria instalación[31].

Es oportuno mencionar que Winbox es una herramienta que permite administrar dichos dispositivos en sistema operativo Windows, para administración sistemas operativos como Linus y Mac se disponen otras herramientas de RouterOS [32].

2.3. Objetivos del prototipo

2.3.1. Objetivo General

Evaluar los riesgos informáticos existentes en Grupo Guerrero Portilla basándose en los principios de la metodología OSSTMM para el fortalecimiento de la seguridad a nivel de su estructura de red.

2.3.2. Objetivo Específicos

- Analizar el enlace de red existente en la intranet mediante el uso de herramientas de testeo.
- Monitorear los dispositivos y la comunicación existente entre los distintos puntos de red a través de software dedicado.
- Optimizar los diagramas de infraestructura actuales mediante herramientas de simulación de red.
- Elaborar un plan de seguridad y fortalecimiento de red mediante la aplicación de directivas, restricciones y/o bloqueos.

2.4. Diseño del prototipo

El diseño o desarrollo del prototipo está basado en dos partes o módulos, los cuales corresponden a análisis y a resolución de dicho análisis.

El análisis va de la mano de la recolección de datos y la evaluación de los mismos, basándose en los puntos más importantes de los principios de la metodología OSSTMM, mediante los cuales arrojarán detalles que servirán para la siguiente fase.

En la fase de resolución, se toman los resultados o variables que arrojen los análisis previamente realizados, para con ello establecer o diseñar un plan evaluación de factibilidad con respecto a la propuesta de un plan de optimización y/o mejora a nivel de seguridad que permita mejorar o superar al sistema actualmente establecido y con ello fortalecer la infraestructura de red.

2.4.1. Diseño de la Arquitectura de Red

2.4.1.1 Arquitectura de Red Actual

En la **Figura 3** se encuentra la representación de la arquitectura que posee actualmente la empresa, misma que consta de un router de borde que recibe el servicio de internet por parte del proveedor, de allí se divide en el sector de primera zona y al de los switchs de distribución, en la primera zona se encuentran conectados los primeros equipos del área de atención al público, establecidos así por un sistema anterior de infraestructura de red. Partiendo de los switchs de distribución, se brinda conectividad para el área faltante de la zona de atención al público, distribuye conectividad al servidor y a los equipos dentro del área administrativa, brinda comunicación a los equipos de la sección de Bodega, que se interconectan mediante un switch básico, y de igual manera otorga de internet y acceso al servidor al punto de venta anexo al establecimiento, mismo que brinda conectividad mediante un switch básico a los equipos del mismo, además de soporte inalámbrico a través de un router interconectado.

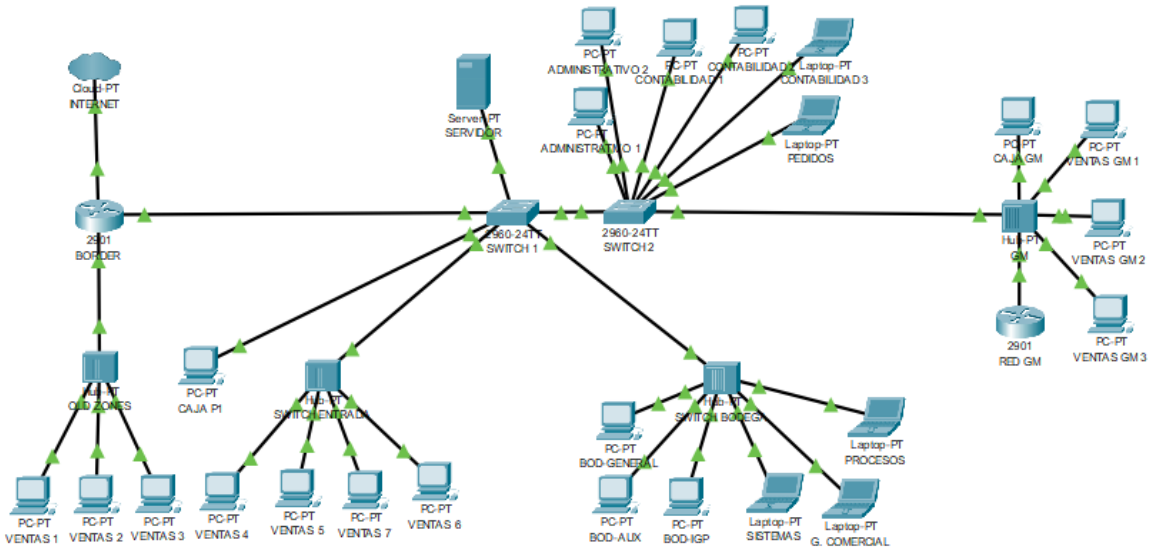


Figura 3. Arquitectura de Red Actual

2.4.1.2 Arquitectura propuesta con optimización según OSSTMM

El diseño de red propuesto en el cual se emplea el plan de mejora aplicando los conceptos de los principios de la metodología OSSTMM para ser analizado, se aprecia en la **Figura 4**, la cual se puede describir con una estructura organizacional segmentada, partiendo por el router de borde que conecta la puerta de enlace de salida a internet por parte del proveedor del servicio, la implementación de un firewall por el cual se establecerán reglas y permisos de acceso hacia la intranet, posterior a ello se ingresaría al sistema de distribución central de switchs, mismos que interconectaran a las diversas área de manera organizada. Iniciando por el área administrativa, donde encuentra el servidor; allí brinda soporte de comunicación a los periféricos existentes dentro de la zona, inmediatamente partiría de manera directa a la sección de bodega y procesos, dentro del segundo grupo se establecerían ambos puntos de atención al cliente distribuidos por grupos y sector geográfico.

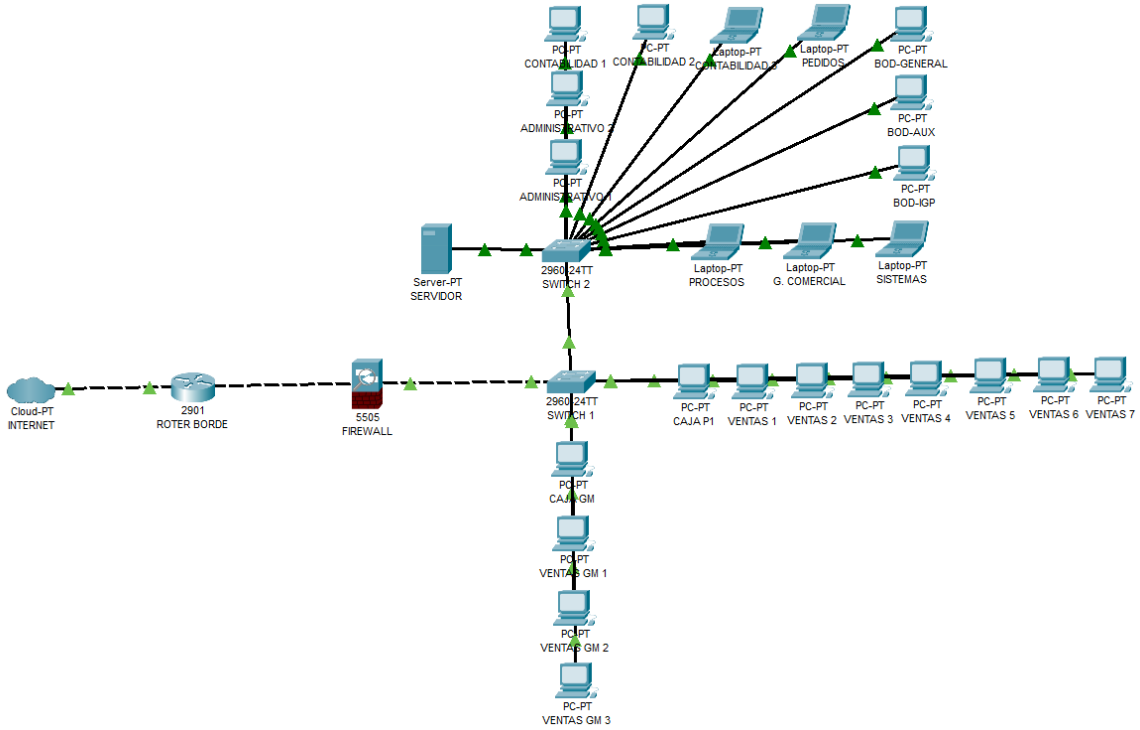


Figura 4. Arquitectura Optimizada Propuesta

2.4.2. Evaluación según OSSTMM

2.4.2.1 Seguridad de la Información

La empresa actualmente no consta con un sistema que provea soporte de seguridad correspondiente a la información que se maneje, a nivel de software se encuentran deshabilitados los protocolos básicos como el firewall que ofrece el sistema operativo, tal como se puede apreciar en la **Figura 5**, a nivel físico no existe periférico que controle o proteja el tráfico de datos.

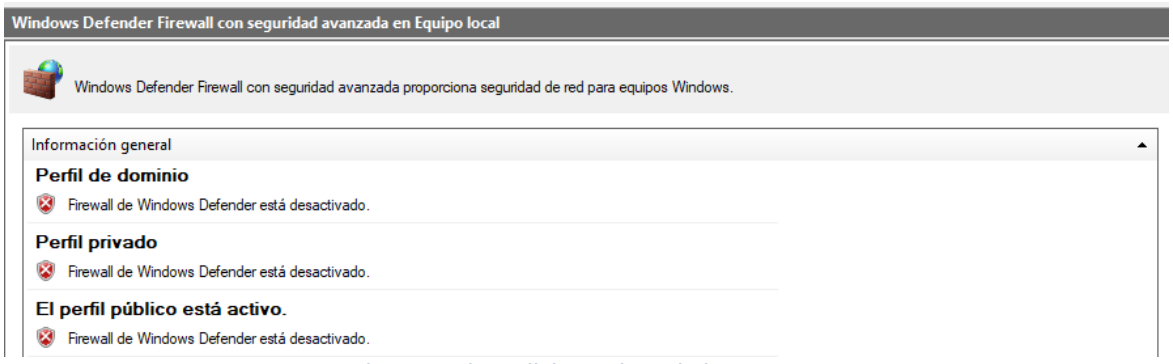


Figura 5. Firewall de Equipos de la Empresa

Para el manejo del sistema principal, se cuenta con un servidor local basado en tecnología Linux del cual depende el correcto funcionamiento y gestión para cada terminal. Detalles se aprecian en la **Figura 6**.

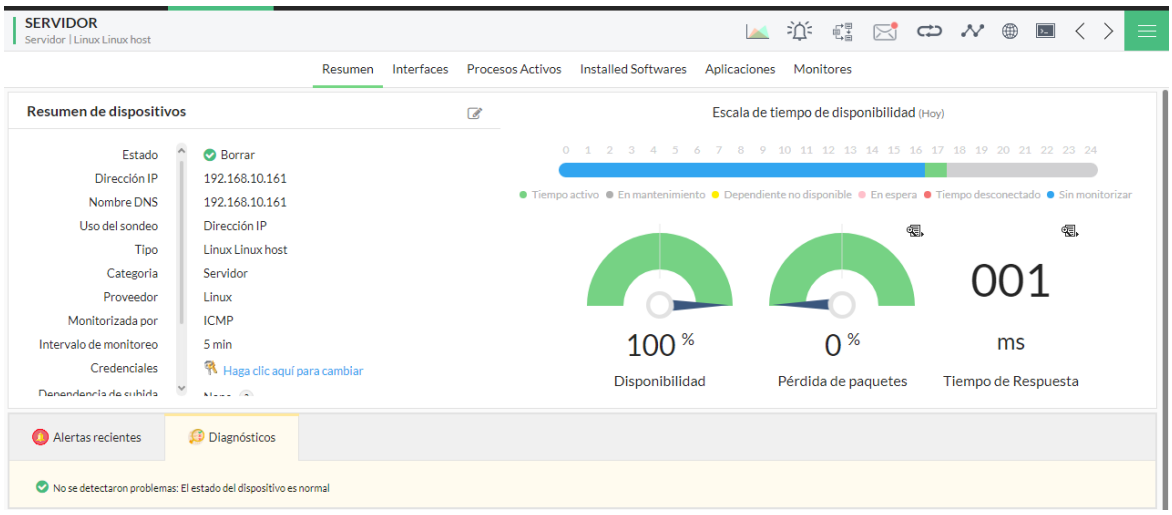


Figura 6. Estado del Servidor en Tiempo Real

Figura 7.Estado del Servidor Reporte

En la **Figura 7**, se puede observar que, a pesar de tener una pronta respuesta por parte del servidor, existen pérdidas a nivel de comunicación en reiteradas ocasiones, lo que implica problemáticas de gestión.

2.4.2.2 Seguridad de los Procesos

La empresa posee varios departamentos dedicados, mismos que son detallados en la **Tabla 1**, por ende, el manejo de la información se divide según corresponda a la pertinencia o dependencia de cada uno de ellos.

Tabla 1. Información en Base de Dependencia

Nombramiento	Información de Dependencia
Administrador(a)	- Datos del Sistema - Información del Personal - Manejo de Rubros - Datos de Inventario - Conocimiento de Cartera de Clientes.
Departamento Contable	- Datos del Sistema - Información del Personal - Manejo de Rubros. - Datos de Inventario - Conocimiento de Cartera de Clientes.
Encargado de Procesos	- Información básica de la Empresa. - Conocimiento de etapas a cumplir por parte del personal.
Jefe de Personal	- Datos del Sistema. - Información del Personal.
Analista de Datos y Sistema	- Datos del Sistema, - Información del Personal. - Estado de base de datos y servidor. - Datos de Inventario. - Usuarios, contraseñas y control de acceso. - Información de la Empresa. - Activos Tecnológicos.
Cajera – Administradora	- Datos del Sistema. - Manejo de Rubros. - Conocimiento de Cartera de Clientes.
Personal de Venta y Atención al Público	- Datos del Sistema. - Datos de Inventario.

2.4.2.3 Seguridad en las Tecnologías de Internet

En las **Figuras 8 y 9** se muestra las restricciones que posee respecto a la interacción en internet mediante un tipo de usuario.

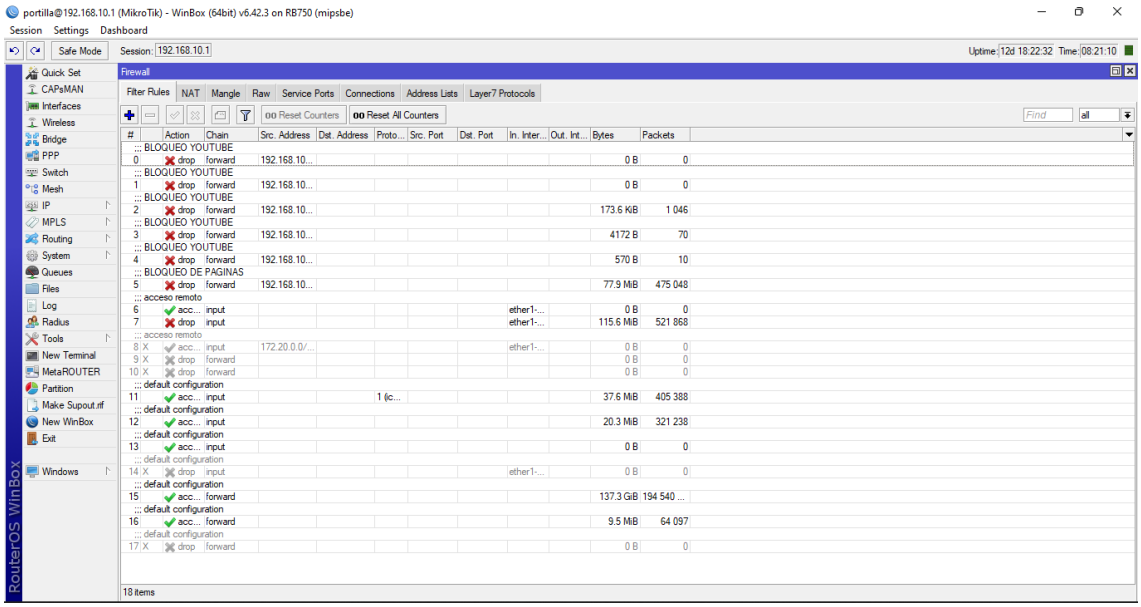


Figura 8. Bloqueos de Páginas

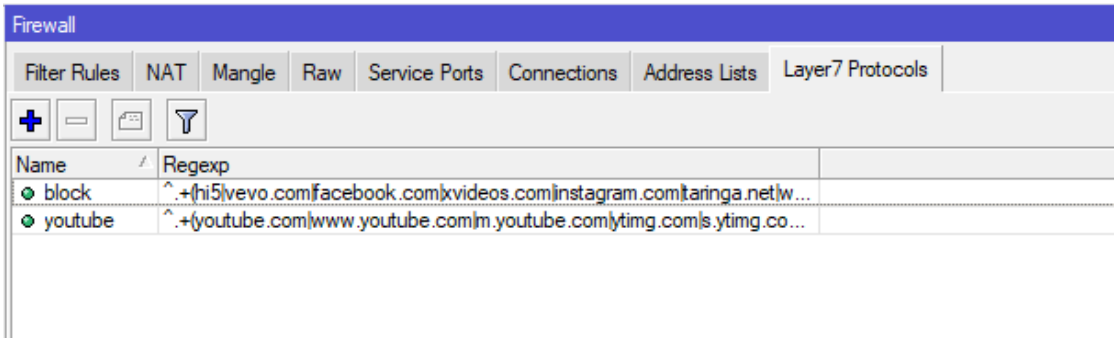


Figura 9. Restricciones por Firewall

En el parámetro de Exploración de Red, se pueden identificar los diversos equipos o direcciones de enrutamiento que poseen los periféricos, los cuales se identifican y se agrupan según la funcionalidad. La lista de equipos se aprecia en las **Figuras 10, 11 y 12.**

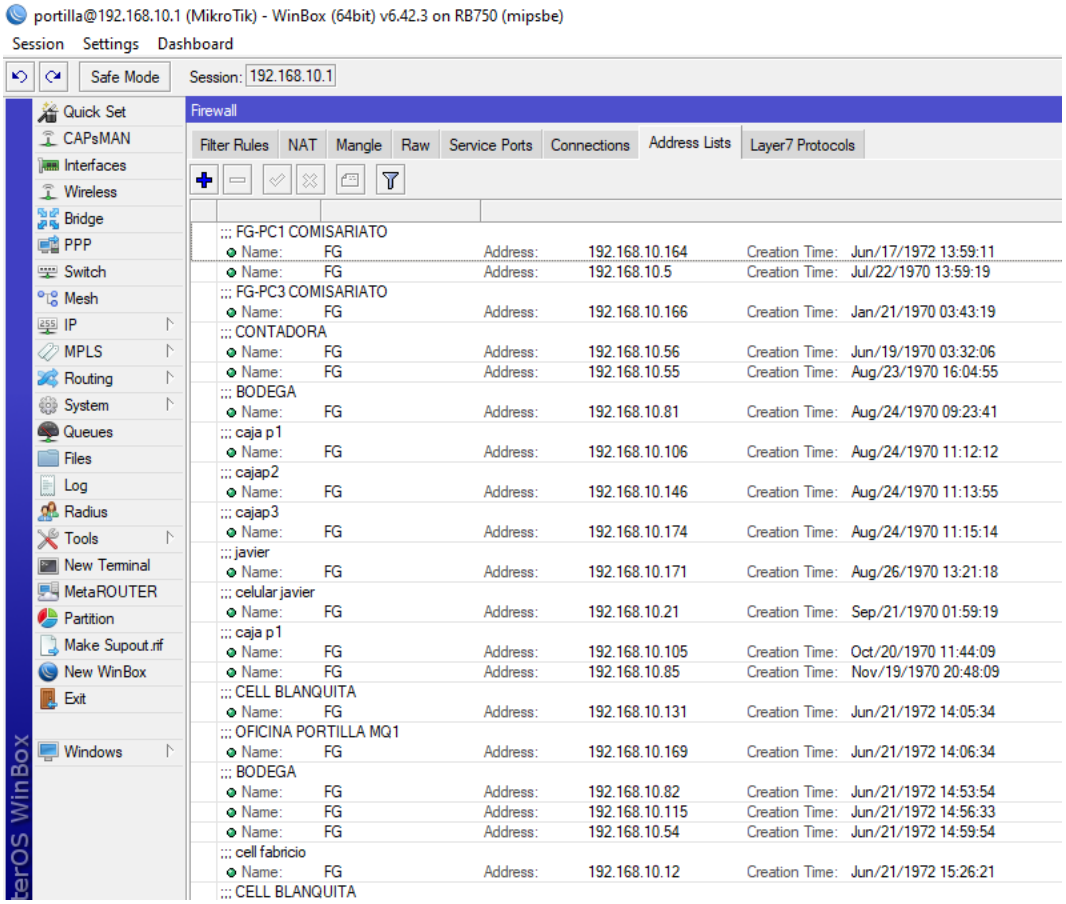


Figura 10. Lista de IP

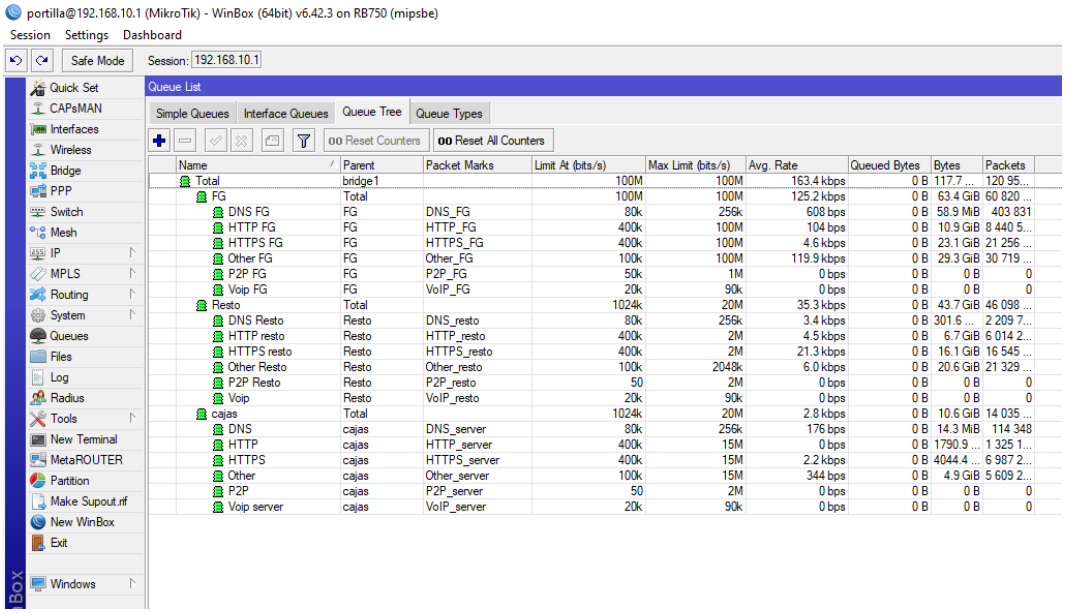
	Name:	FG	Address:	192.168.10.75	Creation Time:	Jun/21/1972 15:31:50
	;;; DVR GUERRERO					
	Name:	FG	Address:	192.168.10.121	Creation Time:	Jun/22/1972 06:12:08
	;;; DVR OFICINA2					
	Name:	FG	Address:	192.168.10.101	Creation Time:	Jun/22/1972 06:22:06
	;;; DVR OFICINA3					
	Name:	FG	Address:	192.168.10.114	Creation Time:	Jun/22/1972 06:30:02
	;;; DVR CENTRO COMERCIAL					
	Name:	FG	Address:	192.168.10.113	Creation Time:	Jun/22/1972 07:32:53
	;;; DVR FRENTE LUCES					
	Name:	FG	Address:	192.168.10.142	Creation Time:	Jun/22/1972 12:02:04
	;;; javier					
	Name:	FG	Address:	192.168.10.181	Creation Time:	Jul/13/1972 09:15:56
	;;; FG-PC4 COMISARIATO					
	Name:	FG	Address:	192.168.10.197	Creation Time:	Jul/30/1972 12:15:17
	;;; TVBOX COMISARIATO					
	Name:	FG	Address:	192.168.10.109	Creation Time:	Oct/30/1972 19:56:28
	;;; LENOVO LAPTOP					
	Name:	FG	Address:	192.168.10.144	Creation Time:	Jan/27/1973 14:11:15
	;;; BODEGA-GUERRERO					
	Name:	FG	Address:	192.168.10.63	Creation Time:	Feb/21/1973 08:43:11
	;;; HYUNDAI					
	Name:	FG	Address:	192.168.10.198	Creation Time:	Mar/09/1973 15:07:18
	;;; CAJA GUERR					
	Name:	FG	Address:	192.168.10.120	Creation Time:	Mar/16/1973 08:17:01
	Name:	FG	Address:	192.168.0.10	Creation Time:	Mar/20/1973 12:59:42
	;;; BOD AUX					
	Name:	FG	Address:	192.168.10.137	Creation Time:	Mar/20/1973 13:00:25
	;;; PRUEBAS					
	Name:	FG	Address:	192.168.10.201	Creation Time:	Apr/30/1973 19:22:12
	;;; BODEGA2					
	Name:	FG	Address:	192.168.10.88	Creation Time:	May/01/1973 21:17:09
	;;; caja					
	Name:	FG	Address:	192.168.10.32	Creation Time:	May/07/1973 14:26:54

Figura 11. Lista de IP 2

	Name:	FG	Address:	192.168.10.32	Creation Time:	May/07/1973 14:26:54
	;;; SUPPORT					
	Name:	FG	Address:	192.168.10.225	Creation Time:	May/07/1973 19:15:28
	;;; CAJA CCA					
	Name:	FG	Address:	192.168.10.112	Creation Time:	May/10/1973 19:55:42
X	;;; CCA-ALEX					
	Name:	FG	Address:	192.168.10.165	Creation Time:	Jun/05/1973 17:00:18
	;;; PC-ALEX					
	Name:	FG	Address:	192.168.10.165	Creation Time:	Jun/09/1973 21:48:02
	;;; LAPTOP A.A LENOVO					
	Name:	FG	Address:	192.168.10.36	Creation Time:	Jun/20/1973 17:48:30
	;;; CELL-PROCESOS					
	Name:	FG	Address:	192.168.10.194	Creation Time:	Jul/15/1973 08:12:07
	;;; PC-MJ					
	Name:	FG	Address:	192.168.10.6	Creation Time:	Aug/07/1973 18:11:38
	;;; NVR-GUERRERO MATRIZ					
	Name:	FG	Address:	192.168.10.168	Creation Time:	Aug/07/1973 18:14:57
	;;; CAJA-PR					
	Name:	FG	Address:	192.168.10.150	Creation Time:	Aug/09/1973 05:21:10
	;;; TVBOX GUERRERO					
	Name:	FG	Address:	192.168.10.103	Creation Time:	Aug/13/1973 16:06:37
	;;; HP-SISTEMAS					
	Name:	FG	Address:	192.168.10.191	Creation Time:	Sep/03/1973 15:17:43
	;;; VGM-2					
	Name:	FG	Address:	192.168.10.22	Creation Time:	Sep/09/1973 04:19:13
	;;; HP-CONTABILIDAD					
	Name:	FG	Address:	192.168.10.167	Creation Time:	Sep/12/1973 01:17:03
	;;; HP-SISTEMAS-ETH					
	Name:	FG	Address:	192.168.10.172	Creation Time:	Sep/12/1973 20:25:29
	;;; MAQ-PED-GUER-MAT					
	Name:	FG	Address:	192.168.10.133	Creation Time:	Sep/16/1973 04:25:44
	;;; HP-WIRELLESS-2					
	Name:	FG	Address:	192.168.10.173	Creation Time:	Sep/16/1973 20:38:46
	;;; LAPTOP JAVIER					

Figura 12. Lista de IP 3

Para mayor control de acceso y funcionamiento referente a las necesidades y requerimientos, mediante el sistema de administración de Mikrotik Winbox, se han creado grupos que manejan distintos parámetros de apertura de ancho de banda, brindando el que corresponda a cada periférico, tal cual se puede apreciar en la **Figura 13**.



Name	Parent	Packet Marks	Limit At (bits/s)	Max Limit (bits/s)	Avg. Rate	Queued Bytes	Bytes	Packets
Total	bridge1		100M	100M	163.4 kbps	0 B	117.7 ...	120 95...
FG	Total		100M	100M	125.2 kbps	0 B	63.4 GiB	60 820 ...
DNS FG	FG	DNS_FG	80k	256k	608 bps	0 B	58.9 MiB	403 831
HTTP FG	FG	HTTP_FG	400k	100M	104 bps	0 B	10.9 GiB	8 440 5...
HTTPS FG	FG	HTTPS_FG	400k	100M	4.6 kbps	0 B	23.1 GiB	21 256 ...
Other FG	FG	Other_FG	100k	100M	119.9 kbps	0 B	29.3 GiB	30 719 ...
P2P FG	FG	P2P_FG	50k	1M	0 bps	0 B	0 B	0
Voip FG	FG	VoIP_FG	20k	90k	0 bps	0 B	0 B	0
Resto	Total		1024k	20M	35.3 kbps	0 B	43.7 GiB	46 098 ...
DNS Resto	Resto	DNS_resto	80k	256k	3.4 kbps	0 B	301.6 ...	2 209 7...
HTTP resto	Resto	HTTP_resto	400k	2M	4.5 kbps	0 B	6.7 GiB	6 014 2...
HTTPS resto	Resto	HTTPS_resto	400k	2M	21.3 kbps	0 B	16.1 GiB	16 545 ...
Other Resto	Resto	Other_resto	100k	2048k	6.0 kbps	0 B	20.6 GiB	21 329 ...
P2P Resto	Resto	P2P_resto	50	2M	0 bps	0 B	0 B	0
Voip	Resto	VoIP_resto	20k	90k	0 bps	0 B	0 B	0
cajas	Total		1024k	20M	2.8 kbps	0 B	10.6 GiB	14 035 ...
DNS	cajas	DNS_server	80k	256k	176 bps	0 B	14.3 MiB	114 348
HTTP	cajas	HTTP_server	400k	15M	0 bps	0 B	1790.9 ...	1 325 1...
HTTPS	cajas	HTTPS_server	400k	15M	2.2 kbps	0 B	4044.4 ...	6 987 2...
Other	cajas	Other_server	100k	15M	344 bps	0 B	4.9 GiB	5 609 2...
P2P	cajas	P2P_server	50	2M	0 bps	0 B	0 B	0
Voip server	cajas	VoIP_server	20k	90k	0 bps	0 B	0 B	0

Figura 13. Lista de Reglas de Ancho de Banda

Mediante la herramienta de monitoreo PRTG Network Monitor, se logran obtener datos de sondeo de la infraestructura de red. En la **Figura 14** se pueden percibir el listado de la mejor disponibilidad de comunicación de los dispositivos.

Mejor disponibilidad (disponibilidad más alta)

Tiempo activo [%]	Sensor	Dispositivo
100,0000%	HTTP	192.168.10.3
100,0000%	Ping	192.168.10.172
100,0000%	HTTP	192.168.10.4
100,0000%	HTTP	192.168.10.2
100,0000%	HTTP	192.168.10.188
100,0000%	HTTP	192.168.10.114
100,0000%	HTTP	192.168.10.5
100,0000%	HTTP	192.168.10.142
100,0000%	Estado del servidor central (autónomo)	Servidor central de PRTG
100,0000%	Realtek RTL8822CE 802.11ac PCIe Adapter	Dispositivo de sonda

Figura 14. Mejor Disponibilidad de Sondeo

Con lo que respecta a los dispositivos con mayor número de pérdida de paquetes de datos, se pueden observar en la **Figura 15.**

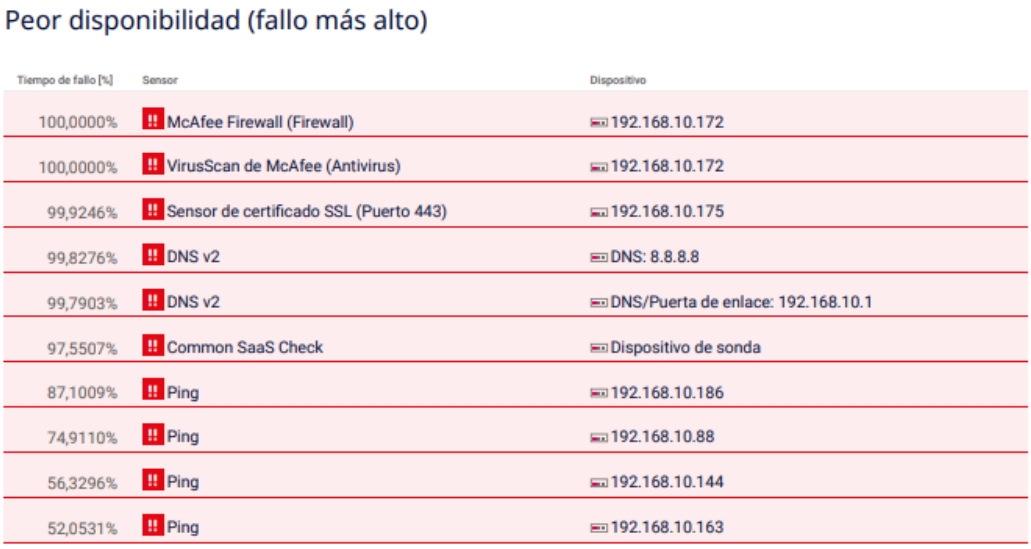


Figura 15. Peor Disponibilidad de Sondeo

2.4.2.4 Seguridad en las Comunicaciones

Para determinar las comunicaciones que posee la infraestructura, se debe evaluar al dispositivo de administración de red, aquel que recibe el servicio de internet y permite la intercomunicación entre cada periférico.

En la **Figura 16,** se puede observar que se realiza un monitoreo continuo al router de borde, no obstante, existen intermitencias con respecto a la comunicación, esto se pude ocasionar debido a los diversos consumos de ancho de banda que no se encuentran controlados, o también a la misma infraestructura en general.

Figura 16. Evaluación de Router

Para profundizar el análisis, se evalúa el DNS del router de puerta de enlace con la finalidad de obtener mayores datos de su comportamiento. De igual manera en las **Figuras 17 y 18** se observa pérdida e intermitencia de conectividad en la línea de tiempo.

Figura 17. Evaluación del DNS

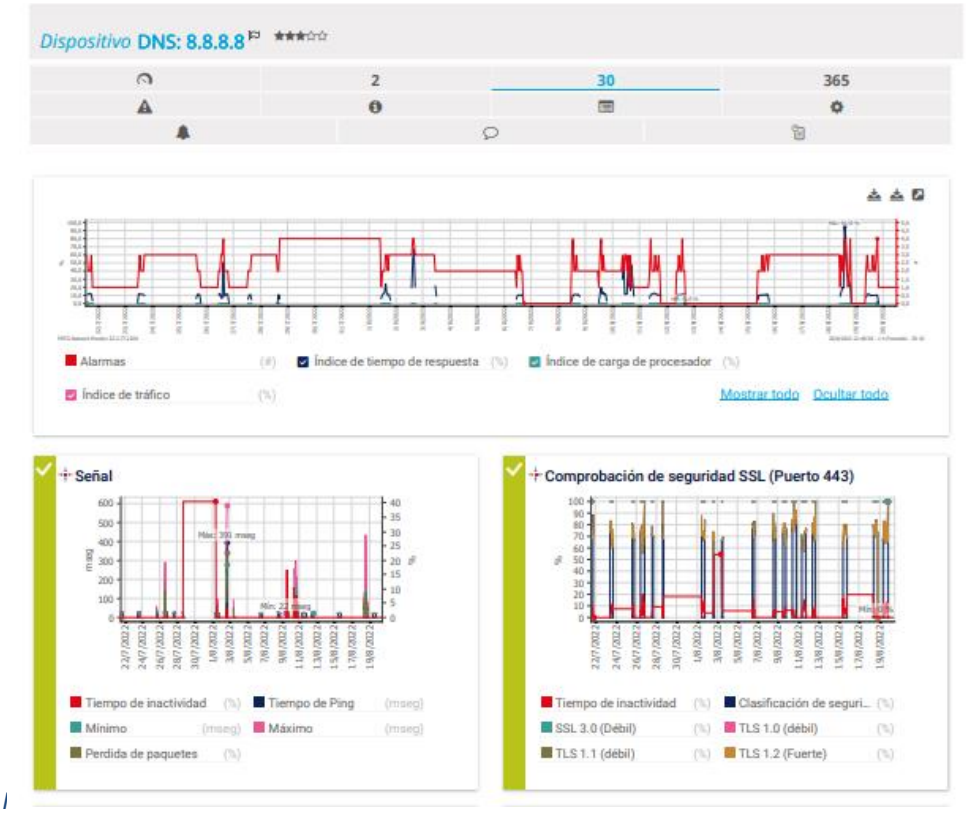


Figura 18. Evaluación del DNS 2

2.4.2.5 Seguridad Inalámbrica

Brindar seguridad a nivel de infraestructura implica proteger el perímetro en el cual se encuentra alojado cada uno de los periféricos informáticos, ya sean estos de usuario final, de almacenamiento de datos o de enrutamiento y distribución de red. La empresa consta con un sistema de sensores infrarrojos conectados directamente a la alarma de seguridad que brinda alertas ante anomalías fuera de los horarios habituales, los cuales se presentan en la **Tabla 2** sectorizando la cantidad y ubicación por sector.

Tabla 2. Lista de Sensores Infrarrojos

Sector	Nro. de Sensores
Entrada Principal	2
Mezanine	2
Bodega/ Recepción	1
Almacén de Partes de Motor	1
Almacén de Partes de Motor 2	1
Escaleras	2
Bodega Superior	3
Total de Sensores	**12**

2.4.2.6 Seguridad Física

Al referirse a la infraestructura física y ubicación geográfica de los dispositivos de enrutamiento dentro de la empresa, la misma no cuenta con un espacio óptimo ni adecuado para los mismos, por lo cual se ven comprometidos a no mantener un lineamiento de orden, mucho menos de identificación estructural, tal como se logra apreciar en las **Figuras 19 y 20**.

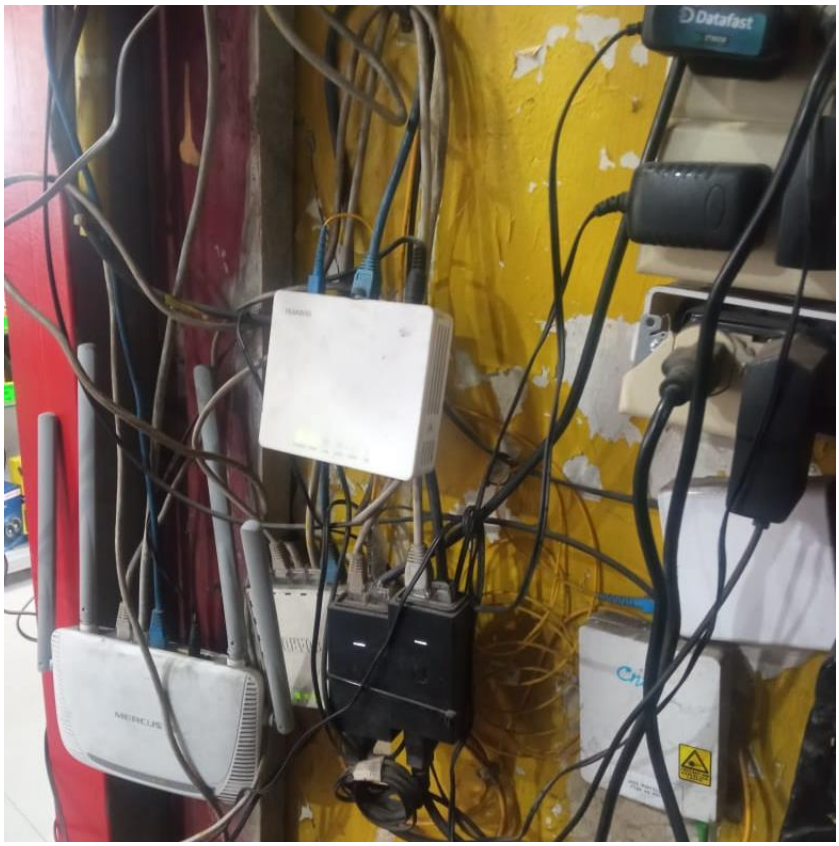


Figura 19. Estado Actual de Router de Borde

Figura 20. Estado Actual de Rack de Switch

2.5 Ejecución y/o Ensamblaje del Prototipo

Una vez finalizada la evaluación tras la recolección y análisis de datos de la infraestructura de red existente, se da paso a la identificación de riesgos existentes en la institución, para posterior a ello elaborar un plan de mejora u optimización para la seguridad de dicha infraestructura.

Cabe recalcar que la identificación de riesgos se basará en los puntos de análisis de la Norma ISO 27001, que brindará soporte para la elaboración del plan de mejora fundamentado en los principios de la Metodología OSSTMM, haciendo uso de herramientas que permitan fortalecer la seguridad de la infraestructura.

2.5.1 Análisis de Riesgo Según Norma ISO 27001

2.5.1.1 Inventario de Activos

Cómo se refleja en la **Tabla 3**, se identifican los activos o bienes que posee la empresa, con la finalidad de conocer los involucrados en el prototipo planteado.

Tabla 3. Lista de Activos

Activo/Bien	Tipo de Activo
Servidor	Hardware
Infraestructura de Red	Comunicación
Archivos – Documentación	Datos/ Información
Internet	Servicio
Correo Electrónico	Servicio
Sistema Contable	Software
Sistema Video Vigilancia	Hardware
Sistema de Rastro de Movimientos	Hardware
Impresoras	Hardware
Computadoras/ Laptops	Hardware
Talento Humano	Persona

2.5.1.1.1 Valoración de Activos

El proceso de valoración o tasación de activos corresponde a la asignación de valor que posee el activo para la empresa o institución, para con ello determinar los más relevantes, dicha acción es necesaria ya que con ello se conocerá aquellos activos de mayor valor y por ende los de mayor prioridad. Para valorar un activo se deben tomar en cuenta puntos donde se pueda ver afecto, siendo estos: Integridad, Disponibilidad y Confidencialidad, determinando con ello lo siguiente:

Tabla 4. Fórmula de Valor de Activos

Variables	Representación / Fórmula
Va: Valor del Activo	$\mathrm{Va} = \frac{\mathrm{V1} + \mathrm{Vd} + \mathrm{Vc}}{3}$
Vi: Valor de Integridad	
Vd: Valor de Disponibilidad	
Vc: Valor de Confidencialidad	

Para evaluar cada activo, se considerarán un rango de valores de parámetros en una escala del 1 al 5; determinando así la importancia de salvaguardar a cada uno de los activos, reflejándolos con valores numéricos según corresponda, tal como se muestra en las **Tablas 5 y 6**.

Tabla 5. Escala de Valoración

Descripción	Valor
Muy Bajo	1
Bajo	2
Medio	3
Alto	4
Muy Alto	5

Tabla 6. Valoración de Activos

Activo/Bien	Tipo de Activo	Vc	Vi	Vd	Promedio
Servidor	Hardware	5	5	5	5
Infraestructura de Red	Comunicación	5	5	5	5
Archivos – Documentación	Datos/ Información	4	4	3	3.67
Internet	Servicio	4	4	4	4
Correo Electrónico	Servicio	3	3	3	3
Sistema Contable	Software	5	5	5	5
Sistema Video Vigilancia	Hardware	5	5	4	4.67
Sistema de Rastro de Movimientos	Hardware	4	4	4	4
Impresoras	Hardware	2	3	3	2.67
Computadoras/ Laptops	Hardware	5	4	3	4
Talento Humano	Persona	4	4	5	4.33

2.5.1.2 Identificación de Amenazas y Vulnerabilidades

2.5.1.2.1 Amenazas

Dentro de la empresa pueden surgir distintos incidentes no deseados que pueden generar daño a los activos, correspondiente a la necesidad, tenemos:

Tabla 7. Tipos de Amenazas

Tipo de Amenaza	Ejemplo
Amenaza Natural	Inundaciones, Sismos, Tormentas, Incendios Forestales etc.
Amenaza de Infraestructura Física	Riesgos eléctricos, Entorno en mal estado, Pérdida de acceso a ubicación geográfica, Explosiones.
Amenaza de Talento Humano	Enfermedad, Pérdida de personal imprescindible, Problema de Acceso.
Amenaza Tecnológica	Virus, Cracking, Fallas de Software, Fallas de Hardware, Inconvenientes con infraestructura de red.

Habiendo determinado el tipo de amenazas que pueden presentarse o afectar a los activos de la empresa, es oportuno medir la posibilidad de ocurrencia o de que se presenten dichas amenazas, para ello se determina por valor por rangos según dicha posibilidad, tal como se pude observar en la **Tabla 8.**

Tabla 8. Posibilidad de Ocurrencia de Amenaza

Posibilidad	Valor
Muy Baja	1
Baja	2
Media	3
Alta	4
Muy Alta	5

2.5.1.2.2 Vulnerabilidades

Se consideran como vulnerabilidad a los posibles puntos de quiebre o de posible acceso ante una amenaza, en la **Tabla 9** se listan los tipos de vulnerabilidades que se pueden presentar eventualmente.

Tabla 9. Tipos de Vulnerabilidades

Tipo Vulnerabilidad	Ejemplo
Seguridad de los Recursos Humanos	Mal uso de los equipos e información por parte del Personal.
Sistema de Control de Acceso	Desprotección de los equipos de comunicación y los que con ellos se involucran.
Seguridad Física y Ambiental	Infraestructuras en mal estado, espacios físicos sujetos a desastres naturales, carencia de plan de respaldo de suministros.
Gestión de Operaciones y Comunicación	Interfaces no intuitivas, desvío o pérdida de paquetes de datos, enlaces redundantes o innecesarios, carencia de control de firewall.
Mantenimiento, desarrollo y adquisiciones de sistemas de gestión de información	instalación o aplicación de software de terceros con origen desconocido que pongan en riesgo a la información.

2.5.1.2.3 Asociación de Amenazas y Vulnerabilidades

Identificados los tipos de Amenazas y Vulnerabilidades que puedan afectar a un activo, se las debe asociar entre si tal como se detalla en la **Tabla 10** para determinar el caso de estudio en el cual se puedan identificar el grado y capa del Modelo OSI en que se encuentran involucradas.

Tabla 10. Amenazas y Vulnerabilidades de los Activos

Activo/Bien	Va	Amenaza	Vulnerabilidad	Capa Involucrada
Servidor	5	Daño al software con mal intención.	Sistema operativo obsoleto	Aplicación
		Daño al software con mal intención	Software pirata - virus	Aplicación
		Daño Físico – Mal estado	Falta de Mantenimiento	Física
		Daño Físico – Mal estado	Partes deterioradas por longevidad	Física
		Daño Físico – Mal Estado	Equipos Ubicados en zonas de riesgos	Física
		Paralización – Suspensión de la comunicación o del servicio	Falta y/o mala administración de recursos.	Enlace de Datos
		Falla de Acceso Lógico	Baja o nula seguridad de acceso.	Sesión
		Desastre Natural	Inexistencia de plan de emergencia ante desastres	---------
Infraestructura de Red	5	Daño Físico – Mal Estado	Periféricos desgastados	Física
		Daño Físico – Mal Estado	Defectos de fábrica de Periféricos	Física
		Paralización – Suspensión de la comunicación o del servicio	Falta y/o mala administración de recursos.	Enlace de Datos
		Uso indebido del acceso	Falta de controles de acceso y privilegios otorgados.	Sesión
		Falla de Acceso Lógico	Baja o nula seguridad de acceso.	Sesión
Sistema Contable	5	Paralización – Suspensión de la comunicación o del servicio	Falta y/o mala administración de recursos.	Enlace de Datos
		Uso indebido del acceso	Falta de controles de acceso y privilegios otorgados.	Sesión
		Filtración de Información	Ausencia de auditoría y control	Transporte
		Falla de Acceso Lógico	Baja o nula seguridad de acceso.	Sesión
Sistema Video Vigilancia	4.67	Daño Físico – Mal Estado	Falta de Mantenimiento	Física
		Daño Físico – Mal Estado	Equipos Obsoletos	Física
		Daño Físico – Mal Estado	Equipos Ubicados en zonas de riesgos	Física
		Daño Lógico	Falta de controles de acceso al sistema	Sesión
		Falla de Acceso Lógico	Baja o nula seguridad de acceso.	Sesión
		Paralización – Suspensión de la comunicación o del servicio	Falta y/o mala administración de recursos.	Enlace de Datos

Talento Humano	4.33	Indisponibilidad del Personal	Pérdida o Enfermedad	---------
		Errores por falta de conocimiento o de concentración	Personal con poca motivación	---------
		Sistemas maliciosos en equipos celulares	Dispositivos con baja o nula seguridad ante malware	Aplicación
Computadoras/ Laptops	4	Daño Físico – Mal Estado	Falta de Mantenimiento	Física
		Daño Físico – Mal Estado	Equipos Obsoletos	Física
		Daño Físico – Mal Estado	Equipos Ubicados en zonas de riesgos	Física
		Daño al software con mal intención.	Sistema operativo obsoleto	Aplicación
		Daño al software con mal intención	Software pirata - virus	Aplicación
		Falla de Acceso Lógico	Baja o nula seguridad de acceso.	Sesión
		Desastre Natural	Inexistencia de plan de emergencia ante desastres	---------
Sistema de Rastro de Movimientos	4	Daño Físico – Mal Estado	Falta de Mantenimiento	Física
		Daño Físico – Mal Estado	Equipos Obsoletos	Física
		Daño Físico – Mal Estado	Equipos Ubicados en zonas de riesgos	Física
Internet	4	Daño a los puntos de acceso con malware	Baja o nula seguridad de navegación	Enlace de Datos
		Paralización – Suspensión de la comunicación o del servicio	Proceso de Enrutamiento comprometido	Enlace de Datos
		Paralización – Suspensión de la comunicación o del servicio	Falta y/o mala administración de recursos.	Enlace de Datos
Archivos - Documentación	3.67	Acceso o uso no previsto ni autorizado	Falta de control de acceso	Sesión
		Acceso o uso no previsto ni autorizado	Inexistencia de clasificación de información	Sesión
		Filtración de Información	Uso de dispositivos de almacenamiento extraíbles	Transporte
		Filtración de Información	Falta de control de transferencia de archivos por red	Transporte
		Alteración de Información	Ingreso o modificación de información de manera errónea	Presentación
		Pérdida de información	Falta de plan de respaldos	Presentación
Correo Electrónico	3	Acceso o uso no previsto ni autorizado	Error en credenciales	Sesión
		Acceso o uso no previsto ni autorizado	Falta de control de seguridad	Sesión
		Daño al Servicio con mal intención	Sistema obsoleto	Aplicación
		Filtración de Información	Falta de control de transferencia de archivos por red	Transporte
		Paralización – Suspensión de la comunicación o del servicio	Falta y/o mala administración de recursos.	Enlace de Datos
Impresoras	2.67	Daño Físico – Mal estado	Falta de Mantenimiento	Físico
		Daño Físico – Mal estado	Partes deterioradas por longevidad	Físico

2.5.1.3 Evaluación del Riesgo

Para determinar los niveles que posee un riesgo, se considera optar por los siguientes parámetros:

- Impacto económico.
- Tiempo de recuperación de la empresa.
- Posibilidad real de que ocurra el riesgo.
- Posibilidad de pausar las actividades de la empresa

De igual manera para determinar el grado de impacto que puede alcanzar cada uno de los parámetros, se pone a consideración valores como se observa en la **Tabla 11.**

Tabla 11. Grado de Impacto

Nivel de Impacto	Valor
Muy Bajo	1
Bajo	2
Medio	3
Alto	4
Muy Alto	5

2.5.1.3.1 Cálculo del Riesgo

Para determinar el valor de que ocurra el riesgo en base a una amenaza existente, se considera el valor del activo y el valor asignado de que ocurra dicha amenaza, manejándolos en el resultante del producto de dichas variables, obteniendo el Valor del riesgo por amenaza. En la **Tabla 12** se detalla la fórmula establecida.

Tabla 12. Fórmula de Cálculo del Riesgo

Variables	Fórmula
Va: Valor Activo	Vr= Va*Vp
Vr: Valor del Riesgo	
Vp: Valor de Probabilidad	

Para definir el nivel de aceptación del Riesgo se ha diseñado una escala, la cual se detalla en la **Tabla 13**, y la evaluación del riesgo en la **Tabla 14.**

Tabla 13. Nivel de Aceptación del Riesgo

Rango	Nivel	Acción	Identificación
0 - 6	Aceptable	No aplicar controles	
7 - 12	Bajo	Aplicar controles para considerar aceptable	
13 - 18	Medio	Aplicar controles para considerar bajo o menor	
19 - 25	Alto	Aplicar controles para considerar medio o menor	

Tabla 14. Variables de Aplicación

Variables
Va: Valor Activo
Pma: Probabilidad Más alta de Ocurrencia de Amenaza
Vp: Valor de Probabilidad de Amenaza
Vr: Valor de Riesgo
Vra: Valor de Riesgo del Activo
Ec: Económico
Tr; Tiempo de Recuperación
Lg: Legal
Im: Imagen
Ia: Interrupción de Actividades
Vtir: Valor Total Impacto del Riesgo

Tabla 15. Análisis y Evaluación del Riesgo

									Impacto					
Activo/Bien	**Va**	**Pma**	**Amenaza**	**Vulnerabilidad**	**Capa Involucrada**	**Vp**	**Vr**	**Vra**	**Ec**	**Tr**	**Lg**	**Im**	**Ia**	**Vtir**
Servidor	5	5	Daño al software con mal intención.	Sistema operativo obsoleto	Aplicación	3	15	25	4	3	1	3	5	3.2
			Daño al software con mal intención	Software pirata - virus	Aplicación	3	15							
			Daño Físico – Mal estado	Falta de Mantenimiento	Física	4	20							
			Daño Físico – Mal estado	Partes deterioradas por longevidad	Física	3	15							
			Daño Físico – Mal Estado	Equipos Ubicados en zonas de riesgos	Física	5	25							
			Paralización – Suspensión de la comunicación o del servicio	Falta y/o mala administración de recursos.	Enlace de Datos	4	20							
			Falla de Acceso Lógico	Baja o nula seguridad de acceso.	Sesión	3	15							
			Desastre Natural	Inexistencia de plan de emergencia ante desastres	---------	5	25							
Infraestructura de Red	5	4	Daño Físico – Mal Estado	Periféricos desgastados	Física	4	20	20	4	3	1	3	5	3.2
			Daño Físico – Mal Estado	Defectos de fábrica de Periféricos	Física	3	15							
			Paralización – Suspensión de la comunicación o del servicio	Falta y/o mala administración de recursos.	Enlace de Datos	3	15							
			Uso indebido del acceso	Falta de controles de acceso y privilegios otorgados.	Sesión	3	15							
			Falla de Acceso Lógico	Baja o nula seguridad de acceso.	Sesión	4	20							
Sistema Contable	5	4	Paralización – Suspensión de la comunicación o del	Falta y/o mala administración de recursos.	Enlace de Datos	4	20	20	3	4	1	3	5	3.2

			servicio										
			Uso indebido del acceso	Falta de controles de acceso y privilegios otorgados.	Sesión	2	10						
			Filtración de Información	Ausencia de auditoría y control	Transporte	2	10						
			Falla de Acceso Lógico	Baja o nula seguridad de acceso.	Sesión	2	10						
Sistema Video Vigilancia	4.67	4	Daño Físico – Mal Estado	Falta de Mantenimiento	Física	3	14.01	18.68	5	4	1	1	3	2.8
			Daño Físico – Mal Estado	Equipos Obsoletos	Física	4	18.68						
			Daño Físico – Mal Estado	Equipos Ubicados en zonas de riesgos	Física	4	18.68						
			Daño Lógico	Falta de controles de acceso al sistema	Sesión	3	14.01						
			Falla de Acceso Lógico	Baja o nula seguridad de acceso.	Sesión	3	14.01						
			Paralización – Suspensión de la comunicación o del servicio	Falta y/o mala administración de recursos.	Enlace de Datos	3	14.01						
Talento Humano	4.33	3	Indisponibilidad del Personal	Pérdida o Enfermedad	---------	2	8.66	12.99	2	4	2	1	4	2.6
			Errores por falta de conocimiento o de concentración	Personal con poca motivación	---------	3	12.99						
			Sistemas maliciosos en equipos celulares	Dispositivos con baja o nula seguridad ante malware	Aplicación	3	12.99						
Computadoras/ Laptops	4	4	Daño Físico – Mal Estado	Falta de Mantenimiento	Física	3	12	16	4	4	1	1	2	2.4
			Daño Físico – Mal Estado	Equipos Obsoletos	Física	4	16						
			Daño Físico – Mal Estado	Equipos Ubicados en zonas de riesgos	Física	4	16						
			Daño al software con mal intención.	Sistema operativo obsoleto	Aplicación	4	16						

			Daño al software con mal intención	Software pirata - virus	Aplicación	4	16							
			Falla de Acceso Lógico	Baja o nula seguridad de acceso.	Sesión	3	12							
			Desastre Natural	Inexistencia de plan de emergencia ante desastres	---------	3	12							
Sistema de Rastro de Movimientos	4	4	Daño Físico – Mal Estado	Falta de Mantenimiento	Física	4	16	16	4	3	1	1	1	2
			Daño Físico – Mal Estado	Equipos Obsoletos	Física	4	16							
			Daño Físico – Mal Estado	Equipos Ubicados en zonas de riesgos	Física	3	12							
Internet	4	4	Daño a los puntos de acceso con malware	Baja o nula seguridad de navegación	Enlace de Datos	4	16	16	3	4	1	3	3	2.8
			Paralización – Suspensión de la comunicación o del servicio	Proceso de Enrutamiento comprometido	Enlace de Datos	3	12							
			Paralización – Suspensión de la comunicación o del servicio	Falta y/o mala administración de recursos.	Enlace de Datos	3	12							
Archivos - Documentación	3.67	3	Acceso o uso no previsto ni autorizado	Falta de control de acceso	Sesión	3	11.01	11.01	2	3	1	1	3	2
			Acceso o uso no previsto ni autorizado	Inexistencia de clasificación de información	Sesión	3	11.01							
			Filtración de Información	Uso de dispositivos de almacenamiento extraíbles	Transporte	2	7.34							
			Filtración de Información	Falta de control de transferencia de archivos por red	Transporte	2	7.34							
			Alteración de Información	Ingreso o modificación de información de manera errónea	Presentación	2	7.34							
			Pérdida de información	Falta de plan de respaldos	Presentación	3	11.01							
Correo Electrónico	3	3	Acceso o uso no previsto ni autorizado	Error en credenciales	Sesión	2	6	9	1	3	3	3	3	2.6

			Acceso o uso no previsto ni autorizado	Falta de control de seguridad	Sesión	2	6							
			Daño al Servicio con mal intención	Sistema obsoleto	Aplicación	2	6							
			Filtración de Información	Falta de control de transferencia de archivos por red	Transporte	3	9							
			Paralización – Suspensión de la comunicación o del servicio	Falta y/o mala administración de recursos.	Enlace de Datos	3	9							
Impresoras	2.67	3	Daño Físico – Mal estado	Falta de Mantenimiento	Físico	2	5.34	8.01	4	3	1	1	2	2.2
			Daño Físico – Mal estado	Partes deterioradas por longevidad	Físico	3	8.01							

2.5.2 Estrategias para Tratamiento del Riesgo

Teniendo la clasificación y cálculo del índice riesgos, es necesario determinar qué hacer con el mismo, la metodología propone 4 fases relevantes a consideración para un óptimo desenlace del riesgo existente, mismas que se detallan en la **Tabla 16.**

Tabla 16. Estrategias de Tratamiento de Riesgo

Metodología	Significado
Reducir	Se aplican procesos o medidas de control según propone la Norma.
Evitar	Consiste en cambiar actividades o la forma de desempeño, con la finalidad de evitar la presencia del riesgo.
Transferir	Consiste en darle paso de responsabilidad a un agente externo que se encargue del riesgo, cuando los dos primeros puntos no son suficiente.
Aceptar	Consiste en aceptar la responsabilidad de correr el riesgo existente, teniendo en cuenta que no se lo puede mitigar por distintos factores.

2.5.3 Plan de Tratamiento de Riesgo

Una vez que ya se han recolectado los datos y evaluado los parámetros correspondientes a las amenazas, vulnerabilidades y el valor de probabilidad de que se ejecute el riesgo, se debe determinar la mejor opción de manejo y control para el tratamiento de dichos riesgos, tal como se plasma en la **Tabla 17**.

Tabla 17. Plan de Tratamiento del Riesgo

Activo/Bien	Amenaza	Vulnerabilidad	Capa Involucrada	Opción de Tratamiento	Medidas de Control
Servidor	Daño al software con mal intención.	Sistema operativo obsoleto	Aplicación	Reducción	Monitoreo del uso del sistema.
	Daño al software con mal intención	Software pirata - virus	Aplicación		Controles contra software malicioso
	Daño Físico – Mal estado	Falta de Mantenimiento	Física		Mantenimiento de equipos
	Daño Físico – Mal estado	Partes deterioradas por longevidad	Física		Mantenimiento de equipos
	Daño Físico – Mal Estado	Equipos Ubicados en zonas de riesgos	Física		Instalación y protección de equipos
	Paralización – Suspensión de la comunicación o del servicio	Falta y/o mala administración de recursos.	Enlace de Datos		Planificación de la Capacidad
	Falla de Acceso Lógico	Baja o nula seguridad de acceso.	Sesión		Diagnóstico remoto y configuración de protección de seguridad de los puertos.
	Desastre Natural	Inexistencia de plan de emergencia ante desastres	---------		Protección contra amenazas externas y ambientales
Infraestructura de Red	Daño Físico – Mal Estado	Periféricos desgastados	Física	Reducción	Mantenimiento de equipos
	Daño Físico – Mal Estado	Defectos de fábrica de Periféricos	Física		Mantenimiento de equipos
	Paralización – Suspensión de la comunicación o del servicio	Falta y/o mala administración de recursos.	Enlace de Datos		Planificación de la capacidad
	Uso indebido del acceso	Falta de controles de acceso y privilegios otorgados.	Sesión		Control de conexión a las redes
	Falla de Acceso Lógico	Baja o nula seguridad de acceso.	Sesión		Diagnóstico remoto y configuración de protección de seguridad de los puertos.
Sistema Contable	Paralización – Suspensión de la comunicación o del servicio	Falta y/o mala administración de recursos.	Enlace de Datos	Reducción	Planificación de la capacidad
	Uso indebido del acceso	Falta de controles de acceso y privilegios otorgados.	Sesión		Política de control de accesos
	Filtración de Información	Ausencia de auditoría y control	Transporte		Salvaguardar los registros de la organización
	Falla de Acceso Lógico	Baja o nula seguridad de acceso.	Sesión		Gestión de Privilegios

Sistema Video Vigilancia	Daño Físico – Mal Estado	Falta de Mantenimiento	Física	Reducción	Mantenimiento de equipos
	Daño Físico – Mal Estado	Equipos Obsoletos	Física		Mantenimiento de equipos
	Daño Físico – Mal Estado	Equipos Ubicados en zonas de riesgos	Física		Instalación y protección de equipos
	Daño Lógico	Falta de controles de acceso al sistema	Sesión		Política de control de acceso
	Falla de Acceso Lógico	Baja o nula seguridad de acceso.	Sesión		Seguridad de los servicios de red
	Paralización – Suspensión de la comunicación o del servicio	Falta y/o mala administración de recursos.	Enlace de Datos		Planificación de la capacidad
Talento Humano	Indisponibilidad del Personal	Pérdida o Enfermedad	---------	Reducción	Segregación de tareas.
	Errores por falta de conocimiento o de concentración	Personal con poca motivación	---------		Inclusión de la seguridad en las responsabilidades y funciones laborales
	Sistemas maliciosos en equipos celulares	Dispositivos con baja o nula seguridad ante malware	Aplicación		Seguridad de oficinas, despachos y recursos
Computadoras/ Laptops	Daño Físico – Mal Estado	Falta de Mantenimiento	Física	Reducción	Mantenimiento de equipos
	Daño Físico – Mal Estado	Equipos Obsoletos	Física		Mantenimiento de equipos
	Daño Físico – Mal Estado	Equipos Ubicados en zonas de riesgos	Física		Instalación y protección de equipos
	Daño al software con mal intención.	Sistema operativo obsoleto	Aplicación		Monitoreo del uso del sistema
	Daño al software con mal intención	Software pirata - virus	Aplicación		Controles contra software malicioso
	Falla de Acceso Lógico	Baja o nula seguridad de acceso.	Sesión		Diagnóstico remoto y configuración de protección de seguridad de los puertos.
	Desastre Natural	Inexistencia de plan de emergencia ante desastres	---------		Protección contra amenazas externas y ambientales
Sistema de Rastro de Movimientos	Daño Físico – Mal Estado	Falta de Mantenimiento	Física	Transferir	Comunicar con agencia de seguridad para que brinde el mantenimiento correspondiente.
	Daño Físico – Mal Estado	Equipos Obsoletos	Física		
	Daño Físico – Mal Estado	Equipos Ubicados en zonas de riesgos	Física		
Internet	Daño a los puntos de acceso con malware	Baja o nula seguridad de navegación	Enlace de Datos	Transferir	Aumento de seguridad en los servicios de red
	Paralización – Suspensión de la	Proceso de Enrutamiento	Enlace de Datos		Control de conexión

	comunicación o del servicio	comprometido			
	Paralización – Suspensión de la comunicación o del servicio	Falta y/o mala administración de recursos.	Enlace de Datos		Planificación de la Capacidad
Archivos - Documentación	Acceso o uso no previsto ni autorizado	Falta de control de acceso	Sesión	Reducción	Identificación y autenticación de usuario
	Acceso o uso no previsto ni autorizado	Inexistencia de clasificación de información	Sesión		Identificación y autenticación de usuario
	Filtración de Información	Uso de dispositivos de almacenamiento extraíbles	Transporte		Gestión de los medios removibles
	Filtración de Información	Falta de control de transferencia de archivos por red	Transporte		Aumento de seguridad en los servicios de red
	Alteración de Información	Ingreso o modificación de información de manera errónea	Presentación		Validación de datos de entrada
	Pérdida de información	Falta de plan de respaldos	Presentación		Salvaguardar los registros de la organización
Correo Electrónico	Acceso o uso no previsto ni autorizado	Error en credenciales	Sesión	Reducción	Validación de datos de entrada
	Acceso o uso no previsto ni autorizado	Falta de control de seguridad	Sesión		Aumento de seguridad en los servicios de red
	Daño al Servicio con mal intención	Sistema obsoleto	Aplicación		Controles contra software malicioso
	Filtración de Información	Falta de control de transferencia de archivos por red	Transporte		Aumento de seguridad en los servicios de red
	Paralización – Suspensión de la comunicación o del servicio	Falta y/o mala administración de recursos.	Enlace de Datos		Planificación de los Recursos
Impresoras	Daño Físico – Mal estado	Falta de Mantenimiento	Físico	Reducción	Mantenimiento de equipos
	Daño Físico – Mal estado	Partes deterioradas por longevidad	Físico		Mantenimiento de equipos

2.5.4 Plan de Mejora basado en los Principios de la Metodología OSSTMM

En primera instancia se planea que la infraestructura de red se rediseñe a nivel de que se administre y se acceda a ella de manera más eficiente resultando en la siguiente:

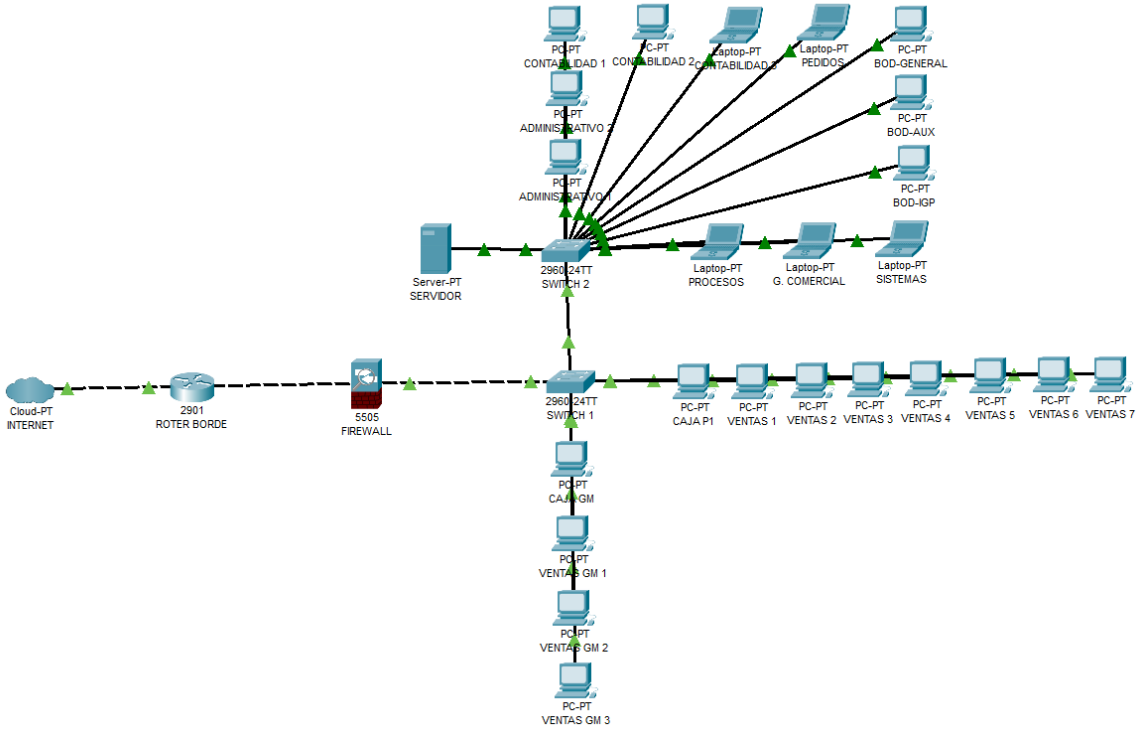


Figura 21. Propuesta de Infraestructura de Red

2.5.4.1 Principio de Seguridad de la Información

Dentro de los parámetros que ofrece el principio se establece como optimización parala seguridad de la empresa lo siguiente:

- Teniendo la aplicación de Administración de Mikrotik RouterOS Winbox, establecer reglas de firewall adicionales a las que actualmente posee, con la finalidad de controlar el tráfico de entrada y salida.
- Manejar respaldos en la nube de la información y base de datos existentes en el servidor, con la finalidad de protegerlo de manera cifrada y tener acceso a ella a nivel de multiplataforma de manera escalable.
- Implementar un sistema de antivirus que sea administrable para con ello eliminar o bloquear softwares maliciosos.

2.5.4.2 Principio de Seguridad de los Procesos

Para el manejo de información se sugiere trabajar bajo las siguientes normativas:

- Todo equipo de cómputo debe ser de uso personal, a excepción de los de puntos de atención al cliente, además de ser protegidos mediante contraseña requerida para inicio de sesión.
- Cada documento de margen delicado, debe ser manejado mediante cifrado con contraseña y con respaldo mediante correo electrónico, para con ello evitar pérdidas en caso de fallo del equipo de cómputo.
- Para la selección de personal de confiabilidad y designio de responsabilidades, se recomienda realizar pruebas de aptitud y psicológicas previamente a la asignación de documentación, para mediante los resultados determinar si es oportuna o no la actividad a otorgarse.

2.5.4.3 Principio de Seguridad en las Tecnologías de Internet

Para la optimización de este parámetro, es oportuno realizar el punto 3.2.1, ya que, al reestablecer la infraestructura de red, se mejorará la comunicación con el router de borde y con ello la salida a internet. Con respecto a la seguridad de los periféricos computacionales, se plantea:

- Contratar un sistema de monitoreo de Red, como la herramienta utilizada, con la finalidad de llevar un control en tiempo real de lo que sucede en la infraestructura de red para con ello tener un conocimiento del comportamiento que tiene durante tiempo de ejecución.
- Cambiar los equipos que no brinden un correcto enrutamiento y ocasionen pérdidas de datos.
- A través de la Herramienta Winbox, establecer reglas de ancho de banda y bloqueo de páginas no comerciales ni empresariales, con la finalidad de reducir el consumo de ancho de banda de manera innecesaria, otorgando enfoque en la comunicación con el servidor y con las consultas necesarias para los procesos requeridos.

2.5.4.4 Principio de Seguridad en las Comunicaciones

Al evaluar el router de borde y la puerta de enlace se determina lo siguiente:

- Mantener un monitoreo constante con la finalidad de reducir la itinerancia de datos y la pérdida de comunicación con el enlace a la intranet.
- Establecer subredes privadas que solo sean visibles a nivel interno, con la finalidad de que no se vuelvan vulnerables al ser detectada la red por un agente externo.

2.5.4.5 Principio de Seguridad Inalámbrica

Para reforzar la seguridad al sistema de seguridad inalámbrica se propone:

- Brindar mantenimiento preventivo a los sensores de movimiento por control infrarrojo en tiempo predeterminado, para alargar la vida útil de los mismos.
- Revisar el sistema de alarma se encuentre configurado y emparejado con la zona correspondiente a cada uno de los sensores de movimiento.
- Calibrar la sensibilidad de los sensores para que no brinden falsas alarmas.

2.5.4.6 Principio de Seguridad Física

Dentro de este principio, también es primordial que se realice el punto 3.2.1 ya que de ello depende la optimización de seguridad de este nivel. Para mejorar la seguridad física de la infraestructura de red dentro de Grupo Guerrero Portilla, es primordial que se realice lo siguiente:

- Designación de un cuarto de datos en el cual se ubiquen dispositivos de enrutamiento, dispositivos de video grabación y video seguridad (nvr - dvr), mediante la estructura física correspondiente, sea esta un gabinete de pared o base.
- Tomar como diagrama ejemplo al de la propuesta y emplearlo de manera física, identificando mediante etiquetación cada uno de los enlaces salientes de los switchs de alimentación.
- Sectorizar y segmentar cada periférico por actividad o grupo dedicado para lo que se lo va a emplear, independientemente cuál sea dicho periférico.

2.5.5 Requerimientos de Mejora

Para el desarrollo de optimización, se ha considerado los recursos existentes que posee actualmente la institución, con la finalidad de mitigar gastos innecesarios o redundantes en suministros y equipos necesarios para la implementación de las mejoras propuestas, por ende, se ha desarrollado un presupuesto de dichos periféricos que se pueden apreciar en la **Tabla 18.**

Como punto adicional, se plantea requerimientos necesarios por cada principio, con enfoque a mejor y optimización de cada uno de los procesos; mejorando de tal manera la seguridad física, lógica, sistemática y de usuario. Todo esto se puede apreciar en la **Tabla 19**.

Tabla 18. Presupuesto de Mejora de Seguridad

Producto/ Material	**Costo**
Firewall Fortinet	$3500,00
Cable UTP Categoría 6A	$150,00
Conectores RJ45 Categoría 6A (X100)	$12,00
Estructura de Pared para switch (Gabinete Empotrado)	$42,00
Total	$3.704,00

Tabla 19. Lista de Requerimientos de Mejora

Descripción	Principio de Aplicación	Función
Sistema de Evaluación de Aptitudes	Seguridad de los Procesos	Determinar si un individuo es apto para funciones desempeño.
Sistema de Monitoreo de Red	Seguridad en las Tecnologías de Internet	Llevar un control más exacto del estado de la intranet, generando reportes, observando anomalías
Sistema de Protección Antivirus	Seguridad de la Información	Proteger a los equipos de cómputo de posibles ataques de softwares maliciosos, y si se presenta el caso, mitigarlos.
Espacio dedicado	Seguridad Física	Administrar todo lo correspondiente a sistemas en un solo lugar.
Ancho de Banda Dedicado	Seguridad en las Tecnologías de Internet	Brindar el fácil y rápido acceso a los usuarios finales, para el uso de los terminales en los requerimientos de navegación que se presenten, sin que se otorguen inconvenientes de carga.

3. CAPÍTULO 3: EVALUACIÓN DEL PROTOTIPO

3.1. Plan de Evaluación

En la actualidad existen varios métodos y herramientas de evaluación de riesgos y análisis de factibilidad de plan de mejora u optimización de sistemas de riesgos informáticos o de parámetros relacionados a ello, no obstante, para la evaluación del plan de mejora establecido para el caso estudiado se utilizará un proceso de recolección de información a través de la realización de encuestas a expertos que posean conocimientos o sean encargados de la seguridad a nivel de infraestructura de red, se propone obtener respuestas a un grupo de 12 expertos, con un banco de preguntas pertinentes a la propuesta planteada como solución de la problemática. Las respuestas serán respecto al nivel de concordancia existente con respecto a la solución planteada y el criterio de cada uno de ellos ante un escenario similar. Para establecer rangos se ha considerado trabajarlo mediante una escala de Likert, en la cual se han planteado las opciones entre Muy de acuerdo, De acuerdo, Neutral. En Desacuerdo y en Muy desacuerdo, con la finalidad de obtener algunos puntos de vista referente al caso planteado

3.2. Resultado de Evaluación

Obtenida la información que brindó la encuesta de factibilidad realizada a un número de 12 expertos exactamente, se presentan resultados en gráficos estadísticos con las decisiones optadas, misma información que se puede observar en la **Tabla 20** conociendo la escala de evaluación y desde la **Tabla 21** a la **Tabla 42** conocer la interpretación que conlleva la recolección informativa.

Tabla 20. Tabla de Rangos

Nivel de Evaluación	Valor
Muy de Acuerdo	5
De Acuerdo	4
Neutral	3
En Desacuerdo	2
Muy en Desacuerdo	1

Tabla 21. Análisis de Pregunta 1

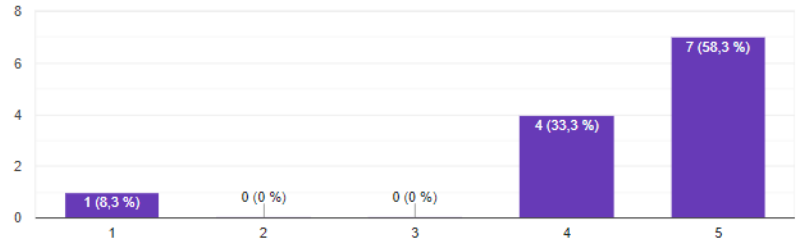
PREGUNTA	GRÁFICO ESTADÍSTICO
¿Cuán factible considera Ud. la aplicación del Plan de Mejora para fortalecer la **Seguridad de la Información** en la Empresa?	 *Figura 22. Pregunta 1*
INTERPRETACIÓN	En un 58.3%, los expertos encuentran con mayor grado de concordancia respecto a la opción de “Muy De acuerdo”, seguido de un 33.3% con un grado de “Acuerdo”, representando un total de 91.6% de factibilidad.

Tabla 22. Análisis de Pregunta 2

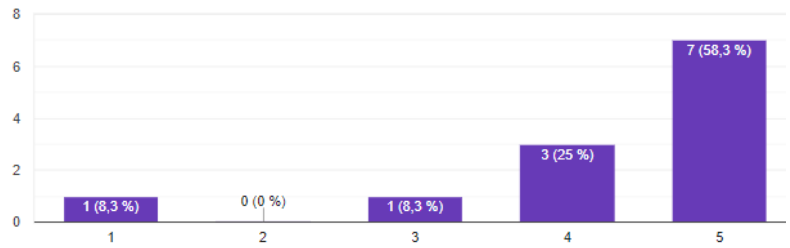
PREGUNTA	GRÁFICO ESTADÍSTICO
¿Cuán factible considera Ud. la aplicación de un Plan de Mejora para fortalecer la **Seguridad de los Procesos** en la Empresa?	 *Figura 23. Pregunta 2*
INTERPRETACIÓN	En un 58.3%, los expertos encuentran con mayor grado de concordancia respecto a la opción de “Muy De acuerdo”, en conjunto a un 25% del parámetro “De acuerdo”, representando un 83.3% como opción más considerable para el caso.

Tabla 23. Análisis de Pregunta 3

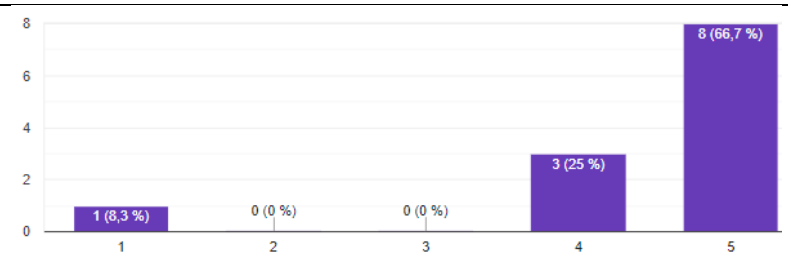
PREGUNTA	GRÁFICO ESTADÍSTICO
¿Cuán factible considera Ud. la aplicación de un Plan de Mejora para fortalecer la **Seguridad de la Infraestructura de Red** en la Empresa?	 *Figura 24. Pregunta 3*
INTERPRETACIÓN	Con un total de 66.7%, los expertos encuentran con mayor grado de concordancia respecto a la opción de “Muy De acuerdo” y un 25% a la opción “De Acuerdo”, representando un 91.7% siendo la opción más considerable para el caso.

Tabla 24. Análisis de Pregunta 4

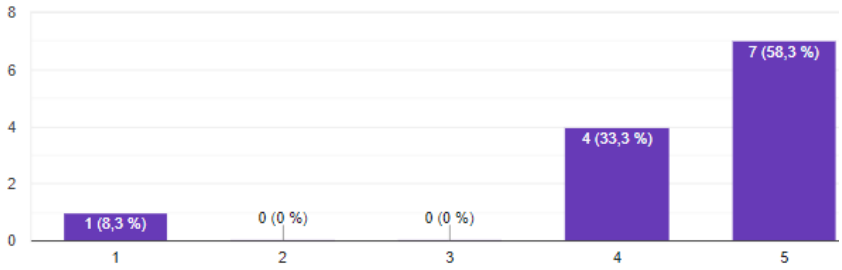
PREGUNTA	GRÁFICO ESTADÍSTICO
¿Cuán factible considera Ud. la aplicación de un Plan de Mejora para fortalecer la **Seguridad en las Comunicaciones** en la Empresa?	 *Figura 25. Pregunta 4*
INTERPRETACIÓN	Con un porcentaje de 58.3% y 33.3%, los expertos coinciden en estar "Muy de Acuerdo y de Acuerdo" respectivamente en base a la interrogante dando un total de aceptación de 91.6%

Tabla 25. Análisis de Pregunta 5

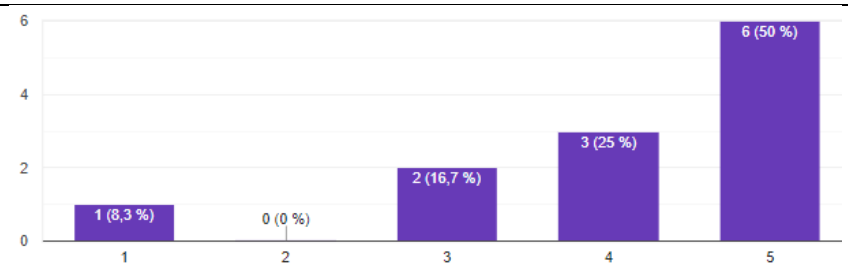
PREGUNTA	GRÁFICO ESTADÍSTICO
¿Cuán factible considera Ud. la aplicación de un Plan de Mejora para fortalecer la **Seguridad Inalámbrica** en la Empresa?	 *Figura 26. Pregunta 5*
INTERPRETACIÓN	Con un 50% y 25% de aceptación tanto en "Muy de Acuerdo y De Acuerdo" respectivamente, dando un 75% de factibilidad de implementación de la propuesta

Tabla 26. Análisis de la Pregunta 6

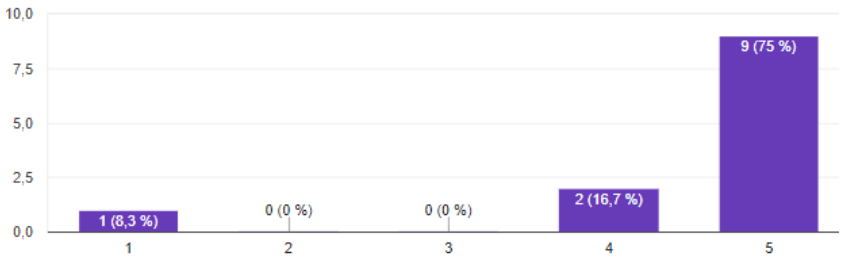
PREGUNTA	GRÁFICO ESTADÍSTICO
¿Cuán factible considera Ud. la aplicación de un Plan de Mejora para fortalecer la **Seguridad Física** en la Empresa?	 *Figura 27. Pregunta 6*
INTERPRETACIÓN	Con un porcentaje de aceptación de un 75%, los expertos consideran estar "Muy de acuerdo" y un 16.7% en estar "De acuerdo" a la propuesta planteada, con un total de 91.7%

Tabla 27. Análisis de Pregunta 7

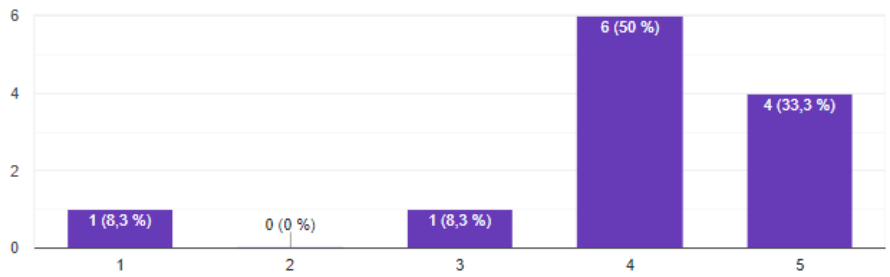
PREGUNTA	GRÁFICO ESTADÍSTICO
¿Qué tan factible considera Ud. el empleo de Opción de Tratamiento de **Reducción** como Medida de Tratamiento de Riesgo?	
INTERPRETACIÓN	La mitad de los expertos se encuentran "De acuerdo" al método de Reducción y un 33.33% están "Muy de Acuerdo", dando un nivel de aceptación de 83.3%.

Figura 28. Pregunta 7

Tabla 28. Análisis de Pregunta 8

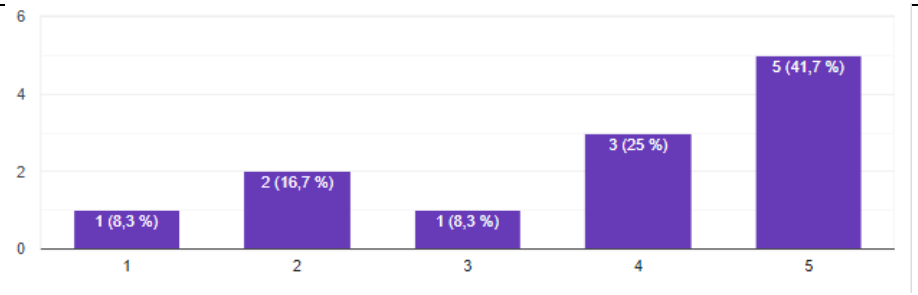
PREGUNTA	GRÁFICO ESTADÍSTICO
¿Qué tan factible considera Ud. el empleo de Opción de Tratamiento de **Evitar** como Medida de Tratamiento de Riesgo?	
INTERPRETACIÓN	La mitad de los expertos se encuentran "Muy De acuerdo" al método de Evitar y un 25% están "De Acuerdo", dando un 75% de aceptación de la propuesta.

Figura 29. Pregunta 8

Tabla 29. Análisis de Pregunta 9

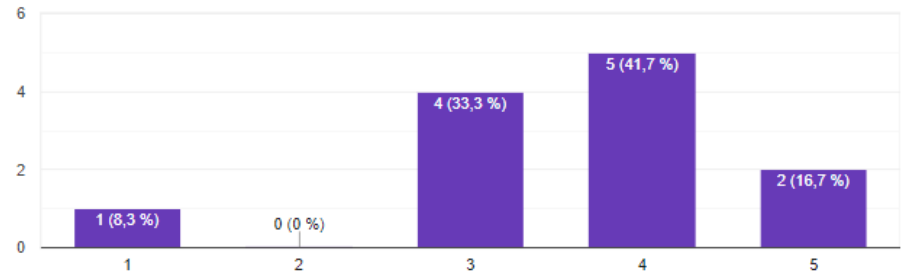
PREGUNTA	GRÁFICO ESTADÍSTICO
¿Qué tan factible considera Ud. el empleo de Opción de Tratamiento de **Transferir** como Medida de Tratamiento de Riesgo?	
INTERPRETACIÓN	Siendo un 50% de coincidencia en que los expertos consideran estar "De acuerdo" con la propuesta de la interrogante.

Figura 30. Pregunta 9

Tabla 30. Análisis de Pregunta 10

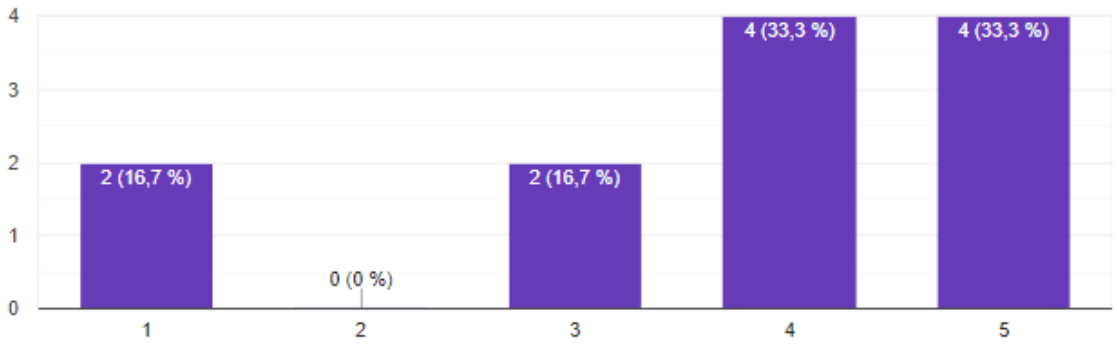
PREGUNTA	GRÁFICO ESTADÍSTICO
¿Qué tan factible considera Ud. el empleo de Opción de Tratamiento de **Aceptar** como Medida de Tratamiento de Riesgo?	
INTERPRETACIÓN	En esta interrogante se ha generado un 66.66% de concordancia considerada por los encuestados, siendo así una igualdad de 33.33% en estar "De acuerdo y Muy de Acuerdo" con la propuesta de la interrogante.

Figura 31. Pregunta 10

Tabla 31. Análisis de Pregunta 11

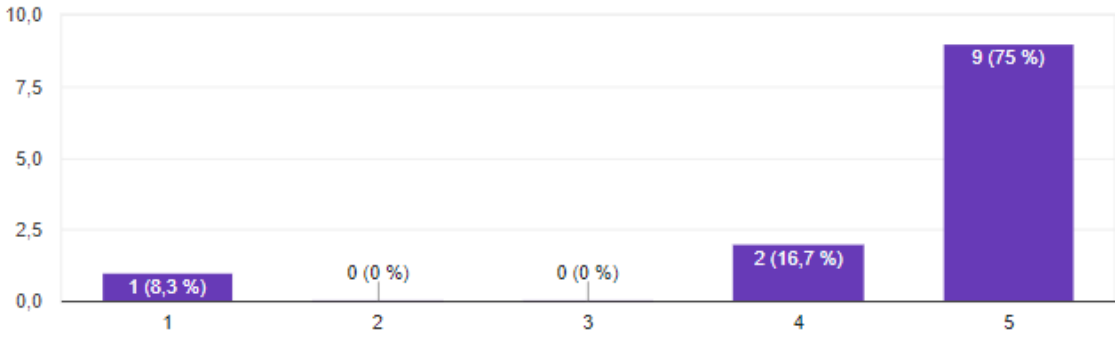
PREGUNTA	GRÁFICO ESTADÍSTICO
¿Qué tan factible considera Ud. el empleo de **Medidas de Control** como "Mantenimiento de Equipos" para reducir el impacto de "Daño Físico por Falta de Mantenimiento"?	
INTERPRETACIÓN	Como medida de control planteada, se considera "Muy de acuerdo" con un 75% y "De Acuerdo" con un 16.7% dando un 91.7% de factibilidad de ser aplicada, según los encuestados.

Figura 32. Pregunta 11

Tabla 32. Análisis de Pregunta 12

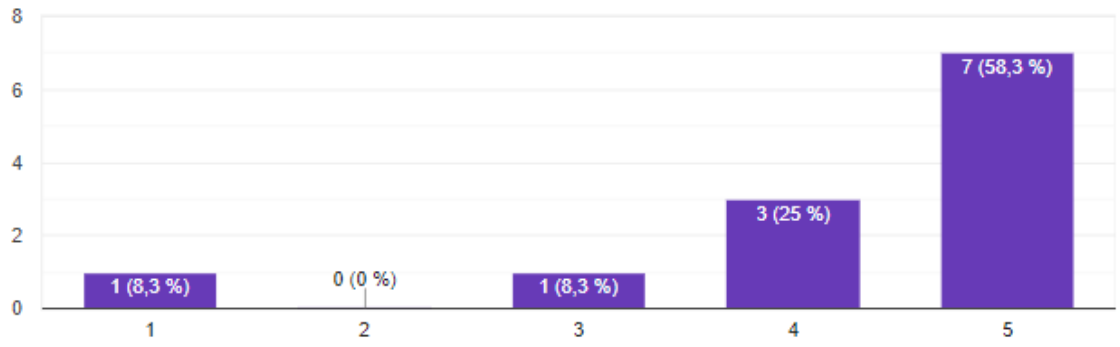
PREGUNTA	GRÁFICO ESTADÍSTICO
¿Qué tan factible considera Ud. el empleo de **Medidas de Control** como "Planificación de la Capacidad" para reducir el impacto de " Paralización – Suspensión de la comunicación o del servicio por Falta y/o Mala Administración de Recursos"?	
INTERPRETACIÓN	Como medida de control planteada, se considera "Muy de acuerdo" con un 58.3% Y "De Acuerdo" con un 25% de factibilidad con un total de 83.3% al ser aplicada, según los encuestados.

Figura 33. Pregunta 12

Tabla 33. Análisis de Pregunta 13

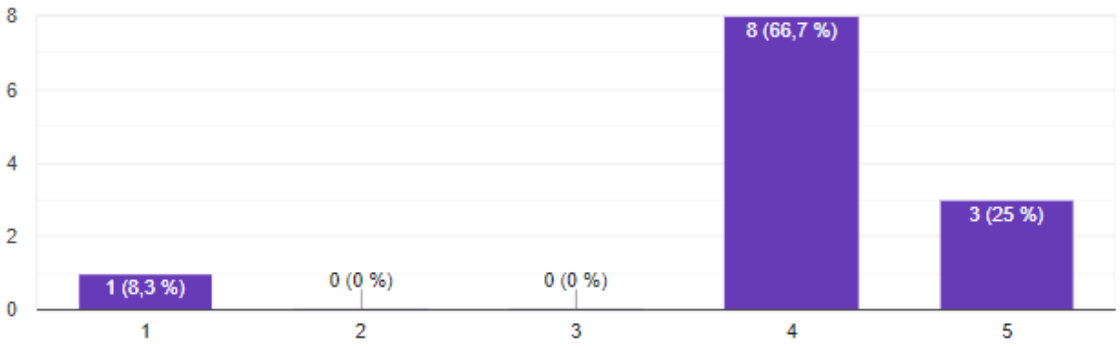
PREGUNTA	GRÁFICO ESTADÍSTICO
¿Qué tan factible considera Ud. el empleo de **Medidas de Control** como "Protección ante amenazas externas y ambientales" para reducir el impacto de " Desastre Natural por la Inexistencia de Plan de Emergencia ante Desastres"?	
INTERPRETACIÓN	Estando "De acuerdo" con la propuesta, se encuentra un 66.7% y "Muy de Acuerdo" con un 25%, se obtiene un 91.7% de sostenibilidad que es factible.

Figura 34.Pregunta 13

Tabla 34. Análisis de Pregunta 14

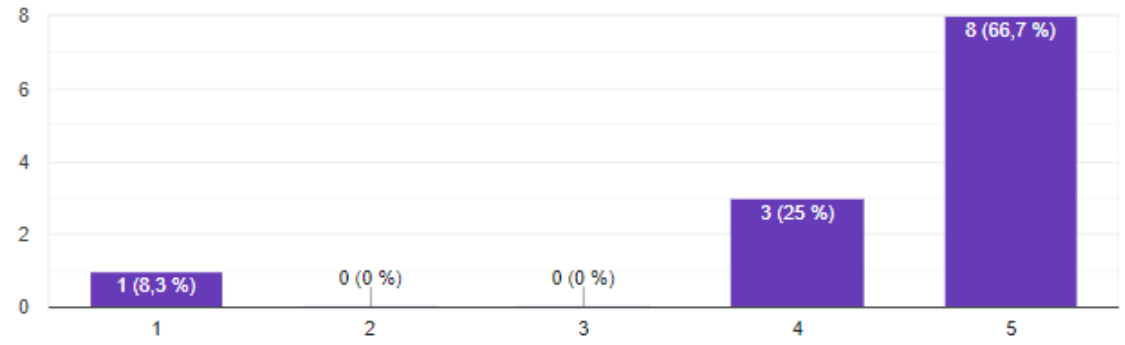
PREGUNTA	GRÁFICO ESTADÍSTICO
¿Qué tan factible considera Ud. el empleo de **Medidas de Control** como "Controles de Software Malicioso" para reducir el impacto de "Daño al software con mal intención por existencia de Software pirata - Virus"?	 *Figura 35. Pregunta 14*
INTERPRETACIÓN	Los resultados coinciden en estar "Muy de Acuerdo" con la propuesta, con un grado de aceptación de un 66.7% y de estar "De Acuerdo" con un grado de 25%, dando un total de aceptación de 91.7%.

Tabla 35. Análisis de Pregunta 15

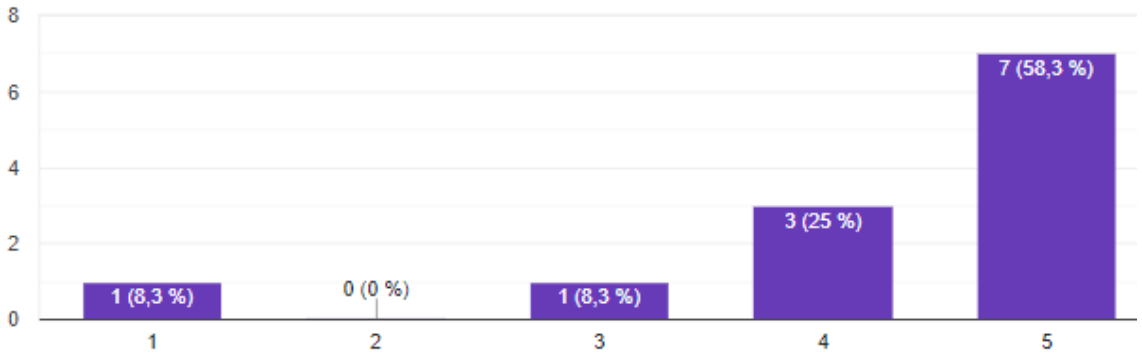
PREGUNTA	GRÁFICO ESTADÍSTICO
¿Qué tan factible considera Ud. el empleo de **Medidas de Control** como "Implementación de Política de control de accesos" para reducir el impacto de "Uso Indebido del acceso por Falta de controles de acceso y privilegios otorgados"?	 *Figura 36.Pregunta 15*
INTERPRETACIÓN	Los resultados coinciden en estar "Muy de Acuerdo" con la propuesta, con un grado de aceptación de un 58.3% y "De Acuerdo" en un 25%, dando como un total de aceptación de 83.3%

Tabla 36. Análisis de Pregunta 16

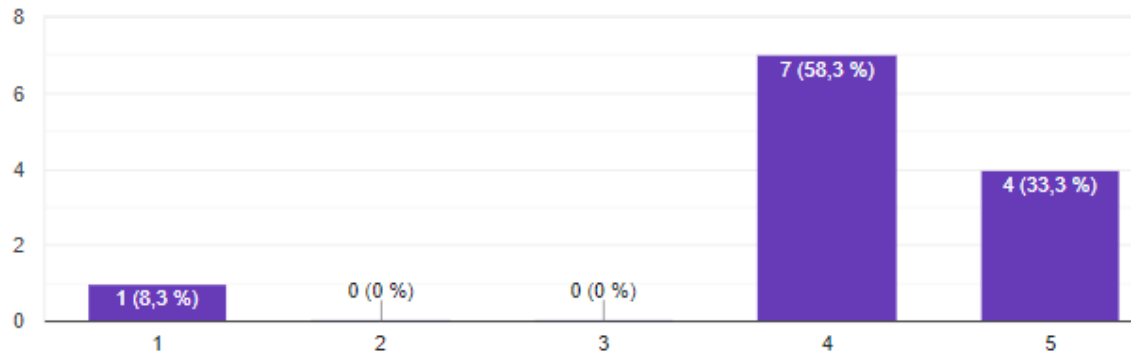
PREGUNTA	GRÁFICO ESTADÍSTICO
¿Qué tan factible considera Ud. el empleo de **Medidas de Control** como "Seguridad de Oficinas, despachos y recursos" para reducir el impacto de "Sistemas Maliciosos en Equipos Celulares en Dispositivos con baja o nula seguridad ante malware"?	
INTERPRETACIÓN	Según los resultados, la propuesta se considera aceptable con un grado de 58.3% estando "De acuerdo" y un 33.33% estando "Muy de Acuerdo", dando un 83.3% en total.

Figura 37. Pregunta 16

Tabla 37. Análisis de Pregunta 17

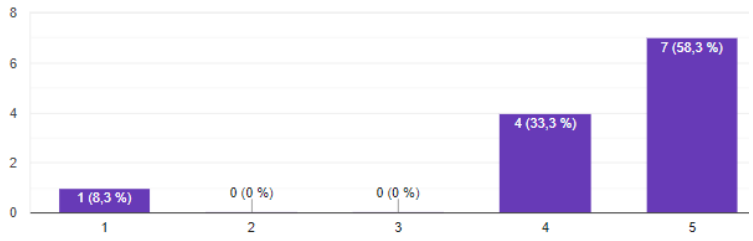
PREGUNTA	GRÁFICO ESTADÍSTICO
¿Qué tan factible considera Ud. el empleo de **Medidas de Control** como "Instalación y Protección de Equipos" para reducir el impacto de "Daño Físico o Mal estado a Equipos ubicados en zonas de Riesgos"?	
INTERPRETACIÓN	Los resultados coinciden en estar "Muy de Acuerdo" con la propuesta, con un grado de aceptación de un 58.3% y con uno de 33.3% de estar "De Acuerdo", danto un total de 83.3%

Figura 38. Pregunta 17

Tabla 38. Análisis de Pregunta 18

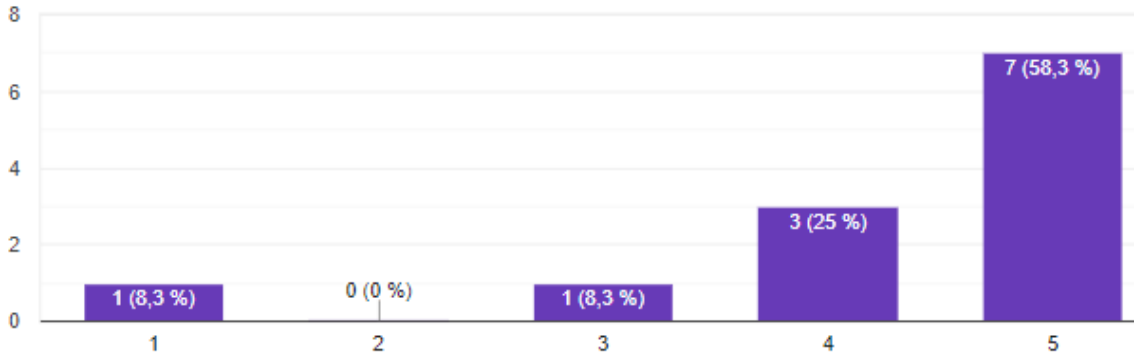
PREGUNTA	GRÁFICO ESTADÍSTICO
¿Qué tan factible considera Ud. el empleo de **Medidas de Control** como "Salvaguardar los Registros de la Organización" para reducir el impacto de "Pérdida de Información por Falta de plan de respaldo"?	
INTERPRETACIÓN	Los resultados brindan un grado de aceptación de 58.3% de estar "Muy de Acuerdo" y de 25% de estar "De Acuerdo" con la propuesta planteada en la interrogante, danto como grado total de aceptación un 83.3%

Figura 39. Pregunta 18

Tabla 39. Análisis de Pregunta 19

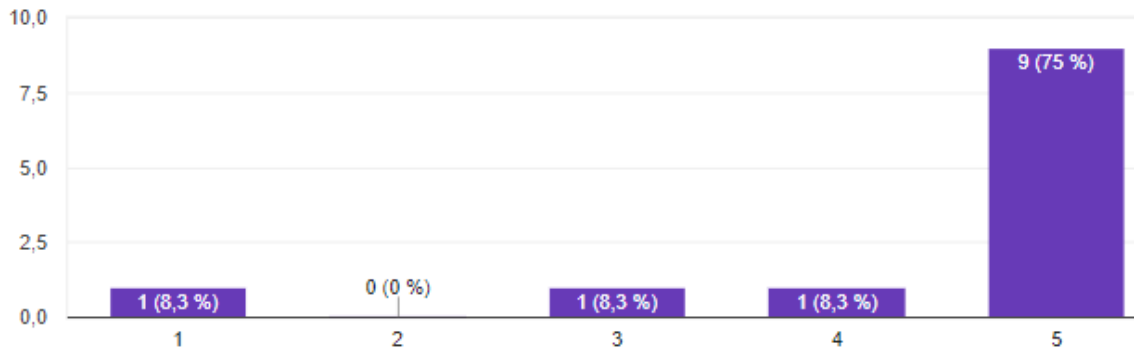
PREGUNTA	GRÁFICO ESTADÍSTICO
¿Qué tan factible considera Ud. el empleo de **Medidas de Control** como "Validación de datos de entrada" para reducir el impacto de "Alteración de Información por Ingreso o Modificación de Información de Manera Errónea"?	
INTERPRETACIÓN	Se obtienen resultados de estar "Muy de acuerdo" con la propuesta con un 75% de consideración y "De Acuerdo" con 8.3%, dando un resultante total de 83.3% de factibilidad.

Figura 40. Pregunta 19

Tabla 40. Análisis de Pregunta 20

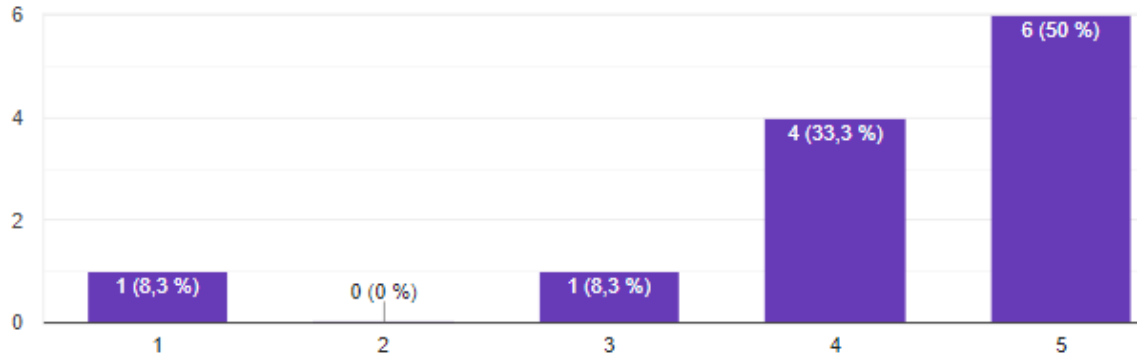
PREGUNTA	GRÁFICO ESTADÍSTICO
¿Qué tan factible considera Ud. el empleo de **Medidas de Control** como "Gestión de Medios Removibles" para reducir el impacto de "Filtración de Información por Uso de dispositivos de Almacenamiento Extraíbles"?	
INTERPRETACIÓN	Exactamente el 50% de encuestados coinciden en estar “Muy de Acuerdo”, mientras que un 33.3% coinciden en estar “De Acuerdo” en que la propuesta de la interrogante es factible.

Figura 41. Pregunta 20

Tabla 41. Análisis de Pregunta 21

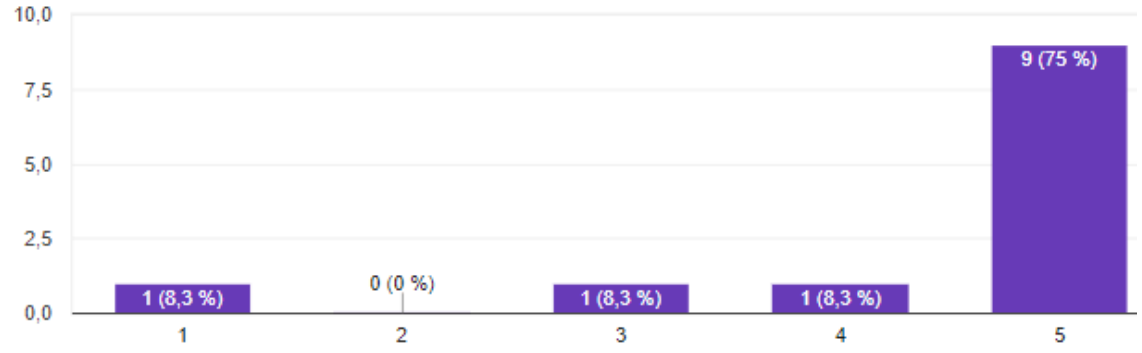
PREGUNTA	GRÁFICO ESTADÍSTICO
¿Qué tan factible considera Ud. el empleo de **Medidas de Control** como "Identificación y autenticación de Usuario" para reducir el impacto de "Acceso o uso no previsto ni autorizado por Inexistencia de Clasificación de Información"?	
INTERPRETACIÓN	Tomando en cuenta la propuesta en la interrogante, los resultados arrojan un 75% de aceptación, estando “Muy de Acuerdo” y un 8.3% en estar “De Acuerdo” en que es factible su implementación, con un valor total de 83.3%.

Figura 42. Pregunta 21

3.3. Conclusiones

Posterior a la realización de la evaluación de la infraestructura de red de Grupo Guerrero Portilla, se puede concluir que:

- Se ha analizado en totalidad el enlace de red existente en la intranet a través del uso de herramientas de testeo, dando a conocer los diversos puntos de conectividad y comunicación existentes.
- Se ha monitoreado cada dispositivo y la comunicación que poseen los puntos de red mediante el uso de software dedicado para su mayor evaluación y análisis.
- Se ha conseguido optimizar la diagramación de la infraestructura de red existente con la finalidad de brindar protección, todo esto gracias a las herramientas de simulación de red como Cisco Packet Tracer.
- Al finalizar el análisis de los datos recolectados previamente, se ha logrado identificar amenazas y vulnerabilidades, para con ello obtener un grado de impacto de que sucedan dichas amenazas, determinando así mismo el riesgo que podría ocasionarse, en base a eso se desarrolló un plan de seguridad y fortalecimiento de red mediante la aplicación de directivas, restricciones y/o bloqueos, adicional a mejoras de infraestructura como plan de optimización general utilizando propuestas que brinda el Anexo A de la Norma ISO 27001.
- Utilizando como método de evaluación a la metodología de análisis de sistemas de información que utiliza la Norma ISO 27001, se concluye que la propuesta planteada en base a los Principios de la Metodología OSSTMM, es factible; ya que comparten criterios de evaluación que determinan cuán oportuna es la ejecución e implementación de un plan de mejora en la seguridad de la información, haciendo énfasis en varios puntos de análisis.

3.4. Recomendaciones

Para un análisis de riesgos informáticos o vulnerabilidades dentro de una infraestructura de red, es recomendable:

- En la elección de herramientas a utilizar, tener en cuenta el alcance y la disponibilidad que posean las mismas, que sean las necesarias para satisfacer la demanda de requerimientos.
- Tener conocimiento de cada uno de los puntos de red físicos, pudiendo ser estos, equipos de enrutamiento, de cómputo, dispositivos de uso inalámbrico, entre otros.
- Conocer previamente el diagrama de red actual para tener una base por la cual partir y plantear una opción de mejora óptima.
- Monitorear en intervalos cortos de tiempo, para con ello tener respuestas más cercanas a la realidad con menos margen de error.

4. BIBLIOGRAFÍA

[1] H. Janampa Patilla, H. L. Huamani Santiago, y Y. Meneses Conislla, «Snort Oprn Source como detección de intrusos para la seguridad de la infraestructura de red», *SCIELO*, vol. 15, n.º 3, sep. 2021, [En línea]. Disponible en: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2227-18992021000300055

[2] Helmer Muñoz Hernández, L. G. Zapata Cantero, D. M. Requena Vidal, y L. Ricardo Villadiego, «Riesgos informáticos y alternativas para la seguridad informática en sistemas contables en Colombia», *Redalyc*, vol. 2, p. 11, 2019.

[3] C. Bracho Ortega, F. Cuzme Rodriguez, C. Pupiales Yepez, L. Suarez Zambrano, D. Peluffo Ordoñez, y C. Moreira Zambrano, «Auditoría de seguridad informática siguiendo la metodología OSSTMMv3: caso de estudio», *CEDIA*, p. 13, may 2017.

[4] K. A. Peñafiel Lucuy, «Factores que determinan la Vulneración Informática y el Desarrollo de una aplicación móvil para concientizar sobre los Impactos en los Activos», *Scielo*, vol. 21, p. 30, mar. 2021.

[5] L Zujovic, V Kecojevic, y D Bogunovic, «Application of a content management system for developing equipment safety training courses in surface mining», *SCIELO*, vol. 120, n.º 8, ago. 2020, [En línea]. Disponible en: http://www.scielo.org.za/scielo.php?script=sci_abstract&pid=S2225-62532020000800005

[6] H. Md Maqubool, K. Sumana, y T. Anjini Kumar, «Compact Filtenna for WLAN Applications», *SCIELO*, mar. 2019, doi: https://doi.org/10.1590/2179-10742019v18i11220.

[7] H. Facchini, S. Perez, A. Dantiacq, y F. Hidalgo, «Evaluación de métricas del comportamiento del tráfico de video en una red experimental multidifusión», *SCIELO*, vol. 11, n.º 1, Mazo 2020, doi: https://doi.org/10.29019/enfoque.v11n1.576.

[8] Khaled Alwasel *et al.*, «IoTSim-SDWAN: A simulation framework for interconnecting distributed datacenters over Software-Defined Wide Area Network (SD-WAN)», *ScienceDirect*, vol. 143, n.º 17-35, sep. 2020, doi: https://doi.org/10.1016/j.jpdc.2020.04.006.

[9] J. Orozco y G. Siles, «Estudio radioeléctrico y problemáticas en una red WiFi con alta densidad de usuarios», *SCIELO*, vol. 9, n.º 1, mar. 2019, [En línea]. Disponible en: http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S1683-07892019000100003&lang=es

[10] J. B. Mariño Arroyo, J. F. Márquez Camarena, y L. A. Núñez Lira, «Evaluation of a wireless Broadband Network for VoIP in Huaytará», *Redalyc*, vol. 10, n.º 4, dic. 2019, doi: https://doi.org/10.29019/enfoque.v10n4.513.

[11] E. Guerra, H. Neira, J. Diaz, y J. Patiño, «Desarrollo de un sistema de gestión para la seguridad de la información basado en metodología de identificación y análisis de riesgo en bibliotecas universitarias», *SCIELO*, vol. 32, n.º 5, oct. 2021, doi: http://dx.doi.org/10.4067/S0718-07642021000500145.

[12] P. Sánchez, J. García, A. Triana, y L. Perez, «Medida del nivel de seguridad informática de las pequeñas y medianas empresas (PYMEs) en Colombia», *SCIELO*, vol. 32, n.º 5, oct. 2021, doi: http://dx.doi.org/10.4067/S0718-07642021000500121.

[13] R. Perdigón Llanes, «Evaluación del rendimiento de cortafuegos basados en software libre», *SCIELO*, vol. 5, n.º 1, ene. 2022, doi: https://doi.org/10.37135/ns.01.09.03.

[14] B. Palate y D. Avila, «Mitigación de vulnerabilidades en la red central de un ISP», *Dialnet*, vol. 5, n.º 2, 2021, [En línea]. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=8266816

[15] M. Lescay Arias, L. A. Montoya Acosta, L. Estrada Ladoy, G. Torres de la Vega, y L. G. Barrera Yero, «Estrategia de superación para la utilización de proxmox y pfSense en las instituciones de salud», *SCIELO*, vol. 11, n.º 2, dic. 2019, [En línea]. Disponible en: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1684-18592019000200100&lang=es

[16] ISTOOLS, «¿Qué es la ISO 27001?», ISTOOLS, INFORMATIVO. [En línea]. Disponible en: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

[17] ISECOM, «OSSTMM 2.1. Manual de la Metodología Abierta de Testeo de Seguridad». noviembre de 2016. [En línea]. Disponible en:

https://issuu.com/dragonjar/docs/osstmm.es.2.1?embed_cta=embed_badge&embed_context=embed&embed_domain=www.dragonjar.org&utm_medium=referral&utm_source=www.dragonjar.org&embed_id=1640921%2F41355784

[18] D. Ordoñez Camacho, «Reduciendo la brecha de seguridad del IoT con una arquitectura de microservicios basada en TLS y OAuth2», *SCIELO*, n.º 25, jun. 2021, doi: https://doi.org/10.17163/ings.n25.2021.09.

[19] P. Vargas Portillo, «Internet negro. El lado oscuro de la red», *Redalyc*, n.º 18, ene. 2020, doi: http://dx.doi.org/10.32870/Pk.a10n18.465.

[20] M. A. Calcaneo Monts, «Internet, redes sociales y libertad de expresión», *SCIELO*, n.º 44, p. 17, jun. 2021, doi: https://doi.org/10.22201/iij.24484881e.2021.44.16157.

[21] Y. A. Ahumada Torres y A. S. Moreno Martinez, «Banda ancha móvil privada y su interacción con redes de voz de la Policía Nacional», *SCIELO*, vol. 14, n.º 1, abr. 2022, doi: https://doi.org/10.22335/rlct.v14i1.1436.

[22] A. Espinel Ortega y J. C. Carreno Perez, «Identificación de activos y ciberactivos críticos en sistemas de transmisión de energía eléctrica», *SCIELO*, vol. 24, n.º 65, sep. 2020, doi: https://doi.org/10.14483/22487638.15388.

[23] Byron, E. Zhuma Mera, G. Bowen Calero, y B. Patiño Maisanche, «Voz IP seguras implementadas en redes definidas por software», *Redalyc*, vol. 27, n.º 3, p. 16, may 2021.

[24] A. Acosta Lopez, E. Y. Melo Monroy, y P. A. Linares Murcia, «Evaluation of the WPFI2-PSK wireless network security protocol using the Linset and Aircrack-ng tools», *SCIELO*, vol. 27, n.º 47, abr. 2018, doi: https://doi.org/10.19053/01211129.v27.n47.2018.7748.

[25] E. A. Arteaga, G. H. Morán, y G. A. Gomez, «Análisis de desempeño a nivel de simulación de un sistema de comunicaciones Li-Fi para la transmisión de datos a alta velocidad», *SCIELO*, vol. 14, n.º 27, jun. 2020, doi: https://doi.org/10.31908/19098367.0009.

[26] R. Vega Vega, «Análisis y detección de ataques informáticos mediante sistemas inteligentes de reducción dimensional», *Dialnet*, p. 125, 2022.

[27] J. E. Herrera Rubio, K. Y. Sanchez Mojica, y E. A. López Jaramillo, «Estudio del modelo de capas de IoT para enlaces descendentes en plataforma de interconexión de la red Sifgox», *SCIELO*, vol. 13, n.º 3, dic.

2021, doi: https://doi.org/10.22335/rlct.v13i3.1454.

[28] C. A. Chicaiza Puedmag, «Simulación de una red empresarial mediante la herramienta Cisco Packet Tracer», *Dialnet*, vol. 2, n.º 3, p. 19, oct. 2021, doi: https://doi.org/10.35290/ro.v2n3.2021.495.

[29] A. M. Ramirez Pilco, «Análisis del consumo de ancho de banda en redes WLAN mediante el uso de sondas remotas utilizando el software PRTG Network Monitor.», Universidad Católica de Santiago de Guayaquil, Guayaquil, 2019. [En línea]. Disponible en: http://repositorio.ucsg.edu.ec/handle/3317/12719

[30] PAESSLER, «PAESSLER - PRTG NETWORK MONITOR». [En línea]. Disponible en: https://www.paessler.com/es/prtg

[31] A. Nuñez Agurto, «Propuesta de una plataforma de gestión de dispositivos de Red basados en RouterOS», *Dialnet*, vol. 13, n.º 1, pp. 89-96, jun. 2020.

[32] J. Aguilar Alvarado, R. Quezada Sarmiento, y K. García Galarza, «Aplicación Java para el control de RB Mikrotik en empresas proveedoras de servicio de Internet», *Redalyc*, vol. 11, n.º 26, p. 15, nov. 2017.

5. ANEXOS

ENCUESTA DE SATISFACCIÓN

La presente Encuesta es para determinar el grado de Factibilidad que posee la Propuesta de Implementación de un Plan de Mejora de Seguridad a nivel de Infraestructura de Red aplicando los Principios de la Metodología OSSTMM y el Plan de Manejo de Riesgo de la Norma ISO 27001

Responder las preguntas a continuación en base a la documentación previamente otorgada

Para acceder al material informativo puede hacerlo mediante el siguiente enlace:

https://docs.google.com/document/d/1A6qjyGsF5jsUpkxflzn3oXrwq2Y9LZl6/edit?usp=sharing&ouid=116408208070791593354&rtpof=true&sd=true

Seleccione la respuesta según el grado de concordancia que posee la pregunta en base a su experiencia y/o criterio.

5= Muy de Acuerdo
4= De Acuerdo
3= Neutral
2= En Desacuerdo
1= Muy en Desacuerdo

1. ¿Cuán factible considera Ud. la aplicación del Plan de Mejora para fortalecer la **Seguridad de la Información** en la Empresa?

   1 2 3 4 5

2. ¿Cuán factible considera Ud. la aplicación de un Plan de Mejora para fortalecer la **Seguridad de los Procesos** en la Empresa?

   1 2 3 4 5

3. ¿Cuán factible considera Ud. la aplicación de un Plan de Mejora para fortalecer la **Seguridad de la Infraestructura de Red** en la Empresa?

1 2 3 4 5

4. ¿Cuán factible considera Ud. la aplicación de un Plan de Mejora para fortalecer la **Seguridad en las Comunicaciones** en la Empresa?

1 2 3 4 5

5. ¿Cuán factible considera Ud. la aplicación de un Plan de Mejora para fortalecer la **Seguridad Inalámbrica** en la Empresa?

1 2 3 4 5

6. ¿Cuán factible considera Ud. la aplicación de un Plan de Mejora para fortalecer la **Seguridad Física** en la Empresa?

1 2 3 4 5

7. ¿Qué tan factible considera Ud. el empleo de Opción de Tratamiento de **Reducción** como Medida de Tratamiento de Riesgo?

1 2 3 4 5

8. ¿Qué tan factible considera Ud. el empleo de Opción de Tratamiento de **Evitar** como Medida de Tratamiento de Riesgo?

1 2 3 4 5

9. ¿Qué tan factible considera Ud. el empleo de Opción de Tratamiento de **Transferir** como Medida de Tratamiento de Riesgo?

1 2 3 4 5

10. ¿Qué tan factible considera Ud. el empleo de Opción de Tratamiento de **Aceptar** como Medida de Tratamiento de Riesgo?

1 2 3 4 5

11. ¿Qué tan factible considera Ud. el empleo de **Medidas de Control** como "Mantenimiento de Equipos" para reducir el impacto de "Daño Físico por Falta de Mantenimiento"?

1 2 3 4 5

12. ¿Qué tan factible considera Ud. el empleo de **Medidas de Control** como "Planificación de la Capacidad" para reducir el impacto de " Paralización –Suspensión de la comunicación o del servicio por Falta y/o Mala Administración de Recursos"?

1 2 3 4 5

13. ¿Qué tan factible considera Ud. el empleo de **Medidas de Control** como "Protección ante amenazas externas y ambientales" para reducir el impacto de " Desastre Natural por la Falta de Emergencia ante Desastres"?

1 2 3 4 5

14. ¿Qué tan factible considera Ud. el empleo de **Medidas de Control** como "Controles de Software Malicioso" para reducir el impacto de "Daño al softwarecon mal intención por existencia de Software pirata - Virus"?

1 2 3 4 5

15. ¿Qué tan factible considera Ud. el empleo de **Medidas de Control** como "Implementación de Política de control de accesos" para reducir el impacto de"Uso Indebido del acceso por Falta de controles de acceso y privilegios otorgados"?

1 2 3 4 5

16. ¿Qué tan factible considera Ud. el empleo de **Medidas de Control** como "Seguridad de Oficinas, despachos y recursos" para reducir el impacto de "Sistemas Maliciosos en Equipos Celulares en Dispositivos con baja o nulaseguridad ante malware"?

1 2 3 4 5

17. ¿Qué tan factible considera Ud. el empleo de **Medidas de Control** como "Instalación y Protección de Equipos" para reducir el impacto de "Daño Físico o Mal estado a Equipos ubicados en zonas de Riesgos"?

1 2 3 4 5

18. ¿Qué tan factible considera Ud. el empleo de **Medidas de Control** como "Salvaguardar los Registros de la Organización" para reducir el impacto de "Pérdida de Información por Falta de plan de respaldo"?

1 2 3 4 5

19. ¿Qué tan factible considera Ud. el empleo de **Medidas de Control** como "Validación de datos de entrada" para reducir el impacto de "Alteración de Información por Ingreso o Modificación de Información de Manera Errónea"?

1 2 3 4 5

20. ¿Qué tan factible considera Ud. el empleo de **Medidas de Control** como "Gestión de Medios Removibles" para reducir el impacto de "Filtración de Información por Uso de dispositivos de Almacenamiento Extraíbles"?

1 2 3 4 5

21. ¿Qué tan factible considera Ud. el empleo de **Medidas de Control** como "Identificación y autenticación de Usuario" para reducir el impacto de "Acceso o uso no previsto ni autorizado por Inexistencia de Clasificación de Información"?

1 2 3 4 5