UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR

POSGRADOS

MAESTRÍA EN
SEGURIDAD DE LA INFORMACIÓN
RPC-SO-28-NO.669-2021

OPCIÓN DE TITULACIÓN:
PROYECTO DE TITULACIÓN CON COMPONENTES DE INVESTIGACIÓN APLICADA Y/O DE DESARROLLO.

TEMA:
ANÁLISIS DE VULNERABILIDAD EN LA INFRAESTRUCTURA TECNOLÓGICA DE LA ORGANIZACIÓN UNISCAN EN EL ÁREA FUNCIONAL DE FRONTERA DE LA EMPRESA.

AUTOR:
LUIS OMAR VILLACRÉS TÚQUERES

DIRECTOR:
JUAN CARLOS DOMÍNGUEZ AYALA

CUENCA – ECUADOR
2023

Autor:

Luis Omar Villacrés Túqueres
Ingeniero en Control y Redes Industriales.
Candidato a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
lvillacrest1@est.ups.edu.ec

Dirigido *por:*

Juan Carlos Domínguez Ayala
Ingeniero de Sistemas.
Magister en Redes de Comunicaciones.
jdominguez@ups.edu.ec

LUIS OMAR VILLACRÉS TÚQUERES
Análisis de vulnerabilidad en la infraestructura tecnológica de la organización Uniscan en el área funcional de frontera de la empresa.

DEDICATORIA.

Dedico principalmente mi proyecto de estudio a Dios, que sirve tanto de inspiración como de fuente de fortaleza, permitiéndome hacer realidad una de mis más queridas aspiraciones.

Agradezco a mis padres su amor, esfuerzo y dedicación a lo largo de los años. Su perseverancia y diligencia me han permitido cumplir otra ambición. Siempre dan ejemplo trabajando duro, siendo valientes y afrontando los retos de frente. Ser su hijo me llena de alegría y respeto; son los padres ideales.

Agradezco el apoyo incondicional de mis hermanos y la orientación espiritual que me han proporcionado en este momento de mi vida. Quisiera expresar mi gratitud a todos los que me han ayudado y han hecho posible el éxito de mi trabajo, especialmente a aquellos que me han abierto las puertas y han compartido su conocimiento y han aportado a mi formación como profesional y a nivel personal.

AGRADECIMIENTO.

Gracias a Dios, por guiarme por la vida, por ser mi apoyo y mi fuerza cuando era débil y por proporcionarme la paciencia y los conocimientos que necesitaba para alcanzar la meta que me había fijado.

Quiero expresar mi gratitud a mis padres por ser mi roca, por su apoyo inquebrantable a pesar de los retos y tribulaciones a los que me he enfrentado, y por la moral y los valores que me han inculcado. Doy las gracias a mis profesores de posgrado por compartir sus conocimientos conmigo mientras me preparaba para mi profesión, especialmente a aquellos que me guiaron paciente, sabiamente y que contribuyeron de forma significativa a mi educación.

Por último, quisiera expresar mi sincero agradecimiento al Ing. Juan Carlos Domínguez, quien ha sido mi principal colaborador durante todo el proceso y cuyo liderazgo, experiencia, enseñanza y colaboración han hecho posible este esfuerzo. Agradezco a la Universidad Politécnica Salesiana por ser la depositaria de toda la información aprendida durante este tiempo.

Tabla de Contenido.

ÍNDICE DE FIGURAS.

ÍNDICE DE TABLAS.

ÍNDICE DE ANEXOS.

ANÁLISIS DE VULNERABILIDAD EN LA INFRAESTRUCTURA TECNOLÓGICA DE LA ORGANIZACIÓN UNISCAN EN EL ÁREA FUNCIONAL DE FRONTERA DE LA EMPRESA.

AUTOR(ES):

LUIS OMAR VILLACRÉS TÚQUERES

Resumen.

Uniscan es una empresa mayorista de tecnología que maneja una base de datos de clientes y un inventario de productos. Dado el ámbito en el que se mueve, es importante ofrecer soluciones para minimizar riesgos y abordar problemas encontrados durante el análisis de vulnerabilidades. De esta manera, se pueden aplicar diversos métodos en una empresa mediana con grandes expectativas de crecimiento, ya que a medida que crece, surgen nuevos cargos, funciones y servicios que deben mantenerse bajo control y documentados en políticas de seguridad.

El proyecto tiene como objetivo proporcionar una gestión adecuada de los datos y una gestión de información efectiva para que Uniscan se convierta en una de las mejores empresas de distribución de tecnología. El proyecto se enfoca en identificar las vulnerabilidades que enfrenta la empresa en desarrollo, debido a que maneja información confidencial de gran valor.

Mantener la seguridad en el tratamiento de los datos, su protección, integridad, confidencialidad, disponibilidad y autenticidad son parámetros esenciales que distinguen a una empresa organizada y responsable y generan confianza en sus clientes. Muchas empresas no le dan la importancia necesaria a la seguridad informática debido a los altos costos de contratar profesionales y servicios de seguridad informática.

Las empresas que usan sistemas de información o servicios en línea son vulnerables a todo tipo de ataques, independientemente de su tamaño. Por ello, deben establecer medidas de seguridad sólidas en su infraestructura de tecnologías de la información y la comunicación y contratar personal especializado en seguridad, ya sea interno o externo, para prevenir o mitigar posibles ataques.

El uso de software antivirus con licencia, la limitación del tiempo en línea, la evitación de descarga de archivos de fuentes dudosas, el filtrado de correos electrónicos sospechosos, la asignación de perfiles de trabajo con acceso restringido a la información y la implementación de medidas de seguridad complejas son algunas de las prácticas recomendadas.

El proyecto no solo beneficia a los clientes, sino también a la dirección, al departamento de contabilidad, marketing, ventas, bodega y al área técnica al proporcionar seguridad y fiabilidad en la información almacenada y distribuida, lo que aumenta la productividad y la competitividad de la empresa para un crecimiento sostenible a largo plazo.

Palabras clave:

Análisis, vulnerabilidades, confidencialidad, integridad, disponibilidad, seguridad, informática.

ABSTRACT.

Uniscan is a technology wholesale company that manages a customer database and product inventory. Given the environment in which it operates, it is important to offer solutions to minimize risks and address problems encountered during vulnerability analysis. In this way, various methods can be applied in a medium-sized company with high growth expectations, since as it grows, new positions, functions and services emerge that must be kept under control and documented in security policies.

The project aims to provide proper data management and effective information management for Uniscan to become one of the best technology distribution companies. The project focuses on identifying the vulnerabilities faced by the developing company, due to the fact that it handles confidential information of great value.

Maintaining security in the treatment of data, its protection, integrity, confidentiality, availability and authenticity are essential parameters that distinguish an organized and responsible company and generate confidence in its clients. Many companies do not give the necessary importance to IT security due to the high costs of hiring IT security professionals and services.

Companies that use information systems or online services are vulnerable to all kinds of attacks, regardless of their size. For this reason, they must establish solid security measures in their information and communication technology infrastructure and hire specialized security personnel, whether internal or external, to prevent or mitigate possible attacks.

The use of licensed antivirus software, limiting online time, avoiding downloading files from dubious sources, filtering suspicious e-mails, assigning work profiles with restricted access to information and implementing complex security measures are some of the recommended practices.

The project not only benefits customers, but also the management, accounting, marketing, sales, warehouse and technical departments by providing security and reliability in the information stored and distributed, thus increasing the company's productivity and competitiveness for long-term sustainable growth.

Keywords:
Analysis, vulnerabilities, confidentiality, integrity, availability, security, computing.

1. Introducción.

Actualmente, estamos viviendo una revolución en cuanto al manejo, almacenamiento y procesamiento de datos, lo que hace que sea muy importante garantizar la confiabilidad de los usuarios y empresas en la gestión de su información. En esta era de la información, los datos son el activo más valioso, especialmente cuando se trata de información de clientes y usuarios internos de la organización.

Por lo tanto, las empresas que buscan crecer en el mercado tienen una necesidad inmediata de implementar procesos de seguridad de información más sólidos y actualizados para evitar intrusiones y robos de información valiosa. Los atacantes pueden aprovechar las vulnerabilidades para infiltrarse en la red de la organización y manipular, robar o comprometer la integridad de los datos, con el objetivo de falsificar identidades, ralentizar procesos o incluso dejar fuera de operación los servicios.

Según el informe ESET Security Report 2022, Ecuador está entre los cinco países de Latinoamérica en cuyas empresas se registran más detecciones informáticas maliciosas. El listado lo encabeza Perú, con un 18 %, seguido de México (17 %), Colombia (12 %), Argentina (11 %) y Ecuador (9 %) [1].

Es importante tener en cuenta que los ataques cada vez son más sofisticados y los ciberdelincuentes utilizan herramientas y técnicas de ingeniería social para lograr sus objetivos. Por lo tanto, es fundamental analizar los problemas a los que se enfrenta la empresa cuando no se han implementado medidas de protección de información y evaluar la efectividad de dichas medidas para proteger la información.

Consideremos la figura 1, donde podemos ver los distintos niveles de protección de la información. En el primer nivel, se tiene en cuenta la seguridad de todo el hardware o componente físico, también conocido como infraestructura, con el que se conecta el software, en el segundo nivel los datos se combinan con los recursos del sistema operativo, lo que permite configurar la seguridad, en el tercer nivel encontramos los

protocolos de comunicación que constituyen las normativas para la transmisión de datos entre dispositivos, seguidamente, se tiene el nivel cuatro de servicios y su protección para todas las posibles aplicaciones del hardware, estos forman parte importante de protección en la infraestructura tecnológica de cualquier organización.

Fig. 1 Niveles de protección de la información.
Fuente: El autor.

La empresa Uniscan ubicada en Quito, se encuentra en la búsqueda para obtener un sistema de información confiable que mantenga con seguridad: los datos de sus transacciones en el sistema contable, los datos de sus clientes, la información que se envía o recibe en el correo institucional, el inventario de bodega, etc.

La protección de los datos mencionados anteriormente permitirá el crecimiento y rentabilidad de la empresa teniendo como visión convertirse en referente mayorista de la distribución de tecnología en el territorio nacional.

Por eso se convierte en necesario evitar riesgos críticos de intentos de ataque a las vulnerabilidades de la empresa, empezando desde ataques Phishing, también intentos de ingreso no autorizado al servidor de la empresa donde está soportado el sistema contable y de bodega, así como el servidor de correo electrónico.

El presente proyecto de análisis de riesgos busca detectar las amenazas, las posibles causas y sus consecuencias, esto sobre la infraestructura tecnológica con la que cuenta en este momento la empresa y que se espera que sea suficiente para mantener protegida la integridad de la red, datos de los usuarios e información importante para el desarrollo de las tareas cotidianas dentro de la institución. El estudio a realizarse va encaminado a proponer una solución a cada uno los problemas en el tratamiento de la

información que se presentan durante las operaciones del negocio. Por lo que se vuelve necesario identificar de manera clara cada uno de los riesgos, también se tendría que discutir acerca de los problemas y cuáles son las posibles soluciones, a continuación, en la figura 2 podemos observar el nivel de preocupación que genera el tipo de amenazas a la que se encuentran expuestas las empresas, así como el objetivo que escogen los cibercriminales para atacar a la infraestructura tecnológica de una organización.

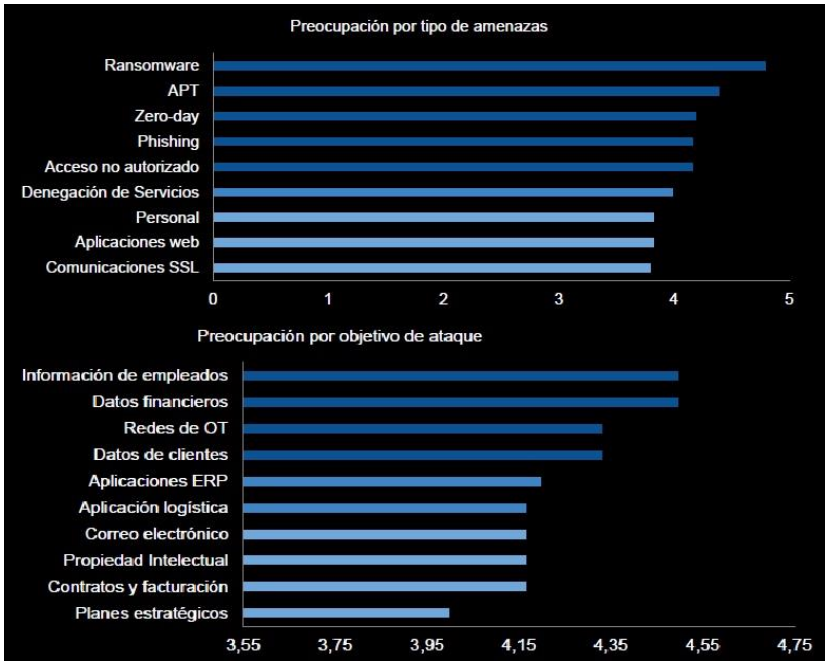


Fig. 2 Preocupación por tipo de amenazas y por objetivo de ataque [23].

2. Determinación del Problema.

2.1. Objetivo General.

Analizar la infraestructura tecnológica en la empresa Uniscan en busca de los riesgos en la seguridad de la información dentro de la frontera de acción de la empresa.

2.2. Objetivos Específicos.

- Identificar las vulnerabilidades en activos como, software y equipos de cómputo que se requiere que mantengan la integridad, confidencialidad, autenticidad y disponibilidad de los datos.

- Determinar las principales amenazas, al momento de realizar el análisis de las vulnerabilidades, en los activos que constituyen la infraestructura de la empresa.

- Proponer un plan de tratamiento para los riesgos de nivel inaceptable detectados durante el análisis de riesgos de seguridad de la información para obtener nociones básicas de cómo prevenir dichos ataques informáticos.

3. Marco teórico.

3.1. Antecedentes Investigativos.

En la actualidad el mundo de la tecnología avanza a pasos agigantados y es crucial que la información personal y empresarial sea almacenada en archivos seguros que brinden confiabilidad a los usuarios. El objetivo principal de este proyecto es analizar diversas vulnerabilidades informáticas en la infraestructura técnica de la organización para prevenir posibles ataques.

El comercio electrónico, el acceso rápido a enormes bibliotecas de material de referencia, la informática colaborativa, el correo electrónico y los nuevos canales de publicidad y difusión de información son sólo algunos de los efectos positivos de la explosiva expansión de Internet. La tecnología tiene un lado malo, como ocurre con otros avances: los hackers criminales. Un especialista en ordenadores y redes conocido como hacker ético asalta un sistema de seguridad en nombre de sus propietarios en un esfuerzo por encontrar agujeros que un hacker hostil pueda explotar. Gobiernos, empresas y ciudadanos de todo el mundo quieren participar en esta revolución, pero dudan en hacerlo por temor a que algún hacker irrumpa en su servidor Web y sustituya el logotipo de su empresa por pornografía, lea sus correos electrónicos, robe la información de sus tarjetas de crédito en una tienda online o inserte un software que transmita de forma encubierta los secretos comerciales de su empresa a la Internet pública. Más adelante, se hará una revisión de la existencia de los diversos métodos que son utilizados por los hackers para piratear la información [2].

Dado que en la actualidad prácticamente toda la comunicación se produce en línea, la seguridad informática es una seria preocupación para Internet. El objetivo de las pruebas de penetración es asegurarse de que no existen fallos de seguridad en el sistema o la red que puedan permitir accesos no deseados. Las pruebas de penetración son un método factible y adecuado para prevenir el pirateo de sistemas y redes [3].

De acuerdo con la tesis de Mara Elena Hurtado Sandoval y Luis Alcides Mendaño Mendaño, la seguridad de los datos sensibles de una empresa puede verse comprometida si caen en manos equivocadas, y existen muchos tipos de ataques que pueden afectar la información que se transmite por redes. Por lo tanto, es importante implementar procesos de seguridad más sólidos a lo largo del tiempo, y realizar simulaciones de ataques controlados para descubrir posibles vulnerabilidades que puedan ser explotadas por ciberdelincuentes sin poner en peligro los sistemas y servicios probados. Este enfoque, conocido como hacking ético, busca identificar agujeros de seguridad y fortalecer las defensas de las organizaciones contra posibles ataques [14].

Ecuador ha experimentado un aumento significativo de la conectividad a Internet en los últimos años. Por ejemplo, los registros del Instituto Nacional de Estadística y Censos (INEC) muestran que la población de Ecuador con acceso a Internet pasó del 22,5% en 2012 al 32,8% en 2015. Estos principios son tangibles cuando vemos cómo las organizaciones financieras y empresariales (como los bancos, las empresas y los sectores de viajes y turismo, entre otros) han ampliado el uso de servicios en línea (como la banca electrónica y las transacciones). Las organizaciones públicas han ampliado la disponibilidad de servicios y bienes a través de Internet (por ejemplo, facturación electrónica, sitios de compras, entre otros) e incluso han automatizado algunos de sus servicios (por ejemplo, pago de propiedades, pago de impuestos, entre otros) [4].

A continuación, en la Tabla I se evidencia la estadística sobre los delitos informáticos más cometidos en el Ecuador y con mayor número de denuncias en la Fiscalía General del Estado.

TABLA I. ESTADÍSTICA DE LOS DELITOS INFORMÁTICOS CON MAYOR FRECUENCIA EN ECUADOR.

	Año 2015	Año 2016	Año 2017	Año 2018	Año 2019	Año 2020	Año 2021	Total
C.O.I.P. Art. 178.- Violación a la intimidad. – 1 a 3 años.	1147	1516	1666	2069	2044	2008	234	10684
C.O.I.P. Art. 186.- Estafa. – 5 a 7 años	14601	15233	14057	14448	17127	18598	2634	96698
C.O.I.P. Art. 230.- Interceptación ilegal de datos. – 3 a 5 años.	55	82	63	41	87	74	5	407

C.O.I.P. Art. 232.- Ataque a la integridad de sistemas informáticos. – 3 a 5 años.	77	76	86	87	112	95	15	548
C.O.I.P. Art. 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones. – 3 a 5 años.	141	144	218	236	245	299	41	1324

Fuente: Sistema Integrado de Actuaciones Fiscales (SIAF) de la Fiscalía General del Estado.

Todos los proveedores de servicios, incluyendo bancos, compañías de seguros, firmas legales, etc., están conectados para recibir y enviar información sensible. Por lo que deben estar adecuadamente protegidos para llevar a cabo este proceso, la infraestructura de seguridad que utilizan y quién está a cargo de ella son factores cruciales; esto les ayudará a evitar ataques o robos por parte de personas no autorizadas y les dará una mayor confianza en el mercado con el que están comprometidos [14].

3.2. Fundamentación teórica sobre ciberseguridad.

Es importante destacar que la ciberseguridad no solo se trata de implementar medidas de seguridad tecnológicas, sino que también involucra la capacitación y concientización de los usuarios, ya que el factor humano es una de las principales causas de las vulnerabilidades en la seguridad informática. Por esta razón, se deben implementar políticas de seguridad que incluyan la educación y entrenamiento constante de los empleados en cuanto a las buenas prácticas de seguridad informática y el manejo seguro de la información. Además, es fundamental realizar pruebas periódicas de vulnerabilidades y actualizaciones de los sistemas y aplicaciones para garantizar la seguridad de la información y prevenir posibles ataques.

Como se ha indicado anteriormente, la ciberseguridad es el resultado de una combinación de estrategias, directrices y tácticas que mejoran el control de las amenazas a la información, mejorando así su disponibilidad, integridad y confidencialidad [15].

3.2.1. Pilares fundamentales de un Sistema de Gestión de la Seguridad de la Información (SGSI).

Cualquier empresa debe atenerse a tres principios para cumplir plenamente los requisitos de eficacia y eficiencia, esto según la norma ISO 27001 de la Organización Internacional de Normalización. Estos tres principios son: la confidencialidad, la integridad y la disponibilidad, los mismos que son generalmente necesarios para mantener un sistema seguro y fiable, estos pueden ser apreciados en la figura 3 donde se muestran como elementos interdependientes de la seguridad de la información [5].

Sólo las personas autorizadas deben tener acceso a la información para que ésta sea confidencial. La autorización y el control son necesarios para el acceso a la información, pero la necesidad de mantener privados algunos datos o recursos se conoce como confidencialidad, la confidencialidad pretende impedir la difusión no autorizada de información sobre la empresa [16].

La integridad indica que, incluso en caso de accidente o mala intención, la información permanece inalterada y sólo puede modificarse con permiso. El objetivo de la integridad es impedir la modificación ilegal de la información [16].

Se dice que un sistema informático está disponible si puede seguir funcionando sin interrupción. Cuando su utilización es necesaria, los usuarios autorizados deben tener acceso a los recursos apropiados. Para evitar el uso ilegal de los recursos informáticos, la información sólo debe estar disponible para los usuarios autorizados [16].

Fig. 3 Elementos interdependientes de la Seguridad de la Información [6].

3.2.2. Auditoría de Seguridad de Sistemas de Información.

Una Auditoría de Seguridad en Sistemas Informáticos es un proceso sistemático que tiene como objetivo evaluar la seguridad de los sistemas informáticos de una organización, identificando las vulnerabilidades y recomendando las medidas necesarias para solucionarlas. Este proceso implica la revisión de políticas y procedimientos de seguridad, la identificación de amenazas y vulnerabilidades, la evaluación de los controles de seguridad existentes y la evaluación de la capacidad de respuesta de la organización ante incidentes de seguridad. El resultado final de una auditoría de seguridad es un informe detallado que describe los hallazgos, las recomendaciones y las acciones que se deben tomar para mejorar la seguridad de los sistemas de la organización. La auditoría de seguridad es una herramienta esencial para garantizar la confidencialidad, integridad y disponibilidad de la información de una organización, también se refiere a una investigación llevada a cabo por especialistas en tecnologías de la información, que tiene como finalidad descubrir, clasificar y resumir las diversas vulnerabilidades que puedan presentarse al analizar y gestionar sistemas informáticos. Esta evaluación exhaustiva puede abarcar desde estaciones de trabajo y redes de comunicaciones hasta servidores y aplicaciones [14].

3.2.3. Seguridad informática o Ciberseguridad.

La protección de sistemas informáticos contra el uso ilegal o malintencionado se conoce como seguridad informática. Esto implica tomar medidas para prevenir intrusiones no autorizadas y proteger los recursos informáticos, como hardware, software y datos, que deben ser utilizados o controlados solo por personas autorizadas. La seguridad informática es una disciplina que se enfoca en diseñar normas, procedimientos, metodologías y técnicas para lograr un sistema de información seguro y fiable. En resumen, la seguridad informática se centra en la protección de recursos informáticos y la prevención de accesos no autorizados a los mismos [7].

3.2.4. Seguridad en Redes.

A pesar de que las redes y sistemas informáticos están en constante crecimiento y cada vez tienen mayor éxito, se debe tomar precaución ya que son objetivos atractivos para los ciberdelincuentes. Dentro de una organización es fundamental mantener un nivel de seguridad apropiado en las redes, tanto inalámbricas como con cableado, para poder de esta manera prevenir infiltraciones.

Las amenazas a las redes son de dos tipos: internas y externas.

- **Internas:** son aquellas que se encuentran dentro de la organización.
- **Externas:** son aquellas que no están afiliadas a la organización.

La protección de la red se refiere a todas las medidas tomadas para preservar la privacidad, la integridad y el uso apropiado de los datos de la red y de la empresa. Según Andrews Tanenbaum en su libro "Computer Networking", la seguridad es un tema amplio que abarca diversos delitos, pero en esencia se enfoca en prevenir el acceso no autorizado a los servicios remotos y garantizar que los mensajes destinados a otros no sean leídos o modificados por fisgones.

Basándose en las ideas anteriores, la seguridad de la red pretende disuadir, corregir y evitar que los piratas informáticos accedan a la red burlando la seguridad de la misma, garantizando así un grado aceptable de seguridad durante la transmisión de datos [17].

En este proyecto se analizará la arquitectura técnica de las redes activas de la empresa Uniscan. Para ello, se utilizará el programa Airgeddon en una máquina virtual con el sistema operativo Kali-Linux.

3.2.5. Definición de Red de Informática.

Un conjunto de dispositivos enlazados que se comunican entre sí, estos dispositivos que comparten recursos e intercambian información se conocen como red informática. En una red de ordenadores, la comunicación consiste esencialmente en un proceso en el que las entidades vinculadas: el emisor y el receptor, entidades que cumplen dos papeles distintos comparten datos e información [16].

3.2.6. Clasificación de las redes informáticas.

• **PAN (Personal Area Network) o red de área personal:** comprende los elementos que utiliza un solo individuo. Su alcance es de varios metros. Red inalámbrica de área personal (WPAN), es una red red PAN que se comunica mediante tecnologías inalámbricas [8].

• **LAN (Local Area Network) o red de área local:** una habitación, un edificio, un avión, etc. son ejemplos de espacios relativamente compactos donde el alcance de esta red es restringido [8].

• **WLAN (Wireless Local Area Network) o LAN inalámbrica:** esta red de área local utiliza técnicas de transmisión inalámbrica. Debido a su escalabilidad y a la ausencia de conexiones de instalación, es una disposición muy utilizada [8].

• **CAN (Campus Area Network) o red de área de campus:** es una red de dispositivos rápidos conectados a una LAN que abarca una región determinada, como un campus universitario, un puesto militar, etc [8].

• **MAN (Metropolitan Area Network) o red de área metropolitana:** se trata de una red de alta velocidad (banda ancha) que tiene más cobertura que un campus universitario pero que, sin embargo, ofrece su área de cobertura limitada [8].

• **WAN (Wide Area Network) o red de área amplia:** utiliza métodos de comunicación no convencionales, como satélites, cables transoceánicos, fibra óptica, etc., para cubrir una gran región geográfica [8].

• **VLAN (Virtual LAN):** una LAN lógica o virtual que se ha añadido a una red física para aumentar la seguridad y la funcionalidad. En algunas circunstancias, se pueden construir redes virtuales en una WAN utilizando el protocolo 802.11Q (también conocido como QinQ), es crucial distinguir esta implementación de la tecnología VPN [8].

3.3. Análisis de Riesgos.

La gestión de riesgos implica la identificación de los activos de información, así como sus vulnerabilidades y amenazas, y evalúa la probabilidad y el impacto de los riesgos para determinar los controles adecuados que se deben aplicar. Esto se conoce como análisis de riesgos [14].

3.3.1. Definición de amenaza.

Cualquier acción que se aproveche de un punto débil para comprometer la seguridad de un sistema de información se considera una amenaza. En otras palabras, algunos componentes de nuestro sistema pueden verse afectados negativamente por el peligro. Los ataques (fraudes, robos, virus), las catástrofes naturales (incendios, inundaciones) o los descuidos y decisiones de la organización pueden constituir amenazas (uso indebido de contraseñas, no utilización del cifrado). Pueden ser tanto internas como externas desde la perspectiva de la organización [16].

3.3.2. Definición de vulnerabilidad informática.

Es esencial detectar y corregir las debilidades de seguridad informática lo más pronto posible ya que representan una amenaza para la protección de los datos almacenados

en el sistema, al permitir que los hackers comprometan su confidencialidad, integridad o disponibilidad. Estas vulnerabilidades pueden ser causadas por diversos problemas, tales como un diseño deficiente, una configuración inadecuada o errores de programación [16].

A continuación, en la Tabla II se explica cada categoría de vulnerabilidad:

TABLA II. CRITERIO DE CRITICIDAD EN VULNERABILIDADES SEGÚN LA SEVERIDAD [9].

CLASIFICACIÓN	DESCRIPCIÓN
Crítica	Vulnerabilidades con riesgo efectivo de explotación a la confidencialidad, integridad y disponibilidad de la información del objetivo.
	Vulnerabilidad sin CVE (common vulnerabilities and exposures) que comprometa realmente al objetivo o con código CVE certificado.
Alta	Vulnerabilidades con riesgo de explotación posible con acceso a información del objetivo.
	Vulnerabilidades con riesgo posible de explotación a la confidencialidad, integridad y disponibilidad de la información del objetivo.
	Vulnerabilidad sin CVE que comprometa posiblemente al objetivo o con código CVE certificado.
Media	Vulnerabilidad con riesgo de explotación baja con acceso a información del objetivo.
	Vulnerabilidad con riesgo bajo de explotación a la confidencialidad, integridad y disponibilidad de la información del objetivo.
	Vulnerabilidad sin CVE que difícilmente pueda comprometer al objetivo o con código CVE certificado.
Baja	Vulnerabilidades con ningún riesgo de explotación a la confidencialidad, integridad y disponibilidad de la información del objetivo.
	Vulnerabilidad sin CVE que no pueda comprometer al objetivo o con código CVE certificado.
Informativa	No se considera como una vulnerabilidad, se considera como información importante sobre el servicio analizado.

3.3.3. Definición de Riesgo.

El riesgo en seguridad se define como la probabilidad de que se produzca un evento que genere daños o pérdidas, y se basa en la existencia de vulnerabilidades que puedan ser explotadas por diferentes amenazas, como hackers, virus o ataques de denegación de servicio. La probabilidad de que estas amenazas se materialicen y afecten a los sistemas de información se encuentra determinada por distintos factores, como se muestra en la figura 4, y el nivel de riesgo se establece a través de la intersección de estos elementos [10].

Fig. 4 Representación del Riesgo [10].

3.3.4. Definición de Impacto.

El impacto se refiere a la forma en que una amenaza aprovecha la vulnerabilidad de un activo y generalmente se mide por el grado de disminución que afecta el valor del activo, donde una pérdida total del activo se consideraría del 100%.

La figura 5 representa la interrelación entre los conceptos clave previamente discutidos hasta este punto.

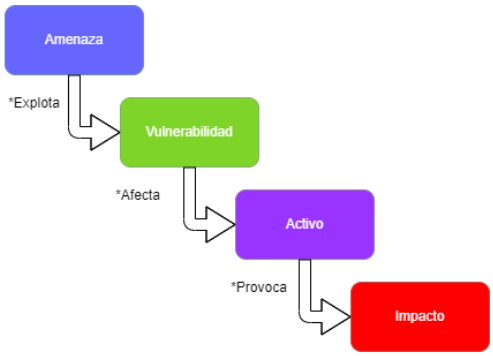


Fig. 5 Definición de impacto: amenaza, vulnerabilidad y activo.
Fuente: El autor.

3.3.5. Hacking Ético.

Se ha demostrado que las computadoras son vulnerables a los ataques de piratas informáticos que pueden ingresar a los sistemas informáticos y robar información crucial. Por lo tanto, es importante comprender los sistemas y redes de datos para determinar su seguridad contra cualquier tipo de ataque. Dicho esto, el hacking ético, también conocido como ethical hacking, es la modelización de posibles situaciones de

ataque con la inclusión deliberada de acciones características de los ciberdelincuentes con el fin de actuar con rapidez [17].

Otra noción describe el hacking ético como el uso de medidas preventivas y la simulación del peor escenario posible para mostrar lo que hay que hacer para garantizar que no se produzca [11].

El objetivo del hacking ético es probar y evaluar la seguridad física y lógica de los sistemas de información, redes, aplicaciones web, servidores y bases de datos, entre otros, al aprovechar los puntos débiles de los sistemas mediante técnicas de intrusión. Por lo tanto, la utilización de las diferentes técnicas que puede utilizar la persona que se dedica al hacker ético puede beneficiar enormemente a las empresas para tomar medidas preventivas que permitan protegerse contra los ataques maliciosos.

3.4. Test de Intrusión (Pentesting).

Se ha vuelto cada vez más popular en las empresas hoy en día el uso de la táctica de hacking ético conocida como Pentesting debido a los robos de información y delitos informáticos que han afectado a varias empresas recientemente. El Pentesting es un proceso que consiste en atacar varios entornos o sistemas controlados con el fin de descubrir vulnerabilidades y prevenir posibles ataques externos o internos a los sistemas, redes o hardware. El término Pentesting se origina de la combinación de los términos "penetración" y "testing" [17].

3.4.1. Clasificación del Test de Intrusión o Pentesting.

El test de intrusión o penetración se divide en categorías:

- **Pentesting de caja blanca (White Box).**

  En este tipo de prueba, el pentester tiene un conocimiento previo del sistema o red de la organización, incluyendo información como la estructura, contraseñas

y cortafuegos. Esto permite que la prueba sea más completa y efectiva, ya que se pueden ajustar o mejorar partes del diseño del sistema gracias a la información previa obtenida [17].

- **Pentesting de caja negra (Black Box).**

  En este caso, el pentester no tiene acceso previo a la información del sistema o red de la organización, por lo que se comporta como un ciberdelincuente para identificar los puntos débiles, la estructura y los peligros de la red. Este tipo de pentesting es el más exhaustivo o realista [17].

- **Pentesting de caja gris (Gray Box).**

  En este tipo de prueba, el auditor tiene un conocimiento parcial de la empresa, lo que lo hace un híbrido entre pentesting de caja negra y de caja blanca. Aunque no parte de cero, este tipo de pentesting es recomendado para las organizaciones, ya que requiere tiempo y recursos suficientes para llevar a cabo las pruebas de manera efectiva [17].

3.4.2. Fases de un Pentesting.

Para completar su procedimiento, una prueba de penetración implica varios pasos o fases, si bien cada etapa requiere el consentimiento del cliente antes de poder comenzar.

Estas etapas suelen aplicarse como se indica a continuación:

- **Fase de reconocimiento.**

  En esta etapa inicial se establecen los objetivos y se recopilan los datos necesarios para la auditoría, como nombres, direcciones de correo electrónico, diagramas de red y direcciones IP de los activos de información de una organización [17].

- **Fase de Exploración.**

  Usando la información recopilada en la fase anterior, se buscan posibles vectores de ataque, lo que implica escanear puertos, servicios y versiones. Luego, se examinan las vulnerabilidades para determinar el tipo de ataque [17].

- **Fase de Enumeración.**

  Encontrar información sobre datos de usuario, nombres de dispositivos y servicios de red, entre otras cosas, este es el objetivo de esta fase [17].

- **Fase de Acceso.**

  En esta fase, se lleva a cabo el acceso al sistema utilizando las debilidades descubiertas en las fases anteriores [17].

- **Fase siguiente a la Explotación.**

  Tras obtener acceso al sistema, se busca una técnica que permita permanecer en él durante más tiempo, adquirir más privilegios y realizar más operaciones [17].

- **Fase del Informe.**

  En esta etapa final, se informa detalladamente al cliente de las vulnerabilidades descubiertas y de cómo se han explotado para que puedan tomar las mejores decisiones en materia de seguridad [17].

Aunque los procesos pueden variar según el autor de un libro de ciberseguridad, el resultado final siempre será el mismo: identificar y corregir las vulnerabilidades para mejorar la seguridad de los sistemas y redes.

3.4.3. Metodologías del Pentesting.

Debe seleccionarse una técnica para ejecutar un pentesting de acuerdo con las exigencias de la auditoría y las necesidades de la empresa. A continuación, se enumeran algunos de los enfoques más populares:

- **ISSAF (Information Systems Security Assessment Framework).**
  Se trata de una estrategia organizada y especializada que permite al pentester planificar cada etapa del proceso de prueba. Su marco ofrece enfoques vanguardistas que se adaptan para satisfacer todos los criterios de un pentesting [17].

- **PTES (Penetration Testing Methods and Standard).**
  Este enfoque, que comprende siete pasos y garantiza la eficacia de las pruebas de penetración, es ampliamente utilizado por conocidos especialistas en seguridad informática y sirve de guía en la literatura de instrucción [17].

- **OSSTMM (Open Source Security Testing Methodology Manual).**
  Aunque carece de metodologías innovadoras, es una práctica bien conocida, y muchas empresas confían en ella cuando necesitan pruebas de alta calidad, eficaces y organizadas [17].

- **OWASP (Open Web Application Security Project).**
  Es una norma utilizada para detectar vulnerabilidades en aplicaciones móviles y de plataforma web. Proporciona más de 66 controles con diversas funcionalidades para evaluar diferentes tipos de vulnerabilidades [17].

3.4.4. Pruebas de Penetración.

Se puede categorizar las pruebas de penetración en cinco áreas diferentes:

- **Pruebas de servicios de red:** esta evaluación se enfoca en la infraestructura de red de la empresa para identificar debilidades que puedan ser fortalecidas. Esta área incluye la evaluación de la configuración del firewall, pruebas de filtrado de estado, entre otros [18].

- **Pruebas de aplicaciones Web:** este tipo de pruebas de penetración se profundiza ya que cada análisis es muy minucioso y porque las vulnerabilidades se encuentran más fácilmente dependiendo de la búsqueda en aplicaciones en línea [18].

- **Pruebas del lado del cliente:** con esta forma de prueba, el consultor es capaz de investigar el software, las herramientas de producción de contenidos y los navegadores web en las máquinas de los consumidores, incluyendo Chrome, Firefox, Explorer y Opera [18].

- **Pruebas de redes inalámbricas:** este tipo de prueba de penetración se enfoca en examinar todas las redes inalámbricas que una organización utiliza. Se busca evaluar los puntos de acceso, los protocolos de red inalámbrica y las credenciales administrativas para detectar posibles vulnerabilidades [18].

- **Prueba de ingeniería social:** esta técnica trata de persuadir a un empleado para que divulgue cosas que deberían mantenerse en secreto con el fin de robar información y datos sensibles [18].

3.4.5. Métodos de Pruebas de Penetración.

- **Manual:** es el enfoque inicial para entender un ataque, permite un mayor control sobre el proceso, aunque se apoye en herramientas y guiones básicos, este método es lento en comparación con otros [7].

- **Automático:** las herramientas comprueban un sitio web rápidamente e informan de cualquier vulnerabilidad que descubran. El inconveniente es que hay menos

control sobre la conducta del ataque, lo que hace más probables los falsos positivos [7].

- **Híbrido:** al combinar procesos manuales y automáticos se pueden obtener mejores resultados. Se utiliza un escáner de vulnerabilidades para proporcionar una línea de base y punto de partida, mientras se realizan inspecciones manuales para detectar problemas en el sitio. Los hallazgos del escáner se verifican para su uso posterior en la mejora de la seguridad de la aplicación [7].

3.5. Fases de un Ataque Informático.

En la figura 6, podemos observar la representación gráfica de las diferentes etapas de un ciberataque, a continuación, se realiza la descripción de cada una de ellas:

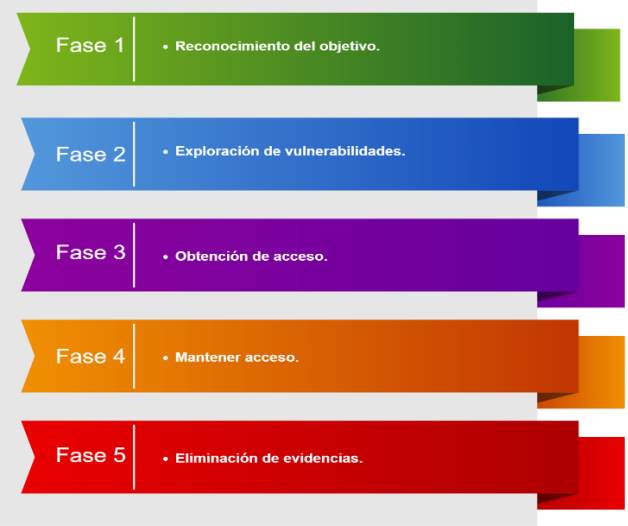


Fig. 6 Etapas de un Ciberataque.
Fuente: El autor.

1. **Etapa de reconocimiento:** esta fase se centra en recopilar información utilizando diversas tácticas.

2. **Etapa de escaneo:** en esta fase se analiza la información recopilada para identificar posibles vulnerabilidades de seguridad que ya pueden existir en el sistema.

3. **Etapa de acceso:** en esta fase, se lleva a cabo el ataque aprovechando las debilidades y vulnerabilidades del sistema.

4. **Etapa de mantenimiento:** para mantener el acceso al sistema, se establecen mecanismos adicionales que permiten una conexión persistente a Internet.

5. **Etapa de eliminación de rastros:** en esta fase se eliminan por completo todas las huellas del usuario no autorizado que accedió al sistema.

Una vez identificadas las diferentes etapas de un ataque, se pueden categorizar por autoría, como se muestra en la Tabla III.

TABLA III. CLASIFICACIÓN DE LAS AUTORÍAS DE CIBERATAQUES [22].

Autores	Objetivos		
	Gobierno	Sector Privado	Ciudadanos
Ataques patrocinados por estados.	Espionaje, ataques contra infraestructuras críticas, APT.	Espionaje, ataques contra infraestructuras críticas, APT.	-
Ataques patrocinados por el sector privado.	Espionaje.	Espionaje.	-
Terroristas, extremismo político e ideológico.	Ataques contra las redes, sistemas o servicios de terceros, ataques contra servicios de internet, infección con malware.	Ataques contra las redes, sistemas o servicios de terceros, ataques contra servicios de internet, infección con malware.	-
Hacktivistas.	Robo y publicación de información clasificada o sensible, ataques contra las redes, sistemas o servicios de terceros, ataques contra servicios de internet, infección con malware.	Robo y publicación de información clasificada o sensible, ataques contra las redes, sistemas o servicios de terceros, ataques contra servicios de internet, infección con malware.	Robo y publicación de datos personales.
Crimen organizado.	Espionaje	Robo de identidad digital y fraude.	Robo de identidad digital y fraude.
Ataques de perfil bajo.	Ataques contra las redes, sistemas o servicios de terceros, ataques contra servicios de internet, infección con malware.	Ataques contra las redes, sistemas o servicios de terceros, ataques contra servicios de internet, infección con malware.	-
Ataques de personal con accesos privilegiados.	Espionaje, ataques contra infraestructuras críticas.	Espionaje, ataques contra infraestructuras críticas.	-

3.5.1. Presentación de los posibles escenarios.

El lugar donde el consultor llevará a cabo las pruebas de seguridad, también conocidas como Pentesting, se denomina escenario, a continuación, en la Tabla IV se hace

referencia a los posibles escenarios en el que tiene que desenvolverse un profesional de la seguridad de la información, mientras que en la figura 7 se puede observar un análisis gráfico de los escenarios que se pueden presentar durante las pruebas de intrusión a realizarse en una organización.

TABLA IV. DESCRIPCIÓN DE ESCENARIOS.

Escenario	Descripción
1	El consultor se encuentra ubicado en un punto de acceso a la red LAN/WAN de la empresa.
2	En este lugar, el consultor se encuentra ubicado dentro del firewall que protege el área a ser analizada.
3	En este escenario, el consultor realiza las pruebas de seguridad desde una red externa a la empresa. En la mayoría de los casos se hace desde internet.

Fuente: El autor.

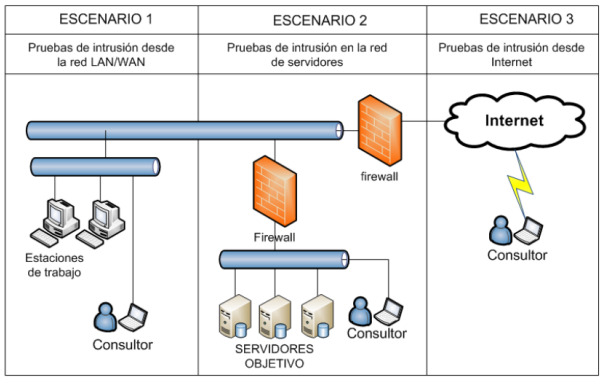


Fig. 7 Diagrama de escenarios de análisis [7].

3.6. Ataques Informáticos o Ciberataques.

Se pueden identificar varios tipos de ataques cibernéticos, pero algunos de ellos son:

- **Malware:** es un software dañino diseñado para propagarse a través de archivos, correos electrónicos y descargas de sitios web poco fiables con el fin de dañar la computadora, robar archivos y acceder a los derechos del sistema [17].

- **Spyware:** programa que realiza un seguimiento de la actividad del usuario en un dispositivo con el fin de hacer un uso indebido de los datos [17].

- **Rasomware:** es un tipo de software malintencionado que cifra los archivos y datos de un usuario, y solicita un pago para permitir el acceso a ellos [17].

- **Inyección SQL:** es una técnica de ataque que involucra la inserción de código malicioso en una base de datos a través de una consulta SQL, con el objetivo de obtener datos privados [17].

- **Spear Phishing:** se trata de un tipo de engaño digital que se basa principalmente en el correo electrónico con el propósito de obtener acceso no autorizado a información esencial y confidencial. Estos ataques suelen seguir un patrón predecible y pueden afectar tanto a organizaciones del sector público como privado. Cuando un destinatario hace clic en un enlace dentro de un correo electrónico fraudulento que aparentemente proviene de una institución bancaria, una agencia gubernamental u otra empresa reconocida, se le redirige a un sitio web falso donde se le solicita que proporcione información personal y financiera como su número de tarjeta de débito, detalles de la cuenta bancaria, número de tarjeta de crédito, entre otros. El objetivo principal de este tipo de ataque es el robo de datos financieros y personales [22].

- **Watering-hole:** este tipo de ciberataque se basa en la observación y el análisis de los sitios web que la víctima potencial visita con frecuencia. A continuación, se instalan programas maliciosos o virus informáticos en estos sitios web, que infectan el ordenador de la víctima y permiten a los piratas informáticos recopilar diversos tipos de información. Estos ataques utilizan vulnerabilidades de seguridad de día cero, lo que significa que no se hacen públicos hasta que se explota la vulnerabilidad [22].

- **Man-in-the-Middle:** el ataque de hombre en el medio se produce mediante acciones no autorizadas, como la suplantación de identidad o la duplicación de

transacciones, lo que puede llevar a una brecha en la seguridad de la red, donde la información se almacena sin consentimiento y se reenvía para engañar al destinatario. La forma de protegerse contra este tipo de ataque es utilizando un cifrado sólido entre el servidor y el cliente [22].

- **Modificación:** este ataque se produce cuando alguien o una pieza de software realiza modificaciones ilegales en el código fuente del software, y los datos enviados a través del canal también pueden ser atacados de otras formas [22].

- **Ataque de denegación de servicio (DDoS):** se trata de un tipo de ciberataque que impide el acceso de los usuarios autorizados a los recursos o servicios proporcionados por un sistema o dispositivo de red. Este ataque puede ser clasificado en dos categorías principales: el ataque de denegación de servicio, que explota vulnerabilidades de seguridad, y el ataque de solicitud de denegación de servicio, que envía solicitudes falsas para no responder a peticiones legítimas [22].

- **Ingeniería social:** este tipo de piratería obliga a las víctimas a facilitar información privada, como contraseñas, a los atacantes para obtener acceso a los ordenadores de una empresa [17].

- **Trashing:** un tipo de ataque que examina la basura de un ordenador (como la Papelera de Reciclaje) en busca de información, suele suponer una grave amenaza para los usuarios que borran información sensible o privada sin borrarla definitivamente [17].

- **Ataques de repetición:** este tipo de ataque implica el acto de interceptar información que se está transmitiendo a través de una red, como una orden de autenticación a un sistema informático, y reenviarla al remitente original sin que el receptor original se dé cuenta de que ha sido interceptada. El sistema informático ejecutará la orden como si fuera auténtica y transmitirá la respuesta al atacante, lo que puede permitirle obtener acceso al sistema si el sistema

informático o la aplicación son susceptibles a este tipo de ataque. Para defenderse de este tipo de ataque, el sistema informático puede emplear medidas de seguridad como controles de identificación de comandos, sellado de tiempo, cifrado y firma de comandos para evitar la reutilización de comandos [14].

- **Spoofing:** la suplantación de identidad es un método de suplantación en línea utilizado por los ciberdelincuentes, normalmente tras una investigación exhaustiva o con el uso de malware. La privacidad de los usuarios y la integridad de los datos están en peligro por las amenazas a la seguridad de la red que utilizan métodos de suplantación [14].

- **Los troyanos:** a veces conocidos como caballos de Troya, son programas informáticos que tienen instrucciones ocultas al usuario, de modo que parecen realizar las actividades que el usuario espera que realicen mientras que en secreto llevan a cabo otras operaciones [14].

- **Virus:** se trata de un conjunto de instrucciones que se introducen en un archivo ejecutable, también conocido como "anfitrión", de tal manera que cuando se ejecuta dicho archivo, el virus se reproduce y se infiltra en otros programas [22].

- **Gusanos:** un gusano es un programa ejecutable que puede propagarse a través de redes, a veces portando virus o aprovechándose de las vulnerabilidades de los sistemas a los que se conecta para causar daño [22].

Una de las herramientas disponibles para llevar a cabo un análisis de vulnerabilidades es Nessus, la cual se puede utilizar en un escenario de red que incluya servidores y estaciones de trabajo en una LAN, y donde los objetivos estén definidos mediante pruebas de caja blanca.

3.7. Estándares, modelos y normativas de ciberseguridad.

En las siguientes líneas se detalla una breve evaluación de los distintos enfoques y procedimientos utilizados en la actualidad para el análisis de amenazas en el ámbito de la seguridad informática.

3.7.1. Metodología Information Risk Analysis Methodology (IRAM 2).

Se trata de una metodología o marco que permite crear una evaluación de riesgos para la organización Importer Security Filing (ISF), pionera en el estudio y avance de procedimientos de seguridad sensatos. El modelo, creado tras varias conversaciones con numerosos especialistas en ciberseguridad, contiene seis procesos de aplicación, se destacan las principales actividades realizadas para cumplir los objetivos y se señalan también los principales elementos de riesgo.

1. **Identificación del alcance.**

   La actividad inicial en el modelo IRAM 2 es la identificación del alcance, la cual implica un análisis exhaustivo de los procesos de negocio y las características de la tecnología disponible. El objetivo es obtener un perfil de evaluación de riesgos a nivel de procesos de negocio y servicios tecnológicos [21].

2. **Evaluación del impacto en el negocio.**

   En la segunda etapa del modelo IRAM 2 se lleva a cabo la evaluación del impacto en el negocio. En este proceso, se identifica la información crucial para la organización y se determina su plazo de utilidad. También se calcula el impacto que podría tener la pérdida o disminución de los atributos de seguridad cibernética, considerando dos posibles escenarios: uno realista y otro el peor de los casos [21].

3. **Perfilado de amenazas.**

   En esta etapa se lleva a cabo la categorización y detección de amenazas potenciales que puedan poner en riesgo la información manejada por la organización [21].

4. **Evaluación de vulnerabilidades.**

Durante esta fase, se analizan las vulnerabilidades identificadas con el fin de que los ataques previamente identificados en la etapa anterior puedan ser exitosos. Los consultores evalúan la efectividad de los controles y su nivel de fortaleza [21].

5. Evaluación del riesgo.

Se evalúa si una amenaza tendrá éxito en la organización bajo un conjunto específico de circunstancias [21].

6. Tratamiento del riesgo.

La fase final del modelo consiste en la identificación de soluciones y métodos para mitigar o eliminar los riesgos identificados, así como en el diseño de una estrategia de tratamiento de riesgos adecuada [21].

3.7.2. Metodología National Institute of Standards and Technology (NIST).

En 1901, el Instituto Nacional de Normas y Tecnología (NIST) fue establecido por el Departamento de Comercio de los Estados Unidos como una organización federal encargada de supervisar la tecnología. La gestión de la ciberseguridad se desarrolló a partir de la metodología del NIST, la cual se compone de una serie de documentos científicos enfocados principalmente en la seguridad de la información. El proceso es completamente iterativo, compuesto por varias fases consecutivas [21]:

- **Fase 1:** Preparación de la evaluación.
- **Fase 2:** Realizar una evaluación.
- **Fase 3:** Comunicación de los resultados.
- **Fase 4:** Evaluación de la sostenibilidad.

Las tareas necesarias para garantizar una seguridad óptima de la información se definen como: identificación del origen de la amenaza, aparición de la amenaza, investigación de la vulnerabilidad, condiciones de aplicación, probabilidad de aparición, impacto, identificación del riesgo, informe de respuesta al riesgo, informe de evaluación del

riesgo y resumen de la tarea. Cada fase requiere varias acciones específicas para cumplir con sus objetivos.

3.7.3. Metodología MAGERIT.

La metodología MAGERIT es un estándar para el análisis de riesgos de la información en las administraciones públicas españolas. Se basa en el análisis de los riesgos potenciales de los activos de información, ordenados por importancia, siendo los activos más importantes los servicios prestados a los ciudadanos, como los basados en software, servidores, elementos de comunicación, desarrolladores, sistemas, etc. La reglamentación se lleva a cabo en dos etapas: en primer lugar, se examinan los activos de forma dependiente para identificar los peligros que corren dichos activos; en segundo lugar, se aplican las medidas de seguridad existentes para calibrar los riesgos actuales. La metodología MAGERIT se utiliza como herramienta fundamental, con licencias gratuitas a disposición de las entidades gubernamentales y licencias premium a disposición de las empresas dispuestas a utilizarla [21].

3.7.4. Metodología ISO 27000.

La implementación de este enfoque permite a diferentes entidades establecer un sistema que gestione la seguridad de la información, es importante observar que cualquier sistema de gestión debe cumplir mínimo ciertos procesos, los cuales se detallan en la figura 8.

Esta metodología ISO 27000 incluye un Apéndice A que engloba 14 dominios para cubrir la mayoría de los problemas de seguridad de la información que puedan surgir en una organización o institución [21].

A continuación, se lista los 14 dominios de la metodología ISO:27000: políticas de seguridad de la información, organización de la seguridad de la información, seguridad relativa de los recursos humanos, gestión de activos, control de acceso y criptografía, seguridad física y del entorno, seguridad de las operaciones, seguridad de las

comunicaciones, adquisición, desarrollo y mantenimiento de los sistemas de información, relación con proveedores, gestión de incidentes de la seguridad de la información, aspectos de seguridad de la información para la gestión continua, y cumplimiento [21].

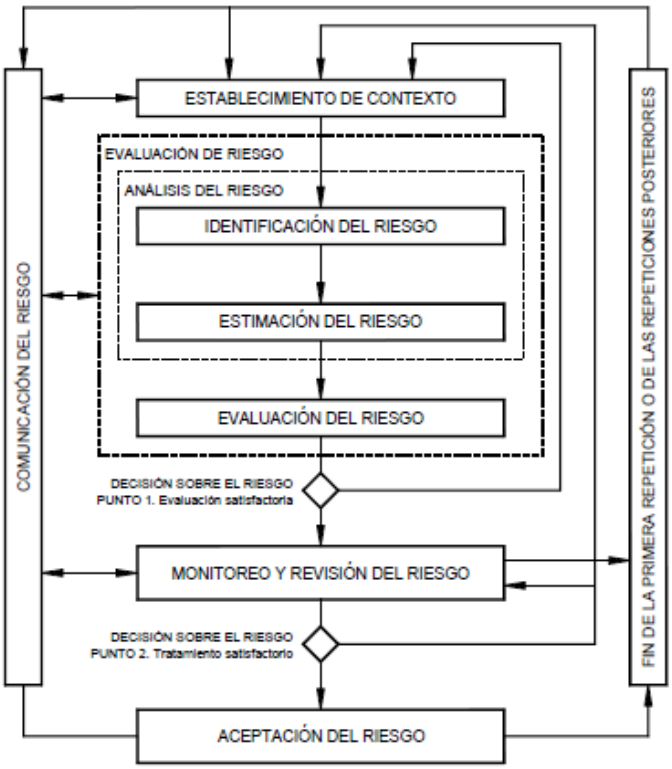


Fig. 8 Proceso de gestión del riesgo en la seguridad de la información [16].

La figura 8 ilustra cómo las actividades de gestión y/o evaluación de riesgos pueden iterar el proceso de gestión de riesgos para la seguridad de la información. La profundidad y el detalle de cada iteración de una evaluación de riesgos se incrementan utilizando un método iterativo. La técnica iterativa logra un compromiso justo entre acortar la cantidad de tiempo y trabajo necesarios para encontrar controles y garantizar que incluso los mayores riesgos se evalúen con precisión [16].

3.8. Ciclo PHVA (Planificar-Hacer-Verificar-Actuar).

Hoy en día, las empresas públicas y privadas deben mejorar y desarrollar sus operaciones productivas para sobrevivir, así como implantar un proceso de mejora continua que ayude de forma continua y sin fisuras. El estadístico estadounidense Edward Deming desarrolló el ciclo PHVA de mejora continua en la década de 1950 [13].

3.8.1. Las fases del ciclo PHVA.

Los términos "planificar, hacer, verificar y actuar" se abrevian para crear el acrónimo "PHVA", y cada uno de estos principios denota una fase diferente del ciclo, podemos revisar la figura 9 [20].

Planificar: en la etapa de planificación, se identifican los objetivos primarios de cada entidad para optimizar sus procesos y alcanzar otros objetivos. Asimismo, se establecen los requerimientos del cliente para implementar procedimientos que fomenten la productividad empresarial y favorezcan la consecución de resultados alineados con su política. En esta fase, también se definen los criterios de medición para supervisar y hacer seguimiento a los procesos [13].

Hacer: en esta fase se realizan nuevos ajustes o acciones para llevar a cabo las mejoras sugeridas en la fase anterior. Los proyectos piloto suelen crearse como pruebas de rendimiento, ya que facilitan la gestión de posibles problemas de ejecución [13].

Verificar: una vez finalizadas las dos primeras fases, se inicia un plan de mejora que incluye un periodo de prueba para calibrar y evaluar el funcionamiento de las mejoras. Esta fase implica acondicionamiento y adaptabilidad [13].

Actuar: se pueden tomar medidas correctivas si los resultados de la medición no están a la altura de los objetivos deseados y predeterminados. Por otra parte, la empresa toma las decisiones correctas y adopta las medidas necesarias para hacer avanzar el proceso de forma coherente [13].

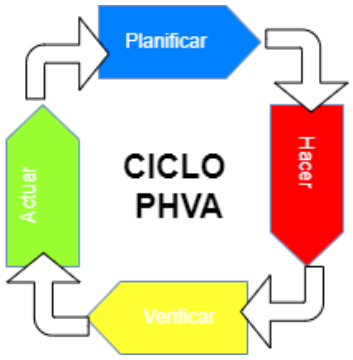


Fig. 9 Ciclo PHVA (planificar, hacer, verificar y actuar).
Fuente: El autor

3.9. Herramientas utilizadas para el desarrollo del proyecto.

3.9.1. Servidor.

Un servidor es un tipo de computadora remota que proporciona datos a otros dispositivos mediante solicitudes realizadas desde navegadores web. Esto significa que, en una red local, hay un software que convierte un ordenador en servidor para facilitar el acceso de los usuarios a la red y a sus servicios. Cuando se recibe una solicitud por parte del cliente, el servidor envía información en formato HTML a través del protocolo HTTP y almacena la información en forma de páginas web en el navegador, un claro ejemplo tenemos en la figura 10 de un modelo cliente-servidor [16].

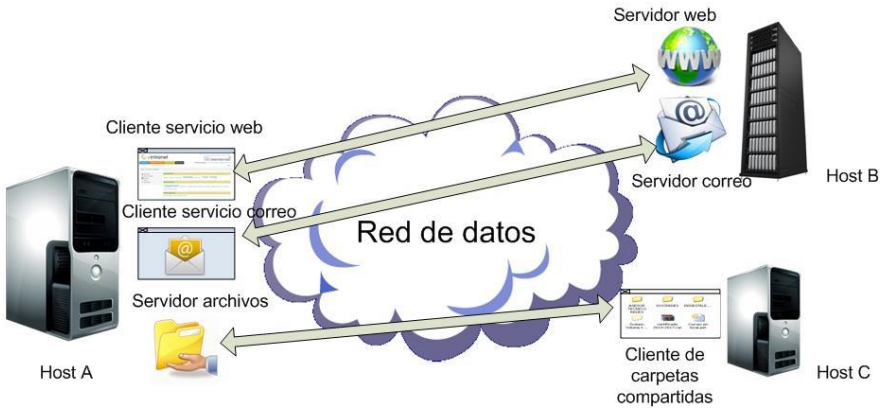


Fig. 10 Modelo Cliente-Servidor [16].

A continuación, se enumeran los distintos tipos de servidores:

- **Servidor FTP (File Transfer Protocol):** es uno de los servicios más antiguos y utilizados para el intercambio de archivos en Internet. Permite la transferencia segura de uno o varios archivos entre diferentes computadoras, además de proporcionar organización de archivos y control de transferencias [16].

- **Los servidores de correo:** son igual de importantes que los servidores web y son ampliamente utilizados. Estos servidores transfieren y almacenan el correo electrónico entre redes empresariales LAN, WAN e Internet. Para acceder a nuestros correos electrónicos, necesitamos un cliente de correo electrónico como Microsoft Outlook, Eudora o Google, aunque también existen servicios de correo web que ofrecen una interfaz web para acceder al correo electrónico, como Google o Hotmail [16].

- **Los servidores de bases de datos:** son el nivel superior de los servidores, no solo por su velocidad, sino porque los datos son el recurso más valioso para cualquier empresa y estos servidores son ricos en datos. Debido a la necesidad de procesar grandes volúmenes de datos complicados y comunicarse con varios clientes, se crearon los servidores de bases de datos [16].

- **Servidor web:** es el más conocido y utilizado, y en esencia carga un archivo y lo envía a través de la red al navegador del usuario para proporcionar contenido estático. El protocolo HTTP (Hypertext Transfer Protocol), uno de los protocolos establecidos para la transmisión de datos en Internet, hace posible todo el procedimiento. El usuario envía una solicitud HTTP cuando abre su navegador web y escribe una dirección web, como http://www.google.com, que viaja por Internet hasta recibir una respuesta de un servidor web. Este servidor transmite el código HTML de la página, que incluye objetos incrustados como animaciones o reproductores de música y textos complejos con enlaces, imágenes, tablas y otros elementos [16].

- **Servidor de archivos:** proporciona un lugar central en una red donde las personas de la red pueden compartir y almacenar archivos. Los usuarios pueden acceder a

ellos en el servidor de archivos en lugar de transferir archivos esenciales entre computadoras [16].

3.9.2. Sistema operativo Kali-Linux.

Kali es una distribución de Linux construida sobre Debian que está pensada para informática forense, pruebas de penetración y auditorías de seguridad, es una parte de Linux muy conocida en todo el mundo y es pionera en pruebas de hacking ético y pentesting, Kali tiene varias aplicaciones que se pueden ejecutar.

Es un entorno seguro con sólo un pequeño número de individuos de confianza que tienen acceso a editar paquetes y comunicarse con los repositorios originales. Está disponible como imágenes ISO para muchas arquitecturas [19].

A continuación, se lista algunas características que posee Kali-Linux:

- **Robusto**: dispone de herramientas de pruebas de penetración más optimizadas que otros sistemas similares [19].

- **Libre**: los autores de los estudios no los modifican, y existe código abierto que no es libre pero que puede obtenerse a través de algunos acuerdos con distribuidores que lo venden [19].

- **Código abierto:** dispone de un repositorio donde se almacena el código fuente del sistema Kali para que pueda ser mejorado o reconstruido [19].

- **Personalizable**: es posible actualizar una característica de Kali Linux que sea complementaria y responda a las necesidades del cliente [19].

- Puede acomodar un número considerable de dispositivos inalámbricos [19].

- Aunque la mayoría de estas partes están codificadas en inglés, contiene una gran variedad de idiomas [19].

- El sistema Kali Linux, desarrollado en un entorno fiable, ejecuta la seguridad de los paquetes y es donde se encuentran muchos de los orígenes de la seguridad [19].

3.9.3. Aplicación NESSUS.

Se trata de un software muy utilizado para detectar debilidades de seguridad, que presenta los resultados en forma de porcentaje. Este programa se encarga de llevar a cabo análisis de seguridad informática y es compatible con los sistemas operativos Windows y Linux. Nessus se actualiza de forma regular y dispone de más de 70.000 plugins que examinan los sistemas de una organización para detectar posibles vulnerabilidades [20].

Además, incluye características de seguridad exclusivas, tanto a nivel local como remoto y autenticado. Nessus se basa en una arquitectura cliente-servidor y cuenta con una interfaz web y un lenguaje de script que permite crear nuevos complementos o mejorar los ya existentes [13].

3.9.4. Aplicación NMAP.

Nmap es un software de código abierto y de acceso público para escanear puertos de red y servicios empresariales. Este software es útil para administradores de redes y sistemas en centros informáticos corporativos para realizar tareas como auditorías de red, programación de actualizaciones de servicios y monitoreo del tiempo de actividad de los servidores [20].

Nmap analiza paquetes IP para identificar que hosts están presentes en la red y que servicios y aplicaciones están en ejecución, incluyendo nombres y versiones de

aplicaciones y sistemas operativos orientados a servidores y estaciones de trabajo. También realiza escaneos de puertos en hosts o en dominios propiedad de la empresa. Todas las versiones de sistemas operativos son compatibles con Nmap y hay paquetes binarios oficiales para Linux, Windows y Mac OS X. Nmap también se puede utilizar desde la línea de comandos y viene con una interfaz gráfica de usuario sofisticada y visores de salida, como ZENMAP, que es una herramienta versátil para transferir, redirigir y limpiar datos [13].

4. Materiales y metodología.

4.1. Diseño metodológico.

4.1.1. Metodología de aplicación.

En base a las preguntas planteadas y tomando en cuenta los objetivos a alcanzar en este proyecto de aplicación, se adopta un enfoque práctico que asegura la obtención de los resultados deseados en lo que respecta a la protección de los activos de información de la empresa Uniscan.

Población y muestra.

Se consideró que todos los trabajadores de Uniscan eran el grupo objetivo de la investigación, y se tomó una muestra del 100% de la población, compuesta por las 25 personas que laboran en la organización.

Gerencia General, el área administrativa se divide en distintos departamentos: 6 personas en el departamento de contabilidad, 3 personas en el departamento de ventas, 5 personas en el departamento marketing y 4 personas en el departamento de logística, mientras que el área técnica está conformada por: 2 personas en el departamento de desarrollo y 4 personas en el departamento técnico.

Técnicas de recopilación de información.

Para la obtención de información necesaria para la planificación del proyecto, se aplicaron técnicas de observación con el objetivo de analizar detalladamente los recursos existentes. Además, se realizó un inventario de los activos de información para poder identificar posibles vulnerabilidades de manera precisa y así establecer estrategias de protección adecuadas.

Además de la observación, se recurrió a la recolección de datos mediante entrevistas y encuestas, siguiendo la metodología MAGERIT. De esta forma, se logró recopilar información valiosa y detallada sobre los sistemas y procesos existentes en la empresa,

lo que permitió establecer un marco de trabajo claro y definido para el proyecto. Con esta información, se pudo diseñar un plan de acción adecuado para mejorar la seguridad de los activos de información de la organización, garantizando la protección adecuada contra posibles vulnerabilidades y amenazas informáticas.

4.1.2. Metodología de gestión de riesgos MAGERIT.

La implementación de procesos administrativos en las empresas se ve fortalecida gracias al enfoque en la tecnología y sus avances. La misión y visión de las empresas pueden hacerse realidad mediante esta estrategia.

Una de las principales finalidades de este enfoque es ayudar a mitigar el riesgo, monitoreando y evaluando el uso de activos informáticos en una organización para identificar comportamientos que generan riesgos. Con esta herramienta, los analistas de seguridad de la información pueden proponer mejoras en una amplia variedad de controles, que contribuyen a reducir los riesgos en las áreas de: administración, operaciones, tecnología, logística, marketing y ventas, en empresas que como la organización Uniscan se encuentran en desarrollo.

4.1.3. Utilización de la herramienta de encuesta.

Para obtener información precisa y confiable acerca de un tema en particular, se emplea un método de investigación que consiste en formular una serie de preguntas específicas sobre dicho tema y dirigirlas a un grupo representativo de la población. De esta manera, se busca identificar a los individuos o entidades que están activamente involucrados o interesados en el tema, y obtener información detallada acerca de sus opiniones, actitudes y comportamientos relacionados con el mismo. Esta técnica de investigación es muy útil para conocer las necesidades y preferencias del público objetivo, así como para identificar tendencias y patrones de comportamiento que pueden ser de interés para las empresas y organizaciones en diversos ámbitos, como el marketing, la

publicidad, la salud, la política, entre otros, y principalmente en el área de la seguridad de la información el cual es nuestro campo de estudio en el presente proyecto.

Por este motivo durante la realización de nuestra investigación se desarrolló varios cuestionarios que fueron llenados por el personal que labora en la empresa Uniscan, dos ejemplos son: la Tabla V y la Tabla VI que se muestran a continuación, donde se recopilan varias preguntas necesarias para tener un panorama claro del estado de la seguridad de la infraestructura tecnológica de la organización Uniscan en el presente.

TABLA V. FICHA DE OBSERVACIÓN N° 01

FICHA DE OBSERVACIÓN		**FICHA N°1**
EMPRESA:	UNISCAN	
DEPARTAMENTO:	Departamento Técnico	
OBSERVADOR:	Luis Omar Villacrés Túqueres	
FECHA:		
NOMBRE DE ENTREVISTADO:	**CARGO:**	
ITEMS	**CALIFICATIVOS**	
	SI	**NO**
¿La infraestructura que procesa y almacena la información de las aplicaciones (web) está en área segura?		
¿Se cuenta con personal responsable de la seguridad de la información dentro de la empresa?		
¿Conoce cuáles son las principales amenazas más usuales que se emplean a aplicaciones web?		
¿Se diseñan páginas de inicio de sesión lo suficientemente seguras para evitar el acceso a personas no autorizadas a aplicaciones web?		
¿Cree que es necesario redirigir al usuario a una nueva página después de un inicio de sesión?		
¿Existe alguna política de seguridad en cuanto al manejo de la información dentro de la empresa?		
¿Los usuarios de las aplicaciones web manejan algún tipo de seguridad para el manejo de contraseñas?		
¿Existe algún tipo de herramienta informática para realizar pruebas de seguridad a aplicaciones web?		
¿Se desarrolla software con todas las medidas de seguridad?		
¿Alguna aplicación web se ha visto afectada por algún tipo de ataque informático?		

Fuente: El autor.

TABLA VI. FICHA DE OBSERVACIÓN N° 02

FICHA DE OBSERVACIÓN		**FICHA N°2**
EMPRESA:	UNISCAN	
DEPARTAMENTO:	Departamento Técnico	
OBSERVADOR:	Luis Omar Villacrés Túqueres	
FECHA:		
NOMBRE DE ENTREVISTADO:	**CARGO:**	
ITEMS	**CALIFICATIVOS**	
	SI	**NO**
¿Conoce algún método o técnica para identificar vulnerabilidades en aplicaciones web?		
¿Conoce lo que implica un riesgo informático relacionado a una aplicación web?		
¿Existe algún proceso que indique que la integridad de la información está presente?		
¿Existe algún proceso que indique que la confidencialidad de la información está presente?		
¿Existe algún proceso que indique que la disponibilidad de la información está presente?		
¿Se toma alguna medida de protección para desarrollar una aplicación web segura?		
¿Las aplicaciones web se alojan en un sitio seguro para hacer uso de estas?		
¿Se tiene algún método o técnica para almacenar la información de las aplicaciones web en sitios seguros?		
¿Se realizan copias frecuentes de las aplicaciones web para evitar pérdida de información de estas?		
¿Conoce los términos de riesgo, amenaza y vulnerabilidad?		

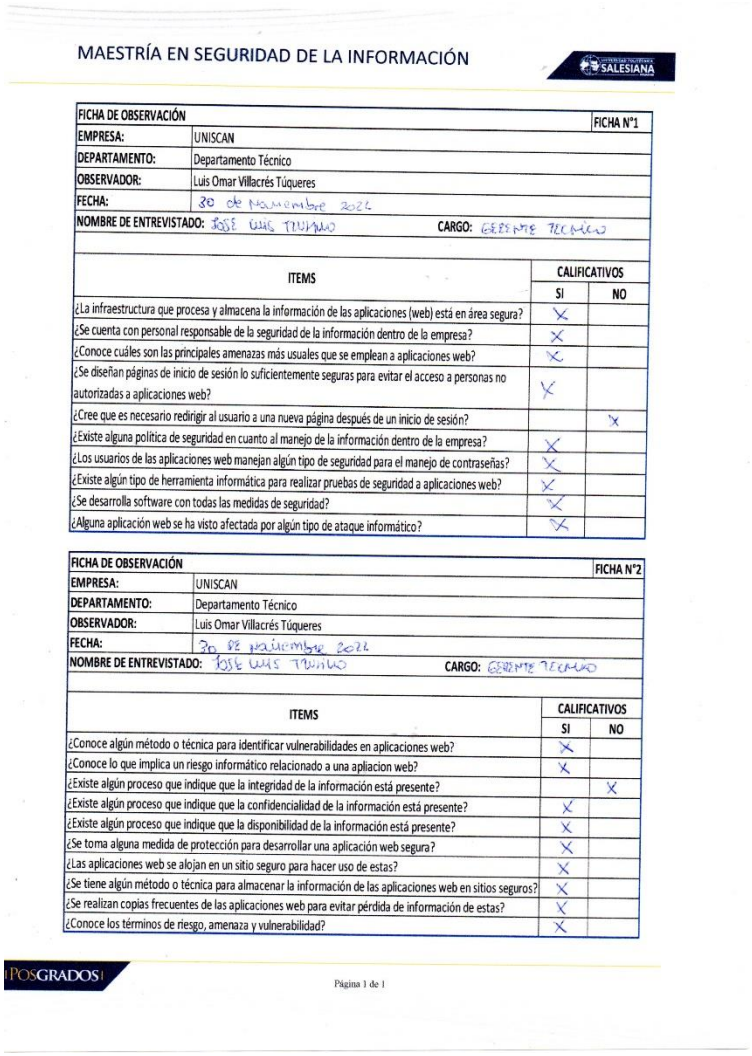
Fuente: El autor.

4.1.4. Utilización de la entrevista como herramienta.

La persona que ejerza el rol de consultor deberá realizar las preguntas y brindar datos de interés a través del diálogo. El punto fuerte de las entrevistas es que los propios participantes proporcionan datos sobre su propio comportamiento, creencias, preferencias, actitudes y expectativas. Las entrevistas estructuradas se realizan de acuerdo a una guía elaborada por el entrevistador, la cual contiene las preguntas que se le harán al entrevistado.

Se puede revisar el Anexo 1, donde se encontrarán las preguntas y respuestas de la entrevista realizada al Ing. José Luis Trujillo (Gerente Técnico de Uniscan). Adicionalmente se realizó una serie de preguntas al Ing. José Luis Trujillo responsable

del área de tecnología de Uniscan, con el cargo de Gerente Técnico para mostrar cómo se encuentra la infraestructura tecnológica en cuanto a seguridad de la información y riesgo que maneja la organización, podemos ver las respuestas brindadas en la figura 11, las soluciones que se presentaron fueron los calificativos SI o NO.



MAESTRÍA EN SEGURIDAD DE LA INFORMACIÓN

FICHA DE OBSERVACIÓN		FICHA N°1
EMPRESA:	UNISCAN	
DEPARTAMENTO:	Departamento Técnico	
OBSERVADOR:	Luis Omar Villacrés Túqueres	
FECHA:	30 de Noviembre 2022	
NOMBRE DE ENTREVISTADO:	JOSÉ LUIS TRUJILLO	CARGO: GERENTE TECNICO

ITEMS	CALIFICATIVOS	
	SI	NO
¿La infraestructura que procesa y almacena la información de las aplicaciones (web) está en área segura?	X	
¿Se cuenta con personal responsable de la seguridad de la información dentro de la empresa?	X	
¿Conoce cuáles son las principales amenazas más usuales que se emplean a aplicaciones web?	X	
¿Se diseñan páginas de inicio de sesión lo suficientemente seguras para evitar el acceso a personas no autorizadas a aplicaciones web?	X	
¿Cree que es necesario redirigir al usuario a una nueva página después de un inicio de sesión?		X
¿Existe alguna política de seguridad en cuanto al manejo de la información dentro de la empresa?	X	
¿Los usuarios de las aplicaciones web manejan algún tipo de seguridad para el manejo de contraseñas?	X	
¿Existe algún tipo de herramienta informática para realizar pruebas de seguridad a aplicaciones web?	X	
¿Se desarrolla software con todas las medidas de seguridad?	X	
¿Alguna aplicación web se ha visto afectada por algún tipo de ataque informático?	X	

FICHA DE OBSERVACIÓN		FICHA N°2
EMPRESA:	UNISCAN	
DEPARTAMENTO:	Departamento Técnico	
OBSERVADOR:	Luis Omar Villacrés Túqueres	
FECHA:	30 de Noviembre 2022	
NOMBRE DE ENTREVISTADO:	JOSÉ LUIS TRUJILLO	CARGO: GERENTE TECNICO

ITEMS	CALIFICATIVOS	
	SI	NO
¿Conoce algún método o técnica para identificar vulnerabilidades en aplicaciones web?	X	
¿Conoce lo que implica un riesgo informático relacionado a una apliacion web?	X	
¿Existe algún proceso que indique que la integridad de la información está presente?		X
¿Existe algún proceso que indique que la confidencialidad de la información está presente?	X	
¿Existe algún proceso que indique que la disponibilidad de la información está presente?	X	
¿Se toma alguna medida de protección para desarrollar una aplicación web segura?	X	
¿Las aplicaciones web se alojan en un sitio seguro para hacer uso de estas?	X	
¿Se tiene algún método o técnica para almacenar la información de las aplicaciones web en sitios seguros?	X	
¿Se realizan copias frecuentes de las aplicaciones web para evitar pérdida de información de estas?	X	
¿Conoce los términos de riesgo, amenaza y vulnerabilidad?	X	

POSGRADOS

Página 1 de 1

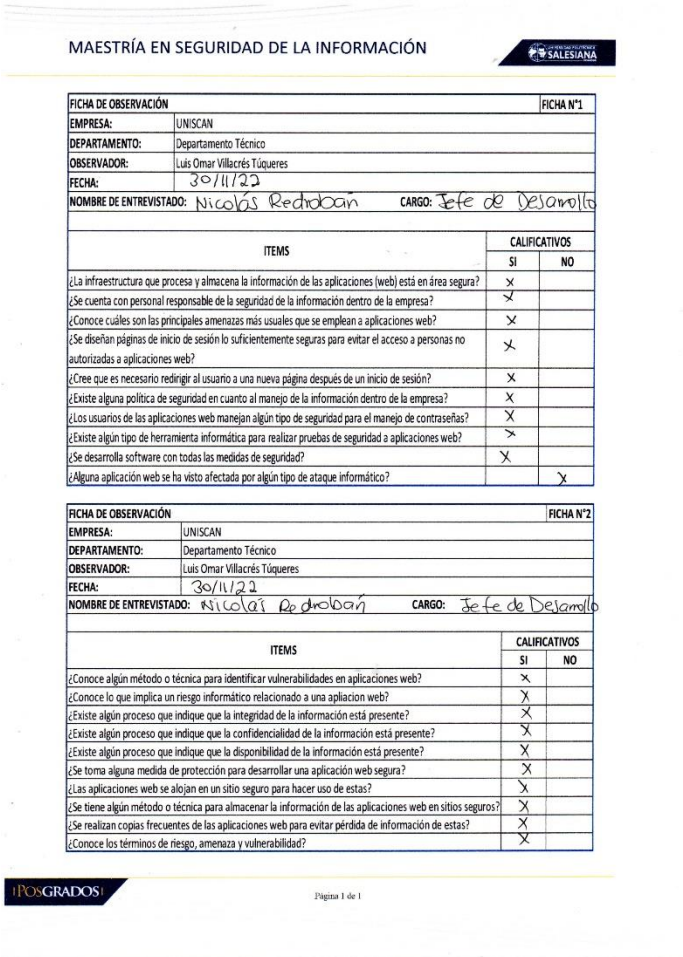
Fig. 11 Documento escaneado de la encuesta realizada al Ing. José Luis Trujillo (Gerente Técnico Uniscan). Fuente: El autor.

Para continuar con la elaboración del proyecto es necesario entrevistar a las personas que forman parte del equipo del Departamento de Desarrollo de la empresa Uniscan, quienes son: Ing. Nicolás Redrobán, con el cargo de Jefe del Departamento e Ing. Briggette Echeverría, con el cargo de Desarrolladora y Soporte. Se puede revisar la figura 12 y figura 13, donde se encontrarán las preguntas y respuestas de las entrevistas realizadas, estos datos permitirán mostrar cómo se encuentra la infraestructura tecnológica en cuanto a seguridad de la información y riesgo que maneja la

organización, en las figuras antes mencionadas podemos ver las respuestas brindadas respectivamente por cada uno de los integrantes del equipo de Desarrollo, las soluciones que se presentaron fueron los calificativos SI o NO.

Desarrollo de la entrevista al Ing. Nicolás Redrobán (Jefe del Departamento de Desarrollo de la Empresa Uniscan).

A las 11:00 am del día miércoles 30 de Noviembre de 2022, previa cita agendada con el Ing. Nicolás Redrobán, se realiza la siguiente entrevista, podemos ver las respuestas brindadas en la figura 12.



MAESTRÍA EN SEGURIDAD DE LA INFORMACIÓN

FICHA DE OBSERVACIÓN		FICHA N°1
EMPRESA:	UNISCAN	
DEPARTAMENTO:	Departamento Técnico	
OBSERVADOR:	Luis Omar Villacrés Túqueres	
FECHA:	30/11/22	
NOMBRE DE ENTREVISTADO:	Nicolás Redrobán	CARGO: Jefe de Desarrollo

ITEMS	CALIFICATIVOS	
	SI	NO
¿La infraestructura que procesa y almacena la información de las aplicaciones (web) está en área segura?	X	
¿Se cuenta con personal responsable de la seguridad de la información dentro de la empresa?	X	
¿Conoce cuáles son las principales amenazas más usuales que se emplean a aplicaciones web?	X	
¿Se diseñan páginas de inicio de sesión lo suficientemente seguras para evitar el acceso a personas no autorizadas a aplicaciones web?	X	
¿Cree que es necesario redirigir al usuario a una nueva página después de un inicio de sesión?	X	
¿Existe alguna política de seguridad en cuanto al manejo de la información dentro de la empresa?	X	
¿Los usuarios de las aplicaciones web manejan algún tipo de seguridad para el manejo de contraseñas?	X	
¿Existe algún tipo de herramienta informática para realizar pruebas de seguridad a aplicaciones web?	X	
¿Se desarrolla software con todas las medidas de seguridad?	X	
¿Alguna aplicación web se ha visto afectada por algún tipo de ataque informático?		X

FICHA DE OBSERVACIÓN		FICHA N°2
EMPRESA:	UNISCAN	
DEPARTAMENTO:	Departamento Técnico	
OBSERVADOR:	Luis Omar Villacrés Túqueres	
FECHA:	30/11/22	
NOMBRE DE ENTREVISTADO:	Nicolás Redrobán	CARGO: Jefe de Desarrollo

ITEMS	CALIFICATIVOS	
	SI	NO
¿Conoce algún método o técnica para identificar vulnerabilidades en aplicaciones web?	X	
¿Conoce lo que implica un riesgo informático relacionado a una apliacion web?	X	
¿Existe algún proceso que indique que la integridad de la información está presente?	X	
¿Existe algún proceso que indique que la confidencialidad de la información está presente?	X	
¿Existe algún proceso que indique que la disponibilidad de la información está presente?	X	
¿Se toma alguna medida de protección para desarrollar una aplicación web segura?	X	
¿Las aplicaciones web se alojan en un sitio seguro para hacer uso de estas?	X	
¿Se tiene algún método o técnica para almacenar la información de las aplicaciones web en sitios seguros?	X	
¿Se realizan copias frecuentes de las aplicaciones web para evitar pérdida de información de estas?	X	
¿Conoce los términos de riesgo, amenaza y vulnerabilidad?	X	

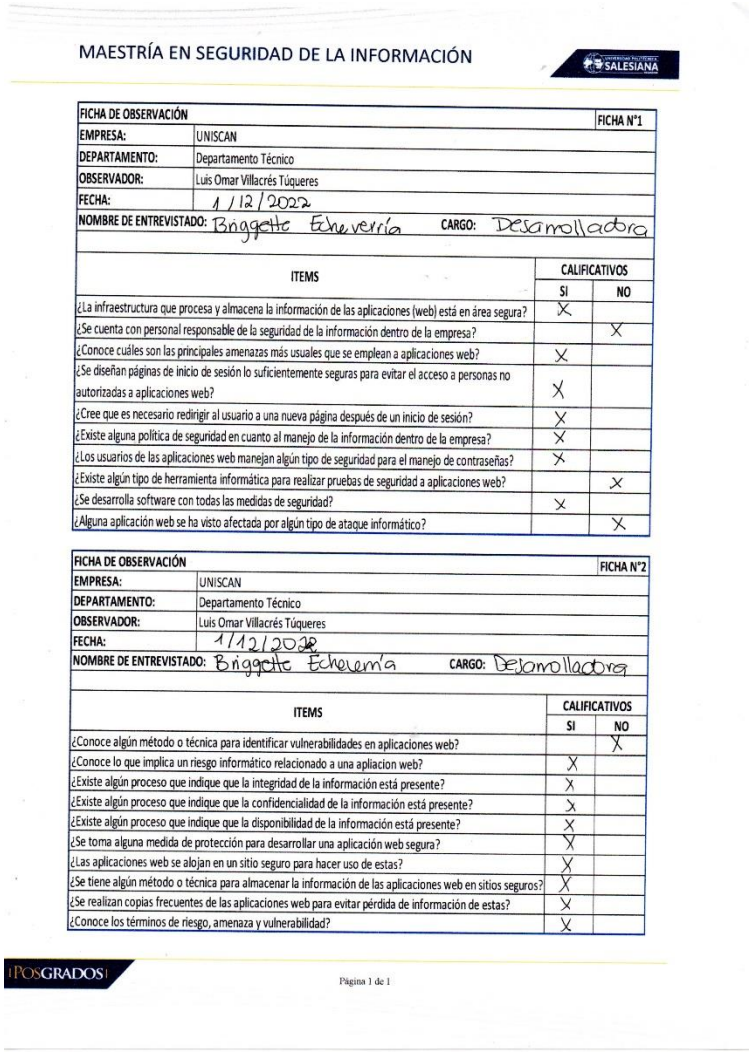
POSGRADOS

Página 1 de 1

Fig. 12 Documento escaneado de la encuesta realizada al Ing. Nicolás Redrobán (Jefe del Dpto. de Desarrollo). Fuente: El autor.

Desarrollo de la entrevista a la Ing. Briggette Echeverría (Desarrolladora y Soporte en el Departamento de Desarrollo de la Empresa Uniscan).

A las 12:00 am del día Jueves 01 de Diciembre de 2022, previa cita agendada con la Ing. Briggette Echeverría, se realiza la siguiente entrevista, podemos ver las respuestas brindadas en la figura 13.



MAESTRÍA EN SEGURIDAD DE LA INFORMACIÓN

FICHA DE OBSERVACIÓN		FICHA N°1
EMPRESA:	UNISCAN	
DEPARTAMENTO:	Departamento Técnico	
OBSERVADOR:	Luis Omar Villacrés Túqueres	
FECHA:	1/12/2022	
NOMBRE DE ENTREVISTADO:	Briggette Echeverría	CARGO: Desarrolladora

ITEMS	CALIFICATIVOS SI	NO
¿La infraestructura que procesa y almacena la información de las aplicaciones (web) está en área segura?	X	
¿Se cuenta con personal responsable de la seguridad de la información dentro de la empresa?		X
¿Conoce cuáles son las principales amenazas más usuales que se emplean a aplicaciones web?	X	
¿Se diseñan páginas de inicio de sesión lo suficientemente seguras para evitar el acceso a personas no autorizadas a aplicaciones web?	X	
¿Cree que es necesario redirigir al usuario a una nueva página después de un inicio de sesión?	X	
¿Existe alguna política de seguridad en cuanto al manejo de la información dentro de la empresa?	X	
¿Los usuarios de las aplicaciones web manejan algún tipo de seguridad para el manejo de contraseñas?	X	
¿Existe algún tipo de herramienta informática para realizar pruebas de seguridad a aplicaciones web?		X
¿Se desarrolla software con todas las medidas de seguridad?	X	
¿Alguna aplicación web se ha visto afectada por algún tipo de ataque informático?		X

FICHA DE OBSERVACIÓN		FICHA N°2
EMPRESA:	UNISCAN	
DEPARTAMENTO:	Departamento Técnico	
OBSERVADOR:	Luis Omar Villacrés Túqueres	
FECHA:	1/12/2022	
NOMBRE DE ENTREVISTADO:	Briggette Echeverría	CARGO: Desarrolladora

ITEMS	CALIFICATIVOS SI	NO
¿Conoce algún método o técnica para identificar vulnerabilidades en aplicaciones web?		X
¿Conoce lo que implica un riesgo informático relacionado a una apliacion web?	X	
¿Existe algún proceso que indique que la integridad de la información está presente?	X	
¿Existe algún proceso que indique que la confidencialidad de la información está presente?	X	
¿Existe algún proceso que indique que la disponibilidad de la información está presente?	X	
¿Se toma alguna medida de protección para desarrollar una aplicación web segura?	X	
¿Las aplicaciones web se alojan en un sitio seguro para hacer uso de estas?	X	
¿Se tiene algún método o técnica para almacenar la información de las aplicaciones web en sitios seguros?	X	
¿Se realizan copias frecuentes de las aplicaciones web para evitar pérdida de información de estas?	X	
¿Conoce los términos de riesgo, amenaza y vulnerabilidad?	X	

POSGRADOS

Página 1 de 1

Fig. 13 Documento escaneado de la encuesta realizada a la Ing. Briggette Echeverría (Desarrolladora). Fuente: El autor.

4.2. Procesamiento y análisis de datos.

Después de recolectar los datos de las entrevistas, se procedió a investigar y analizar las vulnerabilidades de la infraestructura técnica de Uniscan. Para lograr esto, los datos obtenidos de las encuestas se clasificaron y agregaron por separado con el fin de obtener información precisa y manejable. De esta manera, se buscó tener una

comprensión más detallada y completa de la situación y se pudo abordar de manera más efectiva las vulnerabilidades identificadas en la infraestructura técnica de la empresa.

Análisis de la entrevista al Ing. José Luis Trujillo, Gerente Técnico de Uniscan.

Luego de llevar a cabo la entrevista con el Ing. José Luis Trujillo, se concluye que la empresa no presenta problemas de seguridad o confiabilidad de la información, lo que sugiere que no ha habido múltiples intentos de intrusiones por parte de hackers malintencionados. No obstante, se reconoce que se comprenden los riesgos de seguridad de la información, pero se hace énfasis en que podrían ser necesarios recursos adicionales para proteger los activos de información y los datos cruciales de la empresa.

Análisis de la entrevista al Ing. Nicolás Redrobán y a la Ing. Briggette Echeverría quienes conforman el Departamento de Desarrollo de la Empresa Uniscan.

En base a las entrevistas realizadas a los dos miembros del departamento de desarrollo, se ha determinado que la empresa cuenta con procedimientos para la protección de la información, los cuales pueden ser utilizados para salvaguardar los activos de información, pero que carece de una política y una organización específica para abordar cualquier problema que surja.

Además, debido a fallas en la arquitectura tecnológica actual, la organización se encuentra expuesta a posibles problemas causados por ataques. Es importante destacar que aún se necesitan recursos técnicos para apoyar la creación de un programa de seguridad de la información que incluya directrices para mantener los principios fundamentales de: confidencialidad, integridad y disponibilidad. Sin embargo, es importante tener en cuenta que ninguna medida de seguridad puede garantizar que una organización sea completamente inmune a los ataques, sino que simplemente sirve como una defensa.

4.2.1. Procesamiento y análisis de las encuestas.

El proceso de investigación comienza con la identificación de quién es el responsable del manejo de la información de la empresa, lo que permite clarificar cada punto de la investigación. Para facilitar la presentación y análisis de los datos obtenidos, se utilizarán gráficos de barras como la herramienta principal para la organización y visualización de los resultados. La información recopilada se procesará utilizando la aplicación de Microsoft Excel, lo que permitirá una comprensión más clara de los datos y facilitará su interpretación, este proceso de análisis de datos es crucial para identificar patrones y tendencias que puedan ayudar a la empresa a tomar decisiones y mejorar su gestión de la información.

Todo el proceso sigue una serie de sencillos pasos que describen las siguientes opciones mencionadas en el texto:

1. Hay 17 preguntas para el personal del área técnica de Uniscan y 20 preguntas para el personal administrativo.
2. Preparar un gráfico de barras que muestre los porcentajes de puntajes obtenidos para cada pregunta.
3. Analizar e interpretar la información de cada punto.

4.2.2. Análisis e interpretación de resultados de las encuestas.

A continuación, se proporcionarán las fuentes que respaldan los resultados, el análisis y la interpretación de los datos, basados en los instrumentos y herramientas utilizadas para recopilar información previamente mencionadas. Durante todo el proceso, cada pregunta fue presentada al personal técnico y administrativo de Uniscan, se brindó opciones de respuesta múltiple, de las cuales se les pidió seleccionar al menos una respuesta.

4.2.2.1. Análisis de las encuestas al personal técnico de la empresa Uniscan.

El cuestionario para el personal técnico de la organización Uniscan consta de 17 preguntas. El propósito de esta actividad es verificar, respaldar y mantener resultados claros y precisos basados en los datos recopilados, a continuación, en la Tabla VII podemos ver cada una de las preguntas con su respectivo porcentaje en las respuestas entregadas y con un breve análisis del resultado, adicional se puede revisar el Anexo 2 en el que encontraremos la representación gráfica utilizando diagramas de barras de cada una de las preguntas.

TABLA VII. ANÁLISIS DE LA ENCUESTA REALIZADA AL PERSONAL TÉCNICO DE LA EMPRESA UNISCAN.

ANÁLISIS DE LA ENCUESTA REALIZADA AL PERSONAL TÉCNICO DE LA EMPRESA UNISCAN		
Nº. DE PREGUNTA	**CONTENIDO DE LA PREGUNTA**	**ANÁLISIS DE LA PREGUNTA**
1	¿Qué propósito principal tiene la seguridad informática?	El 100% de los colaboradores del área técnica de la empresa detallan que el propósito principal de la seguridad informática es proteger los activos de las organizaciones.
2	¿Cuál cree usted que es el nivel de seguridad que actualmente dispone la empresa Uniscan?	Según las respuestas proporcionadas por los colaboradores, se concluye que, el área técnica califica la seguridad de la información como normal a alta.
3	¿Conoce usted alguna de las metodologías de seguridad informática que se indican a continuación?	El 80% del personal del área técnica de la empresa detallan que no conocen ninguna metodología de seguridad informática, mientras que el restante 20% ha escuchado hablar de la Norma ISO 27001.
4	¿Conoce usted si la empresa cuenta con planes de contingencia, políticas de seguridad, reglamentos u otros documentos que regulen el uso de correo electrónico, gestión de contraseñas, uso del wifi, prevención de riesgos informáticos, entre otros?	Según las respuestas proporcionadas por el personal técnico, se concluye que, hay desconocimiento de que la empresa cuente con planes de seguridad, reglamentos u otros documentos que regulen el uso de correo electrónico, gestión de contraseñas, uso del wifi, prevención de riesgos informáticos, entre otros.
5	¿Qué estándar de seguridad de la información maneja la Empresa Uniscan?	Mediante la encuesta realizada se logró obtener que el 80% del personal de tecnología de la empresa Uniscan no maneja ningún estándar de seguridad de la información.
6	La información confidencial que maneja la empresa Uniscan, ¿para qué tipo de usuario es accesible?	Mediante la encuesta realizada se logró verificar que el 60% de los colaboradores en el área técnica que labora en la empresa considera que el acceso a la información confidencial de la organización debe ser para usuarios privilegiados.
7	¿Conoce usted si la empresa tiene una correcta clasificación de la información producida, recibida y almacenada (confidencial, pública, etc.)?	Según las respuestas proporcionadas por el personal técnico, se concluye que, hay desconocimiento que en la empresa Uniscan se mantenga una correcta clasificación de la información producida.
8	¿De la escala del 1 al 4 como usted calificaría la información de la empresa Uniscan donde 1 es información no relevante (NR) y 4 es información muy relevante (MR)?	El 60% de los usuarios técnicos califican que la información que se maneja en la empresa Uniscan es de importancia Relevante, el restante 40% califica a la información como Muy Relevante.

9	Usted como profesional que labora en el departamento técnico de la organización Uniscan. ¿Conoce usted si han sufrido algún incidente de seguridad que haya ocasionado daños en la infraestructura tecnológica?	Durante la encuesta realizada se obtuvo que el 60% de los usuarios técnicos que laboran en la institución en mención detallan que NO han sufrido incidentes de seguridad que pudieran haber causado pérdidas de información, el 20% indica que SI han sufrido incidentes y el 20% restante no recuerda.
10	¿Qué tipo de restricciones se encuentran implementadas en la red en general o en ciertas partes de la red?	Durante la encuesta realizada se obtuvo que el 40% del personal técnico desconoce si existe restricciones en la red de la empresa y otro 40% indica que las políticas de seguridad de acceso a la red se realizan con un control de autenticación en los sistemas informáticos, y el 20% restante indica que se maneja un servidor PROXY.
11	Las restricciones que maneja usted en el departamento técnico informático dentro de la red de trabajo de la empresa, ¿en qué dispositivo se encuentran configuradas?	Durante la encuesta realizada se obtuvo que el 40% de los usuarios técnicos detallan que las configuraciones de reglas de seguridad se las realizan en cada uno de los dispositivos de red, otro 40% indica que en ninguna de las anteriores y el restante 20% indica que se maneja un servidor de seguridad.
12	¿Usted como profesional de tecnología considera que la inversión en seguridad informática es de gran importancia para proteger los activos de información que son de carácter confidencial?	En la encuesta realizada se obtuvo que el 100% de los usuarios técnicos si consideran que la inversión en seguridad informática es factible para la protección de la información.
13	¿Qué tipos de virus informático o ataques informáticos se deben mitigar para evitar los accesos a la información de carácter confidencial?, se debe considerar que es una pregunta de selección múltiple.	El 80% de los usuarios técnicos mencionan que los troyanos son uno de los virus informáticos que dispersan los atacantes maliciosos para tener el acceso ilícito a los sistemas informáticos de la organización, y en mismo porcentaje consideran al SPAM como fuente de distribución de código malicioso, los gusanos y rasonware son considerados en un 60% como malware utilizado para acceder a información relevante, un 40% del personal técnico considera a los backdoors como peligrosos y el restante 20% identifica a los botnets como virus que puedan afectar a la seguridad de la empresa.
14	¿Con qué frecuencia realiza copias de seguridad de su información y correo electrónico personal?	Según la respuesta obtenida en la encuesta, da como resultado que el 40% del personal nunca respalda su correo, por lo que información de vital importancia para la persona se perdería.
15	¿Con qué frecuencia realiza copias de seguridad de su información y correo electrónico de la empresa?	Según la respuesta obtenida en la encuesta, se tiene como resultado que el 60% del personal técnico nunca respalda el correo institucional, por lo que información de vital importancia para la realización de las actividades dentro de la organización es vulnerable a ser afectada y podría resultar en pérdida de la información, un 20% indica que respalda la información mensualmente y de igual manera otro 20% cuando se acuerda.
16	¿Cree que concientizar sobre la ciberseguridad es una medida básica para laborar en un ciberespacio más seguro?	Las respuestas indican que el 60% de los colaboradores del área técnica consideran que una medida básica para mejorar la seguridad es concientizar sobre la ciberseguridad al personal que labora en la empresa Uniscan, y un 40% manifiesta que es muy importante la concientización en el tema de ciberseguridad.
17	¿A través de qué medio cree que se debería realizar campañas de concienciación sobre temas de ciberseguridad?	Se concluye gracias a las respuestas obtenidas en la encuesta, que el 60% de funcionarios cree que un buen medio de comunicación para realizar campañas de concienciación sobre ciberseguridad es hacerlo utilizando redes sociales, y un 40% cree que es buena idea utilizar el correo electrónico.

Fuente: El autor.

Análisis general de las preguntas evaluadas al personal técnico de la empresa Uniscan.

Tras llevar a cabo una investigación entre los empleados técnicos de Uniscan, se ha obtenido información valiosa que apunta a la necesidad de invertir en soluciones de seguridad de la información. Esta inversión se hace imprescindible debido a la alta probabilidad de que se produzcan filtraciones de datos sensibles en la empresa. Asimismo, se ha detectado una falta de medidas de seguridad adecuadas, ya que no existe una forma de comprobar periódicamente el estado de la red y, por tanto, no se pueden mitigar las amenazas a la confidencialidad, integridad y disponibilidad de la información. Además, se ha evidenciado la inexistencia de normas y políticas de acceso a la infraestructura tecnológica de la empresa, lo que puede suponer un grave riesgo para la seguridad de los activos de información. En resumen, el estudio apunta a la necesidad urgente de implementar medidas de seguridad y establecer políticas claras para proteger la información de la empresa.

4.2.2.2. Análisis de las encuestas al personal administrativo de la Empresa Uniscan.

El cuestionario para el personal administrativo de la organización Uniscan consta de 20 preguntas. El propósito de esta actividad es verificar, respaldar y mantener resultados claros y precisos basados en los datos recopilados, a continuación, en la Tabla VIII podemos ver cada una de las preguntas con su respectivo porcentaje en las respuestas entregadas y con un breve análisis del resultado, adicional se puede revisar el Anexo 3 en el que encontraremos la representación gráfica utilizando diagramas de barras de cada una de las preguntas.

TABLA VIII. ANÁLISIS DE LA ENCUESTA REALIZADA AL PERSONAL ADMINISTRATIVO DE LA EMPRESA UNISCAN.

ANÁLISIS DE LA ENCUESTA REALIZADA AL PERSONAL ADMINISTRATIVO DE LA EMPRESA UNISCAN		
Nº. DE PREGUNTA	**CONTENIDO DE LA PREGUNTA**	**ANÁLISIS DE LA PREGUNTA**
1	¿Qué propósito principal tiene la seguridad informática?	El 69.2% de los empleados de la empresa Uniscan detallan que el propósito principal de la seguridad informática es proteger los activos de la organización, un 15.4% indica que es proteger la información de índole personal y en igual porcentaje de 15.4% manifiesta que el propósito de la seguridad informática es ninguna de las anteriores.

2	¿Qué tan segura considera usted la red informática de la empresa que se encuentra laborando?	El 61.5% de los usuarios que laboran en la empresa Uniscan se encuentran muy seguros sobre la seguridad de la red, un 30.8% considera que la red informática es poco segura y un 7.7% manifiesta que es totalmente insegura.
3	¿Ha compartido usted datos de la red con personas ajenas a la empresa?	El 69.2% de los usuarios encuestados que laboran en la empresa Uniscan indican no haber compartido información con terceros, un 23.1% manifiesta que ha compartido datos de la red varias veces y 7.7% indica que no recuerda, como resultado no se ha protegido la red de posibles intrusos y tampoco se ha evitado los riesgos que esta acción puede acarrear.
4	Dentro de la red informática de la empresa. ¿Ha sido usted víctima de ataques informáticos?	El 38.5% del personal administrativo de la organización indica que No, en igual porcentaje del 38.5% manifiesta que No recuerda, mientras que el 23% de los usuarios encuestados que laboran en la empresa Uniscan han sido víctimas de ataques informáticos ejecutados por los piratas cibernéticos.
5	¿Qué datos sensibles almacenados en la empresa es considerada como información?	El 76.9% de los usuarios encuestados que laboran en la empresa Uniscan consideran como datos sensibles toda información que puede causar pérdidas financieras y que paralice los servicios que brinda la organización, 7.7% considera como datos sensibles todas las anteriores y el 15.4% restante ninguna de las anteriores.
6	¿Considera usted que la información es un valor de gran importancia para la empresa y que solamente personal honesto y autorizado puede tener acceso a ella?	El 92.3% de los usuarios encuestados que laboran en la empresa Uniscan considera que el acceso a la información de carácter confidencial solo debe ser para el personal honesto y autorizado a ella, y un 7.7% considera que tal vez.
7	¿Usted cree importante que las empresas inviertan en seguridad informática?	En la encuesta realizada se obtuvo que el 76.9% de los usuarios administrativos consideran muy importante la inversión en seguridad informática para la protección de la información, mientras que el 23.1% solo considera que es importante la inversión.
8	¿Usted cree que la información debe ser de carácter confidencial?	El 76.9% de los usuarios encuestados que laboran en la empresa Uniscan cree que la información que maneja la organización debería ser tratada de manera confidencial, un 15.4% manifiesta que quizás y el restante 7.7% indica que No debería ser tratada de manera confidencial.
9	¿Qué objetivo cree usted que poseen las organizaciones en proteger su información de carácter confidencial?	El 69.2% de los usuarios encuestados de la empresa Uniscan detallan que los objetivos principales de la organización en cuanto a proteger su información de manera confidencial son: evitar pérdidas económicas y tener el control de los activos para evitar que terceros tengan acceso a esta, un 23.1% indica que el propósito es solo evitar pérdidas económicas y el restante 7.7% manifiesta que el objetivo es solo evitar el acceso a terceros.
10	¿Cree usted que los usuarios deben de tener privilegios en el sistema informático de acuerdo a las funciones que desempeñan en la organización?	El 92.3% de los encuestado de la empresa Uniscan detallan que los usuarios Si deben tener privilegios en los sistemas informáticos de acuerdo a las funciones que ejercen, mientras que el restante 7.7% manifiesta que No.
11	¿Conoce usted si la empresa cuenta con personal especializado en seguridad informática o un equipo de respuesta a incidentes de seguridad informática?	El 46.2% de los encuestados de la empresa Uniscan indican que desconocen si la organización cuenta con personal especializado en el área de seguridad informática, un 30.8% manifiesta que la empresa No cuenta con un equipo especializado y el 23 % indica que la organización Si cuenta con personal especializado en el campo de seguridad informática.
12	¿Cuál cree usted que es el nivel de seguridad que	Según las respuestas proporcionadas por los usuarios administrativos, se concluye que, al interior de la empresa Uniscan, el nivel de seguridad de

	actualmente dispone la empresa?	la información es Normal para un 38.5% de los encuestados, mientras que para un 15.4% de las personas el nivel de seguridad en la empresa es Muy Bajo.
13	¿Con que periodo la organización realiza capacitaciones a los funcionarios sobre temas de ciberseguridad?	Según las respuestas proporcionadas, se concluye que las capacitaciones sobre temas de ciberseguridad no se han desarrollado, o tal vez se ha hablado del tema muy poco, el 38.5% de los encuestados manifiestan que Nunca se ha tratado el tema, un 30.8% indica que se habla de ciberseguridad Anualmente, mientras que un porcentaje igual del 15.4% manifiestan que se trata el tema de manera Semestral y Mensual respectivamente.
14	¿Las contraseñas que usted usa tienen una longitud normalmente de?	Según las respuestas proporcionadas por los usuarios administrativos, se concluye que la longitud de las contraseñas usadas va desde: entre 1 a 5 caracteres para el 7.7% de los encuestados, de 5 a 10 caracteres para el 53.8%, y entre 10 a 15 caracteres para el 38.5% de los colaboradores de la organización.
15	¿Las contraseñas que usted implementa por lo general están compuestas de?	Según las respuestas proporcionadas por los usuarios de la empresa Uniscan, se concluye que, las contraseñas en su mayoría de alrededor del 53.8% están compuestas por la mezcla de números, letras y símbolos.
16	¿Con que frecuencia cambia sus contraseñas?	Según la respuesta obtenida el 46.2% que casi llega a la mitad de los usuarios encuestados, actualiza su contraseña solo si el propio sistema lo considera necesario, lo que involucra una alerta de seguridad.
17	¿Dónde almacena las contraseñas que utiliza?	En esta pregunta los usuarios han seleccionado más de una opción, por lo que los resultados, se han clasificado de la siguiente manera, el 46.2 % indica que memoriza las contraseñas, el 30.8% detalla que almacena sus contraseñas en un cuaderno, un 7.7% escribe su contraseña en un papel y lo pega cerca del computador, mientras que en igual porcentaje de 7.7% guarda sus contraseñas en un archivo dentro del disco duro o utilizan un gestor de contraseñas.
18	¿Del siguiente listado seleccione que tecnologías utiliza para desarrollar las labores de la empresa? (puede escoger varias opciones).	En esta pregunta los usuarios tenían la opción de seleccionar más de una respuesta, por lo que se obtiene como resultados que: la tecnología que más usan para desarrollar sus labores dentro de la empresa es el correo institucional, para lo cual utilizan los computadores que la organización les proporciona, también se concluye que la página Web de la empresa es la segunda aplicación de importancia significativa para los colaboradores.
19	¿Ha sufrido accesos ilícitos en cuanto a su información por medio de correo electrónico?	El 69.2% de los encuestados de la empresa Uniscan detallan que No han sufrido algún tipo de acceso ilícito a su información por medio de correo electrónico, y el 30.8% indican que Si han sufrido de algún tipo de penetración maliciosa por medio del correo electrónico.
20	¿Conoce sobre algún sistema de protección contra ciberataques para computador o dispositivo móvil?	El 46.2% de los encuestados de la empresa Uniscan coloca al Antivirus como el principal software de protección de la información contra ciberataques, seguido por el software Antimalware con el 23%, a continuación, con el 15.4% encontramos al Antispam y otro 15.4% de encuestados indican que ninguno.

Fuente: El autor.

Análisis general de las preguntas evaluadas al personal administrativo de la empresa Uniscan.

Después de llevar a cabo una encuesta entre el personal administrativo de Uniscan, se obtuvieron los siguientes resultados: la mayoría de los empleados de la organización no confían en usuarios desconocidos y son conscientes de las posibles consecuencias de proporcionar información crítica a terceros, por lo que prefieren no hacerlo. Sin

embargo, los colaboradores de la empresa no cuentan con medidas de seguridad que los protejan de ser objetivo de ciberataques por parte de atacantes malintencionados que buscan robar activos para su propio beneficio. Por otro lado, los colaboradores piensan que es necesario que la empresa implemente medidas de defensa para prevenir tanto el fraude interno como externo, ya que este último puede involucrar a personas que no tienen ninguna relación con la organización, también la implementación de medidas garantizaría la protección de los datos sensibles.

Los empleados tienen acceso a las instalaciones de acuerdo con su grado de responsabilidad en el tratamiento de los datos, también se pudo determinar que los colaboradores no reciben una formación en seguridad de la información que se adapte a sus cargos y funciones dentro de la empresa.

La mayoría de los encuestados piensa que la cultura institucional de la organización es crucial en el procesamiento de la información y que la seguridad debería ser una norma. Además, los encuestados destacaron la importancia de invertir en medidas de seguridad informática, ya que las redes empresariales que manejan datos sensibles son vulnerables tanto a peligros internos como externos.

Los especialistas en seguridad de la información son de gran importancia para evitar que personas malintencionadas puedan obtener datos que comprometan el rendimiento de la red y las conexiones de los sistemas informáticos de la organización, reduciendo la disponibilidad de los activos. En este sentido, es importante señalar que los ataques no autorizados a las comunicaciones corporativas son una realidad y que los piratas informáticos utilizan engaños para obtener información confidencial.

4.3. Aplicación de la metodología MAGERIT.

El enfoque MAGERIT se empleó como estrategia de procedimiento para identificar y gestionar los riesgos, vulnerabilidades y amenazas que pueden afectar los activos de información de la empresa. La implementación efectiva del proyecto y la protección de

los activos de información son los objetivos principales que se buscan con la utilización de este enfoque. En otras palabras, MAGERIT se ha utilizado para asegurar que se puedan identificar y abordar los riesgos relacionados con los activos de información de la empresa de manera efectiva y además que se puedan establecer salvaguardas para protegerlos [24].

Las siguientes fases han sido acomodadas por una colección de tareas:

- **Fase 1:** consiste en enumerar los activos de información de la empresa Uniscan.

  Actividad 1. En esta fase identificaremos y clasificaremos los activos de información en función de sus características.

- **Fase 2:** consiste en identificar los riesgos, debilidades y amenazas que puedan afectar a los activos de información.

  Actividad 2. En esta fase identificaremos las vulnerabilidades, amenazas y los riesgos, hay que descubrir y evaluar las vulnerabilidades, amenazas y riesgos de cada activo de información mediante la metodología MAGERIT.

- **Fase 3:** consiste en crear un plan de acción para abordar los riesgos y vulnerabilidades identificados en los activos de información.

  Actividad 3. Creación del Plan de tratamiento de riesgos: en esta fase se desarrollará una estrategia de gestión de riesgos basada en los puntos débiles de cada activo de información, se tendrá como propósito la creación de las protecciones y controles necesarios para reducir y gestionar los riesgos. Todo esto se llevará a cabo utilizando la metodología MAGERIT, de forma secuencial y de acuerdo a los objetivos establecidos, en el caso de ser necesario se establecerán los controles para salvaguardar los activos de información de la organización Uniscan.

Los beneficios de emplear el enfoque MAGERIT son diversos y se listan a continuación [12]:

- Análisis exhaustivo de riesgos y cobertura de la gestión.
- Llevar un registro adecuado de fuentes, amenazas y categorías de activos.
- Realización de un exhaustivo análisis de riesgos cuantitativo y cualitativo.
- Gratuito, sin necesidad de licencia.
- Divide los activos para que todos puedan obtener evaluaciones de riesgos oportunas.
- Incluye una base documental compuesta por tres módulos consultables.

El objetivo final del proyecto es realizar un inventario de activos y análisis de riesgos para identificar amenazas o vulnerabilidades que puedan afectar a los activos de información de la empresa Uniscan y tomar medidas de seguridad para protegerlos.

Para lograr esto, se utilizará el libro MAGERIT 2012_Magerit_v3_libro2_catalogo-de-elementos_es_NIPO_630-12-171-8, que describe las propiedades de los activos, en la figura 14 podemos observar de manera resumida los pasos necesarios para llevar a cabo la ejecución de la metodología MAGERIT.

Fig. 14 Pasos para la aplicación de la metodología MAGERIT [12].

4.3.1. Alcance del análisis utilizando la metodología MAGERIT.

La metodología MAGERIT se utiliza para proyectos de análisis de vulnerabilidades en la infraestructura tecnológica de una organización, podemos indicar que el proceso

comienza con la identificación de los riesgos potenciales que pueden afectar a los recursos de información y a la infraestructura tecnológica. A continuación, se establece una estrategia de gestión de riesgos para aplicar medidas de seguridad y reducir las vulnerabilidades y amenazas que puedan afectar a los activos de la organización.

La aplicación de controles de seguridad en los procesos de la organización es fundamental para garantizar la protección de la información, los dispositivos, los servicios y el software utilizados. Además, estos controles también deben facilitar la continuidad del negocio en caso de producirse algún incidente.

La metodología MAGERIT es una herramienta muy útil para llevar a cabo una evaluación exhaustiva de los riesgos y establecer una estrategia de gestión de riesgos efectiva, esto permitirá a la organización identificar y abordar las vulnerabilidades y amenazas que puedan afectar a sus activos, y garantizar la protección de la información y la continuidad del negocio en todo momento.

4.3.1.1. Recursos necesarios para el desarrollo.

Los recursos necesarios para desarrollar un análisis de vulnerabilidades de la infraestructura tecnológica de Uniscan se describen a continuación.

- **Recursos humanos:** debido a que pueden ser el eslabón más crucial de la cadena encargada de salvaguardar la información en una organización, los recursos humanos son un componente crucial de la investigación del análisis de vulnerabilidades de la infraestructura tecnológica. Por lo tanto, es importante que el personal reciba formación y certificación en seguridad de la información, también es fundamental que los funcionarios de varios departamentos sirvan como recursos humanos importantes en términos de concienciación, trabajando junto con el departamento técnico y de desarrollo para reducir los riesgos y salvaguardar los datos de la empresa y de sus clientes.

- **Recursos físicos:** los recursos físicos son uno de los elementos que se debe proteger, por lo que se puede analizar mejor la situación de seguridad teniendo en cuenta su

disponibilidad en el proceso productivo que lleva a cabo junto con el recurso humano, es decir, es importante motivar a los empleados a: cuidar, mantener y proteger la parte tangible, por lo que es fundamental mantener un inventario actualizado por parte del área encargada, en la Tabla IX se realiza una descripción breve de los recursos físicos con los que cuenta la organización Uniscan.

TABLA IX. RECURSOS FÍSICOS.

RECURSO FÍSICO	DESCRIPCIÓN
Equipos de Computo	18 equipos de cómputo portátiles y 3 equipos de cómputo de escritorio.
Funcionarios	Gerencia general, el área administrativa se divide en: departamento de contabilidad con 6 personas, departamento comercial con 5 personas, departamento de ventas con 3 personas y el departamento de logística con 4 personas.
Personal técnico	El área técnica está conformada por: el departamento de desarrollo con 2 personas y el departamento técnico con 4 personas.
Equipos de Red	Servidor, router, switch.

Fuente: El autor.

- **Recursos técnicos:** para la organización Uniscan se debe especificar qué opciones técnicas se han elegido y cómo estás permitirán crear la estrategia de gestión de riesgos. A la hora de plantear una estrategia de gestión de riesgos, hay que tener en cuenta la incorporación de avances técnicos de vanguardia que no siempre proporcionan una seguridad total y si suponen una amenaza para los avances existentes utilizados en diversas partes de la empresa, en la Tabla X se realiza una descripción resumida de la infraestructura técnica con la que en este momento cuenta la empresa Uniscan, esto nos permite tener un panorama más claro del caso en estudio.

TABLA X. RECURSOS TÉCNICOS.

RECURSOS TÉCNICOS	DESCRIPCIÓN
Equipos de Cómputo	18 equipos de cómputo portátiles y 3 equipos de cómputo de escritorio.
Equipos de Red	Servidor, router, switch, firewall, elementos que permitirán mejorar la calidad de seguridad de la información.
Energía Eléctrica-UPS de respaldo	Instalación monofásica regulada con UPS de respaldo.
Protección contra incendios	Equipamiento contra incendios adecuado que responda a las necesidades de respuesta ante una emergencia propiciada por fuego.

Controles de acceso físicos	Controles de acceso a las instalaciones: entrada principal, departamento de contabilidad y el rack.
Licencias de Sistemas Operativos	Verificación de la originalidad de las licencias de los sistemas operativos instalados en el servidor y los 21 equipos de cómputo.
Licencias de Antivirus de alto nivel de seguridad	Verificación de la originalidad de las licencias de antivirus instalados en el servidor y los 21 equipos de cómputo y su pertinencia de respuesta a una posible infección.

Fuente: El autor.

4.4. Identificación e inventario de activos de la información.

La contabilidad de los activos de la empresa Uniscan se basa en todos los elementos (hardware, software, recursos humanos, etc.) con los que la agencia procesa la información.

Para llevar a cabo el proceso de inventario de activos, se inició con una revisión exhaustiva del inventario suministrado por el departamento de desarrollo. Durante la revisión, se identificó la presencia de cada equipo y se observó que algunos equipos que eran importantes, habían sido eliminados de la lista de activos, mientras que otros equipos que no eran importantes seguían formando parte de la lista de la infraestructura principal tecnológica de la empresa. Es importante destacar que la revisión del inventario se realizó en estrecha colaboración con el departamento de desarrollo de la empresa para garantizar la precisión y la actualización del inventario.

Una de las actividades más importantes de realizar, es la identificación de cómo se encuentra estructurada la red de la organización, hasta este momento no se contaba con un mapa de red para facilitar la identificación estructural de la misma, después de un proceso de búsqueda y observación se pudo realizar la construcción de un aproximado de la infraestructura de la red de comunicaciones dentro de la empresa, la red la podemos observar en la figura 15.

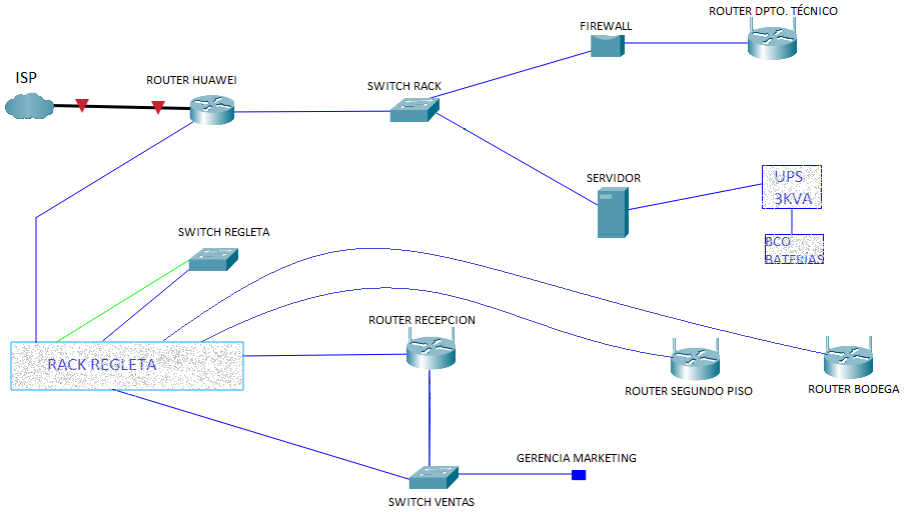


Fig. 15 Diagrama de red de la organización Uniscan.
Fuente: El autor.

En la siguiente Tabla XI se muestra el inventario de activos de red y comunicación de la empresa Uniscan, la cual se ha generado mediante una revisión exhaustiva del inventario proporcionado por el departamento de desarrollo. En ella se detallan los equipos y dispositivos de hardware que forman parte de la infraestructura tecnológica de la organización, así como su ubicación, marca, modelo y serie. Este inventario de activos es una herramienta fundamental para el análisis de vulnerabilidades y la aplicación de medidas de seguridad necesarias para mitigar los riesgos y amenazas que puedan afectar a los activos de información de la empresa.

TABLA XI. INVENTARIO DE ACTIVOS DE RED Y COMUNICACIÓN DE LA EMPRESA UNISCAN.

ROUTERS

MARCA	MODELO	SERIE	DIRECCION MAC	UBICACIÓN
LINKSYS	WRT32X	22C11601900787	24F5A2C2D868	DPTO. TÉCNICO
LINKSYS	WRT1900 AC			RECEPCIÓN PRINCIPAL
LINKSYS	WRT32X	22C10609707674	6038E0C5D438	RECEPCIÓN GERENCIA/SEGUNDO PISO
D-LINK	DIR-615	QX4H1GC003096	1062EB878C21	BODEGA
HUAWEI	EchoLife HG8045H	48575443CF193866	900325CF1938-41 (10)	RACK

SWITCH

MARCA	MODELO	UBICACIÓN
D-Link	DGS-1016D	RACK/REGLETA
D-Link	DGS-1016D	RACK

FIREWALL

MARCA	MODELO	SERIE
SOPHOS	XG210	C23076KHX79M474

CENTRAL TELEFONICA

MARCA	MODELO	SERIE
Panasonic	KX-TA308BX	3HASQ074921

UPS

MARCA	MODELO	SERIE	CAPACIDAD
CDP	UPO11-3	879071000475	3000VA/2700W

Fuente: El autor.

Una vez examinada detalladamente la información de los equipos en cada una de las áreas de la organización, se presenta a continuación en la Tabla XII un inventario de activos clasificados según sus características.

TABLA XII. INVENTARIO DE ACTIVOS DE ACUERDO A SUS CARACTERÍSTICAS.

CLASIFICACIÓN DE ACTIVOS	DESCRIPCIÓN
Activos de Información	• Bases de datos de clientes. • Bases de datos financiera de la aplicación CADILLAC, facturación y contable. • Bases de datos y documentos administrativos, documentación de inventarios.
Software o aplicación	• Windows 10 Home Single Language. • Windows 10 Home. • Windows 10 Profesional. • Windows 11 Home Single Language. • Licencia asociada a cada equipo de cómputo, 21 en total. • Windows Server 2016 Standard. • Google Chrome. • Mozilla Firefox. • No se cuenta con licencias de Office en ninguna de las versiones. • Aplicación CADILLAC que permite la facturación electrónica, también cuenta con varios módulos entre ellos: financiero, contabilidad e inventario.
Hardware	• 18 computadores portátiles. • 3 computadores de escritorio. • 1 servidor local.
Red	• 5 router. • 3 switch. • 1 firewall.
Equipamiento Auxiliar	• 1 UPS. • Cableado estructurado.

	• Instalaciones eléctricas monofásicas no reguladas.
Servicios	• Conectividad a internet de 100 Mb.
Personal	• Un Ingeniero en Sistemas (Jefe del Departamento de Desarrollo, gestor de infraestructura tecnológica). • Un Ingeniero en Sistemas (apoyo a gestión de infraestructura tecnológica, coordinador del Departamento de Desarrollo). • 25 usuarios finales.

Fuente: El autor.

La clasificación previa de los activos según sus características y vulnerabilidad nos facilitará el proceso de evaluación de activos, basado en la metodología de MAGERIT. Además, nos permitirá identificar áreas y controles que requieren mayor atención y análisis para desarrollar un plan de tratamiento de riesgos efectivo, con el objetivo de minimizar su impacto.

Este proceso de evaluación permitirá identificar medidas de seguridad necesarias para proteger los activos de la organización y garantizar su disponibilidad, integridad y confidencialidad, todo esto alineado con los objetivos del enfoque MAGERIT.

4.4.1. FASE 1: IDENTIFICACIÓN Y CLASIFICACIÓN DE ACTIVOS DENTRO DE LA ORGANIZACIÓN UNISCAN.

Para seguir la metodología MAGERIT en su proceso de gestión de riesgos, primero se debe identificar sus activos. A continuación, se evalúan los activos para identificar los riesgos y las amenazas asociadas, debemos tomar en cuenta que los recursos de información son todos los elementos que utiliza una organización para preparar, editar, transmitir y eliminar información.

MAGERIT los clasifica según características específicas, similitudes o usos básicos, esto le permite diseñar mejor el plan de tratamientos para reducir el riesgo y hacer que su infraestructura tecnológica sea más segura [24].

Se presenta en la Tabla XIII la clasificación de los activos de la empresa de acuerdo con los términos de la metodología MAGERIT. Es importante validar la información de los activos antes de clasificarlos según las definiciones establecidas por MAGERIT.

TABLA XIII. IDENTIFICACIÓN DE LOS TIPOS DE ACTIVOS DE INFORMACIÓN.

TIPO	CODIGO	DESCRIPCION
[D] Datos/Información	D-1	Ficheros
	D-2	Copias de Respaldo
	D-3	Credenciales
	D-4	Código fuente
[S] Servicios	S-1	Interno (a usuarios de la propia organización)
	S-2	World wide web
	S-3	Acceso remoto a cuenta local
	S-4	Gestión de Privilegios
[SW] Software-Aplicaciones Informáticas	SW-1	Desarrollo propio
	SW-2	Desarrollo a medida
	SW-3	Servidor de correo electrónico
	SW-4	Sistema de gestión de Base de Datos
[HW] Equipamiento Informático	HW-1	Grandes equipos
	HW-2	Informática personal
	HW-3	Medios de Impresión
	HW-4	Centralita telefónica
[COM] Redes de Comunicaciones	COM-1	Red Telefónica
	COM-2	Red Inalámbrica
	COM-3	Red Local
	COM-4	Internet
[Media] Soportes de Información	Media-1	Discos
	Media-2	Almacenamiento en Red
	Media-3	Memorias USB
	Media-4	Material Impreso
[AUX] Equipamiento Auxiliar	AUX-1	Sistemas de Alimentación Ininterrumpida
	AUX-2	Cableado
	AUX-3	Cable Eléctrico
	AUX-4	Equipos de Destrucción de Soportes de Información
[L] Instalaciones	L-1	Edificio
	L-2	Cuarto
	L-3	Car
	L-4	Instalaciones de Respaldo
[P] Personal	P-1	Usuarios Externos
	P-2	Administradores de Sistemas
	P-3	Desarrolladores/Programadores
	P-4	Proveedores

Fuente: El autor.

Para llevar a cabo este análisis, es necesario trabajar en conjunto con los encargados de administrar los activos de información y comunicaciones en la empresa. De esta forma,

se garantiza la exactitud de la información y se logra una clasificación adecuada de los activos para poder proceder con la aplicación de medidas de seguridad y la gestión de riesgos.

4.4.1.1. Valoración de los activos.

En el proceso de evaluación de MAGERIT existen dos escalas de evaluación, las cuales tienen en cuenta tanto formas cuantitativas como cualitativas, en el marco de la escala cuantitativa se determina la medida numérica de la evaluación del riesgo, mientras que la escala cualitativa se divide en:

- Muy Alto (MA).
- Alto (A).
- Medio (M).
- Bajo (B).
- Muy Bajo (MB).

Para la evaluación de los activos de información pertenecientes a la organización Uniscan mediante la metodología MAGERIT, es esencial tener en cuenta la siguiente información acerca de la valoración de los activos, como se muestra en la Tabla XIV.

TABLA XIV. VALORACIÓN DE LOS ACTIVOS DE INFORMACIÓN.

Nivel	Abreviatura	Valor
Muy alto	MA	$ 300,000.00
Alto	A	$ 100,000.00
Medio	M	$ 20,000.00
Bajo	B	$ 2,000.00
Muy bajo	MB	$ 200.00

Fuente: El autor.

La evaluación de los activos de información en una organización según la metodología MAGERIT se fundamenta en los siguientes aspectos clave: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad. Cada uno de estos aspectos debe ser

cuidadosamente considerado y evaluado para garantizar la seguridad y protección adecuada de los activos de información de la organización [12].

Un activo puede ser evaluado a lo largo de las siguientes dimensiones:

• **Confidencialidad:** ¿Qué daño haría que conozca una información alguien que no debiera? Esta calificación debe aplicarse a los datos de la empresa Uniscan y ser válida.

• **Integridad:** ¿Cuál es el peligro si la información se daña o corrompe? Esta calificación se refiere a datos que pueden ser manipulados, falsificados total o parcialmente, e incluso la posible pérdida de datos de la empresa o del usuario.

• **Disponibilidad:** ¿Cuál es el daño si no se puede usar la información? Esta calificación se aplica a varios servicios de la empresa Uniscan.

• **Autenticidad:** Los activos de información en el dominio de la empresa son creados, editados por colaboradores en estas oficinas, solo puede solicitar a la gerencia que los revise o manipule, los colaboradores siempre acudirán al departamento técnico o departamento de desarrollo en caso de presentarse una novedad durante sus labores.

• **Trazabilidad:** ¿Qué daño hay en no saber a quién se prestan dichos servicios? En otras palabras, ¿quién hace qué y cuándo? Esto está directamente relacionado con el acceso a los datos, por lo que surge otra pregunta para las empresas: ¿cuál es el daño de no saber quién ha accedido a los datos y qué ha hecho con ellos?

Es importante destacar que, en el contexto de este proyecto de estudio, la evaluación de riesgos de los activos de información se enfoca exclusivamente en las dimensiones de confidencialidad, integridad y disponibilidad. Otras dimensiones como la autenticidad y trazabilidad no son consideradas en esta evaluación.

A continuación, se ha agrupado en la Tabla XV los activos por tipo, teniendo en cuenta sus respectivas valoraciones cuantitativas y cualitativas

TABLA XV. VALORACIÓN DE LOS ACTIVOS DE INFORMACIÓN.

Nº	Código	Descripción	Valoración cuantitativa	Valoración cualitativa
[D] Datos/Información				
1	D-1	Ficheros	$ 20,000.00	M
2	D-2	Copias de Respaldo	$ 100,000.00	A
3	D-3	Credenciales	$ 300,000.00	MA
4	D-4	Código fuente	$ 300,000.00	MA
[S] Servicios				
5	S-1	Interno (a usuarios de la propia organización)	$ 20,000.00	M
6	S-2	World wide web	$ 100,000.00	A
7	S-3	Acceso remoto a cuenta local	$ 100,000.00	A
8	S-4	Gestión de Privilegios	$ 100,000.00	A
[SW] Software-Aplicaciones Informáticas				
9	SW-1	Desarrollo propio	$ 20,000.00	M
10	SW-2	Desarrollo a medida	$ 100,000.00	A
11	SW-3	Servidor de correo electrónico	$ 20,000.00	M
12	SW-4	Sistema de gestión de Base de Datos	$ 20,000.00	M
[HW] Equipamiento Informático				
13	HW-1	Grandes equipos	$ 100,000.00	A
14	HW-2	Informática personal	$ 20,000.00	M
15	HW-3	Medios de Impresión	$ 200.00	MB
16	HW-4	Centralita telefónica	$ 2,000.00	B
[COM] Redes de Comunicaciones				
17	COM-1	Red Telefónica	$ 2,000.00	B
18	COM-2	Red Inalámbrica	$ 20,000.00	M
19	COM-3	Red Local	$ 20,000.00	M
20	COM-4	Internet	$ 100,000.00	A
[Media] Soportes de Información				
21	Media-1	Discos	$ 20,000.00	M
22	Media-2	Almacenamiento en Red	$ 100,000.00	A

23	Media-3	Memorias USB	$ 2,000.00	B
24	Media-4	Material Impreso	$ 2,000.00	B
[AUX] Equipamiento Auxiliar				
25	AUX-1	Sistemas de Alimentación Ininterrumpida	$ 100,000.00	A
26	AUX-2	Cableado	$ 20,000.00	M
27	AUX-3	Cable Eléctrico	$ 20,000.00	M
28	AUX-4	Equipos de Destrucción de Soportes de Información	$ 2,000.00	B
[L] Instalaciones				
29	L-1	Edificio	$ 100,000.00	A
30	L-2	Cuarto	$ 2,000.00	B
31	L-3	Car	$ 2,000.00	B
32	L-4	Instalaciones de Respaldo	$ 200.00	MB
[P] Personal				
33	P-1	Usuarios Externos	$ 300,000.00	MA
34	P-2	Administradores de Sistemas	$ 100,000.00	A
35	P-3	Desarrolladores/Programadores	$ 20,000.00	M
36	P-4	Proveedores	$ 2,000.00	B

Fuente: El autor.

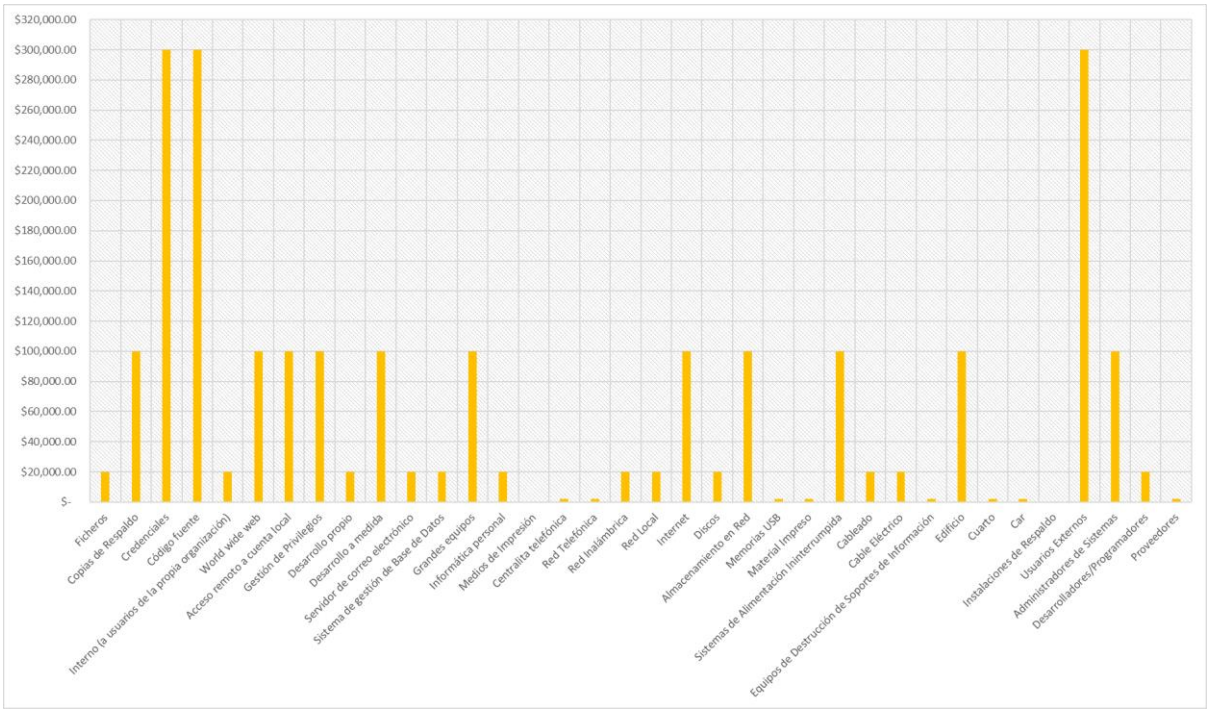


Fig. 16 Representación gráfica de la valoración de activos de la información.
Fuente: El autor.

Podemos describir brevemente la evaluación de los activos utilizando la Tabla XV y figura 16 ubicada en la parte superior: 3 de los activos, equivalentes al 8%, se han valorado como nivel Muy Alto, mientras que 11 activos, que representan el 30%, se han clasificado como nivel de valor Alto, 12 activos, lo que equivale al 33%, se han valorado como nivel Medio, mientras que 8 activos, que representan el 22%, se han clasificado como nivel Bajo y 2 activos, correspondientes al 5%, se han valorado como nivel Muy Bajo. Es recomendable que se revise el archivo de Excel incluido en el Anexo 11 del presente proyecto, específicamente en la hoja "JUSTIFICACIÓN", donde se puede encontrar información sobre por qué se asignó a cada activo un valor y cómo se agruparon. Cabe mencionar que este caso de estudio solo considera las dimensiones de confidencialidad, integridad y disponibilidad en la evaluación de riesgos de cada uno de los activos de información.

4.4.2. FASE 2: Identificar riesgos, vulnerabilidades y amenazas en los activos de información de la empresa Uniscan.

El uso de tecnologías en la gestión de información y comunicación se ha vuelto esencial en la estructura organizacional de la empresa Uniscan, especialmente porque se dedica a la distribución mayorista de equipos tecnológicos. Estas herramientas tecnológicas han mejorado significativamente los procesos administrativos y operativos, en especial en relación a la normativa de facturación electrónica implementada por el Servicio de Rentas Internas. Esto ha permitido una mayor eficiencia en las operaciones administrativas, la toma de decisiones, el procesamiento de datos y el análisis de información.

Es importante indicar que dentro de la organización se presentan varios procesos que se lleva a cabo en cada uno de los departamentos, a continuación, indicaremos uno de ellos a manera de ejemplo, este proceso que señalaremos es el de facturación, podemos

revisar la figura 17, ya que es uno de los más importantes por ser principalmente la razón de ser de la empresa Uniscan.

Para empezar con el estudio del caso, en primer lugar, tendremos que realizar una descripción del proceso en la actualidad, a continuación, se presenta paso por paso el proceso de facturación en la empresa Uniscan.

Se realizará una descripción del proceso de facturación de la empresa Uniscan en la actualidad:

1.- El cliente llama o envía mail solicitando una cotización de algún producto o servicio, el cliente es atendido por el Asesor de Ventas.

2.- El asesor realiza la consulta del stock en el sistema CADILLAC (sistema contable y de control de inventario) para poder indicar la existencia en inventario del artículo que requiere el cliente.

3.- El Asesor de Venta genera la nota de pedido, la cual se debe enviar al Departamento de Cobranzas para que pueda ser facturada.

4.- Se utiliza el correo institucional para enviar la nota de pedido, vía mail llega al Dpto. de Cobranzas para realizar la facturación (se consulta la base de datos para verificar la información del cliente y evitar errores en los campos de datos de la factura).

5.- Se utiliza el sistema CADILLAC para la generación de la factura.

6.- Una vez generada la factura, se registra en el sistema contable para proceder con el cobro.

7.- Se genera la factura, pero la misma aún no se encuentra autorizada por el SRI, hasta este momento todavía no le llega el archivo XML y PDF al cliente.

8.- Una vez autorizada la factura en el sistema contable, automáticamente se envía los documentos digitales de la factura al correo registrado del cliente.

9.- Existen varios métodos de pago que el cliente puede utilizar, estos pueden ser: efectivo, tarjeta de débito, tarjeta de crédito y transferencia bancaria, en este último método se solicita al cliente que envíe el comprobante de la transferencia el cual se toma un tiempo para la comprobación, una vez comprobado el depósito se procede a indicar que la factura está cancelada.

10.- Se imprimen 2 copias de la factura (una para el cobro y otra para el despacho en la bodega de la empresa).

11.- El cliente llega y cancela, con la factura firmada por el Dpto. Cobranzas puede retirar en bodega su pedido.

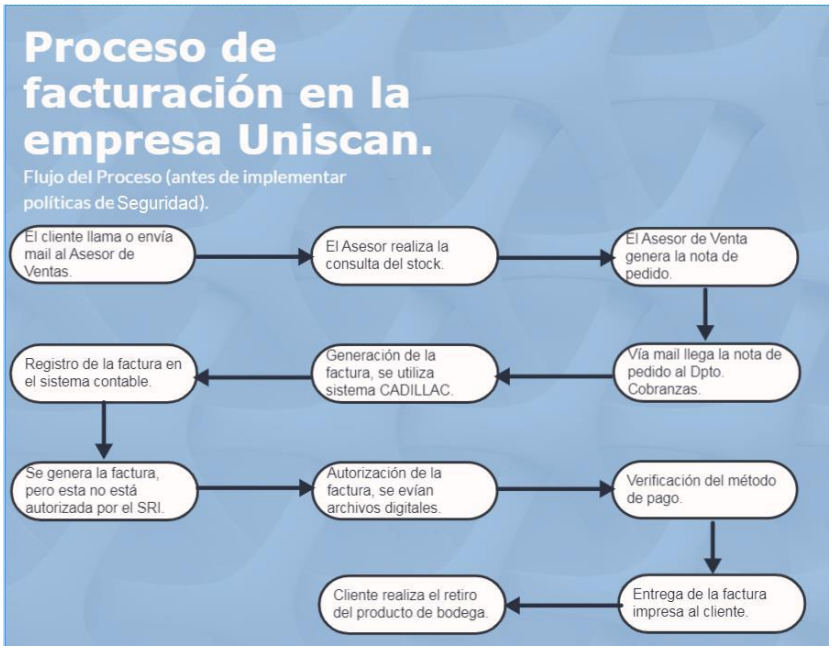


Fig. 17 Descripción del proceso de facturación en la empresa Uniscan en la actualidad.
Fuente: El autor.

A continuación, se realizará la descripción del proceso de facturación de la empresa Uniscan tomando en consideración controles que se implementarán en el plan de tratamiento de vulnerabilidades, esta implementación puede ser revisada en la figura 18, esto con el propósito de poder observar el contraste de llevar a cabo el mismo

proceso cumpliendo con los parámetros que ayuden a proteger los activos de información.

El proceso de facturación se mantendría de la misma manera, pero se agregarían ciertos puntos de seguridad que deben ser tomados en cuenta como medida de protección, en este caso sería un modelo recomendado:

1.- El cliente llama o envía mail solicitando una cotización de algún producto o servicio, es atendido por el Asesor de Ventas.

- Solicitar los datos del cliente, verificar que se encuentren en la base datos de la empresa y que tenga actualizada su información.

2.- El asesor realiza la consulta del stock en el sistema CADILLAC para poder indicar la existencia en inventario del artículo que requiere el cliente.

- Realizar la conexión a la base de datos por medio de una red segura.

3.- Asesor de Venta genera la nota de pedido.

- La nota de pedido debe ser generada en un software de edición de texto distribuido por el Dpto. de Desarrollo durante la entrega del equipo con el que está designado para el trabajo dentro de la organización.

4.- Se utiliza el correo institucional para enviar la nota de pedido, vía mail llega al Dpto. de Cobranzas para realizar la facturación (consulta de la base de datos para verificar la información del cliente).

- El mail debe ser generado y enviado desde el software destinado para esta función y distribuido por el Dpto. de Desarrollo durante la entrega del equipo con el que está designado para el trabajo dentro de la organización.

5.- Se utiliza el sistema CADILLAC para la generación de la factura.

- Cuidar de sus credenciales de ingreso al sistema CADILLAC.
- Abrir el sistema CADILLAC dentro de una red segura.

6.- Una vez generada la factura, se registra en el sistema contable para proceder con el cobro.

- Verificar que el registro de la factura en el sistema contable se haya realizado con éxito.

7.- Se genera la factura, pero por el momento aún no está autorizada por el SRI, hasta este momento no le llega el archivo XML y PDF al cliente.

8.- Una vez autorizada la factura en el sistema contable, automáticamente se envían los documentos digitales de la factura al correo registrado del cliente.

- Utilizar los correos oficiales entregados por la organización para el envío y recepción de documentación.
- Cumplir con la política de seguridad de utilización de correo electrónico, ejemplo para la protección contra PHISHING.

9.- Existen varios métodos de pago que el cliente puede utilizar, estos pueden ser: efectivo, tarjeta de débito, tarjeta de crédito y transferencia bancaria, en este último método se solicita al cliente que envíe el comprobante de la transferencia el cual se toma un tiempo para la comprobación, una vez comprobado el depósito se procede a indicar que la factura está cancelada.

- Tomar en consideración las políticas de seguridad que se deben de llevar a cabo en cuanto a transacciones bancarias, verificación del depósito o de la transferencia correspondiente al pago del cliente.

10.- Se imprimen 2 copias de la factura (una para el cobro y otra para el despacho en la bodega de la empresa).

- Seguir el procedimiento de seguridad en el manejo de documentos físicos para evitar la fuga de información confidencial que puede provocar una afectación al prestigio de la empresa, así como un error de entrega en el producto que adquiere el cliente.
- El manejo de la documentación adecuadamente hará que los procesos se lleven de manera ágil y eficaz, reduciendo significativamente el porcentaje de

equivocaciones durante el cobro de la factura, así como en el despacho de la mercadería.

11.- El cliente llega y cancela, con el documento firmado por parte del Dpto. de Cobranzas retira en bodega su pedido.

- Mantener un control sobre el acceso de personas a las instalaciones de la empresa, para proteger la integridad de la empresa, así como cuidar de los activos que forman parte de los procesos dentro de la organización.
- Se puede presentar eventos que afecten a la seguridad de la información al ser víctimas de espionaje empresarial por parte de la competencia, o la empresa podría sufrir el robo de información por parte de un intruso que no ha sido identificado por algún método de identificación y/o acceso restringido a las diferentes áreas de la empresa.

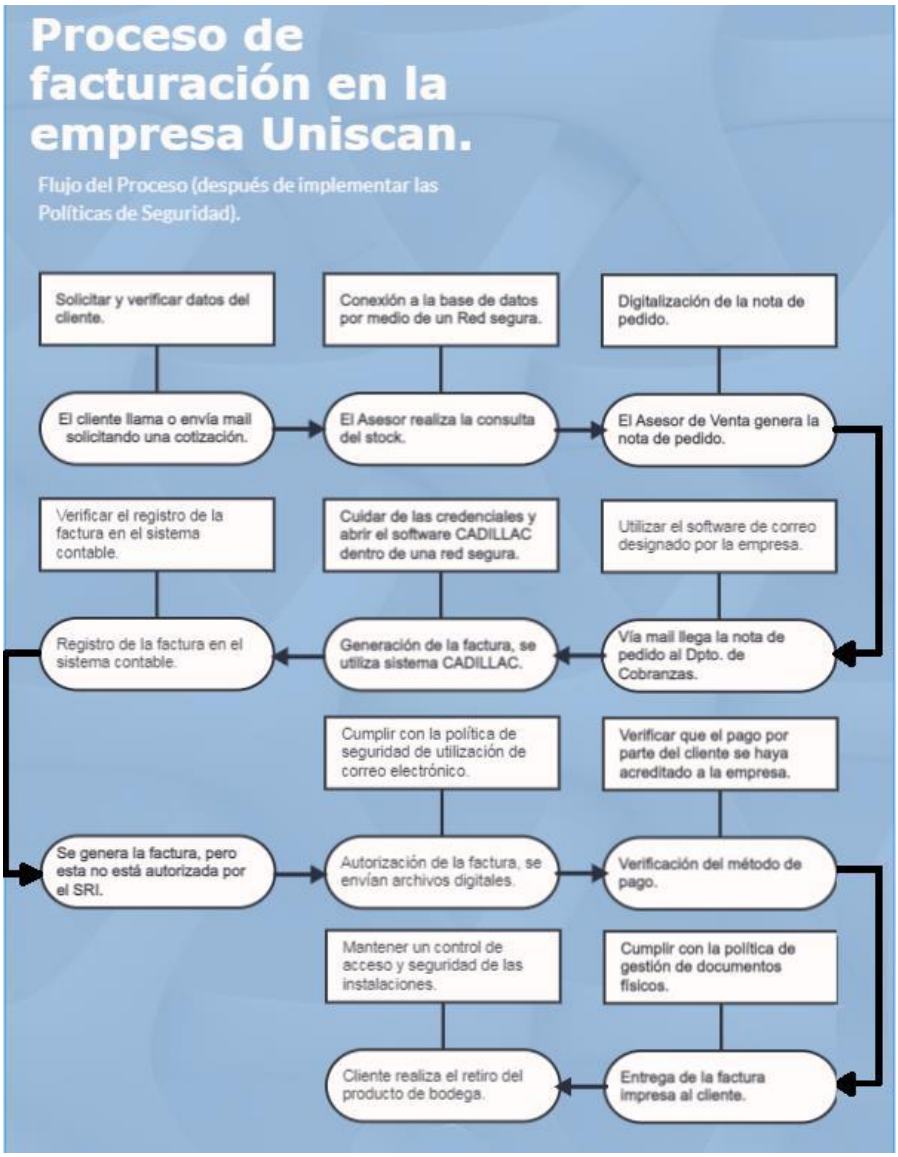


Fig. 18 Proceso de facturación en la empresa Uniscan después de aplicadas varias políticas de seguridad (modelo recomendado).
Fuente: El autor.

4.4.2.1. Análisis FODA del departamento de desarrollo de la organización Uniscan.

El análisis FODA (Fortalezas, Oportunidades, Debilidades y Amenazas) es una herramienta fundamental para evaluar el desempeño de una empresa. En este caso, se realizó un análisis FODA al departamento de desarrollo de la organización Uniscan, esta información se muestra en la Tabla XVI que se presenta a continuación.

TABLA XVI. ANÁLISIS FODA REALIZADO AL DPTO. DE DESARROLLO DE LA EMPRESA UNISCAN.

FORTALEZAS	OPORTUNIDADES
Se cuenta con el departamento de desarrollo dentro de la empresa y no se depende de terceros.	Contar con el presupuesto necesario para la compra e innovación de las herramientas (software y hardware) para tener un mejor cuidado en la seguridad de la información.
Las personas que pertenecen al departamento de desarrollo tienen la experiencia, habilidades, destrezas y conocimientos en el área de tecnologías.	Desarrollo de soluciones dentro de un mercado innovador y de constante expansión.
La empresa reconoce el valor de los datos de los clientes y toda la información que se genera en los procesos que se realizan internamente en la organización.	Entregar un plan de tratamiento de vulnerabilidades que conste de varias directrices para la mejora en cuanto a la seguridad de la información dentro de la organización.
Se tienen proveedores de servicios alterno que facilitan la continuidad del negocio en caso de algún inconveniente que se presente.	Enfoque en la seguridad de la información para la adquisición de nuevas tecnologías que ayuden a proteger los pilares fundamentales en el tratamiento de la información: confidencialidad, integridad y disponibilidad.
Las contraseñas (password) protegen el ingreso de usuarios no autorizados para el uso de los equipos de la empresa, de la aplicación de facturación e inventario de bodega, también se solicita el ingreso de usuario y contraseña en la aplicación SGU (sistema de gestión Uniscan) de la empresa.	En cuanto a la seguridad de la información dar capacitaciones a todo el personal de la empresa, por lo analizado y consultado, sigue siendo el recurso humano en muchas de las organizaciones el activo más débil y vulnerable a amenazas en cuanto al cuidado de datos e información.
La empresa tiene gran presencia dentro del mercado como distribuidor de tecnologías de codificación de activos (etiquetas, lectores de códigos de barra, puntos de venta, etc).	Implementación en cuanto a lo que sea posible dentro de la organización de directrices que ayuden a la seguridad de la información, tomando como guía los procesos de la norma ISO 27001.
	La empresa Uniscan tiene como objetivo el crecimiento fuera del país abriendo sucursales que le permitan ampliar su campo de acción.
DEBILIDADES	**AMENAZAS**
La empresa no cuenta con un servidor alterno, lo que podría ser un problema para la continuidad operativa, ya que en el caso de que el actual que se encuentra en uso sufriera una afectación, la empresa quedaría fuera de servicio hasta que se reponga uno nuevo o el mismo reparado de ser el caso.	Pérdida de información por no revisar las copias de seguridad después de que se ejecuten, no realizar una inspección calendarizada de los datos e información respaldados dentro del servidor de la organización.
El personal no cuenta con licencias de software, dentro de la institución no se maneja software licenciado, se hace uso de versiones de prueba o crackeados, lo que deja una gran vulnerabilidad en la seguridad de la información.	No se instala antivirus en los computadores de la empresa de los cuales hacen uso los colaboradores y en el caso de contar con un antivirus este no brinda una seguridad óptima.
No se tiene un amplio conocimiento sobre la seguridad de la información, tampoco se cuenta con una persona solamente encargada para esta área, a pesar de que en la actualidad se recomienda que exista dentro de toda organización un departamento que tenga como finalidad el tratamiento de la seguridad de la información porque el crecimiento de los	El software CADILLAC no es confiable, el sistema ha presentado errores en ocasiones y ha habido reportes de fallas durante las operaciones que ejecuta el personal de la empresa en las áreas de contabilidad y de logística. El sistema SGU con el que cuenta la organización se encuentra en proceso de pruebas y en ocasiones se han reportado fallas, pero estas han sido corregidas a la brevedad posible.

ataques a pequeñas y medianas empresas sigue en crecimiento.	
El acceso al área del servidor y cuarto de red/comunicación no se encuentra bien protegido, existe falencias en cuanto al acceso a ciertos activos de información, existe la posibilidad de que personal extraño a la empresa tenga acceso a activos importantes de información y comunicaciones.	Falta de espacio físico y de implementación de medidas de seguridad que permitan realizar las diferentes tareas de manera eficiente dentro de los procesos de TIC's, además el cuarto donde se encuentra el servidor, central telefónica, el RACK, router del proveedor de servicio de internet, etc., podría mejorar su instalación física lo que ayudaría en mucho para mejorar la seguridad de las tecnologías que se encuentran instaladas.
La organización no cuenta con normativas en varios de los procesos que se realizan dentro de la organización por lo que el control y análisis se vuelve un poco complicado y en ocasiones no se cuenta con información de importancia para la solución de problemas que se pueden llegar a presentar en un día normal de actividades.	Afectación a la integridad de los datos por accesos permitidos no controlados, este es un área que se puede mejorar con la implementación de diferentes tecnologías que se encuentran al alcance como son: sistema cerrado de video vigilancia, instalación de porteros eléctricos, equipos biométricos, cerraduras electrónicas, etc.
Inexistencia de planes de contingencia en caso de pérdida de información, de ataque a los activos de información o en el caso de que la infraestructura tecnológica sea vea afectada por cualquier agente externo o interno que hubiera vulnerado el perímetro de seguridad de la organización.	Constantes ataques a los sistemas de la empresa por parte de cibercriminales, en los últimos tiempos la organización se ha visto afectada por varios intentos de ataques, unos de los más comunes es el Phishing, de los que ya se ha reportado incidentes y afectaciones a la seguridad de la información.
Falta capacitación con respecto a temas relacionados con la seguridad de la información para los colaboradores de la empresa.	Constante identificación de vulnerabilidades, durante el presente proyecto se evidencia que dentro de la organización existen varias falencias en el área de seguridad de tecnologías de la información y que necesitan ser corregidas para elevar el nivel de protección y evitar incidentes que puedan llevarse a cabo por parte de personas ajenas a la empresa.
Falta de apoyo o la destinación de recursos por parte de gerencia para el departamento de desarrollo, quien se encuentra a cargo de los procesos de tecnologías de la información y comunicación, y que pudieran mejorar el estado actual de la seguridad de la información en la empresa Uniscan.	Dependencia a la financiación para escalar, como en toda organización es necesario el apoyo de gerencia o de las autoridades que puedan brindar los recursos necesarios para la implementación de medidas de seguridad que permita proteger los datos y activos de información que se utilizan en las operaciones de la empresa, es necesario que las personas encargadas del área de tecnología puedan exponer las grandes ventajas que conlleva la inversión en esta área y lo contraproducente que sería no invertir en la seguridad de la información.

Procesos poco consolidados, o que necesitan ser implementados siguiendo una normativa que permita estandarizar y regularizar los procesos que se llevan en la actualidad tomando en cuenta la protección de los datos e información que se maneja dentro de la organización.	

Fuente: El autor.

4.4.2.2. Identificación de amenazas potenciales.

Teniendo en cuenta que las amenazas son eventos que probablemente ocurran, causen pérdidas y amenacen el normal funcionamiento de los activos de la institución, es necesario identificarlas a tiempo, esto para prevenir su ocurrencia y, si ocurren, su impacto no causará daños de mayor importancia [27].

Para identificar las amenazas se consideraron las principales en relación al tipo de organización, y los activos afectados por la amenaza. Las amenazas potenciales en los activos de información de la infraestructura tecnológica de la organización se clasifican en 4 categorías como se describe en el método MAGERIT, esto se puede apreciar en la Tabla XVII.

TABLA XVII. CLASIFICACIÓN DE LAS AMENAZAS.

[N] Desastres naturales	[N.1] Fuego
	[N.2] Daños por agua
[I] De origen industrial	[I.5] Avería de origen físico o lógico
	[I.6] Corte del suministro eléctrico
	[I.7] Condiciones inadecuadas de temperatura o humedad
	[I.8] Fallo de servicios de comunicaciones
	[I.9] Interrupción de otros servicios y suministros esenciales
	[I.11] Emanaciones electromagnéticas
[E] Errores y fallos no intencionados	[E.1] Errores de los usuarios
	[E.2] Errores del administrador
	[E.3] Errores de monitorización (log)
	[E.4] Errores de configuración
	[E.7] Deficiencias en la organización
	[E.8] Difusión de software dañino
	[E.9] Errores de [re-]encaminamiento
	[E.10] Errores de secuencia
	[E.15] Alteración accidental de la información
	[E.19] Fugas de información
	[E.20] Vulnerabilidades de los programas (software)

	[E.21] Errores de mantenimiento / actualización de programas (software)
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)
	[E.24] Caída del sistema por agotamiento de recursos
	[E.25] Pérdida de equipos
[A] Ataques intencionados	[A.3] Manipulación de los registros de actividad (log)
	[A.4] Manipulación de la configuración
	[A.5] Suplantación de la identidad del usuario
	[A.6] Abuso de privilegios de acceso
	[A.7] Uso no previsto
	[A.8] Difusión de software dañino
	[A.11] Acceso no autorizado
	[A.12] Análisis de tráfico
	[A.14] Interceptación de información (escucha)
	[A.15] Modificación deliberada de la información
	[A.18] Destrucción de información
	[A.19] Divulgación de información
	[A.22] Manipulación de programas
	[A.23] Manipulación de los equipos
	[A.24] Denegación de servicio
	[A.25] Robo
	[A.26] Ataque destructivo
	[A.28] Indisponibilidad del personal
	[A.30] Ingeniería social (picaresca)

Fuente: El autor.

4.4.2.3. Determinación y matriz de riesgos por activo.

Luego de haber identificado las posibles amenazas que podrían afectar a la organización, se procedió a la creación de la matriz de riesgo con el fin de determinar los peligros a los que se enfrenta la empresa, esto lo podemos observar en la Tabla XVIII. Para ello, se aplicó el enfoque individual de MAGERIT en cada matriz de amenazas, considerando los riesgos, los impactos y las causas potenciales asociadas a cada amenaza. Cabe destacar que, aunque algunas amenazas puedan ser similares, sus causas de ocurrencia son completamente aisladas entre sí.

TABLA XVIII. MATRIZ DE RIESGO.

TIPO	CODIGO	DESCRIPCION	AMENAZAS
[D] Datos/Información	D-1	Ficheros	[E.1] Errores de los usuarios
			[E.3] Errores de monitorización (log)
			[E.4] Errores de configuración
			[E.15] Alteración accidental de la información
			[E.19] Fugas de información

			[A.3] Manipulación de los registros de actividad (log)
			[A.4] Manipulación de la configuración
			[A.11] Acceso no autorizado
			[A.15] Modificación deliberada de la información
			[A.19] Divulgación de información
			[A.26] Ataque destructivo
	D-2	Copias de Respaldo	[E.1] Errores de los usuarios
			[E.2] Errores del administrador
			[E.3] Errores de monitorización (log)
			[E.4] Errores de configuración
			[E.15] Alteración accidental de la información
			[E.19] Fugas de información
			[A.3] Manipulación de los registros de actividad (log)
			[A.4] Manipulación de la configuración
			[A.6] Abuso de privilegios de acceso
			[A.11] Acceso no autorizado
			[A.15] Modificación deliberada de la información
			[A.18] Destrucción de información
			[A.19] Divulgación de información
			[A.26] Ataque destructivo
	D-3	Credenciales	[E.1] Errores de los usuarios
			[E.2] Errores del administrador
			[E.3] Errores de monitorización (log)
			[E.4] Errores de configuración
			[E.15] Alteración accidental de la información
			[E.19] Fugas de información
			[A.3] Manipulación de los registros de actividad (log)
			[A.4] Manipulación de la configuración
			[A.5] Suplantación de la identidad del usuario
			[A.6] Abuso de privilegios de acceso
			[A.11] Acceso no autorizado
			[A.15] Modificación deliberada de la información
			[A.19] Divulgación de información
	D-4	Código fuente	[E.3] Errores de monitorización (log)
			[E.4] Errores de configuración
			[E.15] Alteración accidental de la información
			[A.3] Manipulación de los registros de actividad (log)
			[A.4] Manipulación de la configuración
			[A.11] Acceso no autorizado
			[A.18] Destrucción de información
			[A.19] Divulgación de información
[S] Servicios	S-1	Interno (a usuarios de la propia organización)	[E.1] Errores de los usuarios
			[E.2] Errores del administrador
			[E.9] Errores de [re-]encaminamiento
			[E.10] Errores de secuencia
			[E.15] Alteración accidental de la información

			[E.19] Fugas de información
			[A.5] Suplantación de la identidad del usuario
			[A.6] Abuso de privilegios de acceso
			[A.7] Uso no previsto
			[A.18] Destrucción de información
			[A.19] Divulgación de información
	S-2	World wide web	[E.1] Errores de los usuarios
			[E.2] Errores del administrador
			[E.9] Errores de [re-]encaminamiento
			[E.10] Errores de secuencia
			[E.15] Alteración accidental de la información
			[E.19] Fugas de información
			[E.24] Caída del sistema por agotamiento de recursos
			[A.5] Suplantación de la identidad del usuario
			[A.6] Abuso de privilegios de acceso
			[A.11] Acceso no autorizado
			[A.15] Modificación deliberada de la información
			[A.18] Destrucción de información
			[A.19] Divulgación de información
			[A.24] Denegación de servicio
	S-3	Acceso remoto a cuenta local	[E.1] Errores de los usuarios
			[E.2] Errores del administrador
			[E.9] Errores de [re-]encaminamiento
			[E.10] Errores de secuencia
			[E.19] Fugas de información
			[E.24] Caída del sistema por agotamiento de recursos
			[A.5] Suplantación de la identidad del usuario
			[A.6] Abuso de privilegios de acceso
			[A.11] Acceso no autorizado
			[A.15] Modificación deliberada de la información
			[A.19] Divulgación de información
			[A.24] Denegación de servicio
	S-4	Gestión de Privilegios	[E.1] Errores de los usuarios
			[E.2] Errores del administrador
			[E.9] Errores de [re-]encaminamiento
			[E.10] Errores de secuencia
			[E.19] Fugas de información
			[E.24] Caída del sistema por agotamiento de recursos
			[A.5] Suplantación de la identidad del usuario
			[A.6] Abuso de privilegios de acceso
			[A.11] Acceso no autorizado
			[A.15] Modificación deliberada de la información
			[A.19] Divulgación de información
			[A.24] Denegación de servicio
[SW] Software-Aplicaciones Informáticas	SW-1	Desarrollo propio	[I.5] Avería de origen físico o lógico
			[E.1] Errores de los usuarios

			[E.20] Vulnerabilidades de los programas (software)
			[E.21] Errores de mantenimiento / actualización de programas (software)
			[A.6] Abuso de privilegios de acceso
			[A.11] Acceso no autorizado
			[A.15] Modificación deliberada de la información
			[A.18] Destrucción de información
			[A.19] Divulgación de información
			[A.22] Manipulación de programas
	SW-2	Desarrollo a medida	[I.5] Avería de origen físico o lógico
			[E.1] Errores de los usuarios
			[E.9] Errores de [re-]encaminamiento
			[E.20] Vulnerabilidades de los programas (software)
			[E.21] Errores de mantenimiento / actualización de programas (software)
			[A.5] Suplantación de la identidad del usuario
			[A.6] Abuso de privilegios de acceso
			[A.7] Uso no previsto
			[A.11] Acceso no autorizado
			[A.15] Modificación deliberada de la información
			[A.18] Destrucción de información
			[A.19] Divulgación de información
			[A.22] Manipulación de programas
	SW-3	Servidor de correo electrónico	[I.5] Avería de origen físico o lógico
			[E.2] Errores del administrador
			[E.8] Difusión de software dañino
			[E.9] Errores de [re-]encaminamiento
			[E.10] Errores de secuencia
			[E.19] Fugas de información
			[E.20] Vulnerabilidades de los programas (software)
			[E.21] Errores de mantenimiento / actualización de programas (software)
			[A.5] Suplantación de la identidad del usuario
			[A.6] Abuso de privilegios de acceso
			[A.7] Uso no previsto
			[A.11] Acceso no autorizado
			[A.15] Modificación deliberada de la información
			[A.18] Destrucción de información
			[A.19] Divulgación de información
			[A.22] Manipulación de programas
	SW-4	Sistema de gestión de Base de Datos	[I.5] Avería de origen físico o lógico
			[E.1] Errores de los usuarios
			[E.2] Errores del administrador
			[E.8] Difusión de software dañino
			[E.9] Errores de [re-]encaminamiento
			[E.10] Errores de secuencia
			[E.19] Fugas de información

			[E.20] Vulnerabilidades de los programas (software)
			[E.21] Errores de mantenimiento / actualización de programas (software)
			[A.5] Suplantación de la identidad del usuario
			[A.6] Abuso de privilegios de acceso
			[A.7] Uso no previsto
			[A.11] Acceso no autorizado
			[A.15] Modificación deliberada de la información
			[A.18] Destrucción de información
			[A.19] Divulgación de información
[HW] Equipamiento Informático	HW-1	Grandes equipos	[N.1] Fuego
			[N.2] Daños por agua
			[I.5] Avería de origen físico o lógico
			[I.6] Corte del suministro eléctrico
			[I.7] Condiciones inadecuadas de temperatura o humedad
			[I.11] Emanaciones electromagnéticas
			[E.2] Errores del administrador
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)
			[E.24] Caída del sistema por agotamiento de recursos
			[A.6] Abuso de privilegios de acceso
			[A.7] Uso no previsto
			[A.11] Acceso no autorizado
			[A.23] Manipulación de los equipos
			[A.24] Denegación de servicio
			[A.25] Robo
			[A.26] Ataque destructivo
	HW-2	Informática personal	[N.1] Fuego
			[N.2] Daños por agua
			[I.5] Avería de origen físico o lógico
			[I.6] Corte del suministro eléctrico
			[I.7] Condiciones inadecuadas de temperatura o humedad
			[I.11] Emanaciones electromagnéticas
			[E.2] Errores del administrador
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)
			[E.24] Caída del sistema por agotamiento de recursos
			[E.25] Pérdida de equipos
			[A.6] Abuso de privilegios de acceso
			[A.7] Uso no previsto
			[A.11] Acceso no autorizado
			[A.23] Manipulación de los equipos
			[A.25] Robo
			[A.26] Ataque destructivo
	HW-3	Medios de Impresión	[N.1] Fuego
			[N.2] Daños por agua

			[I.5] Avería de origen físico o lógico
			[I.6] Corte del suministro eléctrico
			[I.7] Condiciones inadecuadas de temperatura o humedad
			[I.11] Emanaciones electromagnéticas
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)
			[E.24] Caída del sistema por agotamiento de recursos
			[A.7] Uso no previsto
			[A.23] Manipulación de los equipos
			[A.25] Robo
			[A.26] Ataque destructivo
	HW-4	Centralita telefónica	[N.1] Fuego
			[N.2] Daños por agua
			[I.5] Avería de origen físico o lógico
			[I.6] Corte del suministro eléctrico
			[I.7] Condiciones inadecuadas de temperatura o humedad
			[I.11] Emanaciones electromagnéticas
			[E.2] Errores del administrador
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)
			[A.7] Uso no previsto
			[A.11] Acceso no autorizado
			[A.23] Manipulación de los equipos
			[A.25] Robo
			[A.26] Ataque destructivo
[COM] Redes de Comunicaciones	COM-1	Red Telefónica	[I.8] Fallo de servicios de comunicaciones
			[E.2] Errores del administrador
			[E.9] Errores de [re-]encaminamiento
			[E.10] Errores de secuencia
			[E.15] Alteración accidental de la información
			[E.19] Fugas de información
			[E.24] Caída del sistema por agotamiento de recursos
			[A.5] Suplantación de la identidad del usuario
			[A.7] Uso no previsto
			[A.12] Análisis de tráfico
			[A.14] Interceptación de información (escucha)
			[A.18] Destrucción de información
			[A.19] Divulgación de información
			[A.24] Denegación de servicio
			[A.25] Robo
	COM-2	Red Inalámbrica	[I.8] Fallo de servicios de comunicaciones
			[E.2] Errores del administrador
			[E.9] Errores de [re-]encaminamiento
			[E.10] Errores de secuencia
			[E.19] Fugas de información
			[E.24] Caída del sistema por agotamiento de recursos

			[A.5] Suplantación de la identidad del usuario
			[A.7] Uso no previsto
			[A.11] Acceso no autorizado
			[A.12] Análisis de tráfico
			[A.14] Interceptación de información (escucha)
			[A.19] Divulgación de información
			[A.24] Denegación de servicio
			[A.25] Robo
			[A.26] Ataque destructivo
	COM-3	Red Local	[I.8] Fallo de servicios de comunicaciones
			[E.2] Errores del administrador
			[E.9] Errores de [re-]encaminamiento
			[E.10] Errores de secuencia
			[E.19] Fugas de información
			[E.24] Caída del sistema por agotamiento de recursos
			[A.5] Suplantación de la identidad del usuario
			[A.7] Uso no previsto
			[A.11] Acceso no autorizado
			[A.12] Análisis de tráfico
			[A.14] Interceptación de información (escucha)
			[A.19] Divulgación de información
			[A.24] Denegación de servicio
			[A.25] Robo
			[A.26] Ataque destructivo
	COM-4	Internet	[I.8] Fallo de servicios de comunicaciones
			[E.2] Errores del administrador
			[E.9] Errores de [re-]encaminamiento
			[E.10] Errores de secuencia
			[E.15] Alteración accidental de la información
			[E.19] Fugas de información
			[E.24] Caída del sistema por agotamiento de recursos
			[A.5] Suplantación de la identidad del usuario
			[A.7] Uso no previsto
			[A.11] Acceso no autorizado
			[A.12] Análisis de tráfico
			[A.14] Interceptación de información (escucha)
			[A.15] Modificación deliberada de la información
			[A.18] Destrucción de información
			[A.19] Divulgación de información
			[A.24] Denegación de servicio
[Media] Soportes de Información	Media-1	Discos	[N.1] Fuego
			[N.2] Daños por agua
			[I.5] Avería de origen físico o lógico
			[I.7] Condiciones inadecuadas de temperatura o humedad
			[I.11] Emanaciones electromagnéticas
			[E.1] Errores de los usuarios

			[E.2] Errores del administrador
			[E.15] Alteración accidental de la información
			[E.19] Fugas de información
			[E.25] Pérdida de equipos
			[A.7] Uso no previsto
			[A.15] Modificación deliberada de la información
			[A.18] Destrucción de información
			[A.19] Divulgación de información
			[A.25] Robo
	Media-2	Almacenamiento en Red	[N.1] Fuego
			[N.2] Daños por agua
			[I.5] Avería de origen físico o lógico
			[I.7] Condiciones inadecuadas de temperatura o humedad
			[I.11] Emanaciones electromagnéticas
			[E.1] Errores de los usuarios
			[E.2] Errores del administrador
			[E.19] Fugas de información
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)
			[A.15] Modificación deliberada de la información
			[A.18] Destrucción de información
			[A.19] Divulgación de información
			[A.23] Manipulación de los equipos
			[A.25] Robo
	Media-3	Memorias USB	[N.1] Fuego
			[N.2] Daños por agua
			[I.5] Avería de origen físico o lógico
			[I.7] Condiciones inadecuadas de temperatura o humedad
			[I.11] Emanaciones electromagnéticas
			[E.1] Errores de los usuarios
			[E.15] Alteración accidental de la información
			[E.19] Fugas de información
			[E.25] Pérdida de equipos
			[A.7] Uso no previsto
			[A.15] Modificación deliberada de la información
			[A.18] Destrucción de información
			[A.19] Divulgación de información
			[A.25] Robo
	Media-4	Material Impreso	[N.1] Fuego
			[N.2] Daños por agua
			[I.5] Avería de origen físico o lógico
			[I.7] Condiciones inadecuadas de temperatura o humedad
			[E.1] Errores de los usuarios
			[E.2] Errores del administrador
			[E.15] Alteración accidental de la información

			[E.19] Fugas de información
			[A.15] Modificación deliberada de la información
			[A.18] Destrucción de información
			[A.19] Divulgación de información
			[A.25] Robo
[AUX] Equipamiento Auxiliar	AUX-1	Sistemas de Alimentación Ininterrumpida	[N.1] Fuego
			[N.2] Daños por agua
			[I.5] Avería de origen físico o lógico
			[I.6] Corte del suministro eléctrico
			[I.7] Condiciones inadecuadas de temperatura o humedad
			[I.9] Interrupción de otros servicios y suministros esenciales
			[I.11] Emanaciones electromagnéticas
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)
			[A.7] Uso no previsto
			[A.23] Manipulación de los equipos
	AUX-2	Cableado	[N.1] Fuego
			[N.2] Daños por agua
			[I.5] Avería de origen físico o lógico
			[I.6] Corte del suministro eléctrico
			[I.7] Condiciones inadecuadas de temperatura o humedad
			[I.9] Interrupción de otros servicios y suministros esenciales
			[I.11] Emanaciones electromagnéticas
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)
	AUX-3	Cable Eléctrico	[N.1] Fuego
			[N.2] Daños por agua
			[I.5] Avería de origen físico o lógico
			[I.6] Corte del suministro eléctrico
			[I.7] Condiciones inadecuadas de temperatura o humedad
			[I.9] Interrupción de otros servicios y suministros esenciales
			[I.11] Emanaciones electromagnéticas
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)
	AUX-4	Equipos de Destrucción de Soportes de Información	[N.1] Fuego
			[N.2] Daños por agua
			[I.5] Avería de origen físico o lógico
			[I.6] Corte del suministro eléctrico
			[I.7] Condiciones inadecuadas de temperatura o humedad
			[I.9] Interrupción de otros servicios y suministros esenciales
			[I.11] Emanaciones electromagnéticas

			[E.23] Errores de mantenimiento / actualización de equipos (hardware)
			[E.25] Pérdida de equipos
			[A.23] Manipulación de los equipos
[L] Instalaciones	L-1	Edificio	[N.1] Fuego
			[N.2] Daños por agua
			[E.19] Fugas de información
			[A.11] Acceso no autorizado
			[A.15] Modificación deliberada de la información
			[A.19] Divulgación de información
			[A.26] Ataque destructivo
	L-2	Cuarto	[N.1] Fuego
			[N.2] Daños por agua
			[E.19] Fugas de información
			[A.7] Uso no previsto
			[A.11] Acceso no autorizado
			[A.15] Modificación deliberada de la información
			[A.19] Divulgación de información
			[A.26] Ataque destructivo
	L-3	Car	[A.7] Uso no previsto
			[A.15] Modificación deliberada de la información
			[A.26] Ataque destructivo
	L-4	Instalaciones de Respaldo	[N.2] Daños por agua
			[A.7] Uso no previsto
			[A.11] Acceso no autorizado
			[A.15] Modificación deliberada de la información
			[A.26] Ataque destructivo
[P] Personal	P-1	Usuarios Externos	[E.7] Deficiencias en la organización
			[A.30] Ingeniería social (picaresca)
	P-2	Administradores de Sistemas	[E.7] Deficiencias en la organización
			[E.19] Fugas de información
			[A.28] Indisponibilidad del personal
			[A.30] Ingeniería social (picaresca)
	P-3	Desarrolladores/Programadores	[E.7] Deficiencias en la organización
			[E.19] Fugas de información
			[A.28] Indisponibilidad del personal
			[A.30] Ingeniería social (picaresca)
	P-4	Proveedores	[E.7] Deficiencias en la organización

Fuente: El autor.

4.4.2.4. Evaluación del riesgo.

Luego de haber identificado las amenazas y riesgos relacionados con cada activo de información, se procede a llevar a cabo una evaluación de riesgos utilizando el método MAGERIT. El impacto del riesgo generado por cada evento se evaluará de manera

porcentual como se puede apreciar en la Tabla XIX, además se debe tener en cuenta la frecuencia con la que se produce en los activos de información, se puede observar la Tabla XX donde se entrega un valor numérico de ocurrencia de la amenaza [27].

TABLA XIX. IMPACTO DEL RIESGO.

Nivel	Abreviatura	Valor
Crítico	C	95%
Alto	A	75%
Medio	M	50%
Bajo	B	20%

Fuente: El autor.

TABLA XX. PROBABILIDAD DE OCURRENCIA DE LA AMENAZA.

Nivel	Abreviatura	Valor	Descripción
Extremadamente frecuente	EF	1.0000	1 vez al día
Muy frecuente	MF	0.1425	1 vez cada semana
Frecuente	F	0.0329	1 vez cada mes
Frecuencia normal	FN	0.0055	1 vez cada 6 meses
Poco frecuente	PF	0.0027	1 vez al año
Extremadamente poco frecuente	EPF	0.0005	1 vez cada 5 años

Fuente: El autor.

En este punto se sugiere que se consulte el Anexo 11 del presente proyecto donde se encuentra la tabla que muestra la evaluación de riesgo intrínseco de los activos considerados en el desarrollo de este proyecto. Esta información es relevante y puede proporcionar una mejor comprensión sobre la valoración de riesgos de cada uno de los activos.

4.4.2.5. Análisis de resultados de la matriz de riesgos.

A continuación, se expondrá un examen detallado de los riesgos que se consideran críticos, importantes y medios.

Riesgo de nivel crítico.

Se ha encontrado muy importante para los datos de información de la empresa Uniscan implementar controles para reducir el riesgo de accesos no autorizados y controles para las condiciones ambientales que puedan afectar significativamente la infraestructura tecnológica. Lo mencionado en el párrafo anterior tiene como objetivo la protección de la documentación almacenada, y poder así brindar a los colaboradores de la empresa la garantía de acceder a la información cuando lo requieran y en el caso de ser necesario volver a consultar nuevamente los datos.

Riesgo de nivel importante.

Se descubrió que varios activos de información de la empresa corren grave peligro, los datos pueden perderse porque no se toman las precauciones necesarias para evitar que personas no autorizadas los roben, y los socios comerciales de algunas empresas tienen acceso a información que no deberían debido al principio de confidencialidad, esto se debe a que el acceso a la información del servidor no está controlado, dado que algunas personas pueden lograr instalar programas informáticos sin la debida autorización, lo que podría dar lugar a violaciones de la seguridad, es obvio que hay que instruir a los empleados en las mejores prácticas de uso de los recursos ofimáticos.

Por otro lado, es práctica común renunciar a las actualizaciones del antivirus y del sistema operativo, lo que provoca que algunos ordenadores sean demasiado lentos para ser utilizados por el personal. Esto revela una ausencia significativa de formación en seguridad de la información para los miembros del personal y de políticas de seguridad. Al no mantener actualizadas las aplicaciones, los equipos no pueden funcionar a una velocidad que les permita realizar eficazmente las tareas asignadas, también impide que los trabajadores de determinadas ubicaciones tengan acceso a activos específicos en términos de mantenimiento y actualizaciones de hardware. Por ello, es crucial que el personal del departamento técnico pueda ofrecer asistencia en sitio y disponga de una estrategia de mantenimiento y actualización para solucionar los fallos a medida que surjan.

Riesgo de nivel medio.

Las circunstancias que ponen en peligro los activos de información, como las condiciones de temperatura inadecuadas que influyen en el hardware, sobre todo en el servidor local, no están muy documentadas.

Además, como muchos de los colaboradores de la empresa no llevan a cabo los procesos de actualización del software, como los antivirus y otros instalan aplicaciones que no tienen nada que ver con sus funciones, esto evidencia que el personal de la empresa no se encuentra cualificado para tratar cuestiones de seguridad de la información o de gestión de software.

Los cortes inesperados del suministro eléctrico, se trata de un fallo de seguridad que, si se utiliza de forma malintencionada, podría poner en peligro la disponibilidad de los datos. Los dispositivos de estabilización de tensión o UPS son los activos que faltan en los sistemas de alimentación de los ordenadores de los distintos departamentos, lo que impide un suministro continuo de energía durante los cortes de electricidad. Sólo hay un UPS en la empresa, y únicamente alimenta el servidor y el rack. Cuando se está trabajando y se produce un apagón inesperado, esto pone en peligro los equipos informáticos y aumenta la probabilidad de que se pierdan datos.

TABLA XXI. CARACTERIZACIÓN DEL RIESGO INTRÍNSECO, EFECTIVO Y CONTROLADO.

N°	CODIGO	NOMBRE	Riesgo intrínseco total diario	Riesgo efectivo total diario	Riesgo Controlado por Salvaguardas
1	D-1	Ficheros	$ 958.90	$ 767.12	$ 191.78
2	D-2	Copias de Respaldo	$ 3,424.66	$ 2,678.08	$ 746.58
3	D-3	Credenciales	$ 6,205.48	$ 4,779.45	$ 1,426.03
4	D-4	Código fuente	$ 17,260.27	$ 13,808.22	$ 3,452.05
5	S-1	Interno (a usuarios de la propia organización)	$ 235.62	$ 188.49	$ 47.12
6	S-2	World wide web	$ 1,794.52	$ 1,373.97	$ 420.55
7	S-3	Acceso remoto a cuenta local	$ 2,178.08	$ 1,434.25	$ 743.84

8	S-4	Gestión de Privilegios	$ 2,397.26	$ 1,671.23	$ 726.03
9	SW-1	Desarrollo propio	$ 350.68	$ 280.55	$ 70.14
10	SW-2	Desarrollo a medida	$ 2,712.33	$ 2,046.58	$ 665.75
11	SW-3	Servidor de correo electrónico	$ 1,249.32	$ 999.45	$ 249.86
12	SW-4	Sistema de gestión de Base de Datos	$ 619.18	$ 433.70	$ 185.48
13	HW-1	Grandes equipos	$ 2,947.95	$ 2,125.75	$ 822.19
14	HW-2	Informática personal	$ 392.33	$ 307.62	$ 84.71
15	HW-3	Medios de Impresión	$ 2.78	$ 2.16	$ 0.62
16	HW-4	Centralita telefónica	$ 15.67	$ 11.91	$ 3.76
17	COM-1	Red Telefónica	$ 20.44	$ 16.35	$ 4.09
18	COM-2	Red Inalámbrica	$ 424.11	$ 326.96	$ 97.15
19	COM-3	Red Local	$ 355.62	$ 284.49	$ 71.12
20	COM-4	Internet	$ 4,821.92	$ 3,734.25	$ 1,087.67
21	Media-1	Discos	$ 181.37	$ 145.10	$ 36.27
22	Media-2	Almacenamiento en Red	$ 1,734.25	$ 1,313.42	$ 420.82
23	Media-3	Memorias USB	$ 15.01	$ 11.29	$ 3.72
24	Media-4	Material Impreso	$ 17.32	$ 10.86	$ 6.46
25	AUX-1	Sistemas de Alimentación Ininterrumpida	$ 956.16	$ 764.93	$ 191.23
26	AUX-2	Cableado	$ 53.70	$ 41.32	$ 12.38
27	AUX-3	Cable Eléctrico	$ 66.85	$ 53.48	$ 13.37
28	AUX-4	Equipos de Destrucción de Soportes de Información	$ 5.37	$ 4.05	$ 1.32
29	L-1	Edificio	$ 309.59	$ 247.67	$ 61.92
30	L-2	Cuarto	$ 8.38	$ 6.71	$ 1.68
31	L-3	Car	$ 36.66	$ 29.01	$ 7.64

32	L-4	Instalaciones de Respaldo	$ 0.62	$ 0.50	$ 0.12
33	P-1	Usuarios Externos	$ 1,561.64	$ 879.45	$ 682.19
34	P-2	Administradores de Sistemas	$ 958.90	$ 767.12	$ 191.78
35	P-3	Desarrolladores/Programadores	$ 739.73	$ 591.78	$ 147.95
36	P-4	Proveedores	$ 2.74	$ 2.19	$ 0.55

Fuente: El autor.

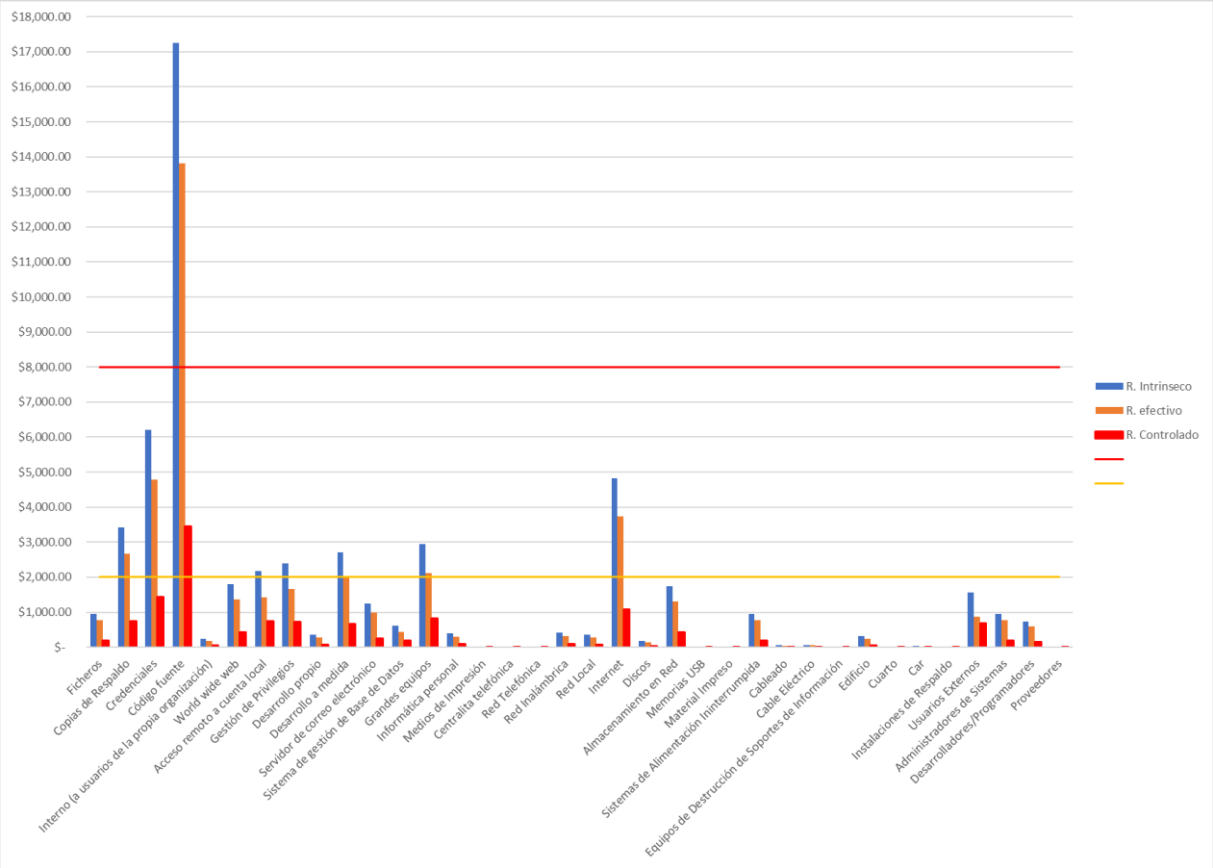


Fig. 19 Representación gráfica del riesgo: intrínseco, efectivo y controlado de los activos de información.
Fuente: El autor.

Después de llevar a cabo el análisis de riesgos con la ayuda de la Tabla XXI que se encuentra en la parte superior, se pudo identificar las amenazas que afectan a los activos de información en la empresa Uniscan, para tener una comparación gráfica de fácil interpretación podemos revisar la figura 19, donde podemos concluir que el activo Código Fuente es crítico, pero después de aplicar las salvaguardas correspondientes se situó en un nivel importante, muy cercano a ser apreciable para la empresa. Además, se detectó que 7 activos (copias de respaldo, credenciales, accesos remotos a la cuenta

local, gestión de privilegios, desarrollo a medida e internet), que representan el 19% de los activos de información, están en un nivel importante de riesgo. Sin embargo, una vez implementadas las medidas de seguridad adecuadas, estos activos pasarán a ser apreciables por parte de la empresa.

Por otro lado, se encontró que 27 activos, que representan el 75% de los activos de información de la organización, tales como: ficheros, activos internos, World Wide Web, desarrollo propio, servidor de correo electrónico, sistema de gestión de base de datos, informática personal, medios de impresión, central telefónica, red telefónica, red inalámbrica, red local, discos, almacenamiento en red, memoria USB, material impreso, sistemas de alimentación ininterrumpida, cableado, cable eléctrico, equipos de destrucción de soportes de información, edificio cuarto, car, instalaciones de respaldo, usuarios externos, administradores de sistemas, desarrolladores y proveedores, se sitúan en la franja de nivel apreciable por la organización.

Sin embargo, se hace necesario estudiar la seguridad de la información en estos activos y reforzarla con la implementación de salvaguardas para disminuir el riesgo de ser víctimas de un ataque malicioso. Todo esto permitirá desarrollar una estrategia de protección de los activos de información y de la infraestructura tecnológica que respalda las operaciones de la empresa, con el objetivo de prevenir o mitigar cualquier amenaza o vulnerabilidad que pueda influir en la integridad, confidencialidad y privacidad de la información, así como en su disponibilidad.

4.4.3. FASE 3: Desarrollo de un plan de remediación para los riesgos y vulnerabilidades identificadas en los activos de información de la organización Uniscan.

Con base en el proceso de enfoque de MAGERIT, se procede a realizar el detalle de diferentes salvaguardas que podrían implementarse dentro de la organización Uniscan, y que acompañadas con las acciones determinadas en el plan de tratamiento de vulnerabilidades que se adjunta en el presente proyecto se puede cumplir con los propósitos de mitigar los riesgos y pérdidas, teniendo en cuenta los tipos de amenazas

que enfrenta la empresa, así como la gestión y tratamiento de riesgos es responsabilidad de la empresa aplicar la propuesta que se acompaña en este trabajo, en la cual se han formulado varias recomendaciones y dependerá a criterio de la organización su puesta en marcha.

4.4.3.1. Plan tratamiento de riesgos y propuesta de salvaguardas.

Luego de la identificación de las posibles amenazas que podrían afectar a los activos de información y la infraestructura tecnológica de la empresa Uniscan, se procede a la creación de un plan de gestión de riesgos. Este plan se enfoca en la asignación de medidas de seguridad o salvaguardas a cada activo de información, con el objetivo de disminuir los riesgos asociados a las posibles amenazas identificadas. La aplicación de estas salvaguardas permitirá proteger los activos de información y la infraestructura tecnológica de la organización, evitando posibles vulneraciones de la integridad, privacidad y confidencialidad de la información, y asegurando su disponibilidad.

En la Tabla XXII se realiza una propuesta de salvaguardas que beneficiará al estado actual de seguridad de la información de la organización en estudio, esta tabla cuenta con el respectivo valor económico referencial de implementación de cada una de las salvaguardas.

TABLA XXII. PROPUESTA DE SALVAGUARDAS.

Nº	Código	Descripción	Valoración cuantitativa	Activo
1	SG-001	Sistema de alarma	$ 2,000.00	HW-1 Grandes Equipos HW-2 Informática personal HW-3 Medios de Impresión HW-4 Centralita telefónica COM-1 Red Telefónica COM-2 Red Inalámbrica COM-3 Red Local COM-4 Internet Media-1 Discos Media-3 Memorias USB Media-4 Material Impreso AUX-1 Sistemas de Alimentación Ininterrumpida AUX-2 Cableado AUX-3 Cable Eléctrico AUX-4 Equipos de Destrucción de Soportes de Información L-1 Edificio L-2 Cuarto L-3 Car L-4 Instalaciones de Respaldo P-1 Usuarios Externos P-2 Administradores de Sistemas P-3 Desarrolladores/Programadores
2	SG-002	Extintores	$ 500.00	HW-1 Grandes Equipos HW-2 Informática personal HW-3 Medios de Impresión HW-4 Centralita telefónica COM-1 Red Telefónica COM-2 Red Inalámbrica COM-3 Red Local COM-4 Internet Media-1 Discos Media-2 Almacenamiento en Red Media-3 Memorias USB Media-4 Material Impreso AUX-1 Sistemas de Alimentación Ininterrumpida AUX-2 Cableado AUX-3 Cable Eléctrico AUX-4 Equipos de Destrucción de Soportes de Información L-1 Edificio L-2 Cuarto

				L-3 Car L-4 Instalaciones de Respaldo
3	SG-003	Realizar simulacros de forma periódica	$ 200.00	HW-1 Grandes equipos HW-2 Informática personal HW-3 Medios de Impresión HW-4 Centralita telefónica COM-1 Red Telefónica COM-2 Red Inalámbrica COM-3 Red Local COM-4 Internet Media-1 Discos Media-2 Almacenamiento en Red Media-3 Memorias USB Media-4 Material Impreso AUX-1 Sistemas de Alimentación Ininterrumpida AUX-2 Cableado AUX-3 Cable Eléctrico AUX-4 Equipos de Destrucción de Soportes de Información L-1 Edificio L-2 Cuarto L-3 Car L-4 Instalaciones de Respaldo P-1 Usuarios Externos P-2 Administradores de Sistemas P-3 Desarrolladores/Programadores P-4 Proveedores
4	SG-004	Claves de activa/desact. Sistema de alarma	$ 300.00	HW-1 Grandes equipos HW-2 Informática personal HW-3 Medios de Impresión HW-4 Centralita telefónica Media-1 Discos Media-3 Memorias USB L-1 Edificio L-2 Cuarto L-4 Instalaciones de Respaldo
5	SG-005	Contratos de confidencialidad de plantilla	$ 1,000.00	D-1 Ficheros D-2 Copias de Respaldo D-3 Credenciales D-4 Código fuente S-1 Interno (a usuarios de la propia organización) S-2 World wide web S-3 Acceso remoto a cuenta local S-4 Gestión de Privilegios SW-1 Desarrollo propio SW-2 Desarrollo a medida SW-3 Servidor de correo electrónico SW-4 Sistema de gestión de Base de Datos

6	SG-006	Formación del personal en seguridad	$ 10,000.00	D-1 Ficheros D-2 Copias de Respaldo D-3 Credenciales D-4 Código fuente S-1 Interno (a usuarios de la propia organización) S-2 World wide web S-3 Acceso remoto a cuenta local S-4 Gestión de Privilegios SW-1 Desarrollo propio SW-2 Desarrollo a medida SW-3 Servidor de correo electrónico SW-4 Sistema de gestión de Base de Datos COM-2 Red Inalámbrica COM-3 Red Local Media-1 Discos Media-2 Almacenamiento en Red Media-3 Memorias USB Media-4 Material Impreso P-2 Administradores de Sistemas P-3 Desarrolladores/Programadores
7	SG-007	Mantenimiento de la fotocopiadora	$ 300.00	HW-3 Medios de Impresión Media-4 Material Impreso P-1 Usuarios Externos P-4 Proveedores
8	SG-008	Mantenimiento de la climatización	$ 200.00	HW-1 Grandes equipos COM-4 Internet L-4 Instalaciones de Respaldo P-1 Usuarios Externos
9	SG-009	Mantenimiento preventivo del servidor	$ 500.00	D-1 Ficheros D-2 Copias de Respaldo D-3 Credenciales D-4 Código fuente S-1 Interno (a usuarios de la propia organización) S-2 World wide web S-3 Acceso remoto a cuenta local S-4 Gestión de Privilegios SW-1 Desarrollo propio SW-2 Desarrollo a medida SW-3 Servidor de correo electrónico SW-4 Sistema de gestión de Base de Datos
10	SG-010	Llaves de la puerta principal y de emergencia	$ 150.00	HW-1 Grandes equipos HW-2 Informática personal HW-3 Medios de Impresión HW-4 Centralita telefónica Media-1 Discos Media-3 Memorias USB Media-4 Material Impreso AUX-1 Sistemas de Alimentación Ininterrumpida AUX-4 Equipos de Destrucción de Soportes de Información

				L-1 Edificio L-2 Cuarto L-3 Car L-4 Instalaciones de Respaldo P-1 Usuarios Externos P-2 Administradores de Sistemas P-3 Desarrolladores/Programadores P-4 Proveedores
11	SG-011	Llaves del armario del director técnico	$ 5.00	D-1 Ficheros D-2 Copias de Respaldo D-3 Credenciales D-4 Código fuente HW-2 Informática personal Media-1 Discos Media-2 Almacenamiento en Red Media-3 Memorias USB Media-4 Material Impreso
12	SG-012	Contratos de confidencialidad de colaboradores	$ 100.00	D-1 Ficheros D-2 Copias de Respaldo D-3 Credenciales D-4 Código fuente S-1 Interno (a usuarios de la propia organización) S-2 World wide web S-3 Acceso remoto a cuenta local S-4 Gestión de Privilegios SW-1 Desarrollo propio SW-2 Desarrollo a medida SW-3 Servidor de correo electrónico SW-4 Sistema de gestión de Base de Datos COM-2 Red Inalámbrica COM-3 Red Local Media-1 Discos Media-3 Memorias USB Media-4 Material Impreso P-1 Usuarios Externos P-4 Proveedores
13	SG-013	Llaves del armario del Resp. Software	$ 5.00	D-1 Ficheros D-2 Copias de Respaldo D-3 Credenciales D-4 Código fuente SW-1 Desarrollo propio SW-2 Desarrollo a medida SW-3 Servidor de correo electrónico SW-4 Sistema de gestión de Base de Datos HW-2 Informática personal Media-1 Discos Media-3 Memorias USB Media-4 Material Impreso COM-2 Red Inalámbrica COM-3 Red Local

14	SG-014	Firewall 1	$ 3,000.00	D-1 Ficheros D-2 Copias de Respaldo D-3 Credenciales D-4 Código fuente S-2 World wide web S-3 Acceso remoto a cuenta local SW-1 Desarrollo propio SW-2 Desarrollo a medida SW-3 Servidor de correo electrónico SW-4 Sistema de gestión de Base de Datos
15	SG-015	Destructora de papel	$ 200.00	Media-4 Material Impreso P-1 Usuarios Externos P-2 Administradores de Sistemas P-3 Desarrolladores/Programadores P-4 Proveedores
16	SG-016	UPS 1	$ 1,200.00	HW-1 Grandes equipos HW-4 Centralita telefónica
17	SG-017	UPS 2	$ 1,200.00	HW-2 Informática personal COM-2 Red Inalámbrica COM-3 Red Local COM-4 Internet
18	SG-018	Mantenimiento anual de UPS	$ 500.00	HW-1 Grandes equipos HW-4 Centralita telefónica HW-2 Informática personal COM-2 Red Inalámbrica COM-3 Red Local COM-4 Internet
19	SG-019	Copias de seguridad de datos	$ 2,000.00	D-1 Ficheros D-2 Copias de Respaldo D-4 Código fuente SW-1 Desarrollo propio SW-2 Desarrollo a medida SW-3 Servidor de correo electrónico SW-4 Sistema de gestión de Base de Datos Media-1 Discos Media-2 Almacenamiento en Red Media-3 Memorias USB
20	SG-020	Servicio externo de copias de seguridad	$ 3,000.00	D-1 Ficheros D-2 Copias de Respaldo SW-3 Servidor de correo electrónico SW-4 Sistema de gestión de Base de Datos
21	SG-021	Antivirus	$ 500.00	D-1 Ficheros D-2 Copias de Respaldo D-3 Credenciales D-4 Código fuente SW-1 Desarrollo propio SW-2 Desarrollo a medida SW-3 Servidor de correo electrónico

				SW-4 Sistema de gestión de Base de Datos Media-1 Discos Media-2 Almacenamiento en Red Media-3 Memorias USB
22	SG-022	Actualizar periódicamente las firmas del antivirus	$ 100.00	D-1 Ficheros D-2 Copias de Respaldo D-3 Credenciales D-4 Código fuente SW-1 Desarrollo propio SW-2 Desarrollo a medida SW-3 Servidor de correo electrónico SW-4 Sistema de gestión de Base de Datos Media-1 Discos Media-2 Almacenamiento en Red Media-3 Memorias USB
23	SG-023	Instalación de antimalware	$ 500.00	D-1 Ficheros D-2 Copias de Respaldo D-3 Credenciales D-4 Código fuente SW-1 Desarrollo propio SW-2 Desarrollo a medida SW-3 Servidor de correo electrónico SW-4 Sistema de gestión de Base de Datos Media-1 Discos Media-2 Almacenamiento en Red Media-3 Memorias USB P-2 Administradores de Sistemas P-3 Desarrolladores/Programadores
24	SG-024	Software copias seguridad	$ 500.00	D-1 Ficheros D-2 Copias de Respaldo D-3 Credenciales D-4 Código fuente SW-1 Desarrollo propio SW-2 Desarrollo a medida SW-3 Servidor de correo electrónico SW-4 Sistema de gestión de Base de Datos Media-1 Discos Media-2 Almacenamiento en Red Media-3 Memorias USB
25	SG-025	Monitoreo de recursos de los equipos críticos	$ 50.00	D-1 Ficheros D-2 Copias de Respaldo D-3 Credenciales D-4 Código fuente S-1 Interno (a usuarios de la propia organización) S-2 World wide web S-3 Acceso remoto a cuenta local S-4 Gestión de Privilegios SW-3 Servidor de correo electrónico SW-4 Sistema de gestión de Base de Datos

26	SG-026	Realizar pruebas de actualizaciones previo a la instalación	$ 200.00	SW-1 Desarrollo propio SW-2 Desarrollo a medida SW-3 Servidor de correo electrónico SW-4 Sistema de gestión de Base de Datos
27	SG-027	Pruebas periódicas del firewall	$ 50.00	D-1 Ficheros D-2 Copias de Respaldo D-3 Credenciales D-4 Código fuente S-1 Interno (a usuarios de la propia organización) S-2 World wide web S-3 Acceso remoto a cuenta local S-4 Gestión de Privilegios SW-1 Desarrollo propio SW-2 Desarrollo a medida SW-3 Servidor de correo electrónico SW-4 Sistema de gestión de Base de Datos
28	SG-028	Utilizar autenticación multifactor para conexión remota	$ 50.00	D-3 Credenciales S-3 Acceso remoto a cuenta local S-4 Gestión de Privilegios SW-3 Servidor de correo electrónico SW-4 Sistema de gestión de Base de Datos
29	SG-029	Implementar directivas de contraseñas complejas	$ 100.00	D-1 Ficheros D-2 Copias de Respaldo D-3 Credenciales D-4 Código fuente S-1 Interno (a usuarios de la propia organización) S-3 Acceso remoto a cuenta local S-4 Gestión de Privilegios SW-3 Servidor de correo electrónico SW-4 Sistema de gestión de Base de Datos COM-2 Red Inalámbrica COM-3 Red Local
30	SG-030	Implementar controles avanzados de gestión de cuentas	$ 100.00	D-3 Credenciales S-1 Interno (a usuarios de la propia organización) S-2 World wide web S-3 Acceso remoto a cuenta local S-4 Gestión de Privilegios SW-3 Servidor de correo electrónico SW-4 Sistema de gestión de Base de Datos COM-2 Red Inalámbrica COM-3 Red Local
31	SG-031	Implementar cifrado de datos	$ 150.00	D-1 Ficheros D-2 Copias de Respaldo D-3 Credenciales Media-1 Discos Media-2 Almacenamiento en Red Media-3 Memorias USB

32	SG-032	Contratar personal responsable de la seguridad	$	800.00	D-1 Ficheros D-2 Copias de Respaldo D-3 Credenciales D-4 Código fuente S-1 Interno (a usuarios de la propia organización) S-2 World wide web S-3 Acceso remoto a cuenta local S-4 Gestión de Privilegios SW-1 Desarrollo propio SW-2 Desarrollo a medida SW-3 Servidor de correo electrónico SW-4 Sistema de gestión de Base de Datos COM-1 Red Telefónica COM-2 Red Inalámbrica COM-3 Red Local COM-4 Internet Media-1 Discos Media-2 Almacenamiento en Red Media-3 Memorias USB Media-4 Material Impreso L-1 Edificio L-2 Cuarto L-4 Instalaciones de Respaldo P-1 Usuarios Externos P-4 Proveedores
33	SG-033	Dar charlas al personal referente a la seguridad	$	200.00	D-1 Ficheros D-2 Copias de Respaldo D-3 Credenciales D-4 Código fuente S-1 Interno (a usuarios de la propia organización) S-2 World wide web S-3 Acceso remoto a cuenta local S-4 Gestión de Privilegios SW-1 Desarrollo propio SW-2 Desarrollo a medida SW-3 Servidor de correo electrónico SW-4 Sistema de gestión de Base de Datos COM-2 Red Inalámbrica COM-3 Red Local COM-4 Internet Media-1 Discos Media-2 Almacenamiento en Red Media-3 Memorias USB Media-4 Material Impreso L-1 Edificio L-2 Cuarto L-4 Instalaciones de Respaldo P-1 Usuarios Externos P-4 Proveedores

34	SG-034	Control de acceso	$ 250.00	D-1 Ficheros D-2 Copias de Respaldo D-3 Credenciales D-4 Código fuente S-1 Interno (a usuarios de la propia organización) S-2 World wide web S-3 Acceso remoto a cuenta local S-4 Gestión de Privilegios HW-1 Grandes Equipos HW-2 Informática personal HW-3 Medios de Impresión HW-4 Centralita telefónica COM-2 Red Inalámbrica COM-3 Red Local L-1 Edificio L-2 Cuarto L-4 Instalaciones de Respaldo
35	SG-035	Implementación de sistema de detección de intrusos	$ 2,500.00	HW-1 Grandes equipos HW-2 Informática personal HW-3 Medios de Impresión HW-4 Centralita telefónica COM-1 Red Telefónica COM-2 Red Inalámbrica COM-3 Red Local COM-4 Internet Media-1 Discos Media-3 Memorias USB Media-4 Material Impreso AUX-1 Sistemas de Alimentación Ininterrumpida AUX-4 Equipos de Destrucción de Soportes de Información L-1 Edificio L-2 Cuarto L-3 Car L-4 Instalaciones de Respaldo
36	SG-036	Uso de cables de seguridad para computadores de personal y portátiles	$ 500.00	HW-2 Informática personal Media-1 Discos

Fuente: El autor.

Se presentará a continuación en la Tabla XXIII una lista detallada de los activos de información y su estado después de aplicar las salvaguardas correspondientes, junto con la conclusión sobre el estado final de cada activo.

TABLA XXIII. ESTADO DE LOS ACTIVOS DESPUÉS DE LA APLICACIÓN DE SALVAGUARDAS.

ITEM	Código	Descripción		CONCLUSIÓN
[D] Datos/Información				
1	D-1	Ficheros	El riesgo se reduce considerablemente, manteniéndose en la misma franja.	En el presente proyecto se hace referencia a la importancia del activo ficheros en el contexto de la empresa, aunque este activo es de gran relevancia para el desarrollo de las actividades empresariales, se le asignó una valoración media, lo que significa que su impacto en la organización sería relativamente menor. Sin embargo, es importante destacar que antes de la implementación de las salvaguardas descritas en este documento, la empresa ya contaba con medidas para proteger este activo de posibles amenazas externas. Por ejemplo, se implementó un firewall que permite controlar el tráfico en la red de la empresa. De esta manera, se logra una mayor protección de los archivos, lo que reduce el riesgo de pérdida o robo de información empresarial. Cabe mencionar que estas medidas de seguridad se suman a las que ya existían previamente, lo que refleja el compromiso de la empresa por proteger sus activos y mantener la integridad de su información.
2	D-2	Copias de Respaldo	Disminuye el riesgo.	Después de aplicar medidas para proteger este activo, el cual es de suma importancia para la empresa podemos concluir se ha obtenido resultados favorables, ya que después de aplicadas las medidas podemos ver que el riesgo ha disminuido, aunque la inversión necesaria para la implementación es costosa, pero tendríamos que verlo como una inversión de retorno en el tiempo a mediano plazo.
3	D-3	Credenciales	El riesgo se reduce muy poco, manteniéndose en la misma franja.	En el activo de Credenciales hemos aplicado medidas que pueden reducir el riesgo en el caso de ser implementadas, se ha logrado mejorar en gran medida el riesgo de afectación, después de añadida la medidas de protección se ha logrado obtener los resultados esperados y favorables satisfaciendo las expectativas, ya que este activo no solo depende de la tecnología, sino que tiene como pilar fundamental el recurso humano que es muy difícil de controlar, lo que podemos hacer es crear un plan de concientización y capacitación donde se pueda mejorar mucho más la seguridad de este activo.
4	D-4	Código fuente	Disminuye el riesgo.	Como en el caso del activo Credenciales, la tecnología y las medidas de protección que en el activo Código fuente se implementen mejoraría mucho el riesgo de sufrir un ataque y por lo tanto disminuiría significativamente la posibilidad de verse afectada la organización en el caso de tener un ataque que pueda provocar daños al software y hardware de la empresa. En nuestro análisis utilizando la Metodología MAGERIT, se puede traducir las cifras económicas que tienen como fin dar a conocer la capacidad de afectación que

				pudiera darse en el caso de que se vea vulnerada la seguridad del activo.
[S] Servicios				
5	S-1	Interno (a usuarios de la propia organización)	Riesgo se mantiene dentro los parámetros establecidos como aceptable por la empresa.	Con la implementación de salvaguardas se ha mejorado en algo la afectación del activo Interno, cabe mencionar que este activo tiene que ver mucho con la cultura institucional sobre el tema de protección de la información principalmente del área administrativa de la organización, de acuerdo a la información recolectada se puede evidenciar que en cierta medida los procesos básicos se cumplen en el tema de protección de datos sensibles para la empresa y también tiene una valoración baja, es así por lo que este activo no se ve en gravedad vulnerable, pero siempre puede ser víctima potencial en un ataque informático.
6	S-2	World wide web	Riesgo se mantiene dentro los parámetros establecidos como aceptable por la empresa.	Desde un principio, este activo se encontraba dentro de los parámetros de aceptación de riesgo de la organización. Sin embargo, con la implementación de las salvaguardas descritas en este trabajo, se ha mejorado significativamente el riesgo al que se expone este activo. Es importante destacar que uno de los principales puntos de acceso para los hackers es a través de la recolección de información de datos, aprovechando las vulnerabilidades que pueden encontrarse en los entornos web. Por lo tanto, siempre será crucial mantener un cuidado especial en este tipo de activos, asegurándose de brindar el mantenimiento, revisión e inspección adecuadas. De esta manera, se puede reducir el riesgo de posibles vulnerabilidades y ataques cibernéticos que puedan poner en peligro la integridad de la información empresarial. Cabe mencionar que la implementación de medidas de seguridad no garantiza una protección total, por lo que es importante mantener una constante evaluación y actualización de las salvaguardas para mantener una postura defensiva adecuada frente a posibles amenazas.
7	S-3	Acceso remoto a cuenta local	El riesgo se reduce de manera significativa pasando de activo considerado de riesgo a la franja de los activos dentro del riesgo aceptable por la empresa.	Este activo es uno de los cuales se tiene que tener especial cuidado, esta observación se la realizó desde el inicio del presente trabajo, ya que se lo clasificó con una valoración de riesgo Alto, esto debido a la importancia que tiene cualquier tipo acceso a las cuentas locales de la organización, ya sea una cuenta de usuarios con privilegios simples o como de un administrador donde la seguridad de los datos de la información se puede ver seriamente comprometida, después de las salvaguardas propuestas se puede observar una disminución en el riesgo de sufrir una afectación a este activo.

8	S-4	Gestión de Privilegios	El riesgo se reduce de manera significativa pasando de activo considerado de riesgo a la franja de los activos dentro del riesgo aceptable por la empresa.	Como en el caso anterior del activo Acceso remoto a cuenta local, este activo Gestión de Privilegios es uno de los cuales se tiene que tener especial cuidado, esta observación se la realizó desde el inicio del presente trabajo, ya que se lo clasificó dándole una valoración de riesgo Alto, por la razón de que tiene mucha importancia la gestión de privilegios de los usuarios a los sistemas que se manejan dentro de la empresa, las configuraciones de una cuenta pueden ir desde un usuario con permisos simples hasta la de un usuario con permisos de administrador, según la configuración de cuenta se puede tener la capacidad de realizar ingresos, modificaciones y hasta la eliminación de los datos, por lo que la falta de medidas de seguridad en la gestión de los privilegios puede comprometer seriamente la información, por lo que es importante la implementación de salvaguardas para obtener una disminución en el riesgo de sufrir una afectación a este activo.
[SW] Software-Aplicaciones Informáticas				
9	SW-1	Desarrollo propio	Disminuye el riesgo.	Este activo tiene una valoración de índice medio, la afectación puede ser aceptada por la organización ya que el giro de negocio no es la producción de software por lo que en el caso de sufrir una alteración debido a un agente externo no se comprometería en gran medida el flujo de actividades de la empresa y se puede trabajar con normalidad hasta solventar el inconveniente, pero no por eso podemos dejar a un lado la puesta en marcha de una planificación que tome las medidas necesarias para que este activo en un futuro tenga un buen escudo que lo proteja de actividades maliciosas externas.
10	SW-2	Desarrollo a medida	El riesgo se reduce de manera significativa pasando de activo considerado de riesgo a la franja de los activos dentro del riesgo aceptable por la empresa.	Este activo ha mejorado su capacidad para resistir ataques en caso de presentarse vulnerabilidades. Es importante destacar que este activo no es una aplicación que se encuentra en desarrollo por parte del departamento encargado, sino que depende de un tercero para su desarrollo. Por lo tanto, es fundamental que este tercero haya aplicado normativas y esté direccionado a proteger la confidencialidad, integridad y seguridad en el manejo de la información. Es aún mejor si ha implementado un Sistema de Gestión de Seguridad de Información (SGSI) o cumple con políticas básicas de seguridad de la información. De esta manera, se puede tener mayor confianza en la capacidad de este activo para resistir posibles ataques. Sin embargo, es importante recordar que ninguna medida de seguridad es infalible y siempre existe el riesgo de posibles vulnerabilidades y ataques cibernéticos. Por lo tanto, es crucial mantener una constante evaluación y actualización de las salvaguardas para garantizar una postura defensiva adecuada frente a posibles amenazas.

11	SW-3	Servidor de correo electrónico	Disminuye el riesgo.	Al tener implementado el servidor de correo electrónico en un equipo propio y físicamente dentro de la organización permite tener un mayor control de la configuración de este activo, así como la implementación de protecciones que permiten mitigar posibles amenazas que pueda sufrir, una de ellas es la inversión en un firewall que ha hecho que el servidor de correo electrónico no se vea comprometido de manera grave, además se ha solicitado a los usuarios mucha responsabilidad en el manejo de sus cuentas de mail y que cualquier inconveniente que se presente sea informado a la brevedad posible al personal encargado de la administración del servidor para que se tomen los correctivos necesarios de la manera más inmediata y poder evitar así alteraciones en esta infraestructura de mucha importancia en el desarrollo de las actividades de la organización.
12	SW-4	Sistema de gestión de Base de Datos	Disminuye el riesgo.	Como ocurre con el activo de Desarrollo Propio, este activo tiene una valoración de índice medio, la afectación puede ser aceptada por la organización, se mantiene un respaldo de la base de datos que periódicamente se saca en discos físicos, también se ha contratado un servicio de almacenamiento de datos en la nube lo que le permite a la organización mantener un respaldo de la información más importante, lo que permite volver a la empresa a sus actividades normales en el caso de verse afectada o comprometida la información que esta necesita para que sus colaboradores realicen sus actividades, logrando de esta manera que se pueda regresar a la normalidad del trabajo hasta solventar el inconveniente por parte del personal encargado del área de desarrollo, de igual manera no podemos dejar a un lado la puesta en marcha de una planificación que tome las medidas necesarias para que este activo se mantenga dentro de la franja de aceptación de riesgos y que en un futuro tenga un mejor escudo que lo proteja de actividades maliciosas externas.
[HW] Equipamiento Informático				
13	HW-1	Grandes equipos	El riesgo se reduce de manera significativa pasando de activo considerado de riesgo a la franja de los activos dentro del riesgo aceptable por la empresa.	Después de realizar un análisis de amenazas en el activo de Grandes Equipos, se ha demostrado que la implementación de la infraestructura adecuada y después de indicar que la aplicación de normativas de seguridad que se alinean al funcionamiento de este activo, el cual es parte fundamental en el correcto desenvolvimiento de la empresa por mantener los sistemas informáticos casi indispensables para llevar a cabo todas las transacciones económicas así como el tratamiento de datos de los clientes, ha obtenido un mejoramiento significativo en cuanto a la protección de la información, pero aun así se puede mejorar mucho más, para llevar a cabo este propósito se necesita de mayor inversión, algo que en este momento se dificulta pero que un futuro con el crecimiento de la empresa se puede llegar a

				realizar, y de esta manera tener un sistema de protección robusto.
14	HW-2	Informática personal	Disminuye el riesgo.	En este punto de debe describir el papel del departamento de desarrollo de la empresa en relación con la informática personal. Este departamento es responsable de proporcionar soporte durante la puesta en marcha y configuración de los diferentes equipos de cómputo utilizados por los colaboradores de la empresa. Además, es el encargado de adquirir, instalar y repotenciar los equipos necesarios para realizar las diferentes labores, tomando en cuenta el uso que se les dará. También implementa las medidas de seguridad necesarias para proteger la información que se procesará en estos equipos. Es importante destacar que el departamento de desarrollo debe asegurarse de que todos los equipos estén actualizados y cuenten con las últimas medidas de seguridad para garantizar la protección adecuada de la información de la empresa. Además, debe estar disponible para brindar soporte técnico y resolver cualquier problema que surja durante el uso de los equipos de cómputo. En resumen, el departamento de desarrollo de la empresa es un elemento clave en la gestión de la informática personal y debe asegurarse de proporcionar los equipos adecuados y las medidas de seguridad necesarias para proteger la información de la empresa y garantizar el correcto funcionamiento de los equipos.
15	HW-3	Medios de Impresión	Disminuye el riesgo.	Dentro de la organización se lleva a cabo una política de imprimir lo menos posible la documentación, y también de reciclar el papel, a parte cabe indicar que no se da tratamiento a información sensible utilizando este medio impreso, con la innovación tecnológica y utilizando nuevas herramientas informáticas se ha disminuido la utilización de estos activos, además al inicio del estudio de este caso se le dio una valoración baja y mediante la implementación de las salvaguardas se ha disminuido más el riesgo en la utilización de este activo.
16	HW-4	Centralita telefónica	Disminuye el riesgo.	Estar siempre comunicados es muy importante dentro de la actividad que desarrolla la empresa, por esta razón se cuenta con una central telefónica que es la encargada de direccionar las llamadas de los clientes a los diferentes departamentos facilitando enormemente las comunicaciones, es muy importante que este activo siempre permanezca operativo, pero en el caso de que suceda una afectación por algún tipo de vulnerabilidad, se puede hacer uso de la telefonía móvil con la que cada uno de los colaboradores cuenta, ayudando a que la afectación no sea de gravedad por no contar con este activo, es por este motivo que se le ha asignado con una valoración baja, aun así se han implementado salvaguardas que ayudan a proteger la integridad del bien disminuyendo el riesgo.

[COM] Redes de Comunicaciones				
17	COM-1	Red Telefónica	Disminuye el riesgo.	A continuación, se destaca la importancia de mantener en buen estado la infraestructura de comunicaciones dentro de la empresa. Desde la instalación de la central telefónica y las líneas en cada departamento, se ha logrado mantener una red de comunicación en muy buen estado, lo que garantiza que las comunicaciones de la organización siempre estén operativas. Como resultado, se ha asignado una valoración de riesgo baja a este activo. Es fundamental para el correcto funcionamiento de la empresa que la infraestructura de comunicaciones se mantenga en buen estado, ya que es a través de ella que se establecen las comunicaciones internas y externas. El mantenimiento regular de la infraestructura de comunicaciones garantiza la disponibilidad de los sistemas de comunicación y evita interrupciones en el servicio que pueden afectar el funcionamiento de la organización. Además, se debe prestar atención a la seguridad de la infraestructura de comunicaciones para evitar posibles amenazas externas, ya que el acceso no autorizado a la red puede resultar en la pérdida o el robo de información confidencial de la empresa. En conclusión, es fundamental para la empresa mantener la infraestructura de comunicaciones en buen estado para garantizar la disponibilidad de los sistemas de comunicación y la operación adecuada de la organización. Es importante prestar atención a la seguridad de la infraestructura de comunicaciones para evitar posibles amenazas externas y asegurar la protección de la información confidencial de la empresa.
18	COM-2	Red Inalámbrica	Disminuye el riesgo.	La red inalámbrica de la empresa se encuentra bajo la supervisión del departamento de desarrollo, quienes son los encargados de levantar la señal de internet en cada una de las áreas, así como de llevar a cabo la activación de los parámetros de seguridad necesarios para mantener protegida la información de la empresa, es importante indicar que las redes inalámbricas es uno de los activos más deseados por los atacantes para realizar el ingreso a la infraestructura de la organización y poder lograr su único propósito que es conseguir un beneficio propio.
19	COM-3	Red Local	Disminuye el riesgo.	La red local de la empresa se encuentra bajo la supervisión del departamento de desarrollo, y así como con el activo anterior se le dio una valoración baja, el departamento de desarrollo también es el encargado de levantar la red en cada una de las áreas para lo cual brinda el respectivo soporte de atención al usuario de la red local, también son ellos los responsables de llevar a cabo la activación de los parámetros de seguridad necesarios para mantener protegida la información de la empresa, es importante indicar que la red local de cualquier organización es uno de los activos más deseados por los atacantes para realizar el ingreso a la

				infraestructura de la organización y poder lograr su único propósito que es conseguir un beneficio propio.
20	COM-4	Internet	El riesgo se reduce de manera significativa pasando de activo considerado de riesgo a la franja de los activos dentro del riesgo aceptable por la empresa.	En el inicio de la revisión del caso de estudio se pudo observar que este activo tiene una valoración considerable, por lo cual se cree conveniente la implementación de diferentes salvaguardas que ayuden a bajar el valor del riesgo, tomando en cuenta todas las acciones, se logra como resultado disminuir el riesgo para que este activo ingrese a la franja de valores que son considerados como aceptables, pero se debe recordar que en el caso que suceda una afectación al bien Internet las protecciones implementadas harán su trabajo, que es el de mantener siempre la señal de internet operativa.
[Media] Soportes de Información				
21	Media-1	Discos	Disminuye el riesgo.	Este es un activo de valoración baja, se ha determinado de esta manera ya que poco a poco se está dejando de usar, aunque todavía se utiliza para almacenar documentación del área administrativa por lo que es importante manejar este activo físico de manera responsable para proteger la información, este medio puede ser utilizado por una persona con la capacidad de planificar un ataque a la infraestructura tecnológica de la empresa con ayuda de alguna información que pueda encontrar en este medio de almacenamiento.
22	Media-2	Almacenamiento en Red	El riesgo se reduce de manera significativa pasando de activo considerado de riesgo a la franja de los activos dentro del riesgo aceptable por la empresa.	La preocupación por la seguridad de la información almacenada en el servidor, incluyendo datos de transacciones financieras con los clientes, información de los clientes y otra información crítica para el flujo de las actividades comerciales de la empresa, ha llevado a la gerencia y al departamento de desarrollo a tomar medidas proactivas. Entre ellas, se ha contratado un proveedor de servicios de almacenamiento de datos en la nube, lo que ha aumentado el nivel de confianza en cuanto a la disponibilidad y seguridad de los datos. Además, se han sugerido varias salvaguardas para disminuir el riesgo al que se expone este activo. En resumen, se han tomado medidas importantes para proteger la información crítica de la empresa y minimizar los riesgos asociados con su almacenamiento y tratamiento.
23	Media-3	Memorias USB	Disminuye el riesgo.	Este es un activo de valoración baja, se utiliza para almacenar documentación del área administrativa, área técnica y de logística por lo que es importante manejar este activo físico de manera responsable para proteger la información, ya que este medio puede ser utilizado por una persona con la capacidad de planificar un ataque a la infraestructura tecnológica de la empresa con ayuda de alguna información que pueda encontrar en este tipo de medio de almacenamiento, implementando las salvaguardas propuestas, este

				bien se ha convertido en uno de los activos más seguros dentro de la organización.
24	Media-4	Material Impreso	Disminuye el riesgo.	Dentro de la organización se lleva a cabo una política de imprimir lo menos posible la documentación, y también de reciclar el papel, a parte cabe indicar que no se da tratamiento a información sensible utilizando este medio, con la utilización de nuevas herramientas de comunicación y del avance de las tecnologías informáticas se ha disminuido la utilización de este activo, cabe indicar que al inicio del estudio de este caso se le dio una valoración baja y mediante la implementación de las salvaguardas se ha disminuido aún más el riesgo de estar expuesto a algún tipo de ataque.
[AUX] Equipamiento Auxiliar				
25	AUX-1	Sistemas de Alimentación Ininterrumpida	Disminuye el riesgo.	Este activo se encuentra dentro de la franja de riesgo aceptable por la organización, pero si es importante indicar que mientras el valor del riesgo vaya disminuyendo debido a la implementación de diferentes salvaguardas es mucho mejor, lo que se busca es que con ayuda de este activo los otros activos que dependen de manera directa sufran lo menos posible la falta de energía eléctrica lo que podría dejar inhabilitadas las actividades de la empresa. También lo que se pretende es cuidar la integridad de los bienes y la inversión realizada en la adquisición de equipos.
26	AUX-2	Cableado	Disminuye el riesgo.	Es importante mantener en buen estado el cableado dentro de la infraestructura de la empresa, esto se ha revisado y en ocasiones se ha reemplazado el cableado original, esto ha servido como medida para determinar que la red de comunicación se encuentra en muy buen estado, lo que permite brindar la garantía en las comunicaciones de la organización para que se mantengan siempre operativas. Cabe mencionar que este activo se encuentra en una valoración de riesgo baja.
27	AUX-3	Cable Eléctrico	Disminuye el riesgo.	Aunque pueda parecer que la energía eléctrica es un activo de baja valoración, en realidad es de gran importancia para el correcto funcionamiento de los equipos que procesan, almacenan y distribuyen la información necesaria para las actividades de la organización. Por lo tanto, es crucial que la infraestructura de tendido eléctrico se encuentre en óptimas condiciones para garantizar la disponibilidad y continuidad de los servicios que dependen de ella. De esta manera, se asegura que los equipos puedan operar sin interrupciones y se evita cualquier posible pérdida de datos e información crítica para el negocio. En definitiva, aunque este activo pueda tener una valoración baja, su importancia es vital para el funcionamiento de la organización.

28	AUX-4	Equipos de Destrucción de Soportes de Información	Disminuye el riesgo.	Uno de los principales objetivos de los atacantes es obtener información por todos los medios posibles, una de las maneras menos pensadas es el buscar dentro de lo desechado como basura, que en ocasiones puede ser material impreso, discos duros, memorias USB dañadas, etc. Estas pueden convertirse en fuente de información de mucho valor para los atacantes, que al utilizar diferentes técnicas pueden procesar estos datos y obtener por ejemplo claves que les permitan ingresar al sistema de la organización y poder de manera fácil y rápida efectuar daños en la información almacenada, o también robar datos de vital importancia que luego pueden ser utilizados para un ataque a mayor escala.
[L] Instalaciones				
29	L-1	Edificio	Disminuye el riesgo.	El cuidar de la infraestructura de la empresa ayuda a proteger los demás activos, el tener un sistema contra incendio cuida que no sufran daños los activos físicos de mucha importancia para el funcionamiento de la empresa, así como cuidar el perímetro del edificio al implementar un sistema de alarma para evitar pérdidas por robo que pueden causar grandes afectaciones económicas. La aplicación de normas de seguridad para proteger la integridad del edificio ha demostrado una mejora significativa, siendo una inversión con retorno al mediano plazo.
30	L-2	Cuarto	Disminuye el riesgo.	La seguridad física del perímetro de la organización y también de cada una de las oficinas es muy importante para proteger los activos de algunas amenazas como robo, daño, o incluso la instalación de software malicioso, se debe considerar que ciertos equipos informáticos deben trabajar en un entorno controlado de humedad y temperatura, específicamente en el rack donde se encuentra el servidor, de esta manera se puede asegurar el correcto funcionamiento de este activo, la implementación de salvaguardas reduce el riesgo de que sufra falla que pueda comprometer el desarrollo de las actividades de la empresa.
31	L-3	Car	Disminuye el riesgo.	La distribución de mercadería es una parte fundamental del negocio de la empresa y, por lo tanto, es esencial contar con un activo que permita llevar a cabo esta tarea de manera eficiente. Aunque se ha evaluado este activo con un nivel de riesgo bajo porque se entiende que un posible daño o robo del bien no tendría un impacto significativo en la seguridad de la información dentro de la organización.

32	L-4	Instalaciones de Respaldo	Disminuye el riesgo.	El contar con un respaldo de equipos o de una instalación que albergue la infraestructura tecnológica es muy importante dentro de la continuidad del negocio, puesto que en el caso de que una vulnerabilidad informática haya sido explotada o de que se haya presentado afectaciones a las instalaciones físicas ya sean estas provocadas intencionalmente o que se hayan presentado de una manera circunstancial, el mantener una unidad de respaldo puede ayudar mucho a la continuidad del negocio, se lo ha calificado como un activo de riesgo de valor bajo ya que en este momento la empresa cuenta con respaldo en la nube de la información más importante y protege en gran medida que no se paralice la actividad del negocio.
[P] Personal				
33	P-1	Usuarios Externos	El riesgo se reduce de manera significativa pasando de activo considerado de riesgo a la franja de los activos dentro del riesgo aceptable por la empresa.	Una de las búsquedas más importantes para toda organización es la mejora continua en los procesos para agilizar el movimiento de mercadería y facilitar las transacciones cliente-empresa, para llevar a cabo esta mejora es necesario la implementación de infraestructura, software, así como el cuidado y protección de los datos, información importante en cada uno de los procesos, después de determinar cuáles serían las mejores soluciones que podemos implementar, se puede sacar la conclusión de que existe una mejora considerable de los procesos al permitir que el cliente tenga mayor interacción en la adquisición de sus productos mediante la utilización de aplicaciones web en una tienda electrónica que se ha implementado de manera reciente en el portal de la empresa, una de las desventajas que se puede añadir al proceso es que los controles de los datos que se ingresan no son validados como correctos y que en ocasiones pueden ser falseados creando usuarios fantasmas. También se ha visto la necesidad de implementar salvaguardas que permitan proteger la integridad de la información ya que este acceso a los clientes puede permitir también a los atacantes el ingreso al sistema, y cuya misión es afectar la infraestructura de la organización.
34	P-2	Administradores de Sistemas	Disminuye el riesgo.	El personal encargado del sistema informático, debe mantener una comunicación fluida de datos, ellos son los encargados de que los diferentes sistemas tecnológicos se encuentren operativos para que los procesos se lleven a cabo de manera satisfactoria y sin inconveniente alguno entregando los resultados en el tiempo que se necesitan y con los recursos que se cuenta dentro de lo considerado como normal y de lo posible mejorando el flujo del proceso, por esto ellos se convierten en parte fundamental del todo, aun considerando que uno de los puntos más débiles en cuanto a seguridad de la información es el recurso humano, ya que puede ser afectado por algún tipo de amenaza del tipo ingeniería social, por lo que en toda organización después de haber examinado todas estas consideraciones podemos determinar que las

				salvaguardas elegidas para este activo son de gran ayuda para disminuir el impacto y mejorar la productividad.
35	P-3	Desarrolladores/Programadores	Disminuye el riesgo.	Este activo se ha calificado con una valoración baja, ya que el desarrollo de aplicaciones no es el giro del negocio, el departamento de desarrollo cuenta con el personal encargado de desarrollar aplicaciones de uso interno que en cierta medida no tendrían vulnerabilidades considerables al no ser compartidas de manera abierta en el internet, también a cargo de este departamento se encuentra el mantenimiento de la página web de la empresa y están al frente del portal de ventas en línea, es aquí donde se podría llegar a presentar vulnerabilidades de importancia que pueden ser halladas por un atacante para comprometer en gran medida la información que maneja la empresa, por lo que anteriormente se han implementado medidas de seguridad como la instalación de un firewall físico, ahora con este estudio realizado se implementarán salvaguardas que ayudarán en mayor medida a proteger los pilares básicos de la seguridad de información como lo son: la confidencialidad, la integridad y disponibilidad.
36	P-4	Proveedores	Disminuye el riesgo.	El activo proveedores se lo ha valorado de manera baja, pero es importante considerarlo dentro de la planificación de políticas de seguridad ya que los mismos tienen interacción directa con colaboradores de la empresa por medio de llamadas telefónicas o por medio de correos electrónicos, los cuales pueden ser utilizados por atacantes para hacerse pasar por un proveedor y por ejemplo enviar un mail con algún tipo de archivo malicioso que podría ser instalado sin habernos dado cuenta, por eso es importante mantener una cultura de protección de la información en todo momento y ser desconfiados de todo intento desconocido que tenga como finalidad realizar un ataque a la infraestructura tecnológica de la empresa. Varias de las salvaguardas que se han tratado en el presente trabajo ayudan en gran medida a disminuir el riesgo de que este activo afecte a la organización.

Fuente: El autor.

4.5. Propuesta tecnológica para el tratamiento de vulnerabilidades.

Es necesario mejorar la infraestructura tecnológica de Uniscan para brindar un mejor servicio a sus clientes, colaboradores y proveedores. Para ello, es importante realizar un análisis exhaustivo de las vulnerabilidades de la red corporativa de la empresa y planificar auditorías de seguridad informática utilizando herramientas como NMAP y

NESSUS para encontrar lagunas de seguridad. A pesar de que muchas empresas dudan en gastar dinero en tecnologías de seguridad informática, es esencial revisar con frecuencia los protocolos de seguridad para evitar costosas pérdidas de datos y daños a la infraestructura.

Si bien la subcontratación es una opción, en la actualidad resulta poco práctica para Uniscan debido a los elevados precios. Sin embargo, la empresa puede aprovechar el acceso gratuito a conocimientos y aplicaciones de código abierto para abaratar los costos del estudio.

Los principales problemas en cuanto a seguridad informática están relacionados con el conocimiento inadecuado de los usuarios acerca de las capacidades de los sistemas informáticos, la falta de medidas de seguridad y el uso de sistemas o aplicaciones sin protección. Para prevenir estos problemas, se recomienda invertir en equipos de red que puedan detectar y rastrear intrusiones hostiles, tales como cortafuegos, UTM, IDS/IPS de gama alta y otros dispositivos.

4.5.1. Análisis del costo y beneficio del proyecto de investigación.

En la Tabla XXIV se presenta una comparación entre el valor de implementación y el beneficio, tomando en cuenta el estado actual y como la propuesta desarrollada en el presente proyecto traerá consigo cambios para bien en la infraestructura, así como en los procesos que se realizan en las actividades diarias de la organización

El desarrollo, estudio e investigación del proyecto permitirá elaborar un análisis exhaustivo de los costos y beneficios de la implementación de la propuesta. También es importante realizar una revisión del Anexo 11 de la metodología MAGERIT para realizar una revisión de los costos y beneficios de la implementación de salvaguardas, así nos podemos dar cuenta de lo importante que es en toda empresa realizar este tipo de estudios de vulnerabilidades en la infraestructura tecnológica, y todos los gastos e inconvenientes que pueden ser evitados si ponemos en práctica las recomendaciones de los expertos en el área de seguridad de la información.

TABLA XXIV. ANÁLISIS DE COSTO-BENEFICIO DEL PROYECTO.

ESTADO ACTUAL	VALOR E IMPLEMENTACIÓN	BENEFICIOS
Falta de conocimiento de los usuarios acerca de las funciones de los sistemas informáticos de la organización.	La capacitación del personal de tecnología requiere de un valor monetario debido a la contratación de un especialista.	Capacitar y ampliar el conocimiento del personal para que ellos estén preparados ante un incidente de seguridad.
Falta de conocimiento sobre las nuevas tecnologías de seguridad informática que existen en el mercado.	El tiempo que invierten los auditores de seguridad informática en la ejecución del análisis de vulnerabilidades, logra que las organizaciones ahorren tiempo y dinero debido a la pérdida de información de carácter confidencial y la paralización de los servicios que se proporciona a los clientes en el caso de tener problemas en la infraestructura de la empresa.	Contar con el conocimiento necesario para planificar planes de contingencia que ayuden a disminuir los riesgos y vulnerabilidades de los sistemas de información.
Falta de actualización en las aplicaciones montadas en el servidor y parches en los sistemas operativos clientes.	El departamento de desarrollo no cuenta con aplicaciones licenciadas y se tendría que revisar si tiene los parches actualizados en los equipos para intentar reducir los costos de implementación.	En el estudio de análisis de vulnerabilidades es importante identificar los parches y actualizaciones de los sistemas para cubrir los fallos de seguridad.

Fuente: El autor.

4.5.1.1. ANÁLISIS DE LA FACTIBILIDAD DE LA OPERACIÓN DEL PROYECTO.

En la actualidad, el departamento de desarrollo tiene suficiente personal para implementar algunas de las actividades descritas en el plan de tratamiento de vulnerabilidades que se llevará a cabo como parte de este proyecto. El equipo de desarrollo posee un conocimiento adecuado sobre seguridad de la información y pueden implementar las diversas recomendaciones realizadas en el plan.

Además, el equipo de desarrollo también tiene la capacidad de monitorear la red, el registro del servidor y realizar otras configuraciones para verificar los cambios realizados en la infraestructura tecnológica de la empresa. La realización de tareas como la operación de actualizaciones de parches del sistema y el mantenimiento de las estaciones de trabajo permitirán implementar con éxito las soluciones técnicas propuestas. También se han identificado aplicaciones que permiten actualizar

continuamente la base de datos de vulnerabilidades de las herramientas utilizadas dentro de la organización. Esto resulta muy útil para los directivos del sector tecnológico, ya que estarán continuamente informados de los incidentes de seguridad a medida que se produzcan. De esta manera, podrán estar al tanto de los riesgos actuales que amenazan la infraestructura tecnológica de la empresa.

Desde una perspectiva operativa, se considera completamente viable llevar a cabo la propuesta de tratamiento de vulnerabilidades. Es importante mencionar que los empleados del departamento de desarrollo brindaron todas las facilidades para realizar este análisis de vulnerabilidad y participaron en varias actividades del proyecto.

4.5.1.2. Análisis de la factibilidad técnica del proyecto.

Actualmente, la infraestructura tecnológica de la organización Uniscan incluye los siguientes servicios de red y de equipos para el tratamiento de la información:

- Servidor Apache versión 2.2.
- Sitio Web.
- Servidor de correo.
- Servidor de base de datos MYSQL.
- Dispositivos de Red.
- Equipos de computación: portátiles y de escritorio.
- Software.
- Equipos de respaldo de energía.
- Equipos de comunicación.
- Equipo de control de acceso físico.

Los servidores que se indicaron, se implementan en una sola unidad física instalada en una sala de comunicaciones (rack), esta sala carece del nivel de seguridad necesario para proteger la integridad del equipo, lo que puede permitir a los atacantes obtener acceso no autorizado a información confidencial.

Dentro de la organización existe diferentes equipos y activos de información que pueden ser evaluados con herramientas al alcance de nuestras manos, ya que son de distribución libre, también se puede mencionar que para realizar un análisis y estudio de la infraestructura tecnológica no es necesario de la adquisición de equipos costosos y difíciles de adquirir, durante el proceso y evaluación de este proyecto solo fue necesario dispositivos que utilizamos diariamente, como por ejemplo, un computador portátil con acceso a la red de la empresa e instalado el sistema operativo Kali-Linux, adaptador Wifi de conexión USB, software de distribución libre y recursos de información consultados en internet.

El sistema operativo Kali-Linux utilizado para analizar la infraestructura tecnológica de la organización en busca de vulnerabilidades es de código abierto, por lo que las empresas pueden realizar auditorías de seguridad adecuadas sin invertir en software con licencia, todo lo que mencionamos anteriormente hacen que el desarrollo del presente proyecto sea posible.

4.5.1.3. Análisis económico del proyecto.

La propuesta de análisis de vulnerabilidades se mostró factible en términos de costos, cabe mencionar que en este punto no se realizará un estudio económico financiero para demostrar la factibilidad, solo se realizará un análisis económico con datos conseguidos durante el proceso del presente trabajo, ya que es un proyecto en el que solamente se propone la realización de un plan de tratamiento como objetivo específico para los riesgos de nivel inaceptable que se detecten durante el desarrollo del análisis de riesgos, y queda a decisión de la directiva de la organización la compra de equipos e implementación de tecnología, después de revisar la información y documentación que se entregará de manera física y digital.

Las herramientas presentadas en el proyecto son de código abierto, lo que significa que no habrá necesidad de hacer una inversión financiera por parte de la organización como se puede apreciar en la Tabla XXV. Además, las soluciones de seguridad se identificarán

mediante auditorías de seguridad informática, lo que permitirá a la empresa evitar reflejar gastos mientras se lleva a cabo el proyecto. Esto hace que la propuesta sea atractiva desde un punto de vista financiero, ya que no supone un gasto significativo para la empresa. Al utilizar herramientas de código abierto, se reduce el costo total del proyecto y se maximiza el uso de los recursos internos de la organización para el análisis de vulnerabilidades y la implementación de soluciones de seguridad. Además, el hecho de que las soluciones de seguridad se identifiquen a través de auditorías de seguridad informática permite a la empresa que pueda ahorrar costos en la contratación de consultores externos y también proporciona una mayor transparencia en el proceso de identificación de vulnerabilidades y soluciones de seguridad.

En resumen, la propuesta de análisis de vulnerabilidades es viable financieramente debido a la utilización de herramientas de código abierto y a la identificación de soluciones de seguridad a través de auditorías de seguridad informática.

TABLA XXV. COSTO DE LOS RECURSOS TÉCNICOS UTILIZADOS EN EL PROYECTO.

ITEM	DESCRIPCIÓN DEL RECURSO	CANTIDAD	COSTO UNITARIO	COSTO PARCIAL
1	Laptop ASUS (Procesador CORE i7)	1	$ 980.00	$980.00
2	Adaptador Wifi (conexión USB)	1	$ 10.00	$10.00
3	Sistema Operativo Kali-Linux	1	$ -	$ -
4	Herramienta de Software NMAP	1	$ -	$ -
5	Herramienta de Software NESSUS	1	$ -	$ -
			TOTAL	**$ 990.00**

Fuente: El autor.

4.5.1.4. Análisis de la factibilidad legal del proyecto.

Dado que el objetivo principal del análisis de vulnerabilidad de la infraestructura tecnológica de Uniscan es proporcionar información y asesoramiento a las organizaciones con el fin de evitar que se conviertan en víctimas de ataques cibernéticos por parte de actores maliciosos que buscan atacar información confidencial, es importante tener en cuenta que este análisis no infringe la legislación aplicable en la República del Ecuador.

Es importante destacar que, en Ecuador, existen leyes y regulaciones específicas que protegen los derechos de privacidad y seguridad de la información, tales como la Constitución de la República del Ecuador y la Ley de Protección de Datos Personales, entre otras. Sin embargo, estas leyes y regulaciones no impiden la realización de análisis de vulnerabilidades de la infraestructura tecnológica, siempre y cuando se lleven a cabo de manera adecuada y dentro de los límites de la ley.

Además, es importante destacar que la realización de un análisis de vulnerabilidad de la infraestructura tecnológica puede ser una práctica recomendable para las empresas y organizaciones que buscan proteger sus sistemas y datos de posibles ciberataques y vulnerabilidades de seguridad. En este sentido, la realización de un análisis de vulnerabilidad de la infraestructura tecnológica no solo puede ser compatible con la legislación aplicable en la República del Ecuador, sino que también puede ser una medida importante para proteger los derechos de privacidad y seguridad de la información de las empresas y organizaciones.

4.6. Pruebas de auditoría de Seguridad Informática.

Durante la realización de las pruebas de auditoría, se implementará un enfoque de seguridad de la información desde la fase inicial hasta el punto máximo del proyecto, el cual permitirá separar la recolección y exploración de datos de la validación de la información obtenida. De esta manera, se garantiza una gestión adecuada de la información y se asegura la integridad de los datos recolectados durante el proceso de análisis de vulnerabilidades, para observar lo indicado podemos revisar la figura 20 que es una síntesis del proceso de realización del estudio de las vulnerabilidades durante la ejecución del presente trabajo.

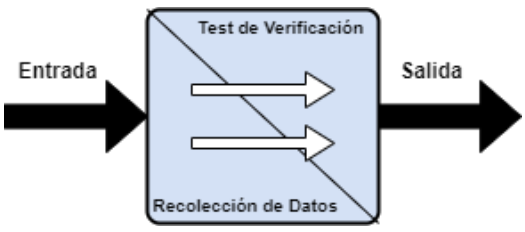


Fig. 20 Gráfica de la metodología a utilizarse para el estudio de vulnerabilidades.

Fuente: El autor.

En cuanto a la etapa de identificación del análisis de vulnerabilidades, se especifica que el conjunto completo de herramientas utilizadas en este proceso son parte del sistema operativo Kali-Linux.

4.6.1. Seguridad en las tecnologías de internet.

En la presente sección, se llevará a cabo un análisis de vulnerabilidades, lo cual requerirá una revisión minuciosa del Anexo 7 y del Anexo 9. Este análisis implica la investigación de la red, el escaneo de puertos, la identificación de servicios y sistemas, la detección y comprobación de vulnerabilidades, la comprobación de aplicaciones de Internet, el enrutamiento, el cifrado de contraseñas, la comprobación de la denegación de servicio y la revisión de la política de seguridad. Para llevar a cabo esta tarea se emplearán dos reconocidas herramientas de gestión de redes: Nmap y Nessus.

4.6.1.1. Resultados del análisis de vulnerabilidades realizado a la organización Uniscan.

Escaneo de puertos.

En esta sección, describimos la cantidad de puertos abiertos que son importantes para los actores malintencionados, la identificación de los puertos nos permite tener conocimiento del estado actual de la infraestructura tecnológica de la organización.

El comando empleado para recopilar información es el siguiente, el mismo que será ingresado con la herramienta Nmap, y se utilizará los atributos que se describen junto con el comando para obtener la mayor cantidad de información, como podemos ver y hacer referencia a la Tabla XXVI.

Nmap -sV -v -O 172.30.1.2

TABLA XXVI. PUERTOS ABIERTOS EN EL SERVIDOR DE LA EMPRESA UNISCAN.

SERVIDORES	PUERTOS ABIERTOS
ftp	21
ssh	22
http	80
xfer	82
ctf	84
msrpc	135
netbios-ssn	139
https	443
microsoft-ds	445
ms-sql-s	1433
pptp	1723
msmg	1801
zephyr-clt	2103
eklogin	2105
memq-mgmt	2107
vmrdp	2179
ms-olap4	2383
ppp	3000
ms-wbt-server	3389
realserver	7070

Fuente: El autor.

Identificación de los servicios.

En esta sección del análisis de vulnerabilidad, se procede a identificar la versión de cada servicio que se encuentra en la infraestructura tecnológica de la organización, lo mencionado anteriormente lo podemos apreciar en la Tabla XXVII, se ha utilizado la herramienta NMAP para poder obtener los resultados que se tabularon. Es importante destacar que esta información es valiosa para los actores malintencionados, ya que les permite enfocarse en ataques específicos y conocidos para la versión de los servidores instalados en la infraestructura tecnológica de la empresa. En este sentido, se detallará el nombre del servicio y su versión correspondiente, lo que permitirá a la organización conocer el estado actual de sus servicios y tomar medidas preventivas para evitar posibles ataques.

TABLA XXVII. IDENTIFICACIÓN DE SERVICIOS CON SU RESPECTIVA VERSIÓN.

SERVIDORES	VERSION
ftp	Microsoft ftpd
http	Microsoft IIS httpd 10.0
xfer	Microsoft IIS httpd 10.0
ctf	Microsoft IIS httpd 10.0
msrpc	Microsoft Windows PRC
netbios-ssn	Microsoft Windows netbios-ssn
https	Microsoft Windows HTTPAPI httpd 2,0 (SSDP/UPnP)
microsoft-ds	Microsoft Windows Server 2008 R2-2012 microsoft-ds
ms-sql-s	Microsoft SQL Server 2008 10.00.1600; RTM
pptp	Microsoft
msmg	-
zephyr-clt	Microsoft Windows RPC
eklogin	Microsoft Windows RPC
memq-mgmt	Microsoft Windows RPC
vmrdp	-
ms-olap4	-
ppp	Node.js Express framework
ms-wbt-server	Microsoft Terminal Service
realserver	-

Fuente: El autor.

4.6.2. Desarrollo de Man in the Middle (MITM) evil twin attack (fake/rouge AP).

Un ataque Man in the Middle (MITM) consiste en crear un punto de acceso falso como copia del original, en el cual el atacante será capaz de escuchar el tráfico de paquetes en esa red wifi, con este tipo de ataque se puede conseguir la contraseña de la red al ser ingresada por algún usuario desprevenido que no se mantenga alerta a las amenazas que puede existir en la red inalámbrica. Este tipo de ataque saca a los usuarios de la red original y luego les pide que para reingresar sea necesario que vuelva a escribir la contraseña, esta solicitud la hace a través de un portal cautivo, una vez que la contraseña sea solicitada e ingresada por algún usuario descuidado, este es el momento en el que nosotros como atacantes conseguimos la clave de la red original [26].

4.6.2.1. Desarrollo de la Metodología de "Evil Twin Attack".

Con el objetivo de obtener los datos e información de las víctimas se puede utilizar varios métodos y técnicas de ataques que estén enfocadas a redes inalámbricas, entre los varios métodos encontramos la metodología "MITM Evil Twin Attack", este método se encuentra entre los más populares y se ha convertido en uno de los más utilizados por los atacantes para vulnerar las redes wifi, en la figura 21 podemos ver un resumen gráfico del método que puede ser implementado para llevar a cabo el ataque. Entre los pasos que conforman el ataque tenemos al atacante ubicado en medio de la transmisión de los datos, en esta posición le resulta fácil capturar la clave de acceso a la red wifi de trabajo de la víctima, hay que indicar que este método de ataque se puede ejecutar en cualquier tipo de enlace inalámbrico [25].

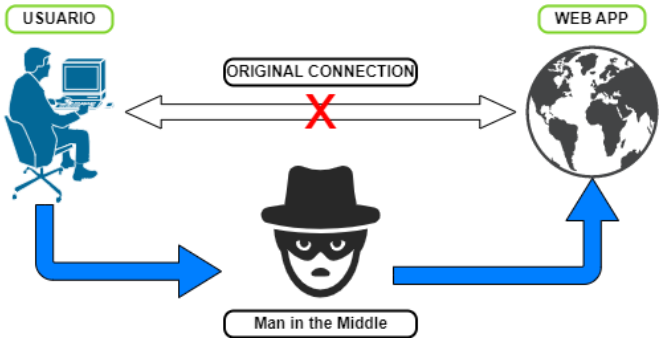


Fig. 21 Imagen del método de ataque Man In The Middle (MITM).
Fuente: El autor

Este método de ataque tiene como finalidad ubicar al atacante en medio de la transmisión para que pueda capturar los datos o información, una vez realizado lo anterior, el atacante debe ser capaz de permitir la conexión entre las partes sin pérdida de información, para que los involucrados no se den cuenta de lo ocurrido.

El ataque que se conoce como *Evil Twin Attack (*ETA), no es más que la implementación de un punto que simula ser el acceso inalámbrico original, este tipo de ataque tiene como objetivo comprometer la seguridad de los dispositivos conectados a la red, se configura un acces-point (punto de acceso) que tiene como objetivo engañar a los

usuarios de una red para que se conecten a una red falsa con el mismo nombre (SSID) que la legítima, esto lo podemos observar de manera gráfica en la figura 22.

Fig. 22 Ilustración del Ataque Evil Twin (Mallik, 2019) [25].

Seguido, listaremos los pasos más comunes utilizados para llevar a cabo este tipo de ataque:

Paso 1: Como atacante deberá realizar una búsqueda intensiva del punto de acceso objetivo. Es necesario que tenga la información del nombre SSID de la red, dirección, número de canal. Posteriormente puede utilizar esa información para crear un punto de acceso idéntico al original en sus características de red.

Paso 2: Los usuarios que están conectados al Acces-Point (AP) legítimo comenzarán a desconectarse de manera repentina y entrarán en un loop de conexión y desconexión, esta falla obliga a los usuarios a conectarse al punto fraudulento de acceso a la red, pues el nombre de la red falsa es similar a la original.

Paso 3: Los usuarios pueden comenzar a navegar por internet tan pronto vuelvan a conectarse al punto de acceso falso y hayan ingresado el password.

Paso 4: El usuario que desee continuar navegando por internet deberá abrir una ventana de uno de los navegadores, puede ser el de su preferencia y podrá ver una advertencia en la ventana web que dirá "Ingrese la contraseña o password de la red para volver a conectarse ".

Paso 5: El momento en el que uno de los usuarios ingrese la contraseña, será redirigido a una página en la que empezará el proceso de carga de la ventana (por ejemplo, Google), mientras tanto la contraseña se mostrará en la máquina atacante, el tipo de comportamiento hace que el ataque Evil Twin sea automatizado.

4.6.2.2. Equipos y materiales utilizados en el desarrollo del ataque "Evil Twin Attack".

Para llevar a cabo el ataque Man in the Middle "Evil Twin Attack", no fue necesario la utilización de muchos recursos como podemos observar en la Tabla XXVIII, pero este laboratorio fue muy necesario para determinar el estado actual de seguridad de las redes inalámbricas dentro de la empresa Uniscan.

TABLA XXVIII. EQUIPOS UTILIZADOS EN EL DESARROLLO DEL ATAQUE "Evil Twin Attack".

ITEM	DESCRIPCIÓN	CANTIDAD	VALOR
1	Antena wifi TP-LINK, modelo TL-WN821N	1	$ 10,00
2	Computador ASUS X512FJ	1	$ 700,00
		Total:	$ 710,00

Fuente: El autor.

4.6.3. Aplicación de la herramienta Nessus en el escaneo de vulnerabilidades.

Como también fue uno de los objetivos del presente proyecto, el no generar costos para la organización durante el desarrollo de las actividades de identificación de vulnerabilidades, y habiendo investigado que varias herramientas tenían limitaciones en sus versiones gratuitas en cuanto a la cantidad de direcciones IP que se pueden analizar y la capacidad de generar informes actualizados, se eligió Nessus como la herramienta más adecuada para el análisis de vulnerabilidades en este caso de estudio, debido a sus grandes ventajas demostradas en varios trabajos anteriores consultados.

Nessus es una herramienta web que escanea y busca puertos abiertos en dispositivos de red, y detecta vulnerabilidades en ellos. Al final del proceso, si hay anomalías en los equipos, Nessus genera un informe detallado que proporciona al personal de soporte

técnico o al administrador una comprensión general de la situación de los equipos. Esto permite tomar medidas necesarias para reducir los riesgos de seguridad. La información entregada por el software Nessus puede exportarse a diferentes tipos de archivo, lo que permite guardar y utilizar para crear una base de datos de las anomalías descubiertas.

A continuación, se describe el método por el que la herramienta Nessus clasifica las vulnerabilidades, o el factor de riesgo. Además, se muestra la Tabla XXIX de criticidad de las vulnerabilidades según el color, que aparece en el informe de la herramienta.

TABLA XXIX. CRITICIDAD DE LAS VULNERABILIDADES SEGÚN EL COLOR.

CRITICA	ALTA	MEDIA	BAJA	INFORMATIVO
8 – 10	7 - 7.9	4 - 6.9	1 - 3.9	0

Fuente: El autor.

Las vulnerabilidades con un factor de riesgo **BAJO** están relacionadas con las características de la configuración del sistema que pueden utilizarse para comprometer su seguridad, pero que no son consideradas como vulnerabilidades en sí mismas. Esto se debe a que se requiere un conjunto específico de condiciones para que puedan ser explotadas, y es posible que un atacante no pueda cumplir con todas ellas en todo momento. Es importante tener en cuenta que estas vulnerabilidades deben ser monitoreadas y corregidas si es necesario, ya que podrían utilizarse para comprometer la seguridad del sistema en el futuro. Por lo tanto, se recomienda que se realice una evaluación periódica de estas vulnerabilidades para garantizar la seguridad del sistema en todo momento.

Las vulnerabilidades con un factor de riesgo **MEDIO** están vinculadas a características accesibles de forma remota en el sistema que ha sido designado como objetivo, que suelen ser utilizadas por los atacantes para explotar otra debilidad. En otras palabras, estas vulnerabilidades constituyen la base de otros fallos más graves que podrían comprometer el sistema, incluido el uso de la escalada de privilegios, en lugar de ser el objetivo final de cualquier asalto.

Las vulnerabilidades con factores de riesgo **ALTO** pueden aprovecharse para acceder a recursos de host remotos que deben protegerse. Estos fallos en su conjunto amenazan el sistema afectado porque, si son explotados por un pirata informático, podrá obtener el control parcial o total del sistema, ver y alterar datos privados y ejecutar comandos y programas en el ordenador comprometido.

Al igual que las vulnerabilidades de factor de riesgo ALTO, las vulnerabilidades de factor de riesgo **CRÍTICO** suelen ser más graves y exigen un rápido examen y remedio por parte de los administradores de tecnologías de la información.

Los fallos INFORMATIVOS no ponen en peligro el equipo, pero proporcionan a un atacante acceso a la información que contiene.

Al crear una estrategia de mitigación, se presta la máxima atención a las vulnerabilidades con un factor de riesgo CRÍTICO y ALTO; en ausencia de este tipo de vulnerabilidades, se examinan las de nivel MEDIO.

En esta parte, examinamos los posibles fallos, errores o vulnerabilidades del sistema operativo.

Un nuevo análisis en Nessus se establece utilizando una política existente; por ejemplo, el Análisis avanzado sugerido requiere introducir la dirección IP del host que se va a analizar y ejecutar el procedimiento.

Lo primero que se nota es que la aplicación ofrece un montón de opciones de hackeo, pero algunas de ellas están bloqueadas y sólo disponibles en la versión de pago. A pesar de esto, todavía hay varias opciones básicas de escaneo disponibles, incluyendo los escaneos avanzados y básicos de malware.

Al elegirlo, se nos indica que debemos proporcionar un nombre y elegir el rango de direcciones IP que el escaneo avanzado analizará para determinar el estado de la red.

En la Tabla XXX y Tabla XXXI se detallan los datos específicos y cantidad de las vulnerabilidades descubiertas mediante la herramienta Nessus, incluyendo su evaluación de riesgo y las posibles correcciones. Nessus no solo identifica las vulnerabilidades presentes en la red, sino que también alerta a los usuarios sobre cómo minimizar el riesgo asociado a cada una de ellas, proporcionando soluciones efectivas.

Además, Nessus tiene la capacidad de exportar un informe detallado en varios formatos, tales como html, pdf y xml.

TABLA XXX. LISTA DE VULNERABILIDADES EN EL SERVIDOR DE LA ORGANIZACIÓN UNISCAN (172.30.1.2).

N°	Vulnerabilidad	Gravedad	CVSS v3.0 Score	Resumen
1	SSL Version 2 and 3 Protocol Detection	Crítica	9,8	El servicio remoto utiliza un protocolo con fallos conocidos para cifrar el tráfico.
2	Microsoft SQL Server Unsupported Version Detection (remote check)	Crítica	10,0	El host remoto está ejecutando un servidor de base de datos que no está soportado oficialmente.
3	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)	Alta	8,1	Muchas vulnerabilidades afectan al host remoto de Windows.
4	Microsoft Windows SMBv1 Multiple Vulnerabilities	Alta	8,1	Existen varias vulnerabilidades en el host Windows remoto.
5	SSL Medium Strength Cipher Suites Supported (SWEET32)	Alta	7,5	El servicio remoto admite cifrados SSL de potencia media.
6	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	Media	6,8	Utilizando servicios habilitados para SSL/TLS, es posible obtener información privada del host remoto.
7	Remote Desktop Protocol Server Man-in-the-Middle Weakness	Media	6,5	El acceso al host remoto puede ser posible.
8	SSL Certificate Cannot Be Trusted	Media	6,5	No se puede confiar en el certificado SSL de este servicio.
9	SSL Self-Signed Certificate	Media	6,5	La cadena de certificados SSL de este servicio termina con un certificado autofirmado que no se reconoce.
10	TLS Version 1.0 Protocol Detection	Media	6,5	El servicio remoto utiliza una versión antigua de TLS para cifrar el tráfico.

11	TLS Version 1.1 Protocol Deprecated	Media	6,5	El servicio remoto utiliza una versión antigua de TLS para cifrar el tráfico.
12	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Media	5,9	El servicio remoto admite el cifrado RC4.
13	SMB Signing not required	Media	5,3	En el servidor SMB remoto, no es necesario firmar.
14	SSL Certificate with Wrong Hostname	Media	5,3	El certificado SSL de este servicio pertenece a otro host.
15	Terminal Services Doesn't Use Network Level Authentication (NLA) Only	Media	4,0	Los servicios de terminal remoto no se limitan a la autenticación a nivel de red.
16	Terminal Services Encryption Level is Medium or Low	Media	4,3*	El host remoto está utilizando criptografía débil.
17	mDNS Detection (Remote Network)	Media	5,0*	Es posible obtener información sobre el host remoto.
18	Terminal Services Encryption Level is not FIPS-140 Compliant	Baja	2,6*	El host remoto no es compatible con FIPS-140.

* indica que la puntuación v3.0 no está disponible; se muestra la puntuación v2.0

Fuente: El autor.

TABLA XXXI. DESCRIPCIÓN DE GRAVEDAD DE VULNERABILIDADES.

Gravedad de las vulnerabilidades	Número de vulnerabilidades encontradas
Crítica	2
Alta	3
Media	12
Baja	1
Informativa	50

Fuente: El autor.

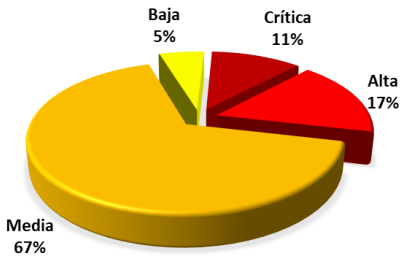


Fig. 23. Gravedad porcentual de las vulnerabilidades.
Fuente: El autor

Como puede verse, Nessus es una de las herramientas más completas para el hacking ético que puede utilizar una empresa. Está claro que varias vulnerabilidades se clasifican

en distintos niveles de gravedad, esto lo podemos observar en la figura 23, donde se indica el porcentaje de cada uno de los niveles de gravedad del presente proyecto de estudio. Por decirlo de otro modo, los técnicos deben evaluar estos datos y, si es necesario, tomar las medidas correctoras oportunas para solucionar el problema.

Se hará un seguimiento de algunas de las alarmas para solucionarlas con el fin de ofrecer información detallada sobre la información descubierta, tal y como se indica en el Anexo 9.

Severidad Crítica.

Durante el procedimiento de escaneado, los resultados del examen de la dirección del servidor: 172.30.1.2, revela que presenta dos vulnerabilidades graves.

Se enumeran las vulnerabilidades de nivel crítico:

- SSL Version 2 and 3 Protocol Detection.
- Microsoft SQL Server Unsupported Version Detection (remote check).

Comentario: Si este problema no se soluciona, el examen de estas vulnerabilidades puede mostrar que nuestro objetivo de investigación puede ser vulnerable a un riesgo de seguridad.

Severidad Alta.

A continuación, presentamos el informe de análisis proporcionado por Nessus, el mismo que revela tres vulnerabilidades graves en el dispositivo escaneado (servidor de la organización Uniscan). El análisis basado en las vulnerabilidades descubiertas puede servir para demostrar que, si no se soluciona este problema, nuestro activo investigado puede ser vulnerable a un riesgo potencial de seguridad.

Se enumeran las vulnerabilidades de nivel alta:

- MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check).
- Microsoft Windows SMBv1 Multiple Vulnerabilities.

- SSL Medium Strength Cipher Suites Supported (SWEET32)

Comentario: Podríamos empezar por activar el Firewall de Windows para evitar este tipo de vulnerabilidades y disminuir el peligro de ataques.

Severidad Media.

Las vulnerabilidades de gravedad media en este caso están resaltadas en naranja, y de ello se desprende que la dirección IP del servidor escaneada tiene 12 vulnerabilidades de este tipo.

Se enumeran las vulnerabilidades de nivel media:

- SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE).
- Remote Desktop Protocol Server Man-in-the-Middle Weakness.
- SSL Certificate Cannot Be Trusted.
- SSL Self-Signed Certificate.
- TLS Version 1.0 Protocol Detection.
- TLS Version 1.1 Protocol Deprecated.
- SSL RC4 Cipher Suites Supported (Bar Mitzvah).
- SMB Signing not required.
- SSL Certificate with Wrong Hostname.
- Terminal Services Doesn't Use Network Level Authentication (NLA) Only.
- Terminal Services Encryption Level is Medium or Low.
- mDNS Detection (Remote Network).

Severidad Baja.

Las vulnerabilidades de gravedad baja en este escenario están resaltadas en amarillo, y se descubrió que el objetivo de estudio tiene una de ellas.

Se enumeran las vulnerabilidades de nivel baja:

- Terminal Services Encryption Level is not FIPS-140 Compliant.

*En este caso, las vulnerabilidades con gravedad informativa han sido identificadas y están resaltadas en azul. Se puede observar que la dirección IP de estudio contiene 50 vulnerabilidades con gravedad informativa.

4.6.4. Criterios de aceptación del producto.

Una vez aplicada la metodología MAGERIT a los proyectos, se procede a su evaluación en relación a los criterios de aceptación de alcance. Para llevar a cabo esta evaluación, se utilizarán la Tabla XXXII y la Tabla XXXIII, las cuales permiten registrar de manera detallada los datos relevantes del proyecto. Estas tablas son de gran utilidad para llevar un seguimiento y control riguroso del proyecto, ya que permiten identificar y analizar los criterios de aceptación de alcance en función de los objetivos del proyecto y sus restricciones. Asimismo, estas tablas facilitan la toma de decisiones y la identificación de posibles desviaciones en el alcance del proyecto, lo que permite realizar ajustes y tomar medidas correctivas de manera oportuna para garantizar el éxito del proyecto.

TABLA XXXII. PRIMERA TABLA DE ACEPTACIÓN DEL PROYECTO.

CRITERIO ALCANCE	POSITIVA	INDIFERENTE	NEGATIVA
Asesorar al personal que labora en el departamento de desarrollo con el fin de aplicar métodos para disminuir los posibles fallos de seguridad identificados a través del escáner de vulnerabilidades.	X		
El resultado de las pruebas de análisis de vulnerabilidades en la infraestructura tecnológica será transmitido a los especialistas para que implementen los controles adecuados los cuales permitan una comprobación clara y precisa.	X		
Se realizará un estudio de vulnerabilidades completo que incluye información confidencial de la red de la organización objeto de estudio por medio de herramientas de código abierto, con el fin de establecer conclusiones precisas las cuales permitirán una solución adecuada y acorde a los requerimientos presentes en la organización.	X		

Fuente: El autor.

TABLA XXXIII. SEGUNDA TABLA DE ACEPTACIÓN DEL PROYECTO.

CRITERIO ALCANCE	POSITIVA	INDIFERENTE	NEGATIVA
Al final del estudio se entregará los reportes de todo el análisis ejecutado en la infraestructura tecnológica de la empresa, sin demostrar que las mitigaciones recomendadas brinden una total protección a los activos de información, ya que no es posible realizar una demostración real debido a que los equipos informáticos prestan servicios en un ambiente de producción, y lo recomendable en estos casos es no realizar ningún tipo de ataque informático debido a la criticidad de los procesos.	X		
Es necesario citar que para la demostración del estudio realizado se replicará un entorno virtual de acuerdo a las características y servicios reales dentro de la infraestructura de red.	X		

Fuente: El autor.

4.7. Implementación de políticas de seguridad en la empresa Uniscan.

Es importante tener en cuenta que no se debe esperar a que se presente una situación de riesgo para implementar políticas y normas de seguridad empresarial. A medida que la empresa crece, es fundamental que todos los miembros de la organización asuman la responsabilidad de proteger la información sensible y poner en práctica las políticas y leyes correspondientes. Con el aumento de la información y su vulnerabilidad a los ataques, es necesario estar preparados para estos incidentes mediante la creación de una estrategia de tratamiento para reducir los riesgos. Todos los empleados de la empresa son responsables de la seguridad de la información, sin embargo, es importante concienciar sobre la importancia de este tema y tener en cuenta las posibles amenazas para las finanzas, la situación legal y la estructura organizativa de la empresa. Además, algunos empleados pueden ser más dedicados que otros en cuanto a la implementación de medidas de seguridad, por lo que es crucial asegurarse de que todos estén alineados en cuanto a la importancia de la seguridad de la información.

4.7.1. Tiempo requerido para implementar un plan de tratamiento.

La duración de la ejecución del plan de protección de información dependerá de los procedimientos fundamentales que la empresa tenga establecidos, los cuales se orientan hacia la implementación de políticas que promuevan la seguridad de la información, así como de la disposición y conocimientos de los empleados, los procesos administrativos de la empresa y su magnitud. Es decir, el tiempo necesario para poner en marcha el plan puede variar significativamente dependiendo de diversos factores internos y externos a la organización. Por lo tanto, es importante considerar estas variables al momento de establecer un cronograma realista para la implementación del plan de protección de información.

4.7.2. Costo necesario para implementar un plan de tratamiento.

El costo de implementar un programa de gestión de riesgos depende de varios factores, por lo que es importante evaluar las capacidades actuales de la organización en términos de conocimientos básicos de seguridad de la información o si ya cuenta con especialistas en la materia. También se puede ahorrar costos utilizando tecnologías de análisis de vulnerabilidades ya existentes y considerando herramientas gratuitas para el escaneo. La creación de una estrategia de gestión de riesgos puede ser costosa, especialmente para empresas de mayor tamaño. Por lo tanto, puede ser beneficioso considerar la implementación de la estrategia por departamento, en función de la estructura organizativa de la empresa como otra forma de reducir costos.

Antes de comenzar a aplicar la estrategia de tratamiento de vulnerabilidades, es esencial definir los siguientes aspectos:

• Establecer los requisitos de seguridad que la estrategia de gestión de riesgos debe proporcionar a la organización Uniscan.

• Identificar los activos de información, incluyendo la identificación y categorización de activos, dentro del marco de análisis de vulnerabilidad de la organización.

• Revisar los aspectos administrativos, técnicos, logísticos, de marketing y ventas relacionados con la seguridad de la información.

• Elaborar un resumen de la situación de la seguridad de la información en la organización de Uniscan. El plan de tratamiento recomendado se adaptará a los requisitos de seguridad y a las regulaciones aceptadas en la nación donde se implementará. Por lo tanto, las empresas con oficinas en múltiples naciones pueden tener un plan de tratamiento diferente, pero en general, debe seguir los principios fundamentales de la gestión de riesgos.

A continuación, se presentan las características y prácticas que se deben emplear en la fase de diseño:

• Crear soluciones para proteger los datos físicos de la organización.
• Implementar planes de tratamiento para los niveles de riesgo demasiado altos.
• Realizar seguimiento y pruebas de los controles en áreas específicas.
• Revisar los plazos y procedimientos de gestión de la organización.
    o Hacer una lista de comprobación de los requisitos de las pruebas de gestión.
    o Definir los pasos a seguir en la revisión de la gestión, como auditorías para evaluar distintos factores relacionados con la implementación.
• Proporcionar educación en seguridad de la información:
    o Proporcionar recursos educativos sobre seguridad de la información.
    o Capacitar al personal en seguridad de la información, incluyendo explicar las obligaciones de cada empleado.
    o Evaluar el procedimiento de formación del personal en materia de seguridad de la información.
• Elaborar el plan definitivo de gestión de riesgos, estandarizar la estrategia de ejecución y proporcionar sugerencias de acciones de gestión para los riesgos inaceptables.

Tras definir el alcance y el plan de gestión de riesgos, deben tenerse en cuenta los siguientes factores:

- Requisitos de seguridad general.
- Desarrollo y administración de los planes de gestión de riesgos.
- Requisitos de documentación.

Antes de iniciar un programa de tratamiento de riesgos en Uniscan, es fundamental contar con la aprobación de las autoridades de la empresa, lo que implica:

- Definir quién será responsable de revisar la estrategia de tratamiento de riesgos, ya sea la alta dirección o la dirección general.
- Asegurar el compromiso de la dirección con el programa.
- Proporcionar las herramientas necesarias a la dirección para crear una estrategia de tratamiento de riesgos para abordar situaciones de riesgo inaceptables.
- Revisar la estrategia de gestión de riesgos y asegurarse de que se ajuste a los requisitos y normas aceptadas en la nación donde se llevará a cabo.
- Realizar una evaluación por parte de la dirección de la estrategia de gestión de riesgos, lo que incluye una visión general de la revisión, el análisis de los datos y los resultados obtenidos.

4.7.3. Estructuración del plan de tratamiento de vulnerabilidades.

El propósito fundamental de una regulación de seguridad es establecer las normas esenciales para que las organizaciones privadas, como Uniscan, implementen una estrategia de gestión de riesgos. Esta estrategia debe seguir un proceso estructurado que incluya la creación de mecanismos registrados y disponibles para todos los miembros de la organización. Es importante tener en cuenta que la aplicación de un plan de tratamiento de riesgos no puede garantizar la seguridad total de los datos de la organización, pero puede ayudar a asegurar que los datos estén documentados para entender, gestionar y reducir los riesgos de seguridad de manera sistemática,

estructurada, eficiente, repetible y adaptable a los cambios en el riesgo, el entorno y la tecnología [23].

Los requisitos para desarrollar un plan de gestión de riesgos consisten en:

- La implementación de estándares que reflejan las mejores prácticas de seguridad de los activos de información, esto puede mejorar significativamente la calidad del programa de gestión de riesgos. Al seguir estos estándares, la organización como Uniscan puede reducir la probabilidad de incidentes de seguridad que afecten a los activos de información en diversas áreas, como la administrativa, técnica, logística, de marketing y de ventas. Esto se debe a que estos estándares establecen medidas y controles específicos que ayudan a proteger los activos de información y reducir la exposición a riesgos de seguridad.

- En el caso de que las organizaciones, como Uniscan, estén interesadas en obtener una certificación, es importante cumplir con un estándar específico que requiere una versión documentada de cada proceso que se llevó a cabo durante la implementación del plan de gestión de riesgos. Este estándar es fundamental para asegurar que se cumplan los requisitos necesarios para obtener la certificación, lo que a su vez demuestra que la organización está comprometida con la mejora de sus prácticas de seguridad de la información y la reducción de riesgos asociados a los activos de información en las diferentes áreas de la empresa.

5. Resultados y discusión.

Es esencial desarrollar procedimientos para la creación de copias de seguridad de la información, ya sea en formato digital o físico, como medida de protección ante posibles daños técnicos en la empresa, tanto accidentales como intencionales, con el objetivo de restaurar los servicios de la empresa en caso de fallos en los sistemas informáticos. Además, es crucial establecer mecanismos de autenticación que permitan el acceso a la información protegida solo al personal autorizado

Recopilar los recursos requeridos para aplicar una política de seguridad de la información que contemple las prácticas óptimas y medidas precisas para salvaguardar la integridad, confidencialidad y disponibilidad de la información dentro de la organización.

Se deben establecer directrices para la protección de los dispositivos informáticos, en especial los equipos de cómputo personal, tanto portátiles como de escritorio, estas directrices deben incluir medidas para prohibir la instalación de software no autorizado, a fin de evitar la posibilidad de alojar archivos maliciosos que puedan comprometer el normal funcionamiento del dispositivo o dejar una puerta abierta para que ciberdelincuentes puedan robar información sensible, estas medidas buscan proteger la integridad, confidencialidad y disponibilidad de los datos almacenados en dichos dispositivos.

Elaborar un programa de capacitación que proporcione a los empleados los conocimientos necesarios sobre las políticas y procedimientos de seguridad de la información que deben aplicarse en sus actividades diarias para garantizar la protección de los datos.

La realización del proyecto demostró el estado actual de la seguridad de la red inalámbrica, este laboratorio se lo realizó mediante el uso de la técnica de ataque MITM Evil Twin. Durante el desarrollo de las pruebas los usuarios pudieron comprender los riesgos involucrados en el uso de redes Wi-Fi, ya sean privadas o públicas,

convirtiéndose en una manera experimental de aprender a proteger cuidadosamente su información, por ejemplo: puede incluir datos privados, datos financieros, datos corporativos, etc., esto permitirá mejorar los estándares de seguridad corporativa.

6. Conclusiones y recomendaciones.

6.1. Conclusiones.

A partir del proyecto titulado "Análisis de vulnerabilidades en la infraestructura tecnológica de la organización Uniscan en el área funcional de frontera de la empresa", se puede inferir que es fundamental establecer requisitos de seguridad adecuados para proteger los activos de información que son utilizados por los empleados en la realización de distintas tareas dentro de la organización, a fin de que el trabajo diario pueda llevarse a cabo con el propósito de alcanzar los objetivos organizacionales. La implementación de medidas y controles de seguridad específicos para abordar las vulnerabilidades, amenazas y peligros asociados con cada activo, conforme a lo desarrollado en el presente proyecto, demuestra que es esencial para la adecuada gestión de los riesgos inherentes.

Es necesario aplicar medidas de seguridad para garantizar que la continuidad del negocio se mantenga sin interrupciones, tomando en cuenta la integridad, confidencialidad y disponibilidad de los activos de información, de tal manera que no se vean comprometidas las actividades en las que la organización participe.

Con el fin de proteger los recursos críticos de la organización, se deben implementar estrategias efectivas para prevenir y mitigar las amenazas de seguridad, así como para asegurar el cumplimiento de las políticas y regulaciones aplicables en el entorno operativo. Al salvaguardar la integridad, confidencialidad y disponibilidad de los activos de información, se garantiza que la organización pueda seguir operando con normalidad y cumplir con sus objetivos de negocio, sin poner en riesgo su reputación y su capacidad para competir en el mercado.

La correcta y efectiva aplicación de la gestión de riesgos, asegura la implementación de los procedimientos necesarios para disminuir o, en su defecto, eliminar las amenazas que puedan afectar a la información y otros activos de hardware y software de propiedad de la empresa. Es necesario indicar que el aplicar una gestión de riesgos adecuada, permite identificar de manera temprana las amenazas y riesgos potenciales y tomar medidas preventivas para mitigar su impacto y evitar su materialización.

Se puede determinar que, en el campo de la seguridad de la información, la prevención es muy importante, ya que esta permite establecer planes y estrategias para hacer frente a las situaciones imprevistas, garantizando la continuidad del negocio y la protección de los activos críticos de la organización. Asimismo, la gestión de riesgos también es una herramienta importante para la toma de decisiones en la empresa, ya que permite evaluar los riesgos en relación con los beneficios esperados, y así tomar decisiones sobre la inversión y el desarrollo de nuevos proyectos.

Es importante implementar un plan de tratamiento de vulnerabilidades para proteger la información, esto se puede realizar utilizando un modelo o metodología específica que permita evaluar la efectividad de las salvaguardas y los controles para disminuir el riesgo de cada activo de información, y determinar si los controles se están aplicando de manera adecuada. Al utilizar este modelo, se pueden identificar las áreas de mejora para garantizar que las salvaguardas y controles estén funcionando de manera efectiva y se puedan introducir mejoras en el plan de tratamiento de la vulnerabilidad. Además, este modelo también debería permitir una evaluación periódica de la eficacia de las medidas de protección de la información, lo que ayudaría a garantizar la continuidad del negocio y la seguridad de los activos críticos de la organización.

Es necesario diseñar un programa de capacitación para los empleados de la empresa acerca de los protocolos de seguridad de la información y su importancia. La política de seguridad de la información establecida para su implementación fomenta el tratamiento adecuado de los datos: personales y de la empresa, basándose en prácticas y reglas fáciles de implementar, mantener y supervisar. La capacitación de los empleados en estas políticas y prácticas es esencial para garantizar que los datos y la información sean

manejados de manera segura y responsable, lo que reduce el riesgo de exposición a amenazas internas y externas. Además, al capacitar a los empleados sobre los protocolos de seguridad de la información, se puede fomentar una cultura de seguridad en toda la organización, lo que puede llevar a una mayor conciencia y responsabilidad por parte de todos los miembros de la organización en la protección de la información y los activos de la empresa.

La información es uno de los activos más importantes de la organización, por lo que durante el desarrollo del proyecto fue necesario incorporar las recomendaciones pertinentes con el fin de garantizar que la información generada durante la ejecución de los diferentes procesos de la empresa sea confiable, íntegra y esté disponible de acuerdo con los estándares de seguridad establecidos. Estas recomendaciones fueron diseñadas para asegurar que la información sea tratada de manera adecuada para reducir el riesgo de exposición a amenazas internas y externas, y proteger la privacidad y confidencialidad de los datos de la empresa. Además, la implementación de estos estándares de seguridad ayuda a garantizar que la información sea manejada de manera responsable y efectiva, lo que puede mejorar la eficiencia de los procesos y la toma de decisiones.

El análisis de las vulnerabilidades en la infraestructura tecnológica de la organización proporciona una visión completa de la red y de las tecnologías que utiliza la empresa en sus procesos. Se llevaron a cabo análisis utilizando herramientas de software especializadas como Nmap y Nessus, lo que permitió realizar un análisis exhaustivo y obtener resultados precisos. Estos resultados permiten comprender los riesgos asociados con la falta de medidas de seguridad y la posible afectación de la productividad del sistema si se lleva a cabo un ataque. Es importante tener en cuenta que, sin este tipo de análisis y el conocimiento adecuado sobre cómo un atacante puede afectar la red y a las tecnologías que se emplean, es difícil tomar medidas preventivas para garantizar la seguridad de la información y los activos de la empresa.

La metodología MAGERIT es uno de los métodos utilizados para reducir los indicadores de vulnerabilidades y riesgos revelados por el análisis de vulnerabilidades con el fin de

lograr el cumplimiento del proceso de auditoría, en base a ello, la organización puede lograr la máxima protección, evitando de esta manera la divulgación de información confidencial. Se analizó las vulnerabilidades en la infraestructura tecnológica de la organización utilizando la metodología internacional MAGERIT, de acuerdo a cada componente que brinda la metodología y aplicable al proyecto de investigación desarrollado. De esta forma, fue posible conocer qué fases son las adecuadas para la propuesta de implementación, que determina: los puertos abiertos, el número de vulnerabilidades y el tipo de ataque con el que se puede acceder a cualquiera de los puertos, etc.

El enfoque MAGERIT ayuda en la preparación de informes de auditoría de seguridad informática, en los que el personal de seguridad informática de Uniscan puede aportar las pruebas relacionadas con el análisis de vulnerabilidades y examinar a fondo los hallazgos. El proceso de auditoría de seguridad de tecnologías de la información de la organización puede finalizar con informes puntuales, y estos informes se conservarán de acuerdo con las políticas de confidencialidad de la empresa y al cuidado de las personas encargadas de la seguridad de la información. Por lo tanto, se pudo determinar que, para evitar intrusiones maliciosas, se debe planificar lo siguiente:

- Realización de auditorías periódicas de seguridad informática.
- Adquisición de equipos de seguridad mejorados.
- Implementación de cifrado de información sensible.
- Establecimiento de conexiones remotas a través de túneles VPN.
- Implementación de un sistema de detección de intrusos.

6.2. Recomendaciones.

Los activos de información identificados con niveles de riesgo críticos en este proyecto deben tratarse con mayor prioridad, ya que su impacto podría tener consecuencias financieras o de reputación negativas para la empresa si no se toman medidas preventivas adecuadas. Por otro lado, los activos de información con niveles de riesgo más bajos pueden ser aceptados o mitigados, dependiendo de lo que se acuerde entre

la gerencia general, la gerencia técnica y el departamento de desarrollo. Por lo tanto, es fundamental que la empresa establezca y eleve sus estándares de seguridad para garantizar la disponibilidad, integridad y confidencialidad de la información. Para llevar a cabo la protección de la información, se pueden implementar medidas de seguridad adecuadas para cada nivel de riesgo, lo que permitirá a la empresa gestionar eficazmente sus activos de información y reducir la posibilidad de daños a su reputación o finanzas.

Para mantener la seguridad de la información, es importante tener en cuenta que la actualización constante de tecnologías y la integración de estas pueden generar nuevas amenazas, lo que significa que los riesgos asociados a los activos de información de la organización también cambiarán. Por lo tanto, es crucial que cualquier actualización realizada en estos activos se base en la revisión de seguridad establecida en el presente proyecto, para garantizar la protección adecuada de la información.

Para mejorar la seguridad de la información en una empresa, es esencial implementar un proceso de gestión de vulnerabilidades que pueda prevenir o mitigar nuevas debilidades que puedan surgir en el futuro. Para lograr esto, se sugiere la utilización de soluciones como UTM (Unified Threat Management) y VPN (Virtual Private Network) de alta calidad. Estas herramientas tienen la capacidad de reducir el acceso no autorizado al sistema informático, bloquear puertos que transportan servicios importantes y establecer conexiones a través de túneles.

Se sugiere realizar auditorías trimestrales utilizando la metodología MAGERIT para que la organización pueda identificar posibles vulnerabilidades y riesgos, de esta manera se podrá actuar oportunamente para prevenir daños o fallas en los sistemas de información.

Se sugiere la generación de informes periódicos que permitan que la organización pueda contar con datos actualizados sobre su estado, por ejemplo, un informe con el nivel de vulnerabilidades de su red. De esta manera, la organización podrá llevar a cabo un análisis detallado y tomar medidas oportunas para implementar las acciones

recomendadas y así prevenir posibles incidentes de seguridad que podrían afectar negativamente a la empresa.

En el presente proyecto se destaca la importancia de confiar únicamente en redes conocidas, como la red de nuestros hogares o las redes que se conocen que se encuentran implementadas por el departamento de desarrollo dentro de la organización Uniscan, y evitar conectarse a redes desconocidas, especialmente en lugares públicos o de transporte, donde los delincuentes pueden aprovecharse para realizar actividades ilegales.

En la actualidad, los sitios web utilizan el protocolo HTTPS para cifrar las sesiones, por lo que es crucial verificar si la página web que se está visitando tiene este prefijo en la barra de URL. En algunos casos, los atacantes pueden redirigir a los usuarios a una versión no segura del sitio web deseado, y si el usuario ingresa información personal en esta página, el atacante podría monitorear sus acciones y obtener información confidencial.

Para lograr una gestión efectiva de la seguridad de la información en una empresa, es recomendable que esta adopte una norma reconocida y establecida, como por ejemplo la ISO 27001:2015. Esta norma proporciona un conjunto de requisitos y controles que ayudan a garantizar la seguridad de los activos de información y los datos de la organización. Al aplicar esta norma, se pueden identificar los controles necesarios para abordar los riesgos específicos de la empresa y establecer un sistema de gestión de seguridad de la información efectivo y confiable. Para aplicar la norma ISO 27001:2015 en el presente proyecto, es importante revisar detalladamente la documentación existente y determinar qué controles son aplicables a la propuesta elaborada. Esto implica una revisión exhaustiva de los procesos de la empresa, identificando los riesgos potenciales y los controles necesarios para mitigarlos.

REFERENCIAS.

[1] ESET. Security Report, Latinoamérica 2022. [Online]. Available: https://www.welivesecurity.com/wp-content/uploads/2022/07/ESET-security-report-LATAM-2022.pdf

[2] S. Begum, S. Kumar, Ashhar, "A COMPREHENSIVE STUDY ON ETHICAL HACKING", INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY, vol. 4, pp. 214-216, 2016, doi: 10.5281/zenodo.59534.

[3] A. Arote, U. Mandawkar, "ANDROID HACKING IN KALI LINUX USING METASPLOIT FRAMEWORK", INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH IN COMPUTER SCIENCE, ENGINEERING AND INFORMATION TECHNOLOGY, vol. 7, pp. 497-504, 2021, doi: 10.32628/CSEIT217311.

[4] R. Borbúa, L. Herrera, R. Reyes. "CIBERDEFENSA Y CIBERSEGURIDAD, MÁS ALLÁ DEL MUNDO VIRTUAL: MODELO ECUATORIANO DE GOBERNANZA EN CIBERDEFENSA.", Revista Latinoamericana de Estudios de Seguridad, vol. 20, pp. 31-45, 2017, doi: 10.17141/urvio.20.2017.2571.

[5] Y. Sandoval. (2014, Junio). ISO 27001: de qué se trata y cómo implementarla. [Online]. Available: https://www.piranirisk.com/es/academia/especiales/iso-27001-que-es-y-como-implementarla.

[6] P. Casas. (2015, 19 de Noviembre). El Triángulo de Seguridad Informática. [Online]. Available: http://blogs.acatlan.unam.mx/lasc/2015/11/19/el-triangulo-de-la-seguridad/

[7] M. Romero, G. Figueroa, D. Vera, J. Álava, G. Parrales, A. Murillo and M. Castillo, "INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA", in Introducción a la Seguridad Informática y el Análisis de Vulnerabilidades, Primera Edición. Alicante: Editorial Área de Innovación y Desarrollo, S.L., 2018, pp. 13-22.

[8] G. Chávez, L. Tuárez, "PROPUESTA DE RED DE DATOS PARA LA GESTIÓN DE LOS SERVICIOS DE RED EN EL CAMPUS POLITÉCNICO DE LA ESPAM MFL", Tesis de Grado Previo a la Obtención del Título de Ingeniero en Informática, Carrera de Informática, ESPAMMFL, Calceta, Ecuador, 2016.

[9] H. Quishpe, "ANÁLISIS DE VULNERABILIDADES EN LA RED LAN JERÁRQUICA DE LA UNIVERSIDAD NACIONAL DE LOJA, EN EL ÁREA DE LA ENERGÍA, INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES", Tesis previa a la obtención del título de

Ingeniero en Sistemas, Carrera de Ingeniería en Sistemas, UNL, Loja, Ecuador, 2016.

[10] INCIBE. (2017, 20 de Marzo). Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian?. [Online]. Available: https://www.incibe.es/empresas/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

[11] A. Verdesoto, "UTILIZACIÓN DEL HACKING ÉTICO PARA DIAGNOSTICAR, ANALIZAR Y MEJORAR LA SEGURIDAD INFORMÁTICA EN LA INTRANET DE VÍA CELULAR COMUNICACIONES Y REPRESENTACIONES", Proyecto previo a la obtención del título de Ingeniero en Electrónica y Redes de Información, Facultad de Ingeniería Eléctrica y Electrónica, EPN, Quito, Ecuador, 2007.

[12] B. Huaygua, C. Abijail, "APLICACIÓN DE LA METODOLOGÍA MAGERIT PARA LA ELABORACIÓN DE UN PLAN DE MEJORA DE LA SEGURIDAD DE LOS ACTIVOS DE INFORMACIÓN DE LA ZONA ESPECIAL DE DESARROLLO – ZED PAITA", Tesis para optar el título profesional de Ingeniero Informático, Facultad de Ingeniería Informática, UNP, Piura, Perú, 2019.

[13] F. Jensen, "Electromagnetic near-field far-field correlations," Ph.D. dissertation, Dept. Elect. Eng., Tech. Univ. Denmark, Lyngby, Denmark, 1970. [Online]. Available: www.tud.ed/jensen/diss

[14] L. Quirola, "ANÁLISIS DE VULNERABILIDADES DE SEGURIDAD INFORMÁTICA DEL SISTEMA DE GESTIÓN MÉDICA SISMEDICALEC, DE LA EMPRESA INCOMSIS.", Trabajo de Graduación previo la obtención del título de Ingeniero en Sistemas Computacionales e Informáticos, Facultad de Ingeniería en Tecnologías de la Información, Telecomunicaciones e Industrial, UTA, Ambato, Ecuador, 2019.

[15] H. Robayo, "MODELO DE MEJORA DEL ESTADO DE LA CIBERSEGURIDAD EN LA GOBERNACIÓN DE TUNGURAHUA.", Proyecto de investigación previo a la obtención del título de Magister en Ciberseguridad, Oficina de Posgrados, PUCE, Ambato, Ecuador, 2022.

[16] M. Lozano, M. Correa, "ANÁLISIS DE LAS VULNERABILIDADES DE LA INFRAESTRUCTURA TECNOLÓGICA MEDIANTE TESTING DE CAJA BLANCA, BAJO LA NORMA ISO 27005 EN LA COMPAÑÍA CARACOL RADIO, NODO PRINCIPAL BOGOTÁ.", proyecto de grado para optar al título de Ingeniero de Sistemas, Facultad De Ingeniería Programa De Ingeniería En Sistemas, UCC, Bogotá, Colombia, 2020.

[17] K. García, “APLICACIÓN DE HACKING ÉTICO MEDIANTE TEST DE INTRUSIÓN “PENTESTING” PARA LA DETECCIÓN Y ANÁLISIS DE VULNERABILIDADES EN LA RED INALÁMBRICA DE UNA INSTITUCIÓN EDUCATIVA DE LA PROVINCIA DE SANTA ELENA”, previo a la obtención del Título de: Ingeniero En Tecnologías De La Información, Facultad De Sistemas Y Telecomunicaciones, UPSE, Ecuador, 2021.

[18] D. Gamboa, “VULNERABILIDADES EN APLICACIONES WEB UTILIZANDO LA METODOLOGÍA DE “PROYECTO ABIERTO DE SEGURIDAD DE APLICACIONES WEB””, Proyecto de investigación previo a la obtención del título de Magister en Ciberseguridad, Oficina de Posgrados, PUCE, Ambato, Ecuador, 2021.

[19] J. Rendón, J. Raza, “ANALISIS DE VULNERABILIDADES EN SISTEMAS INFORMÁTICOS WEB DESDE LA RED DE INTERNET UTILIZANDO HERRAMIENTAS DE HACKING ETICO Y LA METODOLOGÍA OWASP.”, Previa a la obtención del Título de: Ingeniero En Networking Y Telecomunicaciones, Facultad De Ciencias Matemáticas Y Físicas Carrera De Ingeniería En Networking Y Telecomunicaciones, UG, Guayaquil, Ecuador, 2019.

[20] L. Parra, E. Yánez, “ANÁLISIS DE VULNERABILIDADES EN LA INFRAESTRUCTURA TECNOLÓGICA DE UNA EMPRESA, UTILIZANDO HERRAMIENTAS DE TEST DE INTRUSIÓN”, Previa a la obtención del Título de: Ingeniero En Networking Y Telecomunicaciones, Facultad De Ciencias Matemáticas Y Físicas, UG, Guayaquil, Ecuador, 2017.

[21] H. Robayo, “MODELO DE MEJORA DEL ESTADO DE LA CIBERSEGURIDAD EN LA GOBERNACIÓN DE TUNGURAHUA”, Magister en Ciberseguridad, PUCE, Ambato, Ecuador, 2022.

[22] K. Freire, “Estudio y análisis de ciberataques en América Latina, su influencia en las empresas del Ecuador y propuesta de políticas de ciberseguridad.”, previo a la obtención del Título de: Ingeniero en Telecomunicaciones, Facultad de Educación Técnica para el Desarrollo, UCSG, Guayaquil, Ecuador, 2017.

[23] R. Díaz, Anexos, in Estado de la ciberseguridad en la logística de América Latina y el Caribe. 2021, serie Desarrollo Productivo, N° 228 (LC/TS.2021/108), Santiago, Comisión Económica para América Latina y el Caribe (CEPAL), pp. 50.

[24] R. González, “DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA EL ÁREA DE TECNOLOGÍA DE LA EMPRESA BAKER TILLY COLOMBIA LTDA DE LA CIUDAD DE BOGOTÁ, BAJO LA NORMA ISO 27001:2013”, monografía para optar el título de Especialista en Seguridad Informática, Escuela de Ciencias Básicas, Tecnología e Ingeniería, UNAD, Tunja, Colombia, 2016.

[25] S. Ramos, “Propuesta de estudio de la vulnerabilidad o riesgo de dispositivos móviles o tarjetas de red inalámbricas”, Proyecto de Investigación, Ingeniería en Sistemas, USFQ, Quito, Ecuador,2020.

[26] N. Anderson. (2021, Ago 09). ¿Qué es un ataque de gemelos malvados? Comprender la amenaza en las redes públicas [Online]. Available: https://fastestvpn.com/es/blog/ataque-gemelo-malvado/

[27] M. Dávila, G. Párraga, “ANÁLISIS DE RIESGO EN LA INFRAESTRUCTURA DE TECNOLOGÍAS DE INFORMACIÓN EN LA COOPERATIVA DE AHORRO Y CRÉDITO CALCETA LIMITADA”, Previa obtención del Título de: Ingeniero en Informática, Carrera Informática, ESPAM MFL, Manabí, Ecuador, 2015.

ANEXOS.

ANEXO 1. DESARROLLO DE LA ENTREVISTA AL ING. JOSÉ LUIS TRUJILLO (GERENTE TÉCNICO DE UNISCAN).

La siguiente entrevista se realizó el miércoles 30 de noviembre de 2022 a las 11 a.m. previa cita con el Ing. José Luis Trujillo.

1. ¿Qué experiencia tiene en seguridad informática?
Tengo experiencia de nivel intermedio a alto en seguridad informática con conocimientos básicos para prepararme ante un incidente de seguridad.

2. ¿Cómo se maneja la seguridad de la información en la organización?
Existen procesos para implementar protecciones y poder prevenir cualquier interrupción que intente comprometer la seguridad de la información.

3. ¿Está preparado para un incidente de seguridad en un momento dado?
No, sin embargo, tenemos una perspectiva distinta en cuanto a la seguridad de la información, que se basa en un conjunto de medidas de protección para evitar vulnerabilidades.

4. Como administrador de red, ¿tiene un plan de contingencia para diagnosticar los tipos de vulnerabilidades que se encuentran en la infraestructura tecnológica de Uniscan?
Actualmente, no dispongo de un plan de contingencia específico para abordar las vulnerabilidades encontradas en la infraestructura técnica de la empresa. No obstante, en el caso de que se produzca un ataque, colaboramos estrechamente con el departamento de desarrollo para identificar y aplicar una solución adecuada.

5. ¿Cuenta con los recursos informáticos y el personal para hacer frente a los desafíos que tal evento podría generar?
En parte, lo que realizamos es una investigación exhaustiva del incidente con los recursos que contamos con el fin de obtener una cantidad considerable de información y resolver la situación de la mejor manera posible.

6. ¿Ha experimentado alguna vez una intrusión maliciosa en la infraestructura de red de Uniscan?
Hemos detectado correos electrónicos maliciosos que solicitan verificar las cuentas de correo electrónico de los colaboradores y de los socios comerciales de la empresa, por lo tanto, hemos indicado que deben ignorarse y los remitentes deben bloquearse como medida de seguridad para evitar ataques informáticos.

7. ¿Conoce alguna forma de mitigar las brechas de seguridad de la información?
Podemos afirmar que no seguimos un estándar o una normativa, pero contamos con una estrategia para garantizar la seguridad de la información. Para ello, hemos identificado una serie de controles que deben ser implementados para mantener la integridad y confidencialidad de los datos, y para administrar el riesgo asociado.

8. ¿Tiene conocimiento de algún tipo de ataque informático que pueda llevarse a cabo sobre la infraestructura técnica de la empresa?
Instalación de virus informático haciendo clic o ingresando en un enlace adjunto a un correo electrónico de un cliente desconocido.

9. ¿Se ha probado la seguridad de la infraestructura tecnológica interna de la empresa?
Actualmente no, se está formulando un test de prueba que se aplicará para mantener la seguridad de la información.

10. ¿Se justifica la inversión en un sistema de seguridad informática dada la información confidencial que procesa Uniscan?
Si, ya que la información se considera uno de los recursos más valiosos en cualquier empresa.

11. ¿Cuáles son las aplicaciones más utilizadas?
Aplicaciones de facturación y gestión de inventarios, así como aplicaciones desarrolladas para el departamento técnico.

ANEXO 2. DIAGRAMAS DE BARRAS DE LA ENCUESTA REALIZADA AL PERSONAL TÉCNICO DE LA EMPRESA UNISCAN.

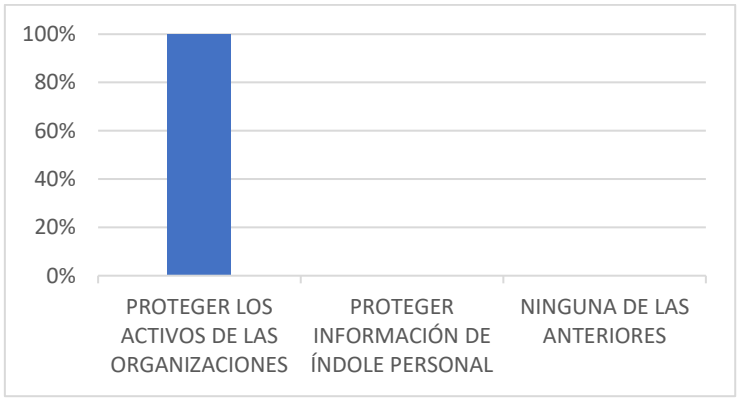


Fig. Pregunta #1. ¿Qué propósito principal tiene la seguridad informática?
Fuente: El autor.

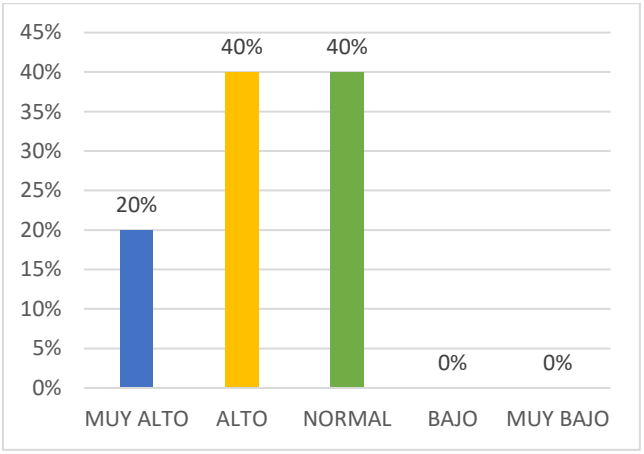


Fig. Pregunta #2. ¿Cuál cree usted que es el nivel de seguridad que actualmente dispone la empresa Uniscan?
Fuente: El autor.

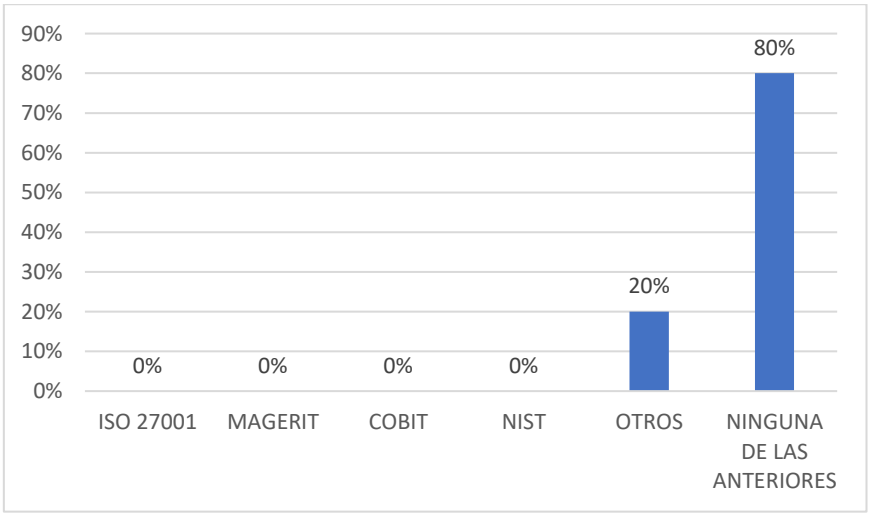


Fig. **Pregunta #3.** ¿Conoce usted alguna de las metodologías de seguridad informática que se indican a continuación?
Fuente: El autor.

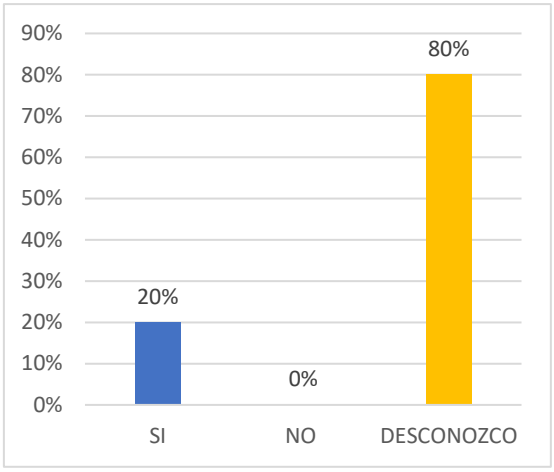


Fig. Pregunta #4. ¿Conoce usted si la empresa cuenta con planes de contingencia, políticas de seguridad, reglamentos u otros documentos que regulen el uso de correo electrónico, gestión de contraseñas, uso del wifi, prevención de riesgos informáticos, entre otros?
Fuente: El autor.

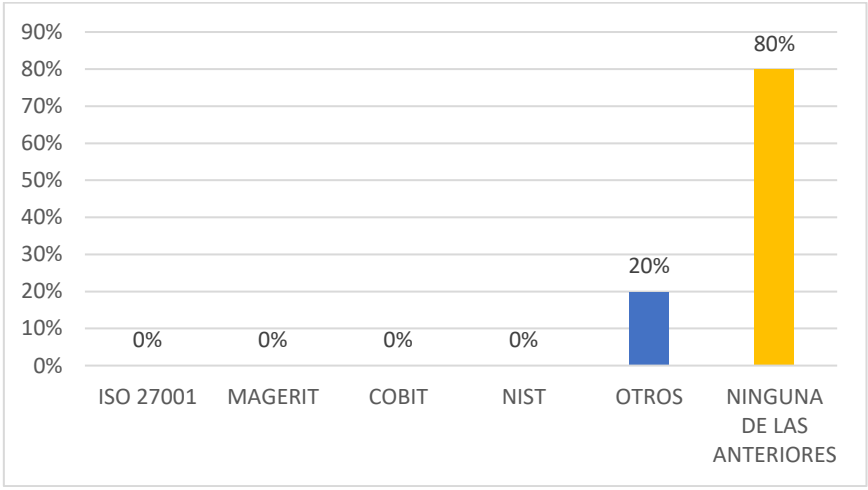


Fig. Pregunta #5. ¿Qué estándar de seguridad de la información maneja la Empresa Uniscan?
Fuente: El autor.

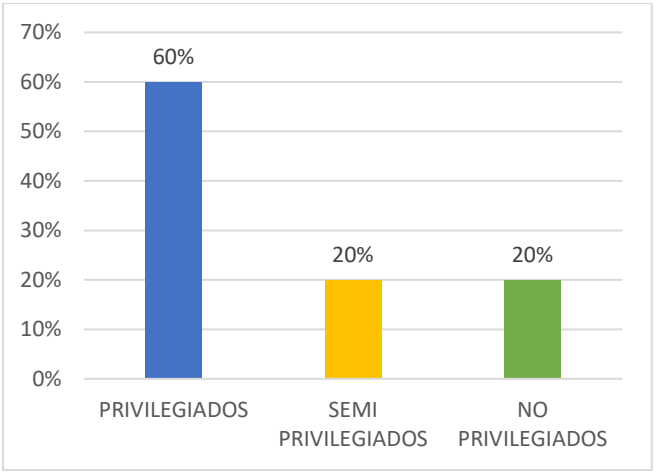


Fig. Pregunta #6. La información confidencial que maneja la empresa Uniscan, ¿para qué tipo de usuario es accesible?
Fuente: El autor.

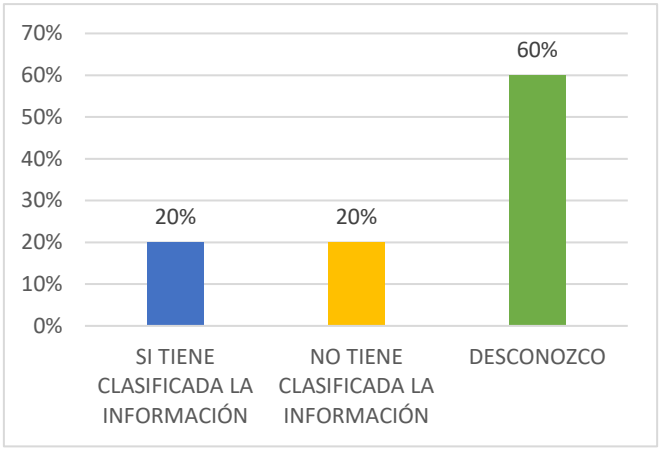


Fig. Pregunta #7. ¿Conoce usted si la empresa tiene una correcta clasificación de la información producida, recibida y almacenada (confidencial, pública, etc.)?
Fuente: El autor.

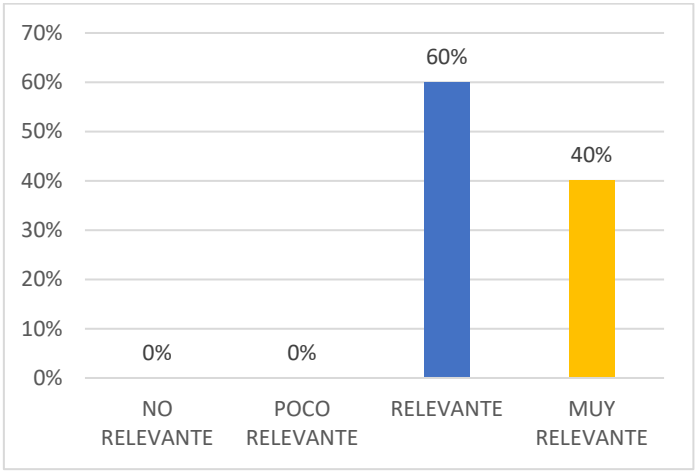


Fig. Pregunta #8. ¿De la escala del 1 al 4 como usted calificaría la información de la empresa Uniscan donde 1 es información no relevante (NR) y 4 es información muy relevante (MR)?
Fuente: El autor.

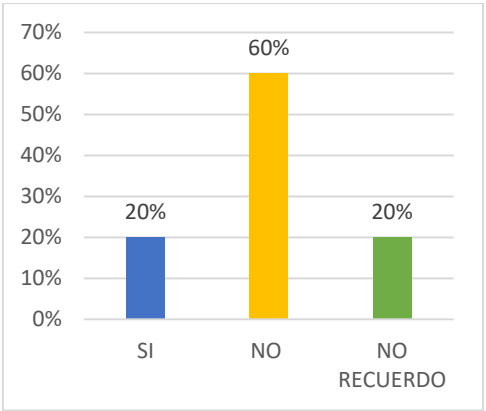


Fig. Pregunta #9. Usted como profesional que labora en el departamento técnico de la organización Uniscan. ¿Conoce usted si han sufrido algún incidente de seguridad que haya ocasionado daños en la infraestructura tecnológica?
Fuente: El autor.

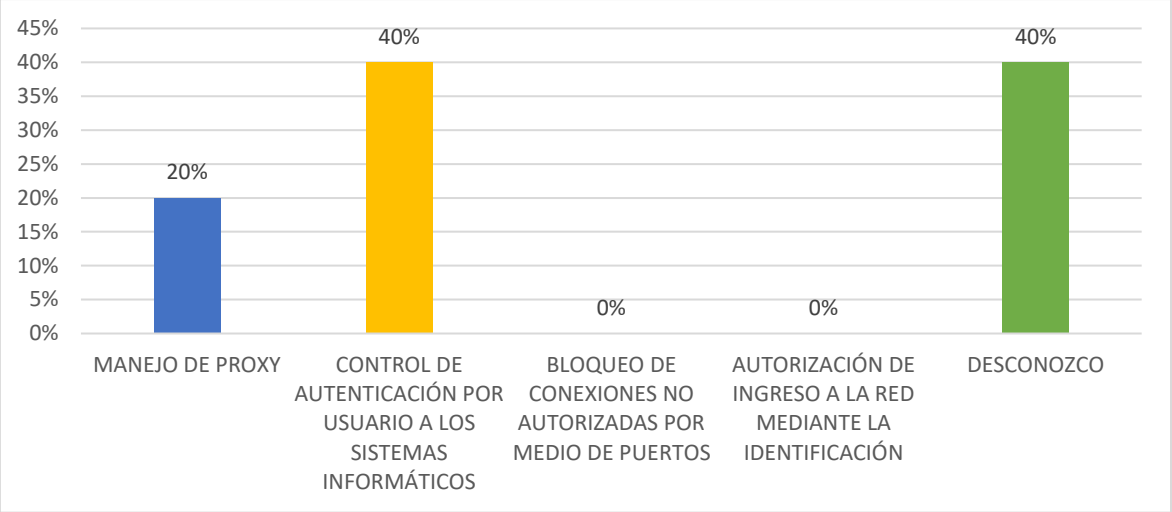


Fig. Pregunta #10. ¿Qué tipo de restricciones se encuentran implementadas en la red en general o en ciertas partes de la red?
Fuente: El autor.

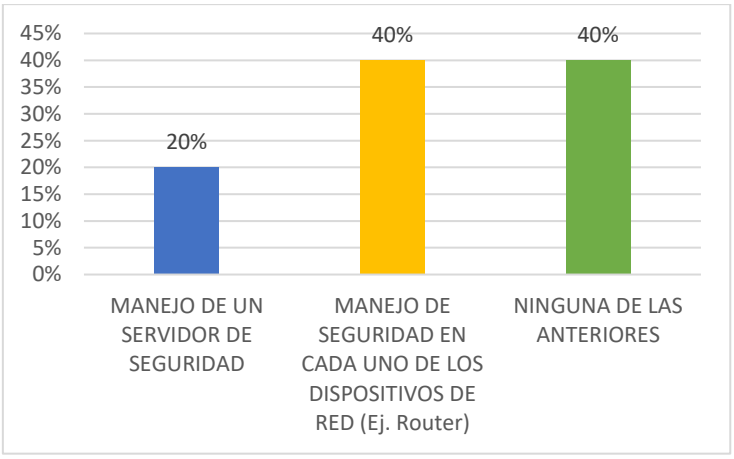


Fig. Pregunta #11. Las restricciones que maneja usted en el departamento técnico informático dentro de la red de trabajo de la empresa, ¿en qué dispositivo se encuentran configuradas?
Fuente: El autor.

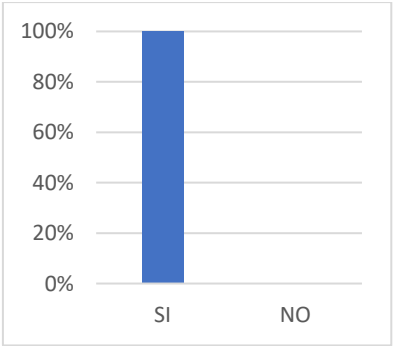


Fig. Pregunta #12. ¿Usted como profesional de tecnología considera que la inversión en seguridad informática es de gran importancia para proteger los activos de información que son de carácter confidencial?
Fuente: El autor.

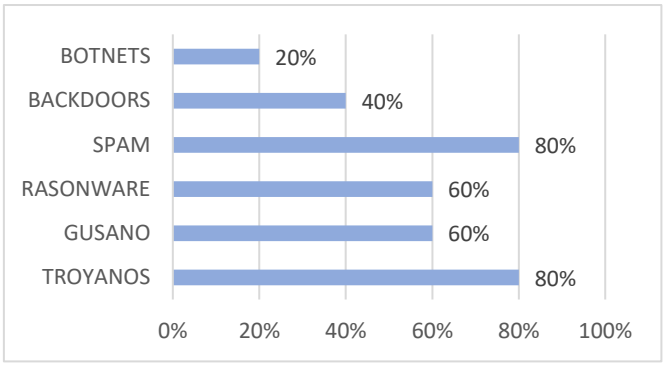


Fig. Pregunta #13. ¿Qué tipos de virus informático o ataques informáticos se deben mitigar para evitar los accesos a la información de carácter confidencial?, se debe considerar que es una pregunta de selección múltiple.
Fuente: El autor.

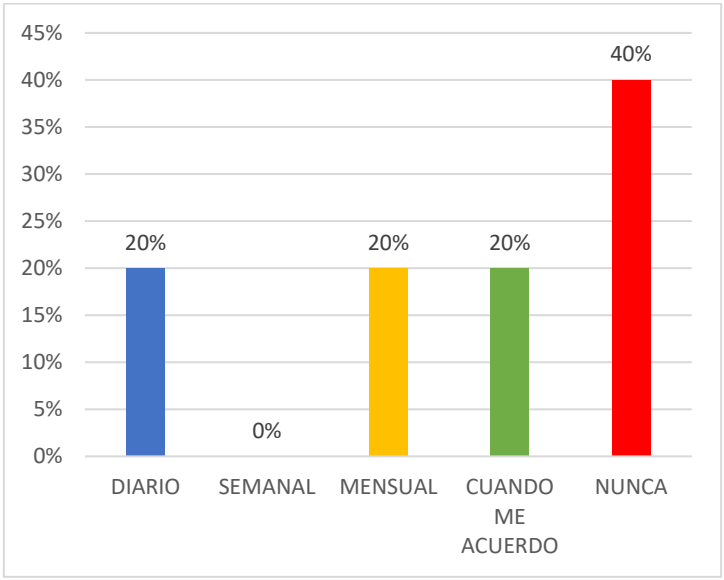


Fig. Pregunta #14. ¿Con qué frecuencia realiza copias de seguridad de su información y correo electrónico personal?
Fuente: El autor.

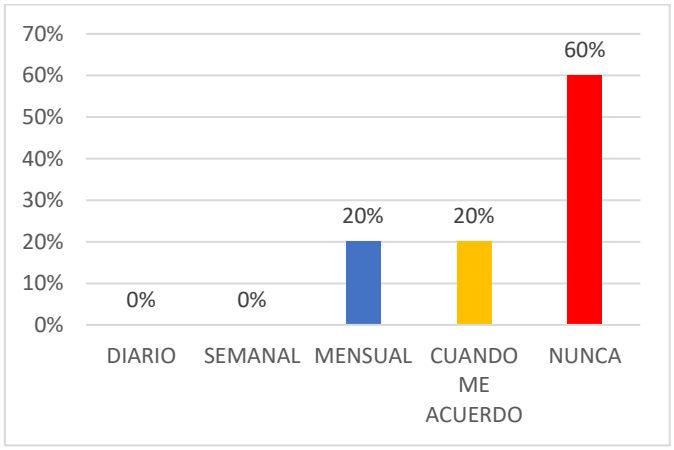


Fig. Pregunta #15. ¿Con qué frecuencia realiza copias de seguridad de su información y correo electrónico de la empresa?
Fuente: El autor.

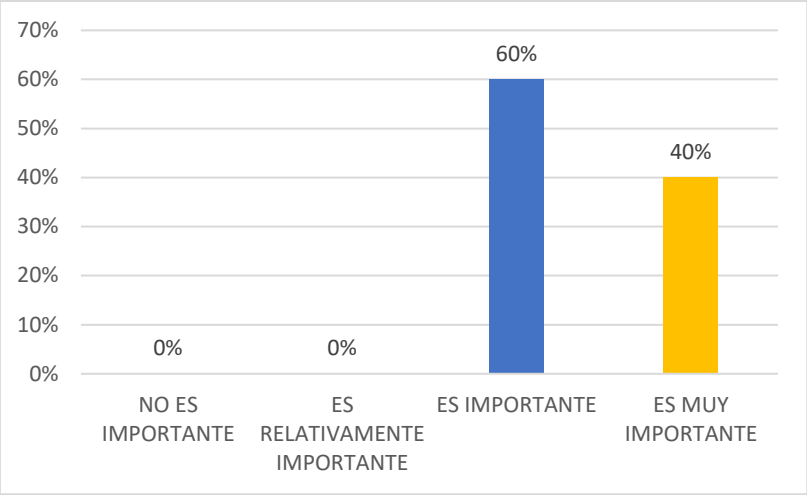


Fig. Pregunta #16. ¿Cree que concientizar sobre la ciberseguridad es una medida básica para laborar en un ciberespacio más seguro?
Fuente: El autor.

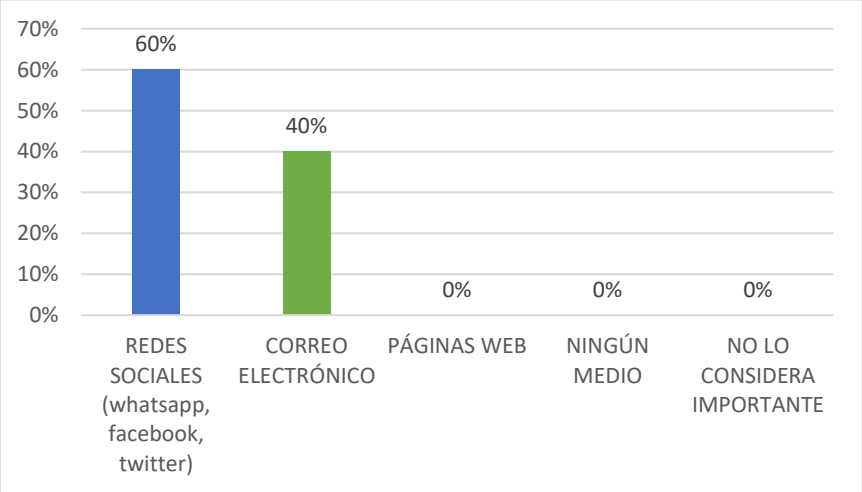


Fig. Pregunta #17. ¿A través de qué medio cree que se debería realizar campañas de concienciación sobre temas de ciberseguridad?
Fuente: El autor.

ANEXO 3. DIAGRAMAS DE BARRAS DE LA ENCUESTA REALIZADA AL PERSONAL ADMINISTRATIVO DE LA EMPRESA UNISCAN.

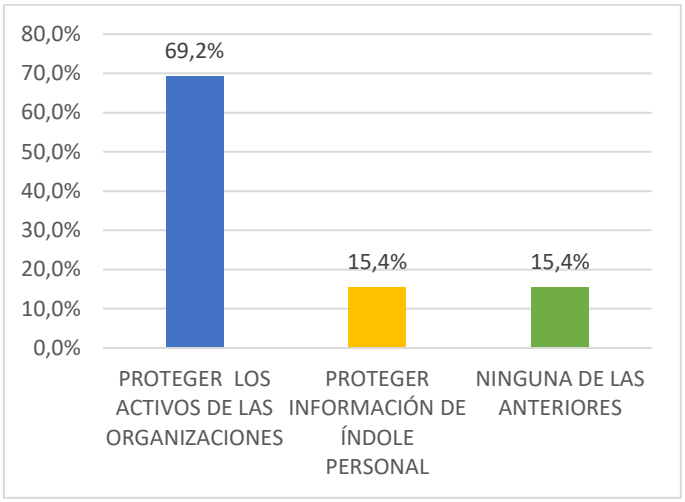


Fig. Pregunta #1. ¿Qué propósito principal tiene la seguridad informática?
Fuente: El autor.

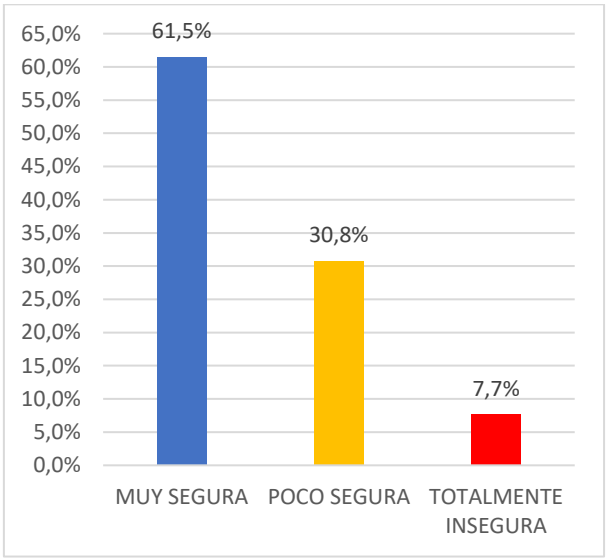


Fig. Pregunta #2. ¿Qué tan segura considera usted la red informática de la empresa que se encuentra laborando?
Fuente: El autor.

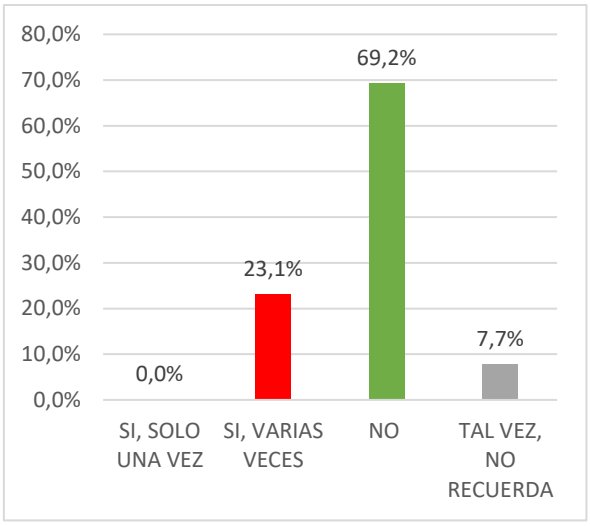


Fig. Pregunta #3. ¿Ha compartido usted datos de la red con personas ajenas a la empresa?
Fuente: El autor.

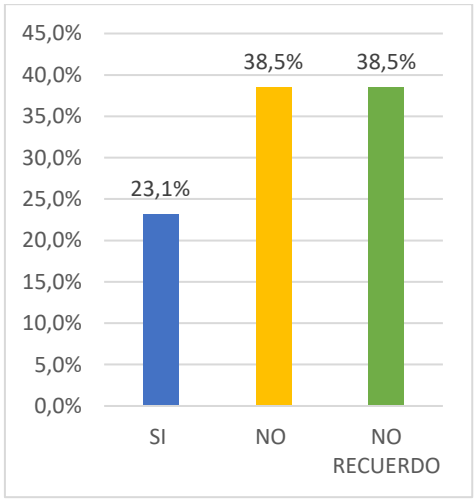


Fig. Pregunta #4. Dentro de la red informática de la empresa. ¿Ha sido usted víctima de ataques informáticos?
Fuente: El autor.

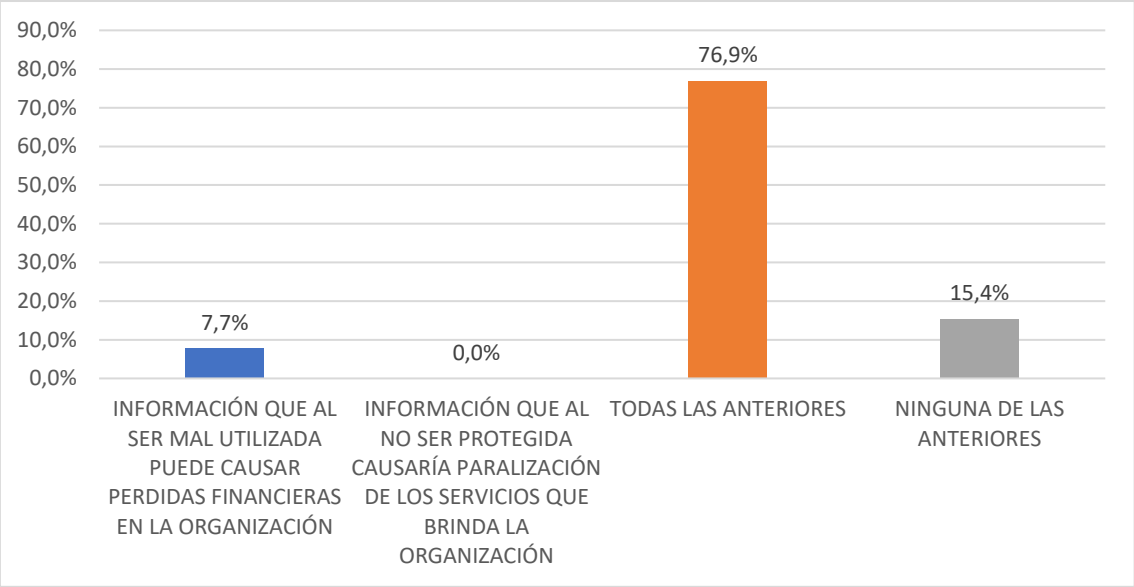


Fig. Pregunta #5. ¿Qué datos sensibles almacenados en la empresa es considerada como información?
Fuente: El autor.

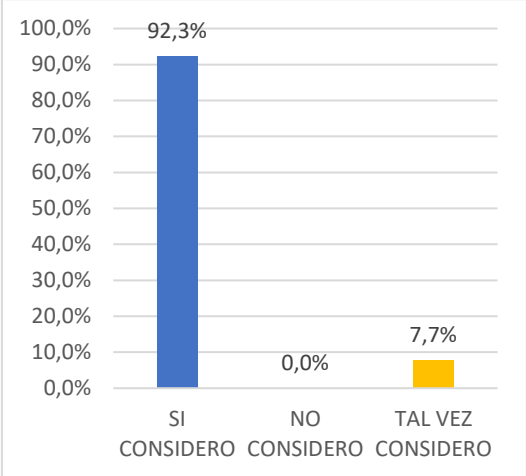


Fig. Pregunta #6. ¿Considera usted que la información es un valor de gran importancia para la empresa y que solamente personal honesto y autorizado puede tener acceso a ella?
Fuente: El autor.

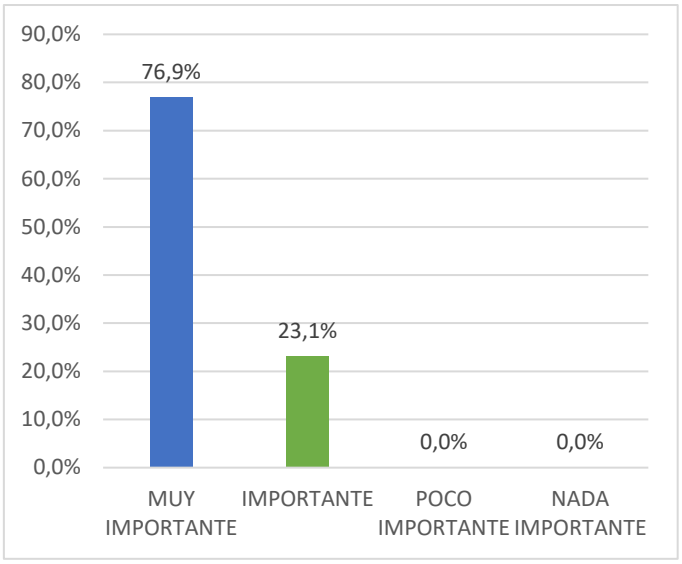


Fig. Pregunta #7. ¿Usted cree importante que las empresas inviertan en seguridad informática?
Fuente: El autor.

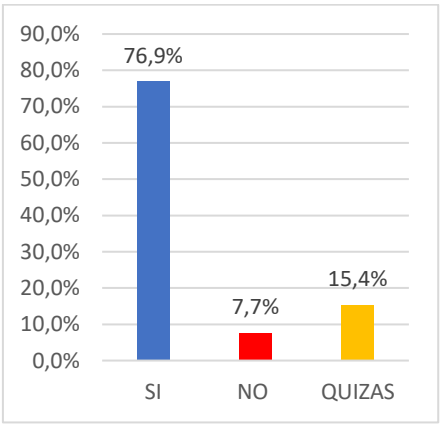


Fig. Pregunta #8. ¿Usted cree que la información debe ser de carácter confidencial?
Fuente: El autor.

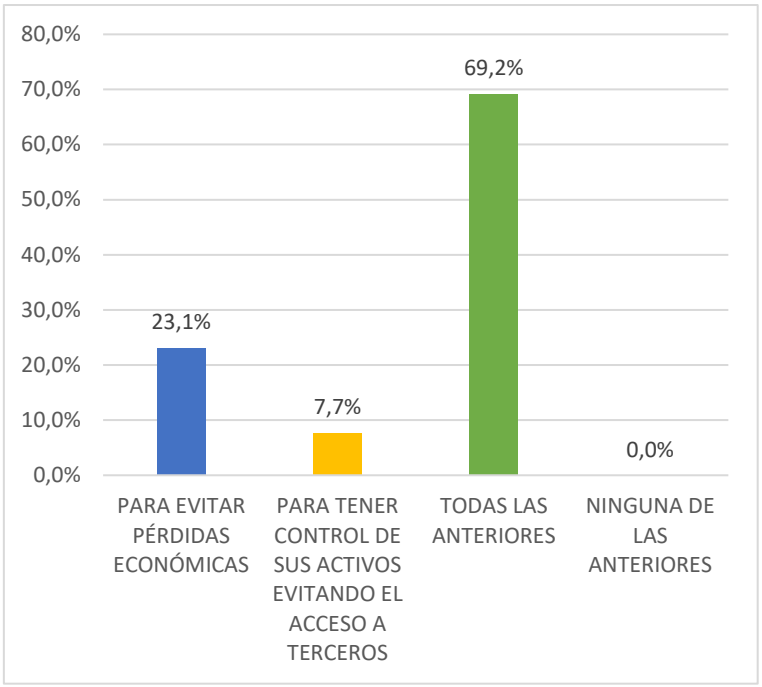


Fig. Pregunta #9. ¿Qué objetivo cree usted que poseen las organizaciones en proteger su información de carácter confidencial?
Fuente: El autor.

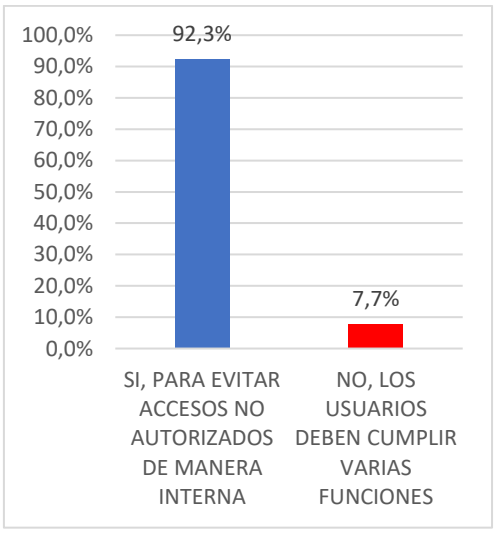


Fig. Pregunta #10. ¿Cree usted que los usuarios deben de tener privilegios en el sistema informático de acuerdo a las funciones que desempeñan en la organización?
Fuente: El autor.

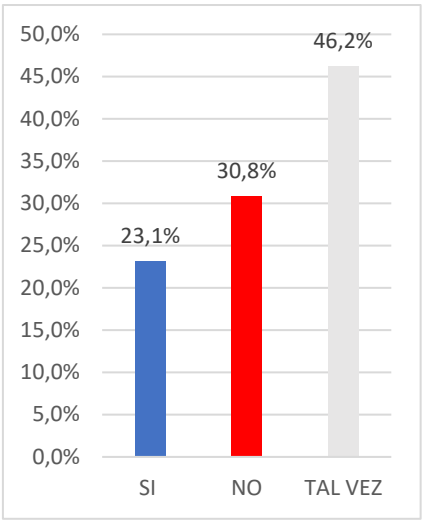


Fig. Pregunta #11. ¿Conoce usted si la empresa cuenta con personal especializado en seguridad informática o un equipo de respuesta a incidentes de seguridad informática?
Fuente: El autor

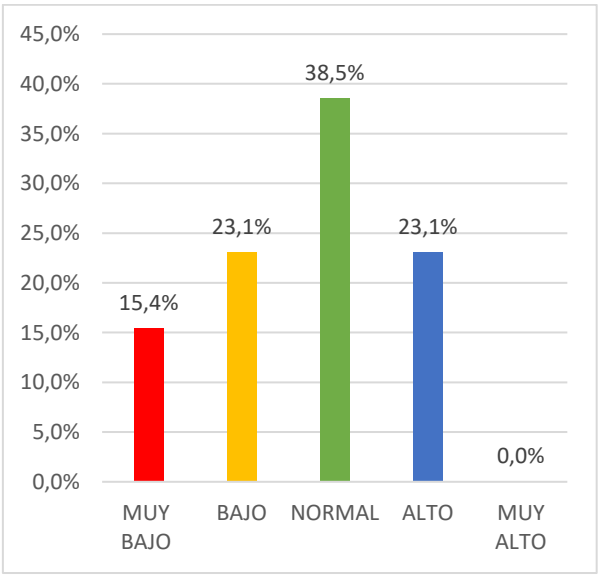


Fig. Pregunta #12. ¿Cuál cree usted que es el nivel de seguridad que actualmente dispone la empresa?
Fuente: El autor.

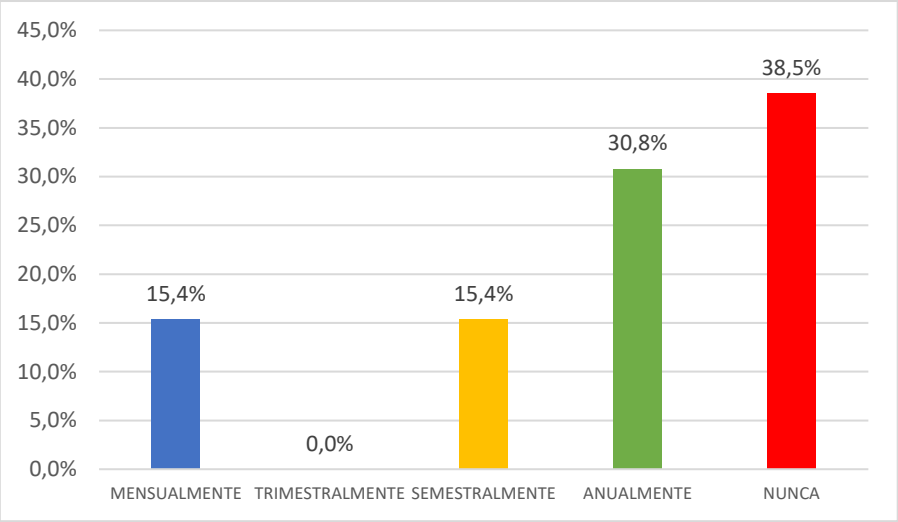


Fig. Pregunta #13. ¿Con que periodo la organización realiza capacitaciones a los funcionarios sobre temas de ciberseguridad?
Fuente: El autor.

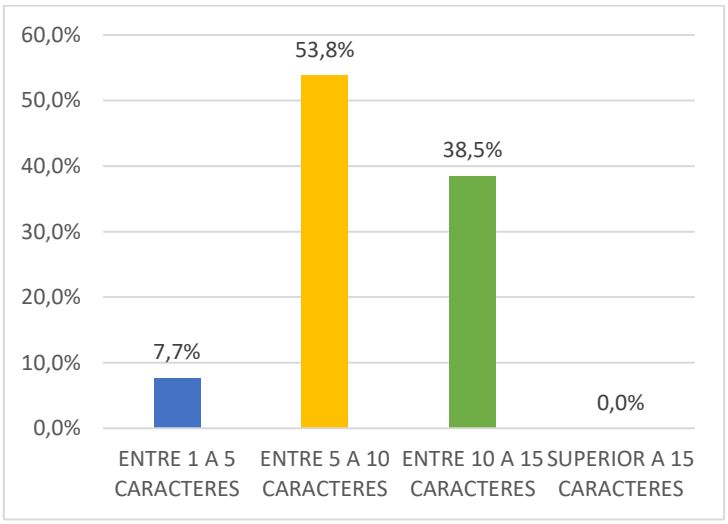


Fig. Pregunta #14. ¿Las contraseñas que usted usa tienen una longitud normalmente de?
Fuente: El autor.

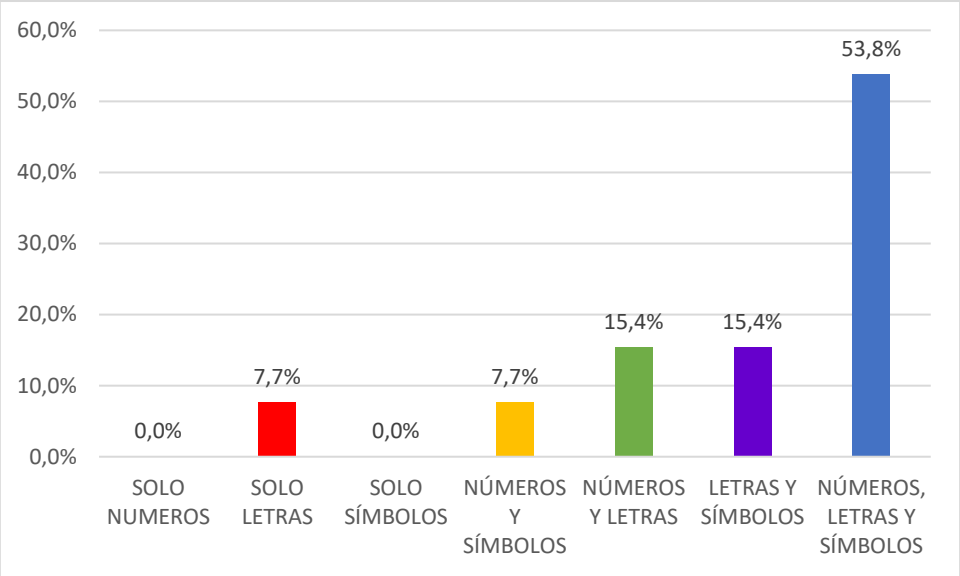


Fig. Pregunta #15. ¿Las contraseñas que usted implementa por lo general están compuestas de?
Fuente: El autor.

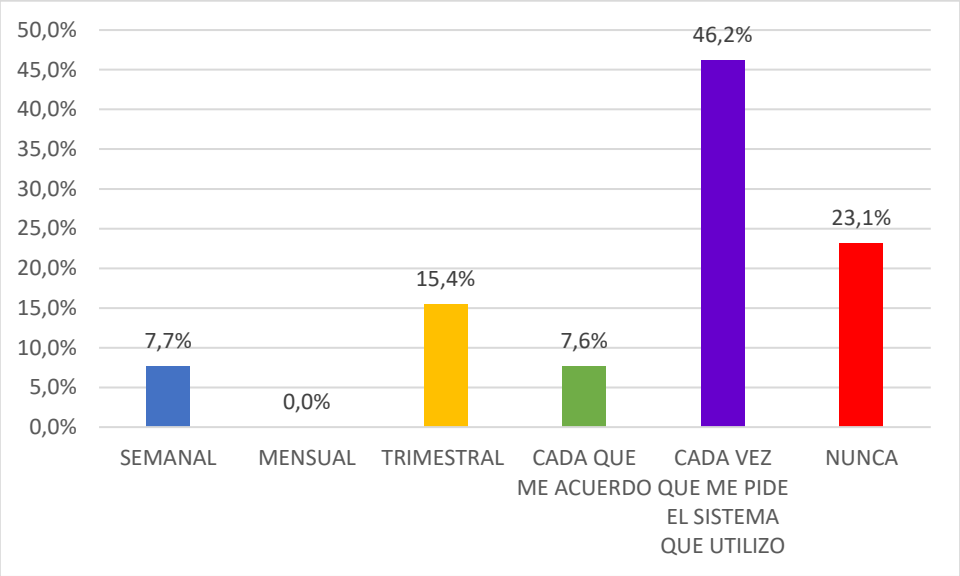


Fig. Pregunta #16. ¿Con que frecuencia cambia sus contraseñas?
Fuente: El autor.

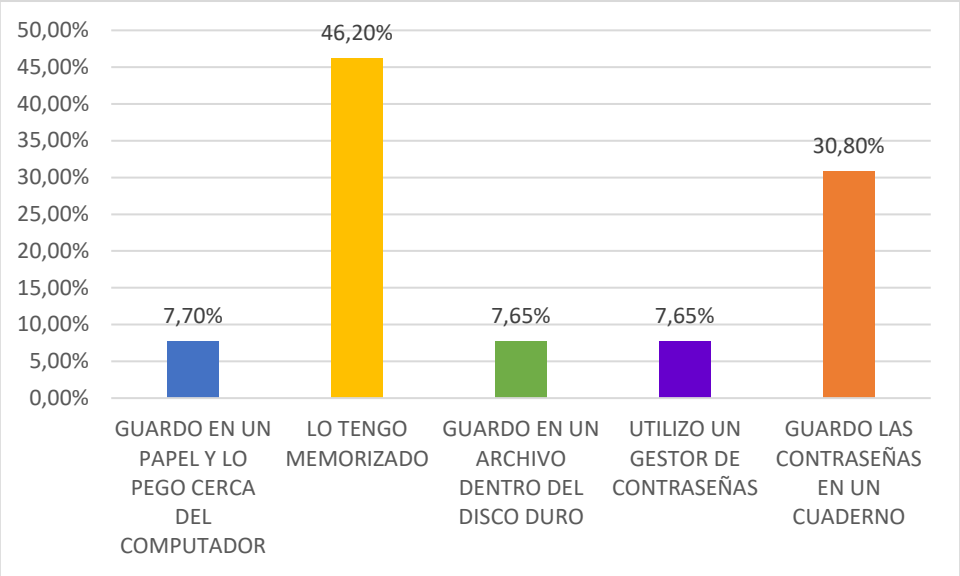


Fig. Pregunta #17. ¿Dónde almacena las contraseñas que utiliza?
Fuente: El autor.

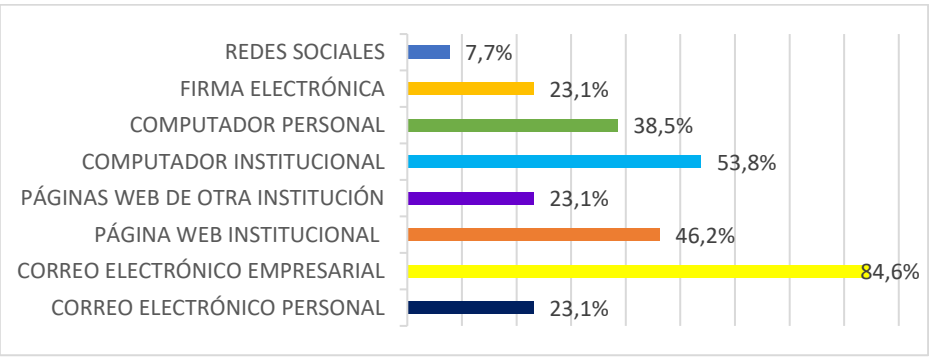


Fig. Pregunta #18. ¿Del siguiente listado seleccione que tecnologías utiliza para desarrollar las labores de la empresa? (puede escoger varias opciones).
Fuente: El autor.

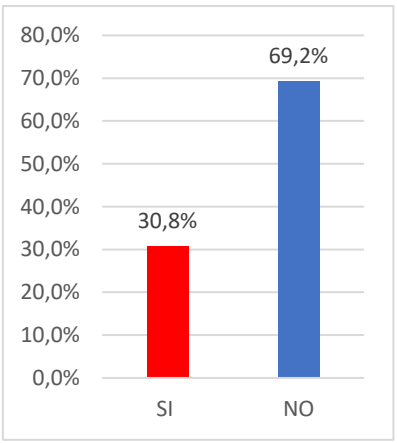


Fig. Pregunta #19. ¿Ha sufrido accesos ilícitos en cuanto a su información por medio de correo electrónico?
Fuente: El autor.

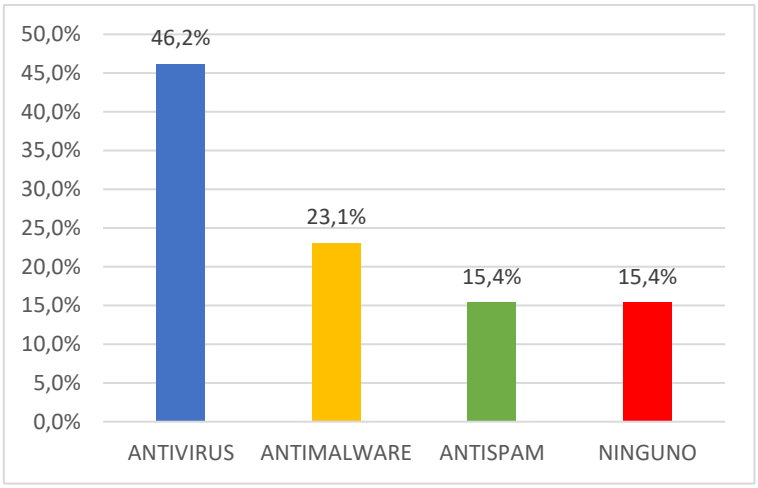
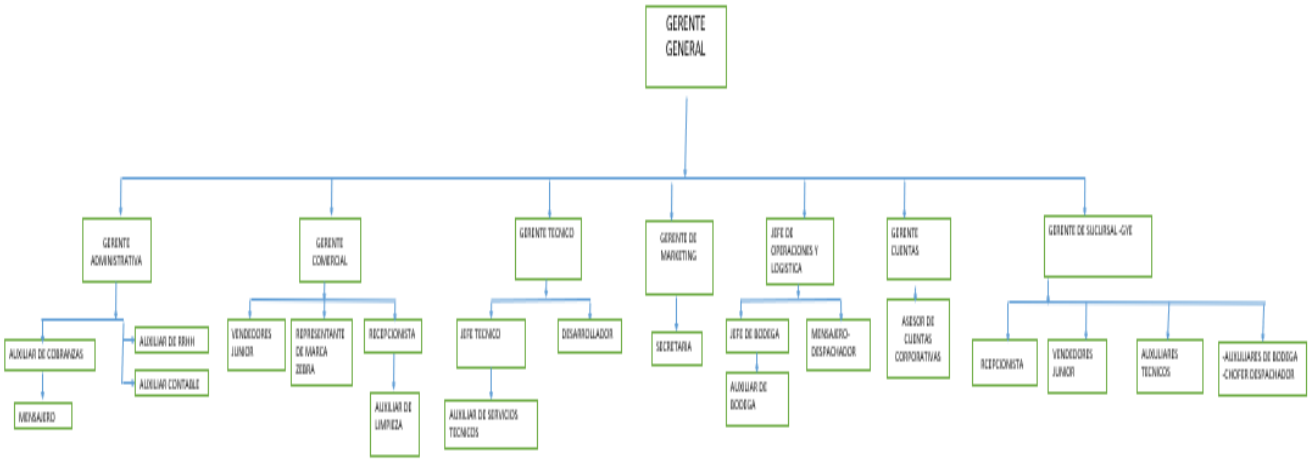


Fig. Pregunta #20. ¿Conoce sobre algún sistema de protección contra ciberataques para computador o dispositivo móvil?
Fuente: El autor.

ANEXO 4. ORGANIGRAMA ESTRUCTURAL DE LA ORGANIZACIÓN UNISCAN.



ANEXO 5. INVENTARIO DEL HARDWARE DE LOS ACTIVOS DE INFORMACIÓN DE LA ORGANIZACIÓN UNISCAN.

Departamento o Área	Nombre de la persona a cargo del activo	Tipo de activo	Marca	Modelo	Tipo de Sistema	Sistema Operativo	Versión S.O.	Procesador	RAM	BIOS	Direccion IP	Dirección MAC	Nombre de HOST	Serie
Departamento Técnico	Milton Navarro	portátil	HP	Pavilion 15-eh0xxx	64 bits	Windows 10 Home Single Language	10.0.19044	AMD64 Family 23 Model 96, 2375 Mhz	8GB	AMI F.17, 08/12/2021	192.168.1.220	fe80::8ef2:3b68:b53b:2527	DESKTOP-CVS8ITE	5CD10111CD
	Jimmy Avilloa	portátil	TOSHIBA	Satellite C55-C5205	64 bits	Windows 10 Home Single Language	10.0.19045	Intel64 Family 6 Model 69, 1700 Mhz	8GB	INSYDE Corp. 5.00, 16/07/2015	192.168.1.128	fe80::25a0:4f93:2abf:db09	DESKTOP-A3D97OU	8F148631C
	Briggette Echeverría	portátil	DELL	G3 3590 (P89F)	64 bits	Windows 10 Pro	10.0.19044	Intel64 Family 6 Model 158, 2592 Mhz	12GB	Dell Inc. 1.11.1, 19/08/2020	192.168.0.135	fe80::dbeb:dc1d:9ae4:3942	DESKTOP-P3VFLVR	B9GNHW2
	Nicolás Redrobán	portátil	LENOVO	81Y4	64 bits	Windows 10 Pro	10.0.19044	Intel64 Family 6 Model 165, 2592 Mhz	16GB	LENOVO E6CN39WW, 05/09/2022		fe80::f281:fb3e:c0dc:6d88	DESKTOP-4Q7J5DO	
	José Luis Trujillo	portátil	DELL	G3 3590 (P89F)	64 bits	Windows 10 Home Single Language	10.0.19044	Intel64 Family 6 Model 158, 2592 Mhz	8GB	Dell Inc. 1.11.1, 19/08/2020	192.168.1.129	fe80::4c0f:5284:1467:3153	DESKTOP-TEU0A1D	
	Luis Villacrés	portátil	ASUS	X512F	64 bits	Windows 10 Pro	10.0.19044	Intel64 Family 6 Model 142, 1792 Mhz	8GB	American Megatrends Inc. X512F.309, 01/02/2021		fe80::7a16:e9a8:3784:4fd3	DESKTOP-JD64J76	
Departamento de Ventas	Belén Aguilar	portátil	HP	Laptop 14-dq0001la	64 bits	Windows 10 Home Single Language	10.0.19044	Intel64 Family 6 Model 78, 1992 Mhz	12GB	INSYDE F.10, 28/07/2017			DESKTOP-T79QL9A	5CD7508V5R
	Enrique Navarro	portátil	DELL	Inspiron 15-3567	64 bits	Windows 10 Home	10.0.19044	Intel64 Family 6 Model 78, 2000 Mhz	8GB	Dell Inc. 2.9.0, 17/01/2019	192.168.1.149	fe80::583b:7752:f46a:9d46	DESKTOP-U4MKMCP	49WL5L2
	Fernanda Patiño	portátil	HP	15-13387wm	64 bits	Windows 10 Home	10.0.19044	AMD64 Family 22 Model 48, 2200 Mhz	8GB	American Megatrends Inc. F.40, 08/08/2017	192.168.0.155	fe80::3d5d:cf48:9d6c:df65	DESKTOP-5QFP9JH	5CD75127QF
Recepción Principal	Estefanía Umaquinga	Escritorio			64 bits	Windows 10 Home	10.0.19044	Intel64 Family 6 Model 42, 3300 Mhz	4GB	Intel Corp. BEH6110H.86A.0041.2012.0319.1659, 19/03/2012	192.168.1.51	fe80::8993:5403:5681:c45c	DESKTOP-DOCE58K	
Recepción Gerencia	Alexandra Betancourt	portátil	HP	14-bp001la	64 bits	Windows 10 Home Single Language	10.0.19044	Intel64 Family 6 Model 61, 2000 Mhz	8GB	Insyde F.36, 06/01/2020	192.168.0.120	fe80::cb5:f258:a667:fc2b	DESKTOP-BLKRFFF	5CG64402PV
Departamento Comercial	José Basantes	portátil	HP	ProBook 450 G6	64 bits	Windows 10 Pro	10.0.19043	Intel64 Family 6 Model 142, 1792 Mhz	8GB	HP R17 Ver. 01.19.00, 13/01/2022	192.168.0.230	fe80::6153:6553:b96d:2a	DESKTOP-2IG5C8K	5CD9388HBY
	Mishell Molina	portátil	TOSHIBA	Satellite S55-C5360	64 bits	Windows 10 Home	10.0.19045	Intel64 Family 6 Model 78, 2492 Mhz	8GB	INSYDE Corp. 1.30, 06/10/2015	192.168.1.136	fe80::1f12:9410:a1ab:190b	DESKTOP-HDB980U	YF049284C
	Diego Cepeda	portátil	DELL	Latitude E7470	64 bits	Windows 10 Home	10.0.19043	Intel64 Family 6 Model 78, 2501 Mhz	8GB	Dell Inc. 1.30.3, 16/07/2021	192.168.0.125	fe80::e46d:2135:1ecc:1526	DESKTOP-JCG1OB2	
	Verónica Betancourt	portátil	TOSHIBA	Satellite C45-A3PM206FL	64 bits	Windows 10 Home Single Language	10.0.19044	Intel64 Family 6 Model 42, 2300 Mhz	8GB	INSYDE Corp. 1.00, 30/04/2013	192.168.1.65	fe80::7592:c6b7:3586:9649	DESKTOP-6LL3V7U	5D0411Z5C
	Lina Andrade	portátil	HP	15-ra0011la	64 bits	Windows 11 Home Single Language	10.0.22621	Intel64 Family 6 Model 142, 1801 Mhz	8GB	Insyde F.02, 24/05/2018	192.168.0.199	fe80::f710:8753:7aa2:47dd	DESKTOP-4P2A0O8	CND8261XX7
	Diana Vásquez	portátil	HP	14-bs011la	64 bits	Windows 10 Home	10.0.19044	Intel64 Family 6 Model 78, 1992 Mhz	12GB	Insyde F.21, 24/07/2017	192.168.0.67	fe80::7ec0:ef67:fb27:f496	DESKTOP-TPDUDGN	5CD7390V2P
Contabilidad	Leslie Silva	Escritorio			64 bits	Windows 10 Pro	10.0.19044	Intel64 Family 6 Model 158, 3600 Mhz	8GB	American Megatrends Inc. 1002, 24/05/2019	192.168.1.120	fe80::7b64:52e7:237e:f6f2	DESKTOP-9AVMJDN	
	Dayanara Patiño	portátil												
Bodega	Diego Pineda	Escritorio			64 bits	Windows 10 Home	10.0.19044	Intel64 Family 6 Model 42, 3300 Mhz	8GB	Intel Corp. BEH61.10H.86A.0041.2012.0319.1659, 19/03/2012	192.168.1.163	fe80::441f:f145:aa16:44a0	DESKTOP-G1FEEL6	
	David	portátil	HP	14-r005la	64 bits	Windows 11 Home Single Language	10.0.19044	Intel64 Family 6 Model 58, 1801 Mhz	4GB	Insyde F.18, 21/05/2014	192.168.1.248	fe80::71ec:7ebd:fde3b:200c	DESKTOP-LGLUOCJ	CND4372PF5
RACK	Servidor	Escritorio	DELL	PowerEdge T130	64 bits	Windows Server 2016 Standard	10.0.14393	Intel64 Family 6 Model 94, 3000 Mhz	64BG	Dell Inc. 1.4.5, 09/08/2016	NIC2 172.30.1.2 26.139.193.219	fe80::8159:6a28:9a3a:3ee9	SERVIDOR	

ANEXO 6. DESARROLLO DEL PROCESO FOOTPRINTING PARA LA ORGANIZACIÓN UNISCAN.

A continuación, tenemos la dirección de la página Web de la organización objetivo de estudio:

Sitio web: ***https://www.uniscan.com.ec/***

Lo primero que debemos revisar es la información que se expone en la página web oficial de la organización, esta puede ser: nombres de los colaboradores, direcciones de las oficinas, números de teléfono y cuentas de correo electrónico.

Nombres de los colaboradores, correos electrónicos y extensión telefónica:

José Luis Basantes: jbasantes@uniscan.com.ec, ext. 105, Corporativo
Diana Vásquez: dvasquez@uniscan.com.ec, Productos Zebra ext. 105, Corporativo
Belén Aguilar: baguilarm@uniscan.com.ec, ext. 107, Ventas
Enrique Navarro: enavarro@uniscan.com.ec, ext. 106, Ventas
Fernanda Patiño: fpatino@uniscan.com.ec, ext. 108, Ventas
José Luis Trujillo: jtrujillo@uniscan.com.ec, ext. 109, Dpto. Técnico

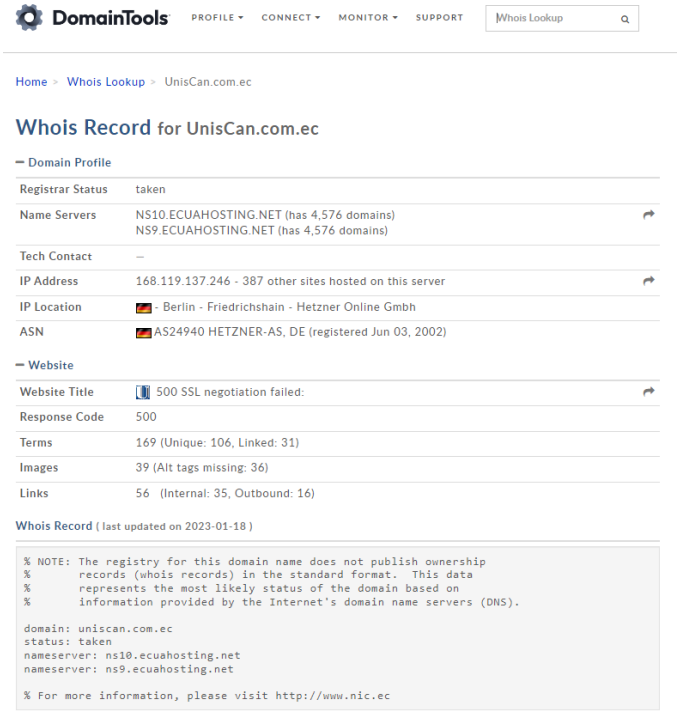
Dirección de la oficina matriz y números telefónicos:

De los Perales N47-164 y Eloy Alfaro (Sector Monteserrín)
Teléfonos: (+593) (02) 2245919 / 2244614 / 2244643 / 2244640
info@uniscan.com.ec
Quito – Ecuador

Recepción: ext. 101
Administración: ext. 104
Mercadeo: ext. 102
Bodega: ext. 110
Desarrollo: ext. 114
Contabilidad: ext. 111
Crédito y Cobranzas: ext. 112
Dpto. Técnico: ext. 115 y 116

Es importante recopilar la mayor información posible de manera pasiva sin interactuar todavía con la red de la empresa objetivo de estudio, para lo cual empezaremos a utilizar herramientas disponibles en el internet.

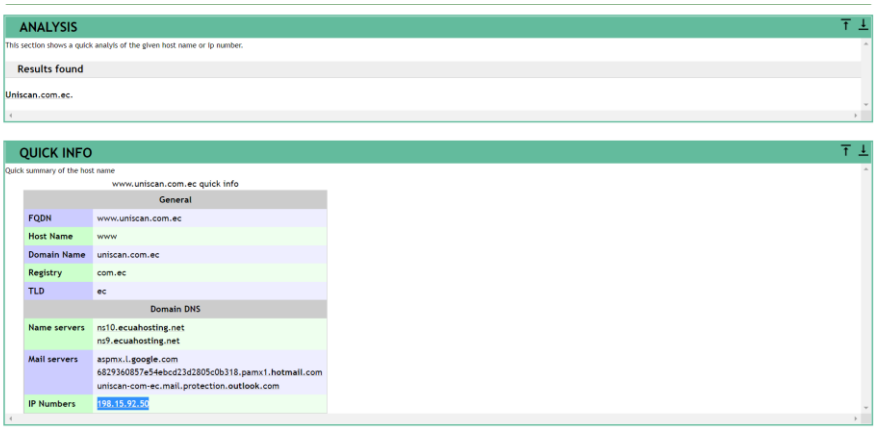
La primera herramienta que utilizaremos será “DomainTools”, que es una plataforma de inteligencia e investigación de amenazas a nivel empresarial basada en dominios y en el nombre del servidor de dominios (DNS). Esta herramienta ayuda a transformar los datos de amenaza en información, esta utilidad hace uso de indicadores de red, incluidos dominios e IP, vinculándolos a casi todos los dominios de internet.



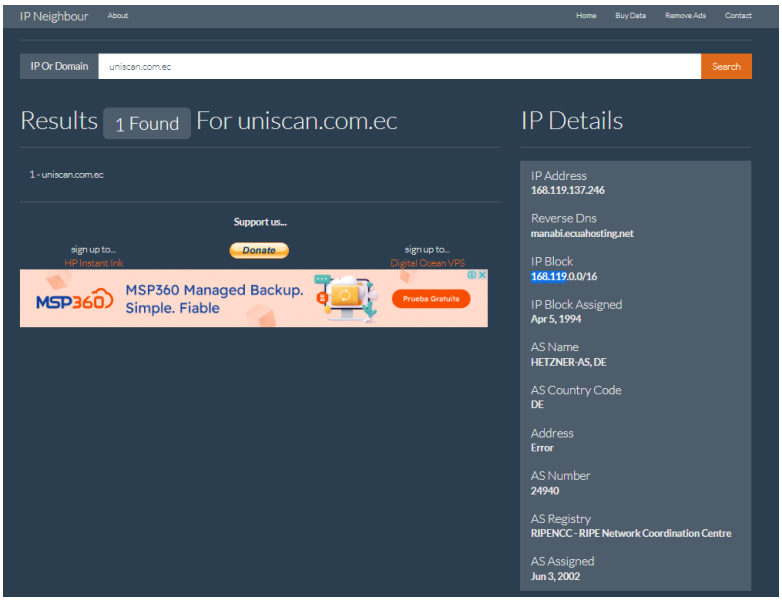
La información de relevancia que podemos observar después de ejecutar la herramienta en línea es que la empresa que brinda el servicio de hosting a la organización Uniscan es EcuaHosting.

Seguimos aplicando otra herramienta de análisis de dominio para ir recopilando más información, esta herramienta lleva el nombre de ROBTEX.

Con la herramienta ROBTEX podemos confirmar que la empresa que brinda el servicio de hosting a la organización Uniscan es EcuaHosting.

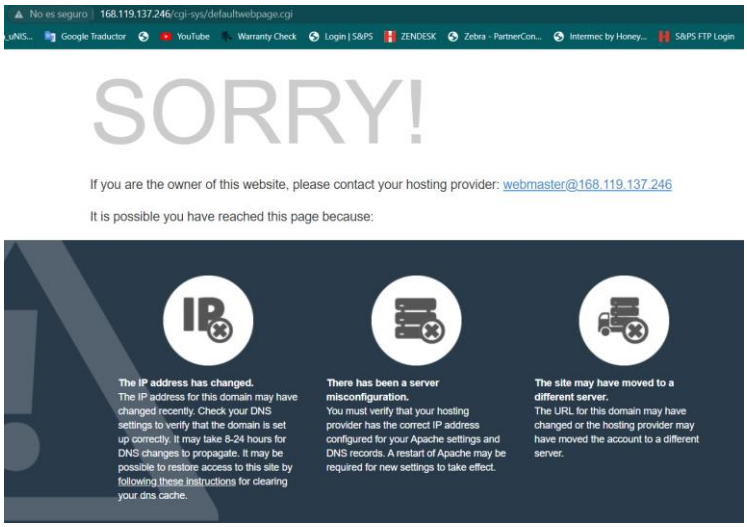


A continuación, utilizaremos la herramienta IP Neighbour para hallar más información importante utilizando la dirección Web o nombre de dominio (uniscan.com.ec) de la empresa que estamos analizando.

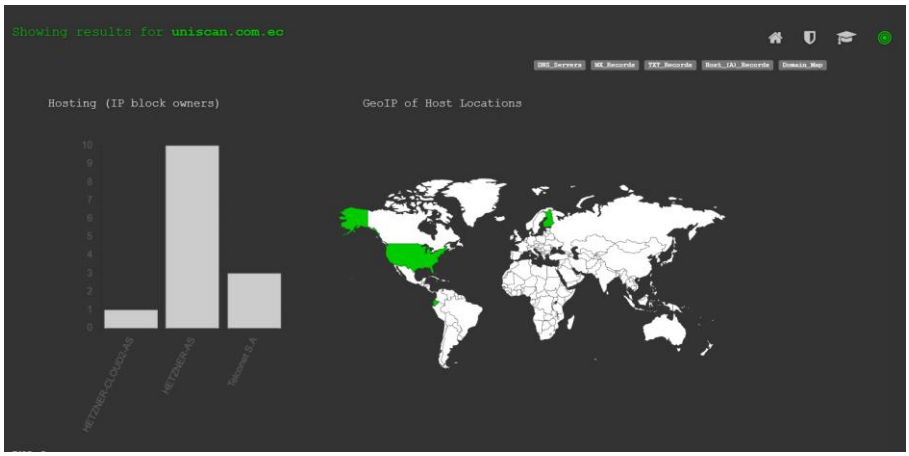


Es importante ejecutar todas las herramientas posibles, entre más información recolectada y siendo esta depurada para que los datos encontrados sean de utilidad en el análisis de vulnerabilidades del objetivo, es así como podremos armar un esquema que facilite el estudio del caso.

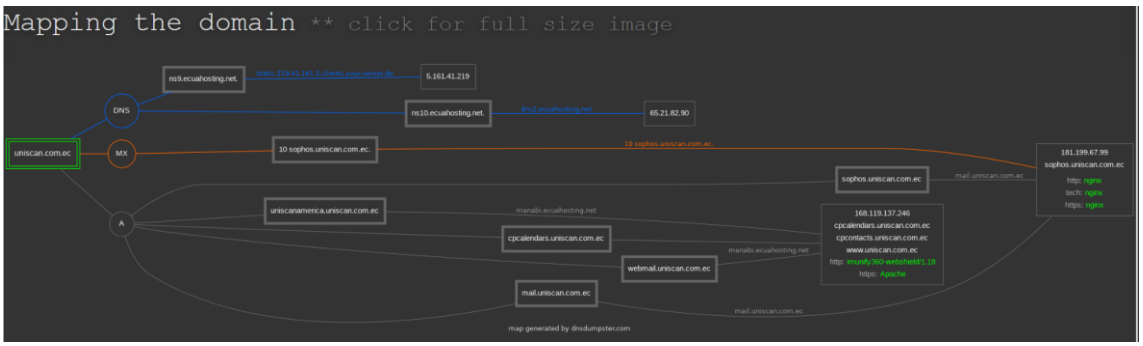
Con las direcciones IP halladas intentaremos ingresar utilizando un navegador y en la barra de ingreso URL colocamos la dirección IP encontrada anteriormente (168.119.137.246).



Como podemos ver en la imagen anterior, no hemos encontrado ningún dato de importancia, por lo que continuamos con el análisis de datos de manera pasiva utilizando la siguiente herramienta (“dnsdumster”) como se puede observar en la imagen que se encuentra a continuación.



De igual manera para ejecutar la búsqueda de información tuvimos que haber ingresado el dominio de interés, para este caso de estudio es: uniscan.com.ec
Lo interesante de esta herramienta on-line es que nos entrega un mapa del dominio que nos puede servir para obtener una ligera idea de la infraestructura con la que la organización cuenta.



Detalle de la información recopilada después de ejecutar la herramienta “dnsdumster”:

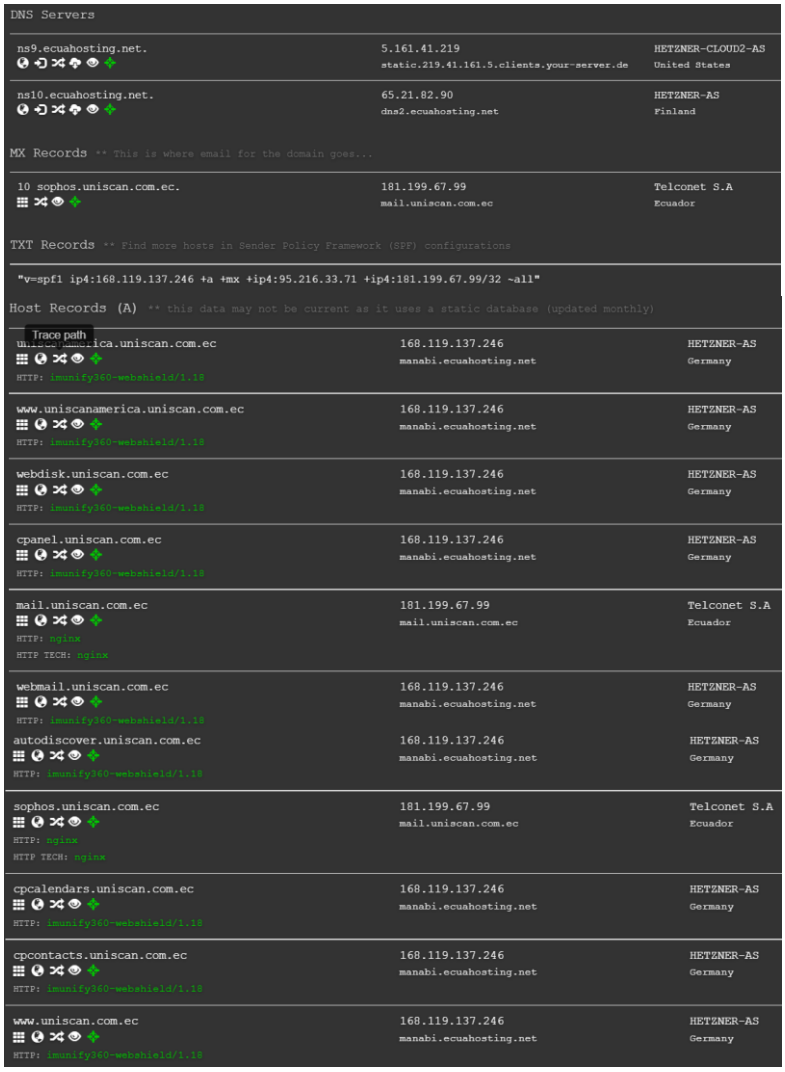
DNS Servers

ns9.ecuahosting.net.
5.161.41.219
static.219.41.161.5.clients.your-server.de HETZNER-CLOUD2-AS
United States
ns10.ecuahosting.net.
65.21.82.90
dns2.ecuahosting.net HETZNER-AS
Finland
MX Records ** This is where email for the domain goes...

10 sophos.uniscan.com.ec.
181.199.67.99
mail.uniscan.com.ec Telconet S.A
Ecuador
TXT Records ** Find more hosts in Sender Policy Framework (SPF) configurations

"v=spf1 ip4:168.119.137.246 +a +mx +ip4:95.216.33.71 +ip4:181.199.67.99/32 ~all"

A continuación, podemos observar diferentes direcciones IP que se pueden utilizar en algún navegador para verificar que no esté abierto algún servicio, y que pudiera ser una ventana abierta para la ejecución de algún tipo de amenaza.

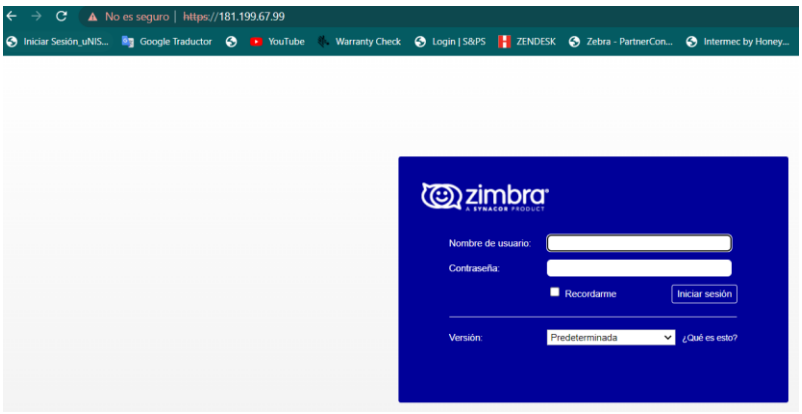


Seguimos obteniendo información con ayuda de la herramienta dnsdumster:

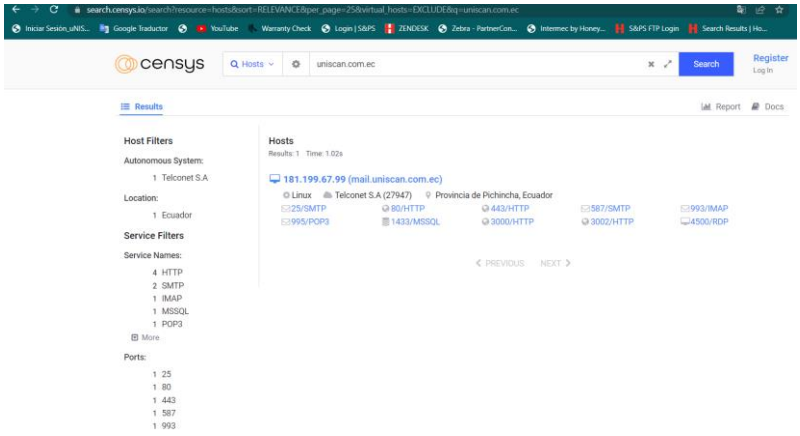
mail.uniscan.com.ec
HTTP: nginx
HTTP TECH: nginx 181.199.67.99
mail.uniscan.com.ec Telconet S.A
Ecuador
sophos.uniscan.com.ec
HTTP: nginx
HTTP TECH: nginx 181.199.67.99
mail.uniscan.com.ec Telconet S.A Ecuador

Probaremos con la siguiente dirección IP (181.199.67.99) utilizando cualquier navegador de su preferencia, lo que podrá notar después del ingreso de la dirección es que se abre

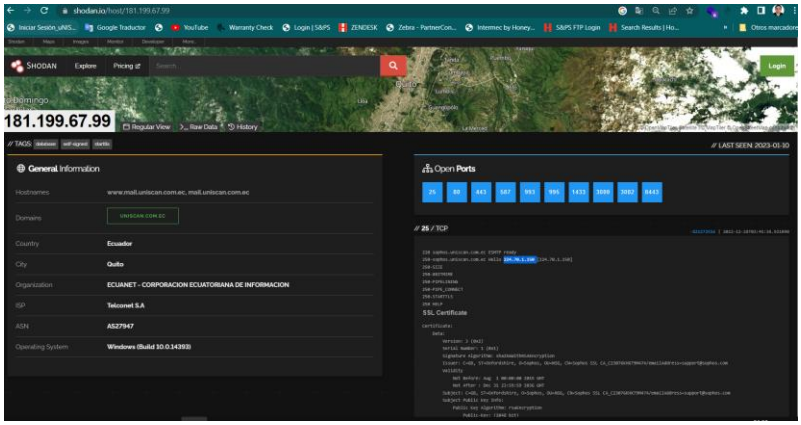
una ventana del servidor de correo electrónico Zimbra de la organización Uniscan, en la cual se nos solicita nombre de usuario y contraseña.



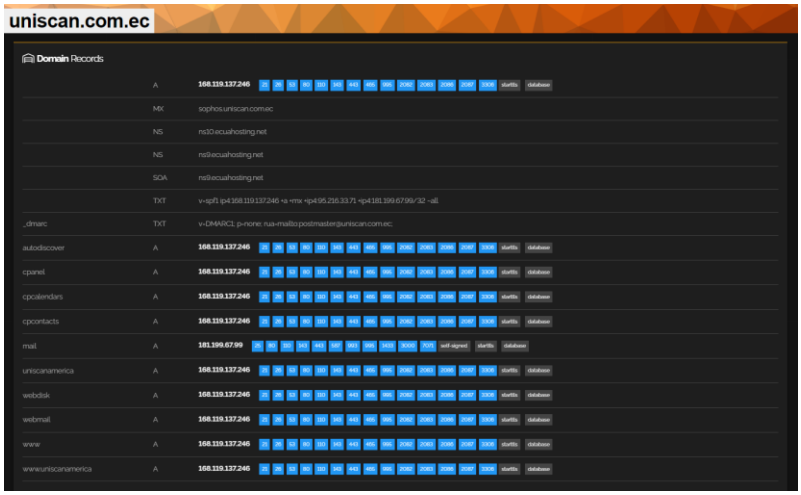
Otra herramienta que nos puede ser de mucha utilidad es CENSYS, en la barra de búsqueda de dominio ingresamos la dirección de la organización, la página se actualiza y nos muestra una dirección IP y una lista de varios puertos, también podemos ver el nombre de la provincia PICHINCHA donde se encuentra ubicada la matriz de la empresa.



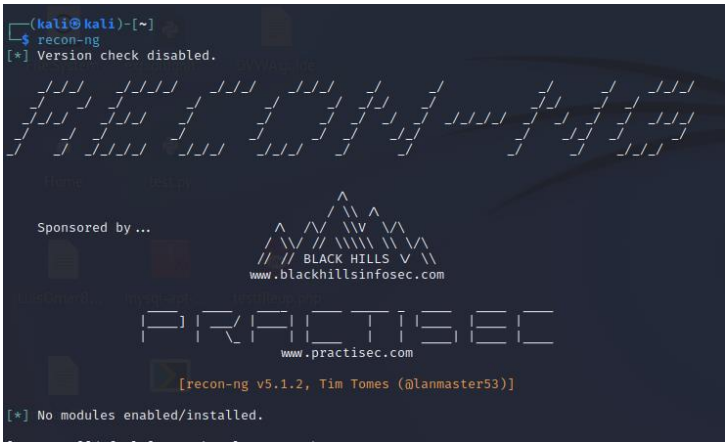
A continuación, utilizaremos la herramienta SHODAN para recopilar la mayor información posible.



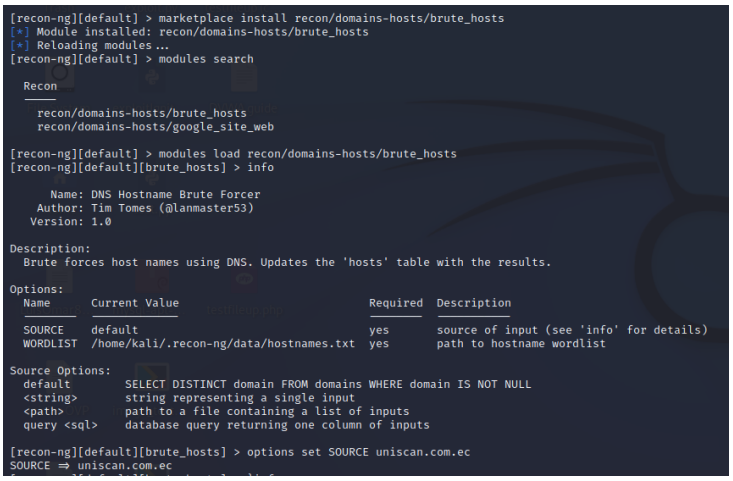
Continuando con la investigación y utilizando la herramienta SHODAN podemos observar información de la estructura tecnológica, estos datos recopilados nos permiten hacernos una idea de cómo está formada la estructura tecnológica de la organización, se puede identificar la marca “SOPHOS” que pertenece a un equipo firewall, y otras direcciones IP que pueden ser revisadas en busca de información relevante.



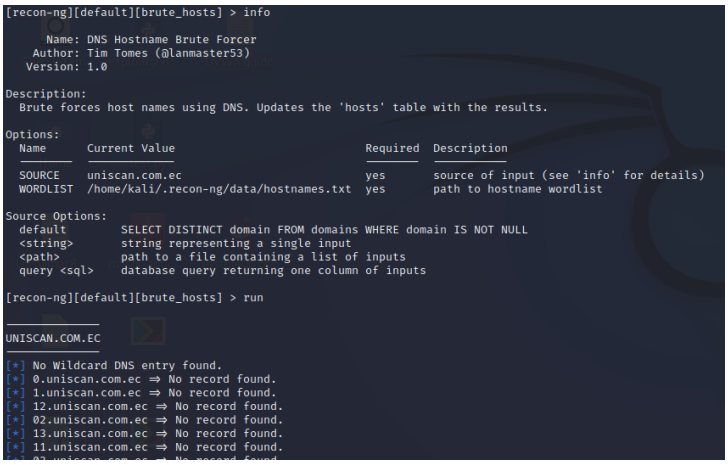
Una de las herramientas que podemos utilizar en el ambiente de Kali-Linux es: Recon-ng, la aplicación es un marco de trabajo de reconocimiento web con todas las funciones escrito en Python, completado con módulos independientes, con interacción con la base de datos, funciones especiales integradas, ayuda interactiva y finalización de comandos. Recon-ng proporciona un entorno poderoso en el que el reconocimiento basado en código abierto se puede realizar de manera rápida y completa sobre un sitio o sistema web.



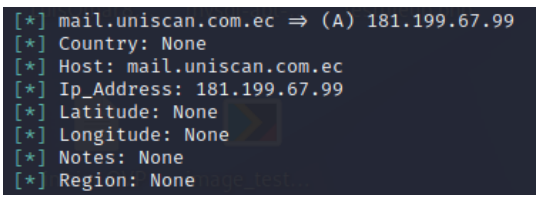
Como anteriormente vimos que es una aplicación modular, es necesario empezar instalando un módulo de la extensa lista que tiene el aplicativo, el módulo elegido fue: **recon/domains-hosts/brute-hosts,** con el comando **marketplace install** realizaremos la instalación.



El comando ***info*** nos permite ver una lista de opciones entre ellas encontramos: SOURCE Y WORDLIST, las cuales podemos modificar para que tengan los valores necesarios para que la aplicación realice una búsqueda más centralizada teniendo como objetivo la organización Uniscan, los valores que podemos configurar son: SOURCE=> uniscan.com.ec y WORDLIST=> es una lista de extensión ***.txt*** que utilizará la aplicación para poder entregar el nombre del host al cual se encuentre asociada un dirección IP , también es posible utilizar el comando SET para configurar los valores de las opciones antes mencionadas.



A continuación, podemos observar uno de los hallazgos de la herramienta, y verificamos una vez más que la dirección: 181.199.67.99 corresponde al servidor de correo electrónico que se encuentra instalado en la organización Uniscan, y que tiene como nombre de host: mail.uniscan.com.ec.

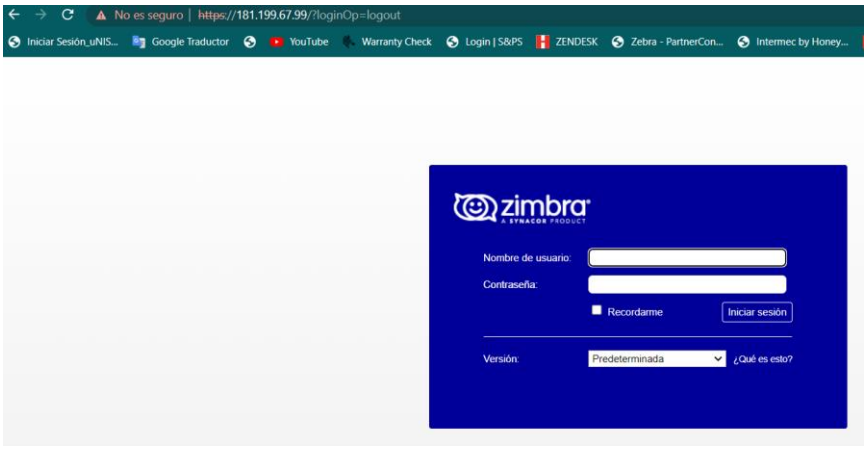


[*] mail.uniscan.com.ec => (A) 181.199.67.99
[*] Country: None
[*] Host: mail.uniscan.com.ec

[*] Ip_Address: 181.199.67.99
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None

Abrimos un navegador Web, realizamos la búsqueda de la dirección IP y podremos observar cómo se despliega la ventana de ingreso al correo de Zimbra donde se nos pide:

nombre de usuario y contraseña.



ANEXO 7. ANÁLISIS DE VULNERABILIDADES DE LAS REDES DE LA ORGANIZACIÓN UNISCAN CON LA HERRAMIENTA NMAP.

ANÁLISIS DE VULNERABILIDADES EN LA RED DEL DEPARTAMENTO TÉCNICO DE LA EMPRESA UNISCAN.

Identificamos la versión de Windows en la cual tenemos instalada nuestra máquina virtual, desde la que realizaremos el pentesting.

Versión de Sistema Operativo:

Microsoft Windows [Versión 10.0.19044.2486]

Utilizamos el comando ipconfig para identificar la dirección IP de nuestra máquina:

```
C:\Users\Luis_PC>ipconfig
Configuración IP de Windows

Adaptador de LAN inalámbrica Wi-Fi:
   Sufijo DNS específico para la conexión. . :
   Vínculo: dirección IPv6 local. . . : fe80::7a26:e9d:8784:4fd3%35
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.1.122
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : 192.168.1.1
```

Realizamos mediante el ***comando ping*** un test de comunicación mediante el uso de la red hacia otros dispositivos que se encuentra en la para verificar que nos encontramos correctamente conectados a la red objetivo de estudio:

```
C:\Users\Luis_PC>ping 192.168.1.148

Haciendo ping a 192.168.1.148 con 32 bytes de datos:
Respuesta desde 192.168.1.148: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.148: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.148: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.148: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 192.168.1.148:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

Utilizando el comando ping ***[ip_addres]***, para identificar la dirección IP del servidor:

```
C:\Users\Luis_PC>ping 172.30.1.2
Haciendo ping a 172.30.1.2 con 32 bytes de datos:
Respuesta desde 172.30.1.2: bytes=32 tiempo=2ms TTL=127
Respuesta desde 172.30.1.2: bytes=32 tiempo=2ms TTL=127
Respuesta desde 172.30.1.2: bytes=32 tiempo=3ms TTL=127
Respuesta desde 172.30.1.2: bytes=32 tiempo=2ms TTL=127
Estadísticas de ping para 172.30.1.2:
   Paquetes: enviados = 4, recibidos = 4, perdidos = 0
   (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
   Mínimo = 2ms, Máximo = 3ms, Media = 2ms
```

Se utilizará la herramienta nmap para encontrar toda la información posible del servidor, se apuntará a la dirección ip: ***172.30.1.2***, la información recolectada servirá para determinar el número de los puertos abiertos y las vulnerabilidades que pueden ser atacadas durante las pruebas de Pentesting.

```
┌──(vagrant㉿kali)-[~/UniScan/172.30.1.2]
└─$ nmap 172.30.1.2
```

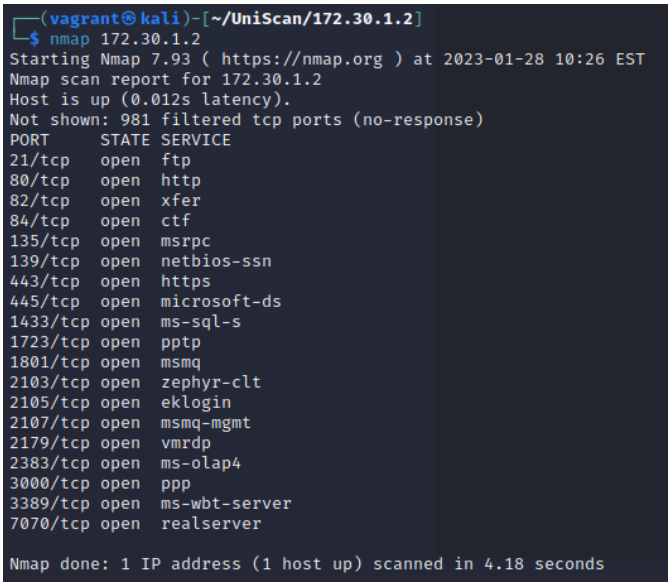


Fig. Análisis del servidor de Uniscan con la herramienta NMAP.

Continuamos con el análisis de los puertos utilizando la herramienta nmap, adicional hemos utilizado el atributo -p- que nos permite analizar más puertos por lo que a continuación tendremos una lista más grande puertos abiertos:

```
┌──(vagrant㉿kali)-[~/UniScan/172.30.1.2]
└─$ nmap -p- 172.30.1.2
```

```
┌──(vagrant㉿kali)-[~/UniScan/172.30.1.2]
└─$ nmap -p- 172.30.1.2
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-28 10:21 EST
Stats: 0:00:37 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 19.12% done; ETC: 10:25 (0:02:37 remaining)
Stats: 0:02:01 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 88.72% done; ETC: 10:24 (0:00:15 remaining)
Nmap scan report for 172.30.1.2
Host is up (0.019s latency).
Not shown: 65499 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
82/tcp    open  xfer
84/tcp    open  ctf
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
1433/tcp  open  ms-sql-s
1723/tcp  open  pptp
1801/tcp  open  msmq
2103/tcp  open  zephyr-clt
2105/tcp  open  eklogin
2107/tcp  open  msmq-mgmt
2179/tcp  open  vmrdp
2383/tcp  open  ms-olap4
3000/tcp  open  ppp
3002/tcp  open  exlm-agent
3389/tcp  open  ms-wbt-server
5656/tcp  open  unknown
5985/tcp  open  wsman
7070/tcp  open  realserver
47001/tcp open  winrm
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown
49667/tcp open  unknown
49668/tcp open  unknown
49669/tcp open  unknown
49670/tcp open  unknown
49671/tcp open  unknown
49672/tcp open  unknown
49704/tcp open  unknown
49733/tcp open  unknown
51384/tcp open  unknown
56633/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 132.58 seconds
```

Fig. Análisis del servidor de Uniscan con la herramienta NMAP (se utiliza el comando ***-p-***).

Se continúa utilizando la herramienta nmap para recolectar más información y hallar la versión de cada uno los puertos, lo que nos permitirá identificar posibles vulnerabilidades, se utiliza el comando nmap con los atributos que se indican a continuación: # ***nmap -sV -v -O 172.30.1.2***

```
┌──(root㉿kali)-[/home/vagrant/UniScan/172.30.1.2]
└─# nmap -sV -v -O 172.30.1.2
```

```
┌──(root㉿kali)-[/home/vagrant/UniScan/172.30.1.2]
└─# nmap -sV -v -O 172.30.1.2
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-28 10:32 EST
NSE: Loaded 45 scripts for scanning.
Initiating Ping Scan at 10:32
Scanning 172.30.1.2 [4 ports]
Completed Ping Scan at 10:32, 0.21s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:32
Completed Parallel DNS resolution of 1 host. at 10:32, 0.00s elapsed
Initiating SYN Stealth Scan at 10:32
Scanning 172.30.1.2 [1000 ports]
Discovered open port 1723/tcp on 172.30.1.2
Discovered open port 80/tcp on 172.30.1.2
Discovered open port 3389/tcp on 172.30.1.2
Discovered open port 139/tcp on 172.30.1.2
Discovered open port 445/tcp on 172.30.1.2
Discovered open port 21/tcp on 172.30.1.2
Discovered open port 443/tcp on 172.30.1.2
Discovered open port 135/tcp on 172.30.1.2
Discovered open port 2179/tcp on 172.30.1.2
Discovered open port 3000/tcp on 172.30.1.2
Discovered open port 2383/tcp on 172.30.1.2
Discovered open port 7070/tcp on 172.30.1.2
Discovered open port 2107/tcp on 172.30.1.2
Discovered open port 1801/tcp on 172.30.1.2
Discovered open port 82/tcp on 172.30.1.2
Discovered open port 84/tcp on 172.30.1.2
Discovered open port 1433/tcp on 172.30.1.2
Discovered open port 2105/tcp on 172.30.1.2
Discovered open port 2103/tcp on 172.30.1.2
Completed SYN Stealth Scan at 10:32, 4.42s elapsed (1000 total ports)
Initiating Service scan at 10:32
Scanning 19 services on 172.30.1.2
Stats: 0:01:33 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 94.74% done; ETC: 10:34 (0:00:05 remaining)
Completed Service scan at 10:35, 156.51s elapsed (19 services on 1 host)
Initiating OS detection (try #1) against 172.30.1.2
Retrying OS detection (try #2) against 172.30.1.2
NSE: Script scanning 172.30.1.2.
Initiating NSE at 10:35
Completed NSE at 10:35, 1.22s elapsed
```

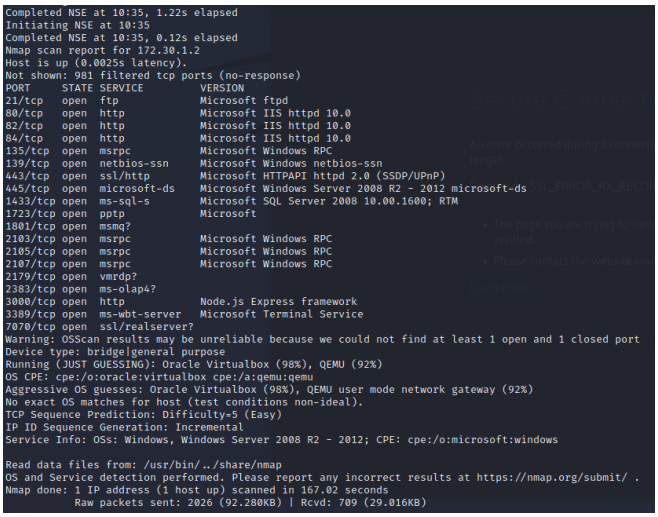
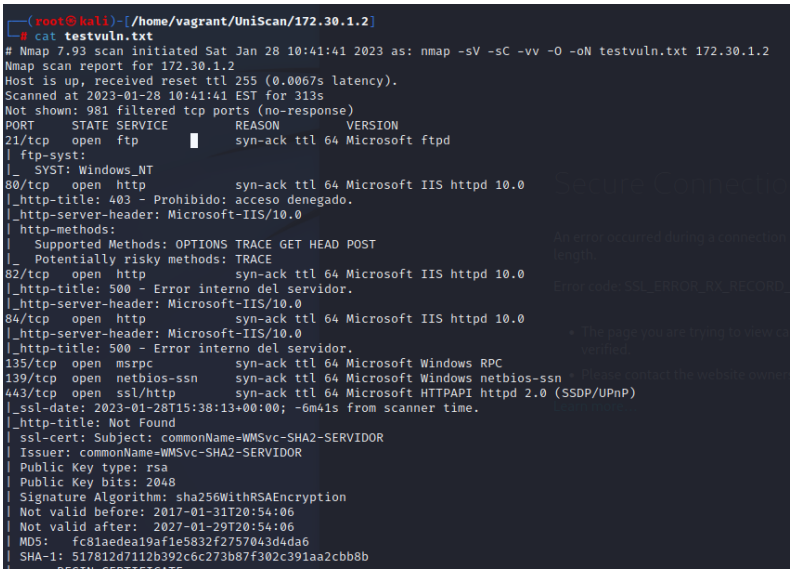
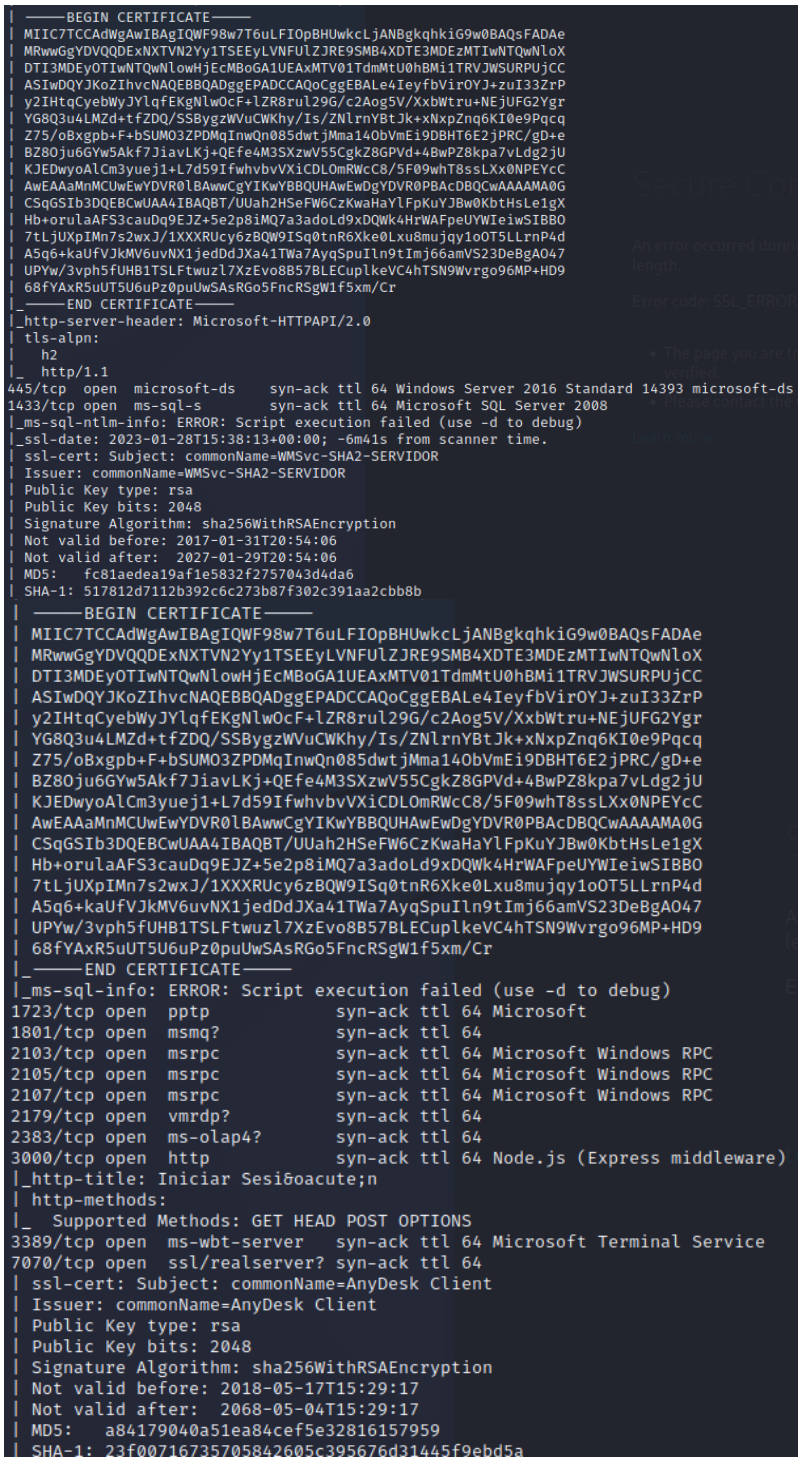


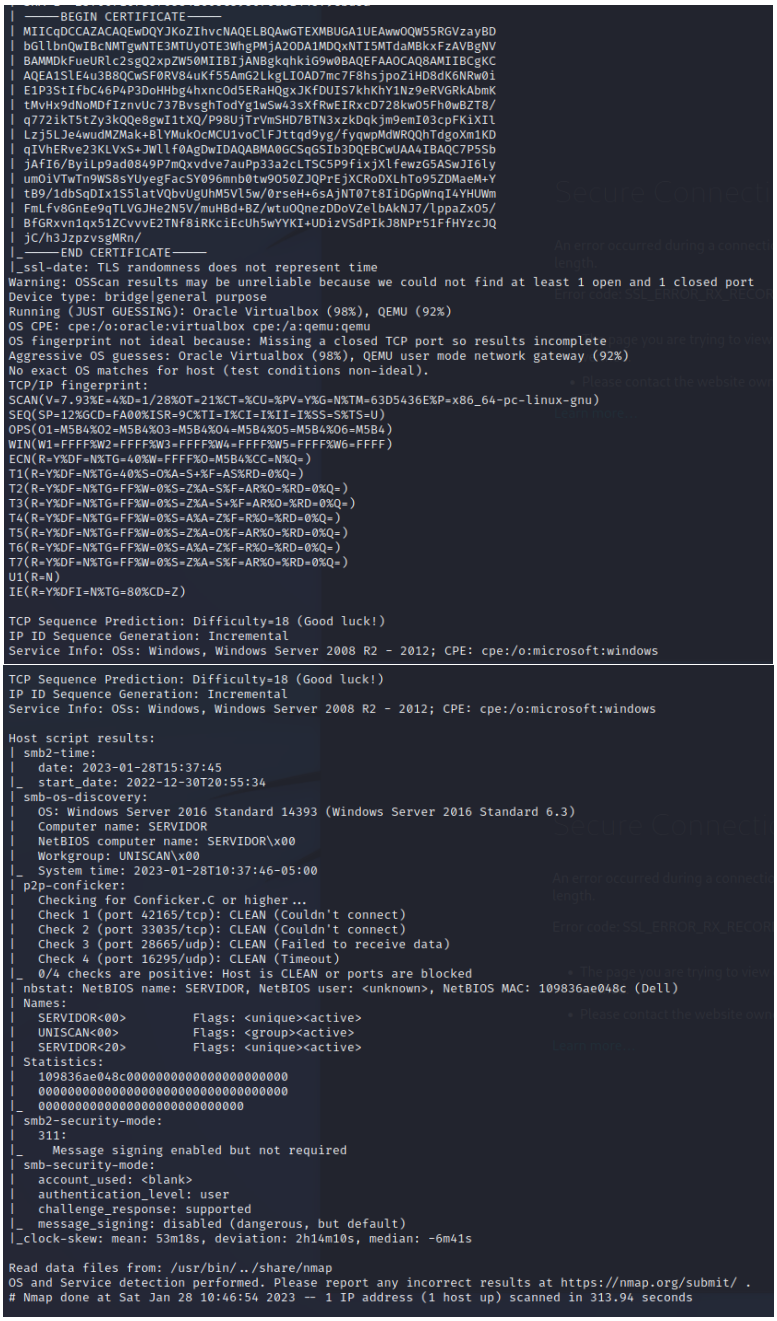
Fig. Análisis con la herramienta NMAP utilizando varios atributos.

Podemos continuar utilizando la herramienta NMAP para hallar más información y también podemos guardar los hallazgos en un archivo de texto de nombre "testvuln.txt", el cual puede ser revisado posteriormente para la búsqueda de vulnerabilidades que pueden ser explotadas, utilizaremos la siguiente línea de comando:
nmap -sV -sC -vv -O 172.30.1.2 -oN testvuln.txt

┌──(root㉿kali)-[/home/vagrant/UniScan/172.30.1.2]
└─# nmap -sV -sC -vv -O 172.30.1.2 -oN testvuln.txt




| -----BEGIN CERTIFICATE-----
| MIIC7TCCAdWgAwIBAgIQWF98w7T6uLFIOpBHUwkcLjANBgkqhkiG9w0BAQsFADAe
| MRwwGgYDVQQDExNXTVN2Yy1TSEEyLVNFUlZJRE9SMB4XDTE3MDEzMTIwNTQwNloX
| DTI3MDEyOTIwNTQwNlowHjEcMBoGA1UEAxMTV01TdmMtU0hBMi1TRVJWSURPUjCC
| ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALe4IeyfbVirOYJ+zuI33ZrP
| y2IHtqCyebWyJYlqfEKgNlwOcF+lZR8rul29G/c2Aog5V/XxbWtru+NEjUFG2Ygr
| YG8Q3u4LMZd+tfZDQ/SSBygzWVuCWKhy/Is/ZNlrnYBtJk+xNxpZnq6KI0e9Pqcq
| Z75/oBxgpb+F+bSUMO3ZPDMqInwQn085dwtjMma14ObVmEi9DBHT6E2jPRC/gD+e
| BZ8Oju6GYw5Akf7JiavLKj+QEfe4M3SXzwV55CgkZ8GPVd+4BwPZ8kpa7vLdg2jU
| KJEDwyoAlCm3yuej1+L7d59IfwhvbvVXiCDLOmRWcC8/5F09whT8ssLXx0NPEYcC
| AwEAAaMnMCUwEwYDVR0lBAwwCgYIKwYBBQUHAwEwDgYDVR0PBAcDBQCwAAAAMA0G
| CSqGSIb3DQEBCwUAA4IBAQBT/UUah2HSeFW6CzKwaHaYlFpKuYJBw0KbtHsLe1gX
| Hb+orulaAFS3cauDq9EJZ+5e2p8iMQ7a3adoLd9xDQWk4HrWAFpeUYWIeiwSIBBO
| 7tLjUXpIMn7s2wxJ/1XXXRUcy6zBQW9ISq0tnR6Xke0Lxu8mujqy1oOT5LLrnP4d
| A5q6+kaUfVJkMV6uvNX1jedDdJXa41TWa7AyqSpuIln9tImj66amVS23DeBgAO47
| UPYw/3vph5fUHB1TSLFtwuzl7XzEvo8B57BLECuplkeVC4hTSN9Wvrgo96MP+HD9
| 68fYAxR5uUT5U6uPz0puUwSAsRGo5FncRSgW1f5xm/Cr
|_-----END CERTIFICATE-----
|_http-server-header: Microsoft-HTTPAPI/2.0
| tls-alpn:
| h2
|_ http/1.1
445/tcp open microsoft-ds   syn-ack ttl 64 Windows Server 2016 Standard 14393 microsoft-ds
1433/tcp open ms-sql-s   syn-ack ttl 64 Microsoft SQL Server 2008
|_ms-sql-ntlm-info: ERROR: Script execution failed (use -d to debug)
|_ssl-date: 2023-01-28T15:38:13+00:00; -6m41s from scanner time.
| ssl-cert: Subject: commonName=WMSvc-SHA2-SERVIDOR
| Issuer: commonName=WMSvc-SHA2-SERVIDOR
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2017-01-31T20:54:06
| Not valid after: 2027-01-29T20:54:06
| MD5:   fc81aedea19af1e5832f2757043d4da6
| SHA-1: 517812d7112b392c6c273b87f302c391aa2cbb8b
| -----BEGIN CERTIFICATE-----
| MIIC7TCCAdWgAwIBAgIQWF98w7T6uLFIOpBHUwkcLjANBgkqhkiG9w0BAQsFADAe
| MRwwGgYDVQQDExNXTVN2Yy1TSEEyLVNFUlZJRE9SMB4XDTE3MDEzMTIwNTQwNloX
| DTI3MDEyOTIwNTQwNlowHjEcMBoGA1UEAxMTV01TdmMtU0hBMi1TRVJWSURPUjCC
| ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALe4IeyfbVirOYJ+zuI33ZrP
| y2IHtqCyebWyJYlqfEKgNlwOcF+lZR8rul29G/c2Aog5V/XxbWtru+NEjUFG2Ygr
| YG8Q3u4LMZd+tfZDQ/SSBygzWVuCWKhy/Is/ZNlrnYBtJk+xNxpZnq6KI0e9Pqcq
| Z75/oBxgpb+F+bSUMO3ZPDMqInwQn085dwtjMma14ObVmEi9DBHT6E2jPRC/gD+e
| BZ8Oju6GYw5Akf7JiavLKj+QEfe4M3SXzwV55CgkZ8GPVd+4BwPZ8kpa7vLdg2jU
| KJEDwyoAlCm3yuej1+L7d59IfwhvbvVXiCDLOmRWcC8/5F09whT8ssLXx0NPEYcC
| AwEAAaMnMCUwEwYDVR0lBAwwCgYIKwYBBQUHAwEwDgYDVR0PBAcDBQCwAAAAMA0G
| CSqGSIb3DQEBCwUAA4IBAQBT/UUah2HSeFW6CzKwaHaYlFpKuYJBw0KbtHsLe1gX
| Hb+orulaAFS3cauDq9EJZ+5e2p8iMQ7a3adoLd9xDQWk4HrWAFpeUYWIeiwSIBBO
| 7tLjUXpIMn7s2wxJ/1XXXRUcy6zBQW9ISq0tnR6Xke0Lxu8mujqy1oOT5LLrnP4d
| A5q6+kaUfVJkMV6uvNX1jedDdJXa41TWa7AyqSpuIln9tImj66amVS23DeBgAO47
| UPYw/3vph5fUHB1TSLFtwuzl7XzEvo8B57BLECuplkeVC4hTSN9Wvrgo96MP+HD9
| 68fYAxR5uUT5U6uPz0puUwSAsRGo5FncRSgW1f5xm/Cr
|_-----END CERTIFICATE-----
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
1723/tcp open pptp   syn-ack ttl 64 Microsoft
1801/tcp open msmq?   syn-ack ttl 64
2103/tcp open msrpc   syn-ack ttl 64 Microsoft Windows RPC
2105/tcp open msrpc   syn-ack ttl 64 Microsoft Windows RPC
2107/tcp open msrpc   syn-ack ttl 64 Microsoft Windows RPC
2179/tcp open vmrdp?   syn-ack ttl 64
2383/tcp open ms-olap4?   syn-ack ttl 64
3000/tcp open http   syn-ack ttl 64 Node.js (Express middleware)
|_http-title: Iniciar Sesiõoacute;n
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
3389/tcp open ms-wbt-server   syn-ack ttl 64 Microsoft Terminal Service
7070/tcp open ssl/realserver? syn-ack ttl 64
| ssl-cert: Subject: commonName=AnyDesk Client
| Issuer: commonName=AnyDesk Client
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2018-05-17T15:29:17
| Not valid after: 2068-05-04T15:29:17
| MD5:   a84179040a51ea84cef5e32816157959
| SHA-1: 23f007167357058426O5c395676d31445f9ebd5a



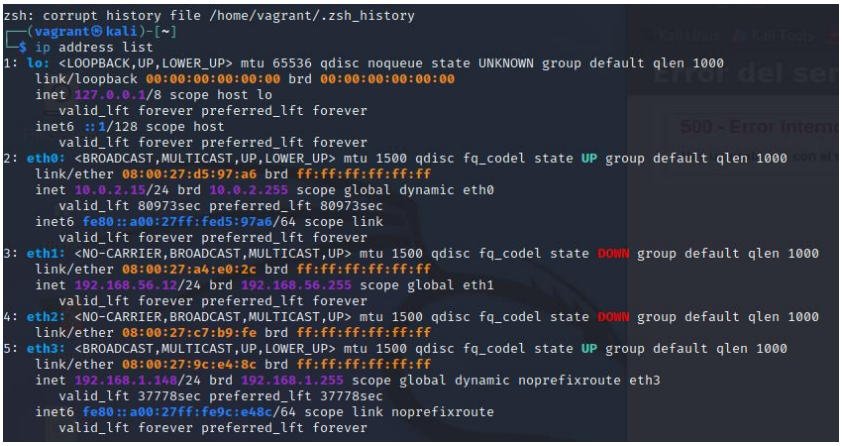
El siguiente comando podrá ser utilizado para obtener más información de nuestro objetivo, servidor de la organización de Uniscan, pero utilizaremos el atributo ***-p [lista de puertos a analizar]:***

```
┌──(root㉿kali)-[/home/vagrant/UniScan/172.30.1.2]
└─# nmap -p 135,445,1723,80,3389,443,21,139,2105,1801,2107,1433,2179,2103,2383,82,3000,84,7070 -sV --script vuln -vv -O 172.30.1.2 -oN test2vuln.txt
```

ANALISIS DE VULNERABILIDADES DENTRO DE LA RED UNISCAN 17 EN LA ORGANIZACIÓN UNISCAN.

Para continuar el análisis de vulnerabilidades haremos uso de nuestra máquina virtual con sistema operativo Kali Linux, abrimos una línea de comandos para poder identificar los adaptadores de red con sus respectivas direcciones IP.

┌──(vagrant㉿kali)-[~]
└─$ ip address list



Haciendo uso del comando: ***arp-scan --interface=eth3 192.168.1.0/24*** dentro de la red Uniscan 17, hallaremos una lista de los equipos que se encuentran conectados a la red que será objeto de análisis, es muy importante tener en cuenta la configuración de adaptadores de red dentro de la aplicación de máquinas virtuales que utilizaremos para la elaboración del pentesting, para este caso estamos utilizando "VirtualBox versión: 7.0".

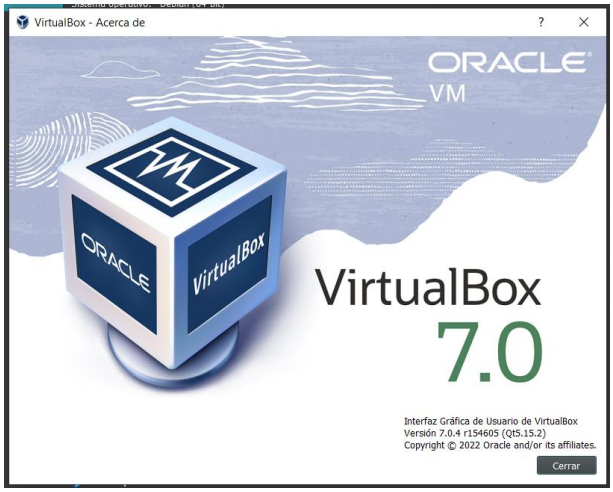


Fig. Versión del software utilizado para la construcción de nuestra máquina virtual.

┌──(vagrant㉿kali)-[~]
└─$ sudo arp-scan --interface=eth3 192.168.1.0/24

```
┌──(vagrant㉿kali)-[~]
└─$ sudo arp-scan --interface=eth3 192.168.1.0/24
Interface: eth3, type: EN10MB, MAC: 08:00:27:9c:e4:8c, IPv4: 192.168.1.148
Starting arp-scan 1.9.8 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.1.1     b4:75:0e:f7:0e:2b       Belkin International Inc.
192.168.1.6     10:62:eb:87:8c:21       D-Link International
192.168.1.22    a4:d7:3c:02:dd:ff       Seiko Epson Corporation
192.168.1.122   90:78:41:be:01:13       Intel Corporate
192.168.1.171   60:38:e0:c5:d4:38       Belkin International Inc.
192.168.1.218   48:f8:b3:3f:00:d4       Cisco-Linksys, LLC

6 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.8: 256 hosts scanned in 2.220 seconds (115.32 hosts/sec). 6 responded
```

A continuación, realizaremos una identificación de los computadores que se encuentran en la red Uniscan 17, esto nos permitirá tener una visión más clara de la infraestructura de la organización.

```
┌──(vagrant㉿kali)-[~]
└─$ nmap 192.168.1.0/24
```

```
┌──(vagrant㉿kali)-[~]
└─$ nmap 192.168.1.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-28 11:33 EST
Stats: 0:00:34 elapsed; 251 hosts completed (5 up), 5 undergoing Connect Scan
Connect Scan Timing: About 96.13% done; ETC: 11:34 (0:00:01 remaining)
Nmap scan report for Linksys27494 (192.168.1.1)
Host is up (0.015s latency).
Not shown: 992 closed tcp ports (conn-refused)
PORT      STATE    SERVICE
53/tcp    open     domain
80/tcp    open     http
139/tcp   open     netbios-ssn
443/tcp   filtered https
445/tcp   open     microsoft-ds
10000/tcp open     snet-sensor-mgmt
49152/tcp open     unknown
49153/tcp open     unknown

Nmap scan report for 192.168.1.6
Host is up (0.042s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT     STATE SERVICE
23/tcp   open  telnet
80/tcp   open  http
5431/tcp open  park-agent

Nmap scan report for 192.168.1.22
Host is up (0.013s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
515/tcp  open  printer
631/tcp  open  ipp
9100/tcp open  jetdirect

Nmap scan report for kali (192.168.1.148)
Host is up (0.000053s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh

Nmap scan report for 192.168.1.171
Host is up (0.0033s latency).
All 1000 scanned ports on 192.168.1.171 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap done: 256 IP addresses (5 hosts up) scanned in 44.26 seconds
```

Fig. Lista de equipos conectados a la red Uniscan 17.

Podemos verificar realizando ping a las direcciones IP que se listaron después de ejecutar el comando: ***nmap 192.168.1.0/24***, esto para saber qué equipo se encuentran activos durante el análisis pentesting a ejecutarse.

```
┌──(vagrant㉿kali)-[~]
└─$ ping 192.168.1.6
PING 192.168.1.6 (192.168.1.6) 56(84) bytes of data.
64 bytes from 192.168.1.6: icmp_seq=1 ttl=30 time=4.77 ms
64 bytes from 192.168.1.6: icmp_seq=2 ttl=30 time=3.57 ms
64 bytes from 192.168.1.6: icmp_seq=3 ttl=30 time=3.40 ms
64 bytes from 192.168.1.6: icmp_seq=4 ttl=30 time=3.76 ms
64 bytes from 192.168.1.6: icmp_seq=5 ttl=30 time=3.88 ms
64 bytes from 192.168.1.6: icmp_seq=6 ttl=30 time=7.81 ms
64 bytes from 192.168.1.6: icmp_seq=7 ttl=30 time=39.8 ms
^C
--- 192.168.1.6 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6025ms
rtt min/avg/max/mdev = 3.398/9.567/39.788/12.418 ms
```

En la tarea de pentesting es necesario realizar varias pruebas de conexión buscando posibles vulnerabilidades o puntos débiles, en ocasiones esta tarea puede tener su dificultad y llevar mucho tiempo en su ejecución, pero es importante empezar desde lo más básico como por ejemplo realizar el ingreso a equipos como un switch o un router que hayamos identificado que se encuentren operativos en la red objetivo de estudio, en estos dispositivos como primera vulnerabilidad sería intentar ingresar utilizando las credenciales que vienen por defecto desde la fábrica, es muy probable que el administrador de la red no haya cambiado dejando esta ventana abierta para el ingreso de cualquier intruso que desee manipular la red de la organización.

Para llevar a cabo el siguiente laboratorio de ingreso a la red se identificó con la herramienta NMAP la siguiente dirección: ***192.168.1.1***, que pertenece a un router de la marca Linksys, se realizará una revisión de los puertos que se encuentran abiertos:

```
┌──(vagrant㉿kali)-[~]
└─$ sudo nmap -O 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-28 12:01 EST
Nmap scan report for Linksys27494 (192.168.1.1)
Host is up (0.0049s latency).
Not shown: 992 closed tcp ports (reset)
PORT     STATE    SERVICE
53/tcp   open     domain
80/tcp   open     http
139/tcp  open     netbios-ssn
443/tcp  filtered https
445/tcp  open     microsoft-ds
10000/tcp open    snet-sensor-mgmt
49152/tcp open    unknown
49153/tcp open    unknown
MAC Address: B4:75:0E:F7:0E:2B (Belkin International)
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.10
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.37 seconds
```

*Es importante identificar que con la información que entregó la herramienta NMAP, se puede identificar que el equipo se trata de un router de la marca Linksys.

A continuación, en un navegador ingresaremos la dirección IP: ***192.168.1.1***, se abrirá una ventana de configuración del equipo que nos solicitará clave de ingreso, utilizaremos una credencial que viene por defecto de fábrica.

PASSWORD: admin

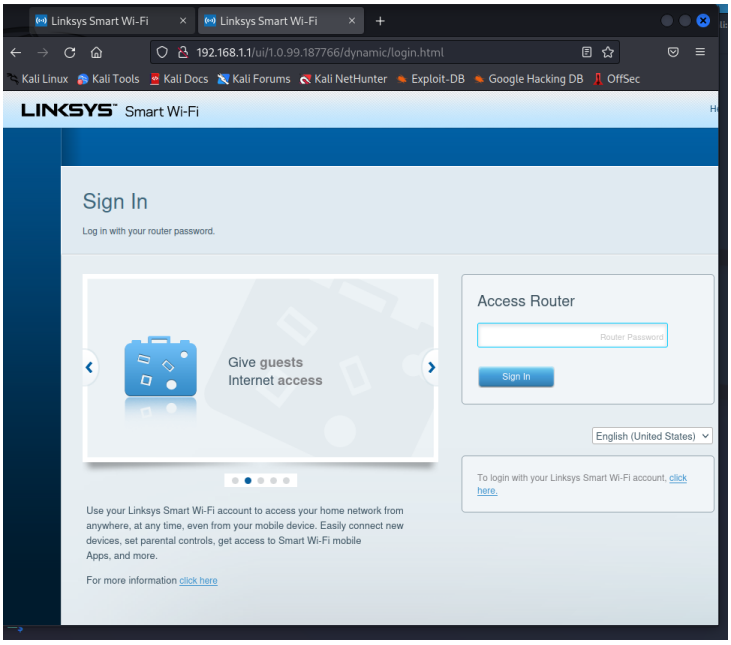


Fig. Ventana de configuración del router abierta desde un navegador.

Una vez ingresado el password podemos verificar que tenemos acceso a todas las configuraciones del dispositivo, podemos ver la lista de los equipos que se conectan a la red, la clave de la red, las diferentes reglas implementadas dentro de la red, y demás opciones que pueden hacer de este dispositivo un acceso importante para realizar un ataque y llevar a cabo una amenaza que afecte en gran medida la infraestructura tecnológica de la organización Uniscan.

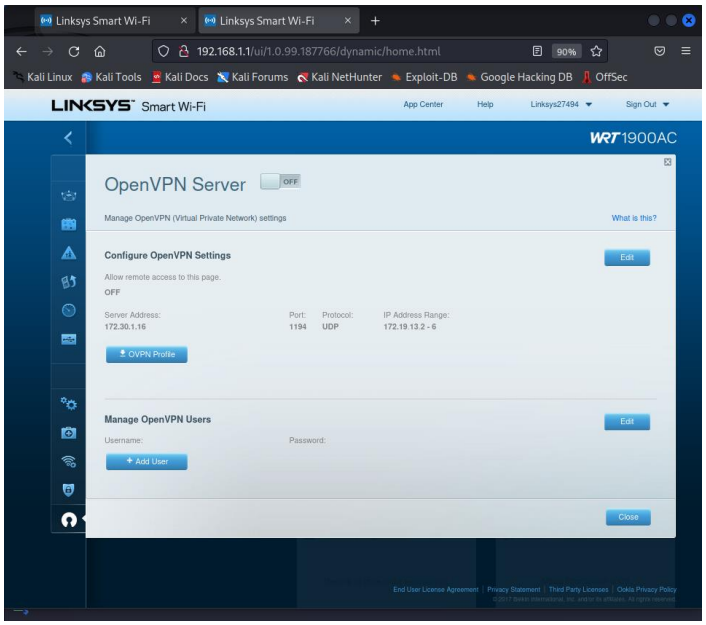


Fig. Ventana de configuración del router de la marca Linksys.

Análisis de las demás direcciones IP que se encuentran dentro de la red Uniscan17 en busca de vulnerabilidades que pueden ser afectadas durante un ataque realizado por un ciber-delincuente.

```
┌──(vagrant㉿kali)-[~]
└─$ sudo nmap -O 192.168.1.6
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-28 12:02 EST
Nmap scan report for 192.168.1.6
Host is up (0.0066s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE
23/tcp   open  telnet
80/tcp   open  http
5431/tcp open  park-agent
MAC Address: 10:62:EB:87:8C:21 (D-Link International)
Device type: switch
Running: Allied Telesyn embedded, D-Link embedded
OS CPE: cpe:/h:alliedtelesyn:at-gs950 cpe:/h:dlink:des-3226l cpe:/h:dlink:dsl-2750u
OS details: Allied Telesyn AT-GS950 or D-Link DES-3226L switch or D-Link DSL-2750U router
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 5.86 seconds

┌──(vagrant㉿kali)-[~]
└─$ sudo nmap -O 192.168.1.22
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-28 12:04 EST
Nmap scan report for 192.168.1.22
Host is up (0.0048s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
515/tcp  open  printer
631/tcp  open  ipp
9100/tcp open  jetdirect
MAC Address: A4:D7:3C:02:DD:FF (Seiko Epson)
Device type: general purpose
Running: Linux 4.X
OS CPE: cpe:/o:linux:linux_kernel:4.4.2
OS details: DD-WRT v3.0 (Linux 4.4.2)
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.00 seconds

┌──(vagrant㉿kali)-[~]
└─$ sudo nmap -O 192.168.1.171
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-28 12:05 EST
Nmap scan report for 192.168.1.171
Host is up (0.0056s latency).
All 1000 scanned ports on 192.168.1.171 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 60:38:E0:C5:D4:38 (Belkin International)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 48.33 seconds
```

Podemos almacenar el informe que entrega la herramienta NMAP utilizando la siguiente línea de comando: ***nmap -sV -sC -vv -O 192.168.1.1 -oN testRouterRecepvuln.txt***, toda la información recopilada por el comando ingresado anteriormente quedará almacenado en el archivo de texto con nombre ***"testRouterRecepVuln.txt"***

```
┌──(root㉿kali)-[/home/vagrant/UniScan/172.30.1.2]
└─# nmap -sV -sC -vv -O 192.168.1.1 -oN testRouterRecepvuln.txt
```

ANALISIS DE VULNERABILIDADES DENTRO DE LA RED DE GERENCIA GENERAL EN LA EMPRESA UNISCAN.

Análisis de la red de Gerencia General de la empresa Uniscan que se encuentra en el segundo piso del edificio, para poder unirse a la red solo es cuestión de que como invitado se solicite la contraseña para tener internet y la clave será compartida por el personal encargado del departamento de desarrollo o del departamento técnico.

Una vez ingresamos a la red objeto de estudio, con la utilización de la herramienta NMAP que se encuentra instalada en nuestra máquina virtual Kali-Linux, ejecutaremos el comando ***"ip addres list",*** con el cual obtendremos una numeración de los adaptadores disponibles en el computador con su respectiva dirección IP.

```
┌──(vagrant㉿kali)-[~]
└─$ ip address list
```

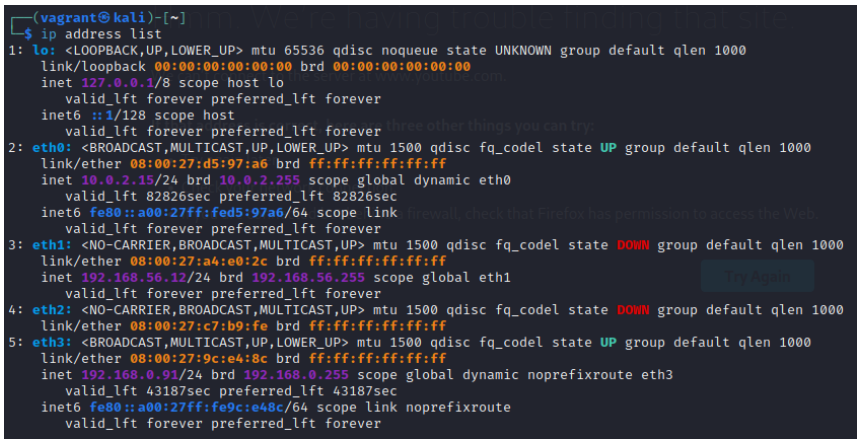
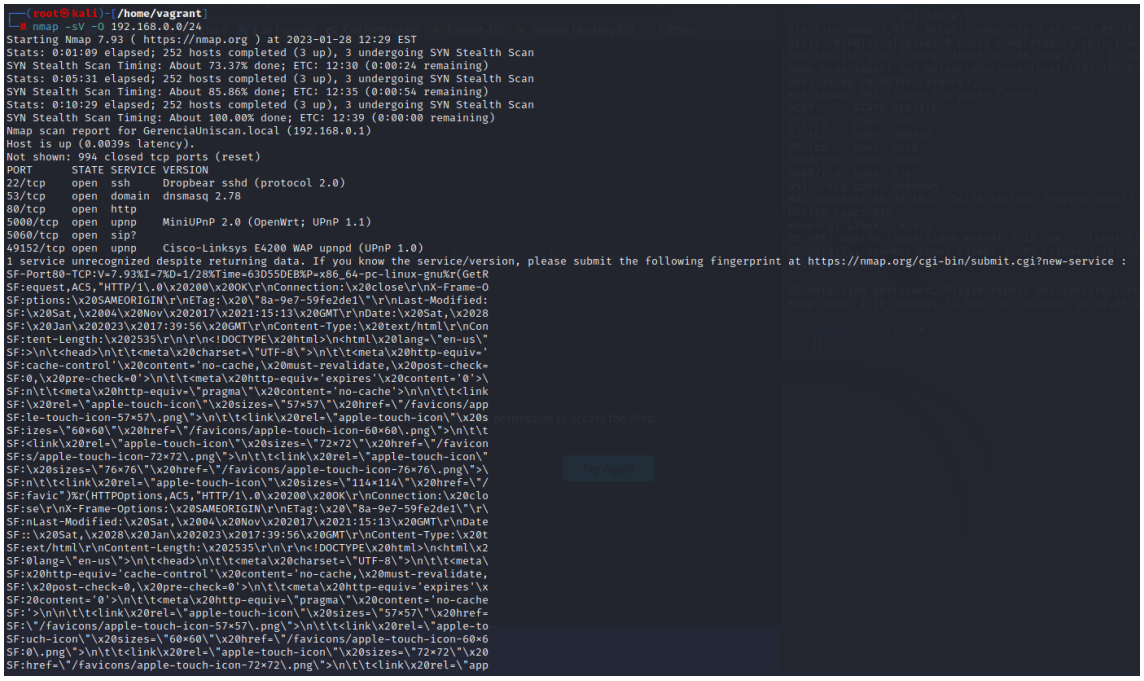


Fig. Utilización del comando ***ip address list*** en la red de Gerencia General de la empresa Uniscan.

Después de observar la pantalla que se desplegó, podemos determinar que la dirección IP que se asignó a nuestro host es: ***192.168.0.91.***

```
┌──(root㉿kali)-[/home/vagrant]
└─# nmap -sV -O 192.168.0.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-28 12:29 EST
Stats: 0:01:09 elapsed; 252 hosts completed (3 up), 3 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 73.37% done; ETC: 12:30 (0:00:24 remaining)
Stats: 0:05:31 elapsed; 252 hosts completed (3 up), 3 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 85.86% done; ETC: 12:35 (0:00:54 remaining)
Stats: 0:10:29 elapsed; 252 hosts completed (3 up), 3 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 100.00% done; ETC: 12:39 (0:00:00 remaining)
Nmap scan report for GerenciaUniscan.local (192.168.0.1)
Host is up (0.0039s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     Dropbear sshd (protocol 2.0)
53/tcp   open  domain  dnsmasq 2.78
80/tcp   open  http
5000/tcp open  upnp    MiniUPnP 2.0 (OpenWrt; UPnP 1.1)
5060/tcp open  sip?
49152/tcp open  upnp    Cisco-Linksys E4200 WAP upnpd (UPnP 1.0)
```



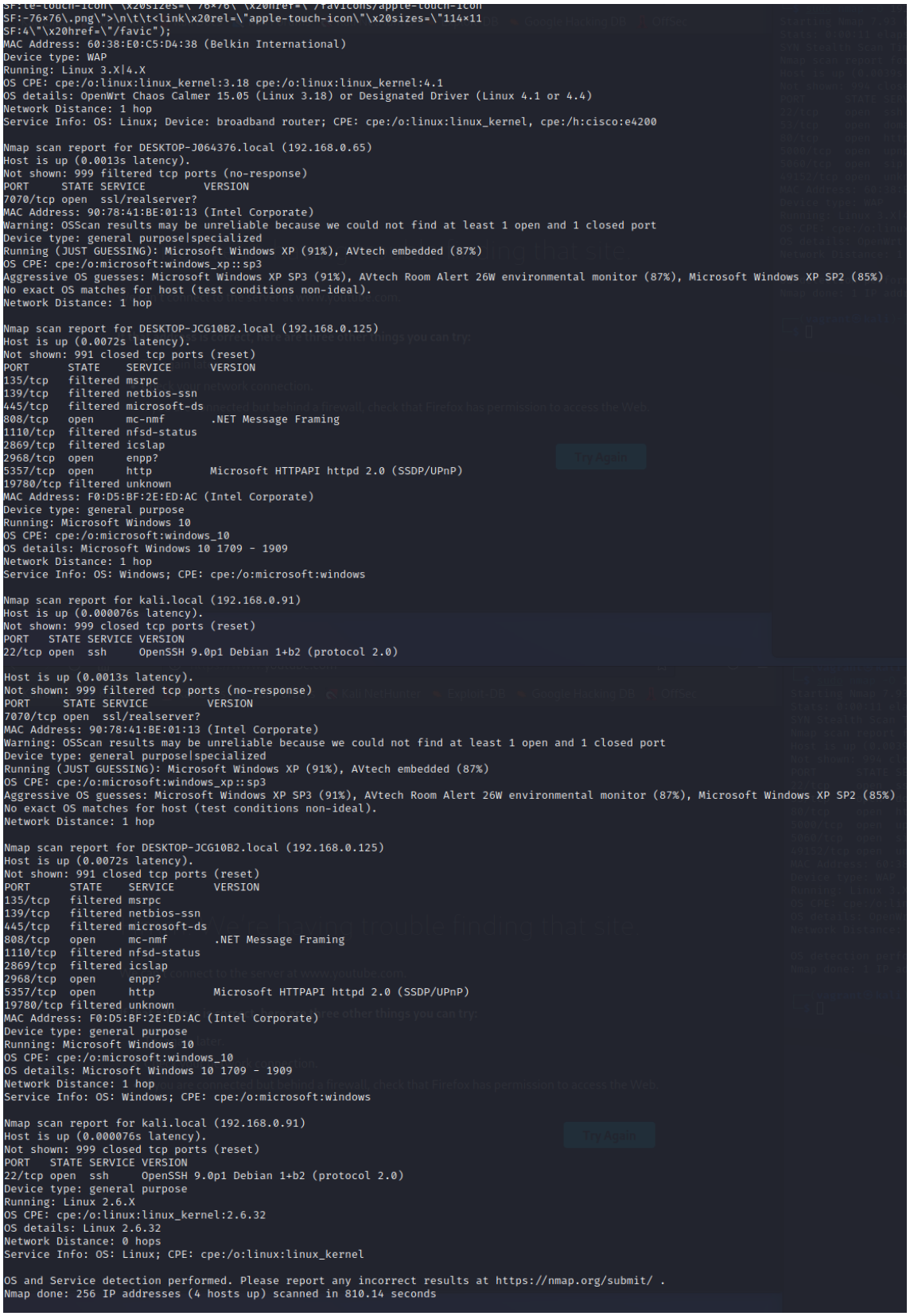


Fig. Ventanas desplegadas después de hacer uso de la herramienta NMAP en la red de Gerencia General de la organización Uniscan.

Con la información que se mostró anteriormente podemos determinar que la dirección IP: ***192.168.0.1,*** pertenece al router que entrega la señal wifi en la red de Gerencia General de la empresa Uniscan por lo que realizaremos un análisis más profundo sobre esta dirección, seguido utilizaremos la herramienta NMAP con el ***atributo -O*** para hallar los puertos que se encuentren abiertos en este dispositivo.

```
┌──(vagrant㉿kali)-[~]
└─$ sudo nmap -O 192.168.0.1
```

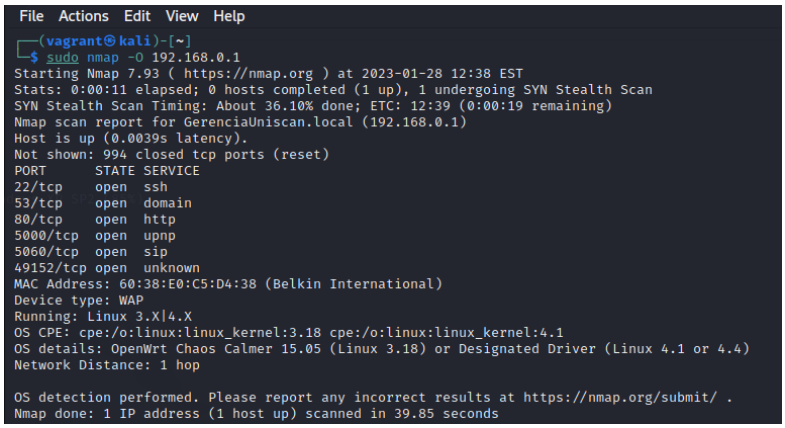
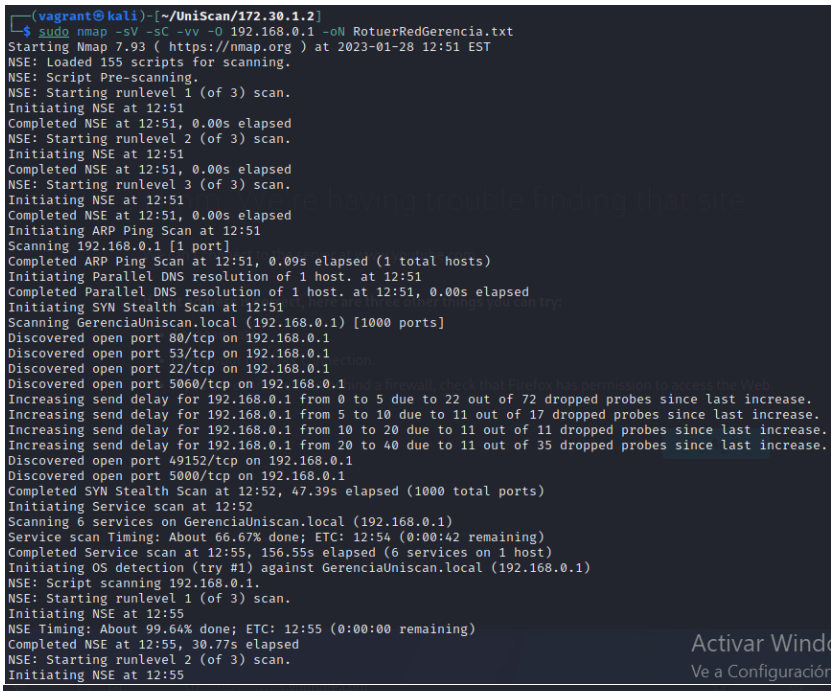


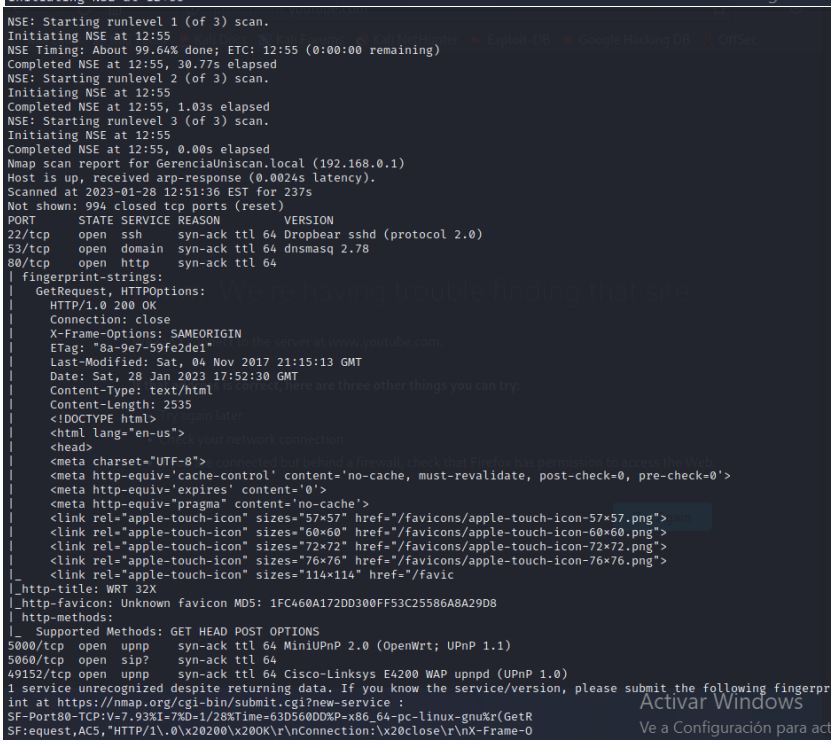
Fig. Hallazgo de los puertos abiertos en el router en la red de Gerencia General de la empresa Uniscan.

A continuación, podemos utilizar la siguiente línea de comando para obtener información detallada del estado de los puertos IP pertenecientes a la dirección: ***192.168.0.1***, adicional almacenaremos los datos en el archivo con nombre "RouterRedGerencia.txt", esto nos permitirá realizar consultas posteriormente y buscar posibles vulnerabilidades que puedan ser explotadas, el comando a utilizar será:

$ sudo nmap -sV -sC -vv -O 192.168.0.1.



```
┌──(vagrant㉿kali)-[~/UniScan/172.30.1.2]
└─$ sudo nmap -sV -sC -vv -O 192.168.0.1 -oN RotuerRedGerencia.txt
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-28 12:51 EST
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 12:51
Completed NSE at 12:51, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 12:51
Completed NSE at 12:51, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 12:51
Completed NSE at 12:51, 0.00s elapsed
Initiating ARP Ping Scan at 12:51
Scanning 192.168.0.1 [1 port]
Completed ARP Ping Scan at 12:51, 0.09s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:51
Completed Parallel DNS resolution of 1 host. at 12:51, 0.00s elapsed
Initiating SYN Stealth Scan at 12:51
Scanning GerenciaUniscan.local (192.168.0.1) [1000 ports]
Discovered open port 80/tcp on 192.168.0.1
Discovered open port 53/tcp on 192.168.0.1
Discovered open port 22/tcp on 192.168.0.1
Discovered open port 5060/tcp on 192.168.0.1
Increasing send delay for 192.168.0.1 from 0 to 5 due to 22 out of 72 dropped probes since last increase.
Increasing send delay for 192.168.0.1 from 5 to 10 due to 11 out of 17 dropped probes since last increase.
Increasing send delay for 192.168.0.1 from 10 to 20 due to 11 out of 11 dropped probes since last increase.
Increasing send delay for 192.168.0.1 from 20 to 40 due to 11 out of 35 dropped probes since last increase.
Discovered open port 49152/tcp on 192.168.0.1
Discovered open port 5000/tcp on 192.168.0.1
Completed SYN Stealth Scan at 12:52, 47.39s elapsed (1000 total ports)
Initiating Service scan at 12:52
Scanning 6 services on GerenciaUniscan.local (192.168.0.1)
Service scan Timing: About 66.67% done; ETC: 12:54 (0:00:42 remaining)
Completed Service scan at 12:55, 156.55s elapsed (6 services on 1 host)
Initiating OS detection (try #1) against GerenciaUniscan.local (192.168.0.1)
NSE: Script scanning 192.168.0.1.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 12:55
NSE Timing: About 99.64% done; ETC: 12:55 (0:00:00 remaining)
Completed NSE at 12:55, 30.77s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 12:55
```

```
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 12:55
NSE Timing: About 99.64% done; ETC: 12:55 (0:00:00 remaining)
Completed NSE at 12:55, 30.77s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 12:55
Completed NSE at 12:55, 1.03s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 12:55
Completed NSE at 12:55, 0.00s elapsed
Nmap scan report for GerenciaUniscan.local (192.168.0.1)
Host is up, received arp-response (0.0024s latency).
Scanned at 2023-01-28 12:51:36 EST for 237s
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE REASON         VERSION
22/tcp    open  ssh     syn-ack ttl 64 Dropbear sshd (protocol 2.0)
53/tcp    open  domain  syn-ack ttl 64 dnsmasq 2.78
80/tcp    open  http    syn-ack ttl 64
| fingerprint-strings:
|   GetRequest, HTTPOptions:
|     HTTP/1.0 200 OK
|     Connection: close
|     X-Frame-Options: SAMEORIGIN
|     ETag: "8a-9e7-59fe2de1"
|     Last-Modified: Sat, 04 Nov 2017 21:15:13 GMT
|     Date: Sat, 28 Jan 2023 17:52:30 GMT
|     Content-Type: text/html
|     Content-Length: 2535
|     <!DOCTYPE html>
|     <html lang="en-us">
|     <head>
|     <meta charset="UTF-8">
|     <meta http-equiv='cache-control' content='no-cache, must-revalidate, post-check=0, pre-check=0'>
|     <meta http-equiv='expires' content='0'>
|     <meta http-equiv="pragma" content='no-cache'>
|     <link rel="apple-touch-icon" sizes="57×57" href="/favicons/apple-touch-icon-57×57.png">
|     <link rel="apple-touch-icon" sizes="60×60" href="/favicons/apple-touch-icon-60×60.png">
|     <link rel="apple-touch-icon" sizes="72×72" href="/favicons/apple-touch-icon-72×72.png">
|     <link rel="apple-touch-icon" sizes="76×76" href="/favicons/apple-touch-icon-76×76.png">
|_    <link rel="apple-touch-icon" sizes="114×114" href="/favic
|_http-title: WRT 32X
|_http-favicon: Unknown favicon MD5: 1FC460A172DD300FF53C25586A8A29D8
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
5000/tcp  open  upnp    syn-ack ttl 64 MiniUPnP 2.0 (OpenWrt; UPnP 1.1)
5060/tcp  open  sip?    syn-ack ttl 64
49152/tcp open  upnp    syn-ack ttl 64 Cisco-Linksys E4200 WAP upnpd (UPnP 1.0)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerpr
int at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port80-TCP:V=7.93%I=7%D=1/28%Time=63D560DD%P=x86_64-pc-linux-gnu%r(GetR
SF:equest,AC5,"HTTP/1\.0\x20200\x20OK\r\nConnection:\x20close\r\nX-Frame-O
```

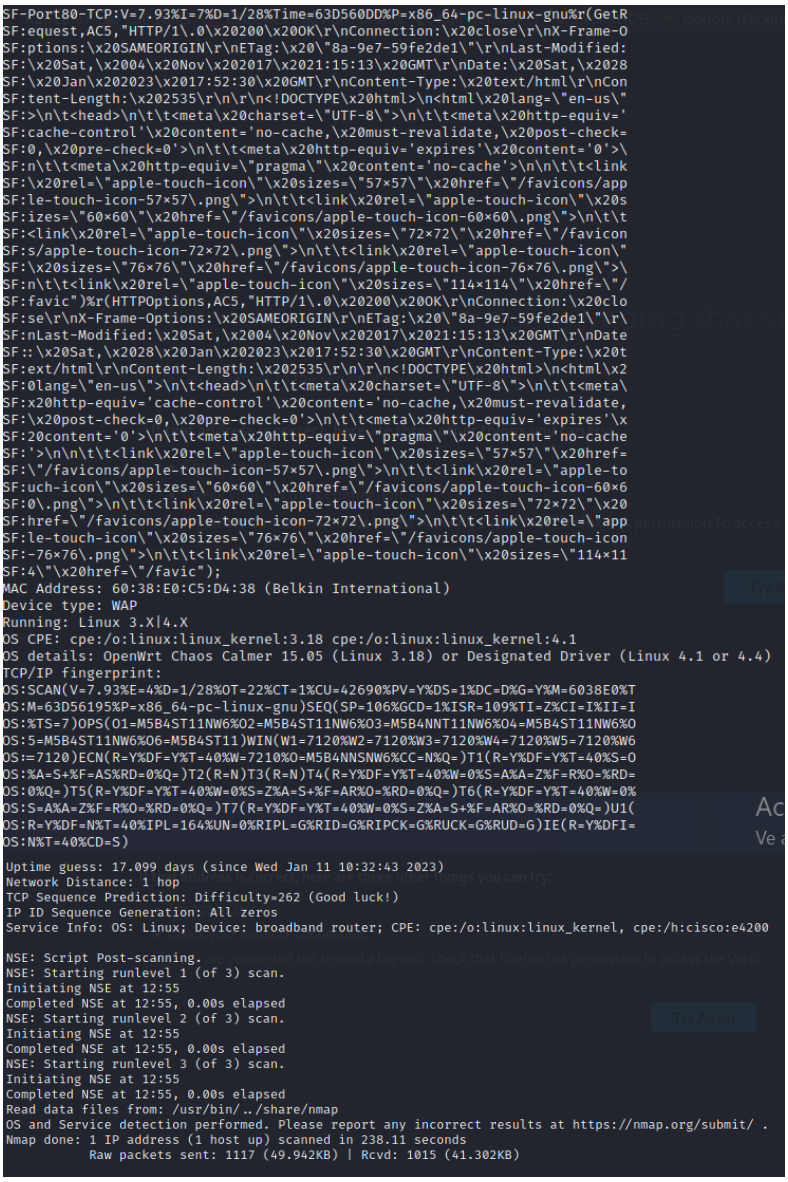


Fig. Lista de puertos abiertos en la dirección IP del router de la red Gerencia General de la empresa Uniscan.

ANEXO 8. ANÁLISIS DE SEGURIDAD DE LAS REDES OPERATIVAS DENTRO DE LA ORGANIZACIÓN UNISCAN CON LA HERRAMIENTA AIRGEDDON.

TABLA.
IDENTIFICACIÓN DE LAS REDES, ÁREA, UBICACIÓN Y ESTADO DE VULNERABILIDAD.

Nombre de Red.	Departamento o Área.	Ubicación.	Vulnerable.	Análisis del Ataque con el software Airgeddon.
Uniscan17	Recepción.	Entrada principal, gerencia marketing, recepción, ventas y contabilidad.	Clave segura.	Se realizó el ataque con el software Airgeddon instalado en nuestra máquina virtual, pero no se pudo vulnerar la red.
DTSupport	Departamento técnico.	Área del Departamento técnico.	Clave segura.	Se realizó el ataque con el software Airgeddon instalado en nuestra máquina virtual, pero no se pudo vulnerar la red.
Gerencia	Gerencia general.	Segundo piso, marketing, gerencia contabilidad, gerencia general.	Clave segura.	Se realizó el ataque con el software Airgeddon instalado en nuestra máquina virtual, pero no se pudo vulnerar la red.
Bodega	Logística.	Bodega.	Clave insegura.	Se realizó el ataque con el software Airgeddon instalado en nuestra máquina virtual, y se pudo vulnerar la red.
DesarrolloUniscan	Departamento de Desarrollo.	Primer piso, Dpto. de Desarrollo.	Clave insegura.	Se realizó el ataque con el software Airgeddon instalado en nuestra máquina virtual, y se pudo vulnerar la red obteniendo la contraseña. Posteriormente ingresamos a la red vulnerada, después de eso se realizó un análisis de la red con el software NMAP y se pudo hallar varias direcciones (revisar anexo "Escaneo de Vulnerabilidades con NMAP") entre las cuales se pudo identificar la siguiente dirección IP: 192.168.1.1, ingresamos la dirección IP en un navegador web y se abre una ventana de ingreso a un router de la marca Linksys solicitando contraseña, se prueba con un password por default, ejemplo: "admin", pudimos ingresar a las configuraciones del dispositivo, haciendo de esta una vulnerabilidad de riesgo crítico.

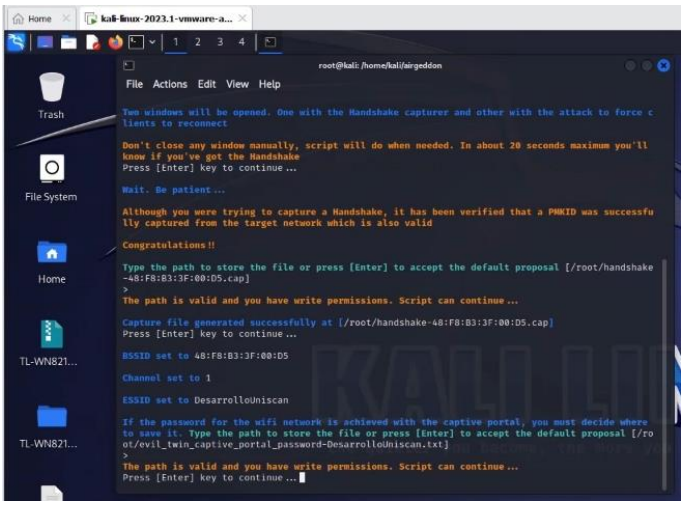


Fig. Recuperación del archivo handshake dentro de la red de Desarrollo.

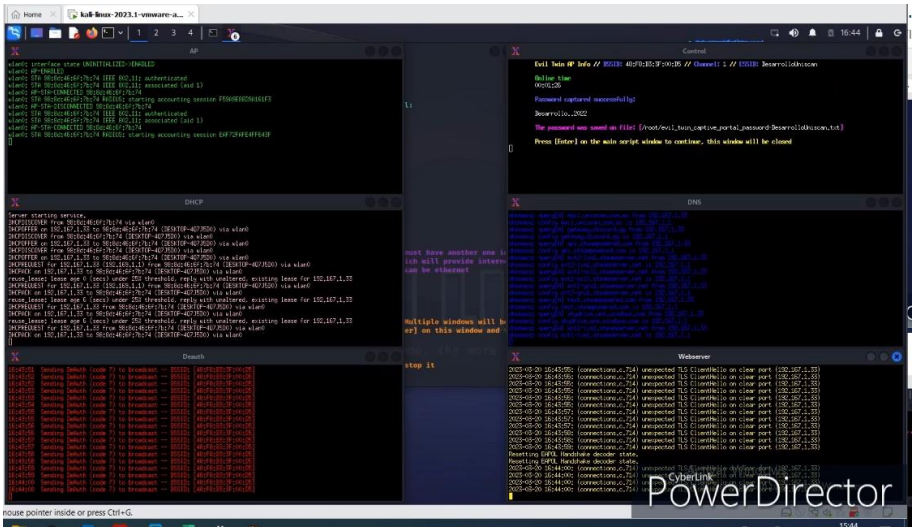


Fig. Obtención de la contraseña de ingreso a la red Desarrollo.

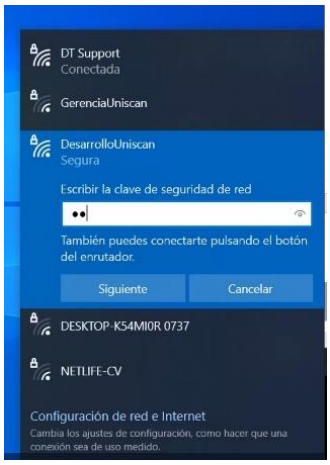


Fig. Ingreso a la red Desarrollo, se utiliza la contraseña capturada con el software Airgeddon.

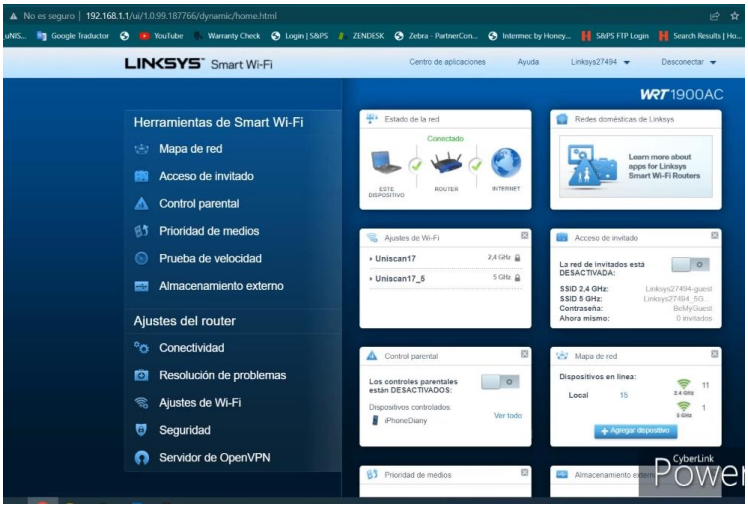


Fig. Ingreso al router de la red Desarrollo con la dirección 192.168.1.1

ANEXO 9. LISTA DETALLADA DE LAS VULNERABILIDADES HALLADAS CON LA HERRAMIENTA NESSUS DENTRO DE LA ORGANIZACIÓN UNISCAN.

Vulnerabilidad #1	
Nombre:	SSL Version 2 and 3 Protocol Detection
Gravedad:	Crítica
Detalles de vulnerabilidad:	
El servicio remoto acepta conexiones cifradas SSL 2.0 y/o SSL 3.0. Hay varias debilidades criptográficas que afectan a ciertas versiones de SSL, incluyendo: • Un esquema de relleno basado en cifrado CBC que no es seguro. • Métodos inseguros de renegociación y reanudación de sesión. Estos agujeros pueden ser utilizados por un atacante para lanzar ataques man-in-the-middle o para descifrar interacciones cliente-servidor. Aunque SSL/TLS ofrece un método seguro para determinar la versión del protocolo a utilizar (de tal forma que estas versiones sólo se utilizarán si el cliente o el servidor no soportan nada mejor), muchos navegadores web implementan esto de una forma arriesgada que permite a un atacante degradar una conexión (como en POODLE). Por lo tanto, se aconseja que estos procedimientos estén completamente desactivados. SSL 3.0 ya no es adecuado para conexiones seguras, según el NIST. A partir de la fecha de entrada en vigor de la norma PCI DSS v3.1, dejará de considerarse que cualquier versión de SSL cumple la definición de "criptografía fuerte" del PCI SSC.	
Solución:	
• Para desactivar SSL 2.0 y 3.0, consulte la documentación de la aplicación. • En su lugar, utilice TLS 1.2 (con suites de cifrado certificadas).	
Referencias adicionales:	
https://www.schneier.com/academic/paperfiles/paper-ssl.pdf	
http://www.nessus.org/u?b06c7e95	
http://www.nessus.org/u?247c4540	

Vulnerabilidad #2	
Nombre:	Microsoft SQL Server Unsupported Version Detection (remote check)
Gravedad:	Crítica
Detalles de vulnerabilidad:	
• La instalación de Microsoft SQL Server en el servidor remoto ya no recibe soporte según su número de versión. • La ausencia de soporte sugiere que el vendedor no proporcionará nuevas actualizaciones de seguridad para el producto. Por lo tanto, es muy probable que tenga fallos de seguridad.	
Solución:	
Actualice a una versión de Microsoft SQL Server que sea compatible actualmente.	
Referencias adicionales:	
http://www.nessus.org/u?d4418a57	

Vulnerabilidad #3	
Nombre:	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
Gravedad:	Alta
Detalles de vulnerabilidad:	
Las siguientes vulnerabilidades afectan al host remoto de Windows: • Existen numerosos defectos de ejecución remota de código en Microsoft Server Message Block 1.0 (SMBv1) como resultado de la forma incorrecta en que se manejan algunas solicitudes. Estos defectos permiten a un atacante remoto no autenticado ejecutar código arbitrario utilizando un paquete cuidadosamente diseñado. Estas vulnerabilidades (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146 y CVE-2017-0148) • Debido al procesamiento deficiente de algunas solicitudes, Microsoft Server Message Block 1.0 (SMBv1) tiene una vulnerabilidad de fuga de información. Esto puede ser utilizado por un atacante remoto no autenticado para revelar información confidencial a través de un paquete cuidadosamente diseñado. (CVE-2017-0147). Las vulnerabilidades y exploits de Equation Group ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE y ETERNALSYNERGY son cuatro de los varios publicados el 14/04/2017 por una organización conocida como Shadow Brokers. El malware ransomware WannaCry/WannaCrypt utiliza la vulnerabilidad ETERNALBLUE, y el gusano EternalRocks hace uso de siete vulnerabilidades de Equation Group. El ransomware Petya utiliza inicialmente la vulnerabilidad CVE-2017-0199 de Microsoft Office antes de propagarse a través de ETERNALBLUE.	
Solución:	
Para Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10 y 2016, Microsoft ha publicado una serie de correcciones. Para sistemas operativos Windows como Windows XP, 2003 y 8, así como otros que ya no reciben soporte, Microsoft también ha publicado correcciones de emergencia. Microsoft aconseja a los usuarios que dejen de utilizar SMBv1 para los sistemas operativos Windows que ya no reciben soporte, como Windows XP. Las funciones de seguridad incluidas en versiones posteriores de SMB están ausentes en SMBv1. Siguiendo los procedimientos del proveedor indicados en Microsoft KB2696547, se puede desactivar SMBv1. Además, el US-CERT aconseja a los usuarios que eviten activamente SMB bloqueando el puerto TCP 445 en todos los dispositivos fronterizos de la red. Bloquee los puertos TCP 137 y 139 y los puertos UDP 137 y 138 en todos los dispositivos fronterizos de red para SMB a través de la API NetBIOS.	
Referencias adicionales:	
http://www.nessus.org/u?68fc8eff	
http://www.nessus.org/u?321523eb	
http://www.nessus.org/u?065561d0	

Vulnerabilidad #4	
Nombre:	Microsoft Windows SMBv1 Multiple Vulnerabilities
Gravedad:	Alta
Detalles de vulnerabilidad:	
Microsoft Server Message Block 1.0 (SMBv1) está habilitado en el host Windows remoto. Como resultado, tiene una serie de vulnerabilidades: • Numerosos defectos de divulgación de información en Microsoft Server Message Block 1.0 (SMBv1) se producen como resultado de cómo se manejan incorrectamente los paquetes SMBv1. Estos defectos permiten a un atacante remoto no autenticado revelar datos confidenciales mediante el envío de un paquete SMBv1 cuidadosamente diseñado. Las vulnerabilidades son (CVE-2017-0267, CVE-2017-0268, CVE-2017-0270, CVE-2017-0271, CVE-2017-0274, CVE-2017-0275 y CVE-2017-0276). • Numerosos fallos de denegación de servicio en Microsoft Server Message Block 1.0 (SMBv1) se producen como resultado de cómo se manejan incorrectamente las solicitudes. Estos fallos permiten a un atacante remoto no autenticado detener la respuesta del sistema mediante una solicitud SMB cuidadosamente diseñada. CVE-2017-0280, CVE-2017-0273 y CVE-2017-0269. • Numerosos defectos de ejecución remota de código en Microsoft Server Message Block 1.0 (SMBv1) ocurren como resultado de cómo los paquetes SMBv1 son manejados incorrectamente. Estos defectos permiten a atacantes remotos no autenticados ejecutar código arbitrario utilizando un mensaje SMBv1 especialmente diseñado. (4) (CVE-2017-0272, (4) (CVE-2017-0277, (4) (CVE-2017-0278, (4) (CVE-2017-0279)) Si el host ejecuta una versión posterior de Windows (por ejemplo, Windows 8.1, 10, 2012, 2012 R2 y 2016), especialmente si se permite el acceso remoto y anónimo a tuberías y recursos compartidos con nombre, es posible que este complemento no siempre evalúe con precisión si el host de Windows es susceptible. Tenable no aconseja esta configuración, y dependiendo de la versión de Windows, los hosts deben ser monitoreados localmente para las actualizaciones utilizando uno de los plugins que se enumeran a continuación: 100054, 100055, 100057, 100059, 100060 o 100061.	
Solución:	
Instale la actualización de seguridad necesaria para la versión de Windows que esté utilizando: - Windows Server 2008: KB4018466 - Windows 7 : KB4019264 - Windows Server 2008 R2 : KB4019264 - Windows Server 2012 : KB4019216 - Windows 8.1 / RT 8.1. : KB4019215 - Windows Server 2012 R2 : KB4019215 - Windows 10 : KB4019474 - Windows 10 Version 1511 : KB4019473 - Windows 10 Version 1607 : KB4019472 - Windows 10 Version 1703 : KB4016871 - Windows Server 2016 : KB4019472	
Referencias adicionales:	
http://www.nessus.org/u?c21268d4	
http://www.nessus.org/u?b9253982	
http://www.nessus.org/u?23802c83	

Vulnerabilidad #5	
Nombre:	SSL Medium Strength Cipher Suites Supported (SWEET32)
Gravedad:	Alta
Detalles de vulnerabilidad:	
El host remoto admite el uso de cifrados SSL que proporcionan un cifrado de nivel medio. Cualquier cifrado que emplee la suite de cifrado 3DES o al menos longitudes de clave de al menos 64 bits, pero no más de 112 bits es considerado de fuerza media por Nessus. Tenga en cuenta que, si el atacante está en la misma red física, el cifrado de fuerza media es mucho más fácil de atravesar.	
Solución:	
Si puede, reconfigure el programa afectado para que deje de utilizar cifrados de fuerza media.	
Referencias adicionales:	
https://www.openssl.org/blog/blog/2016/08/24/sweet32/	
https://sweet32.info	

Vulnerabilidad #6	
Nombre:	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
Gravedad:	Media
Detalles de vulnerabilidad:	
El host remoto se ve afectado por una vulnerabilidad de fuga de información del tipo man-in-the-middle (MitM) denominada POODLE. La fuente de la vulnerabilidad es la gestión de bytes de relleno de SSL 3.0 al descifrar comunicaciones cifradas con cifradores de bloques en modo de encadenamiento de bloques cifrados (CBC). Si un atacante MitM tiene éxito en conseguir una aplicación de destino para enviar repetidamente los mismos datos a través de conexiones SSL 3.0 recién formados, pueden ser capaces de descifrar un byte particular de un texto cifrado en tan sólo 256 intentos. Incluso si el cliente y el servicio admiten TLSv1 o una versión más reciente, una conexión puede "revertirse" a SSLv3 siempre que tanto el cliente como el servicio lo hagan. Sin afectar a los clientes heredados, el mecanismo TLS Fallback SCSV detiene los ataques de "retroceso de versión". No obstante, sólo puede asegurar las conexiones si tanto el cliente como el servicio implementan la técnica. Los sitios web que no puedan detener rápidamente SSLv3 deberían activar esta técnica. Este fallo existe en el estándar SSLv3 y no en una implementación específica de SSL. El único método para prevenir completamente el problema es desactivar SSLv3.	
Solución:	
Desactivar SSLv3. Hasta que SSLv3 pueda desactivarse, los servicios que deban soportarlo deberán activar el método TLS Fallback SCSV.	
Referencias adicionales:	
https://www.imperialviolet.org/2014/10/14/poodle.html	
https://www.openssl.org/~bodo/ssl-poodle.pdf	
https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-00	

Vulnerabilidad #7	
Nombre:	Remote Desktop Protocol Server Man-in-the-Middle Weakness
Gravedad:	Media
Detalles de vulnerabilidad:	
Se pueden realizar ataques Man-in-the-middle (MiTM) contra la versión remota del servidor del Protocolo de Escritorio Remoto (Terminal Service). Al activar el cifrado, el cliente RDP no intenta verificar la identidad del servidor. Un hacker que pueda interceptar la comunicación del servidor RDP puede establecer el cifrado entre el cliente y el servidor sin ser visto. Tal ataque MiTM proporcionaría al atacante acceso a cualquier información sensible enviada, incluyendo las credenciales de inicio de sesión. El servidor RDP tiene una clave privada RSA codificada públicamente, lo que conduce a esta vulnerabilidad. La clave para este ataque está disponible para cualquier atacante en una ubicación de red segura.	
Solución:	
Si es compatible, imponga el uso de SSL como capa de transporte para este servicio, o bien. Si la opción está presente en sistemas operativos Microsoft Windows, elija "Permitir conexiones sólo desde máquinas que ejecuten Escritorio remoto con autenticación a nivel de red".	
Referencias adicionales:	
http://www.nessus.org/u?8033da0d	

Vulnerabilidad #8	
Nombre:	SSL Certificate Cannot Be Trusted
Gravedad:	Media
Detalles de vulnerabilidad:	
No se puede confiar en el certificado X.509 del servidor. La cadena de confianza puede romperse en esta circunstancia de una de las tres formas posibles que se indican a continuación: • Para empezar, la cadena de certificados del servidor puede no tener una autoridad de certificación pública reconocida como su ancestro en la parte superior. Esto puede ocurrir cuando el certificado auto firmado y no reconocido en la parte superior de la cadena está presente, o cuando los certificados intermedios que vincularían el certificado auto firmado a una autoridad de certificación pública reconocida están ausentes. • En segundo lugar, un certificado que no era válido en el momento del escaneado puede estar presente en la cadena de certificados. Esto puede ocurrir cuando el escaneado tiene lugar antes o después de una de las fechas "notAfter" del certificado. • Por último, una firma de la cadena de certificados puede no coincidir con los datos del certificado o ser imposible de verificar. Cuando un certificado tiene una firma defectuosa, puede repararse haciendo que el emisor del certificado vuelva a firmarlo. Cuando el emisor de un certificado emplea una metodología de firma que Nessus no admite o no reconoce, el resultado son firmas que no pueden confirmarse. Cualquier interrupción en la cadena hace que sea más difícil para los usuarios confirmar la legitimidad y la identidad del servidor web si el host remoto es un host público en producción. Esto puede hacer que los ataques man-in-the-middle contra el host remoto sean más sencillos de ejecutar.	
Solución:	
Para este servicio, debe comprar o crear un certificado SSL adecuado.	
Referencias adicionales:	
https://www.itu.int/rec/T-REC-X.509/en	
https://en.wikipedia.org/wiki/X.509	

Vulnerabilidad #9	
Nombre:	SSL Self-Signed Certificate
Gravedad:	Media
Detalles de vulnerabilidad:	
La cadena de certificados X.509 de este servicio no estaba firmada por una autoridad de certificación de confianza. El uso de SSL se vuelve inútil si el host remoto es un host público en producción, ya que cualquiera podría lanzar un ataque man-in-the-middle contra él. Tenga en cuenta que este complemento no comprueba las cadenas de certificados que terminan en certificados que no son auto firmados, sino certificados firmados por una autoridad de certificación que no es de confianza.	
Solución:	
Para este servicio, debe comprar o crear un certificado SSL adecuado.	

Vulnerabilidad #10	
Nombre:	TLS Version 1.0 Protocol Detection
Gravedad:	Media
Detalles de vulnerabilidad:	
El servicio remoto permite conexiones cifradas TLS 1.0. Existen varios problemas de diseño criptográfico con TLS 1.0. Las implementaciones actuales de TLS 1.0 solucionan estos problemas, pero las versiones posteriores de TLS, como 1.2 y 1.3, están diseñadas para solucionarlos y deberían utilizarse siempre que sea posible. A partir del 31 de marzo de 2020, los principales navegadores web y los principales proveedores dejarán de admitir terminales que no estén habilitados para TLS 1.2 y superiores. A excepción de los terminales POS POI (y los puntos de terminación SSL/TLS a los que se conectan), que pueden validarse como no vulnerables a ningún ataque conocido, TLS 1.0 debe terminarse completamente antes del 30 de junio de 2018, según PCI DSS v3.2.	
Solución:	
Desactivar el soporte para TLS 1.0 y activar el soporte para TLS 1.2 y 1.3.	
Referencias adicionales:	
https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00	

Vulnerabilidad #11	
Nombre:	TLS Version 1.1 Protocol Deprecated
Gravedad:	Media
Detalles de vulnerabilidad:	
El servicio remoto permite conexiones cifradas TLS 1.1. TLS 1.1 no admite las suites de cifrado más recientes y aconsejadas. TLS 1.1 prohíbe el uso de GCM y otros modos de cifrado autenticado, así como los cifrados que permiten el cifrado antes del cálculo de MAC. Los terminales que no estén configurados para TLS 1.2 y superior dejarán de funcionar correctamente con los principales navegadores web y los principales fabricantes a partir del 31 de marzo de 2020.	
Solución:	
Deshabilite el soporte para TLS 1.1 y habilite el soporte para TLS 1.2 y/o 1.3.	

Referencias adicionales:
https://datatracker.ietf.org/doc/html/rfc8996
http://www.nessus.org/u?c8ae820d

Vulnerabilidad #12	
Nombre:	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
Gravedad:	Media
Detalles de vulnerabilidad:	
El uso de RC4 en una o más suites de encriptación es soportado por el host remoto. Debido a una debilidad en la forma en que el cifrado RC4 genera bytes pseudoaleatorios, el flujo contiene una serie de sesgos menores que reducen su imprevisibilidad. Un atacante puede ser capaz de deducir el texto plano si éste se cifra con frecuencia (por ejemplo, utilizando cookies HTTP) y el atacante puede acceder a un gran número de textos cifrados (decenas de millones).	
Solución:	
Si es posible, reconfigure el programa afectado para renunciar al uso de cifrados RC4. En caso de que los servidores web y los navegadores lo soporten, piense en emplear TLS 1.2 con suites AES-GCM.	
Referencias adicionales:	
https://www.rc4nomore.com/	
http://www.nessus.org/u?ac7327a0	
http://cr.yp.to/talks/2013.03.12/slides.pdf	

Vulnerabilidad #13	
Nombre:	SMB Signing not required
Gravedad:	Media
Detalles de vulnerabilidad:	
En el servidor SMB remoto, la firma no es necesaria. Esto puede ser utilizado por un atacante remoto no autenticado para lanzar ataques man-in-the-middle contra el servidor SMB.	
Solución:	
Establezca la configuración del host para que requiera la firma de mensajes. Esto puede encontrarse en la opción de política "Servidor de red Microsoft: Firmar digitalmente las comunicaciones (siempre)" de Windows. La configuración de Samba se conoce como "firma del servidor". Para más información, haga clic en los botones "ver también".	
Referencias adicionales:	
http://www.nessus.org/u?df39b8b3	
http://technet.microsoft.com/en-us/library/cc731957.aspx	
http://www.nessus.org/u?74b80723	

Vulnerabilidad #14	
Nombre:	SSL Certificate with Wrong Hostname
Gravedad:	Media
Detalles de vulnerabilidad:	
El certificado SSL suministrado para este servicio tiene una máquina diferente en el parámetro "commonName" (CN).	
Solución:	
Para este servicio, debe comprar o crear un certificado SSL adecuado.	

Vulnerabilidad #15	
Nombre:	Terminal Services Doesn't Use Network Level Authentication (NLA) Only
Gravedad:	Media
Detalles de vulnerabilidad:	
La Autenticación a Nivel de Red (NLA) no es el único método de autenticación disponible para los Servicios de Terminal remotos. La autenticación fuerte del servidor a través de TLS/SSL o Kerberos es llevada a cabo por NLA utilizando el protocolo Credential Security Support Provider (CredSSP), que protege contra ataques man-in-the-middle. Al concluir la autenticación del usuario antes de establecer una conexión RDP completa, NLA no sólo refuerza la autenticación, sino que también ayuda a defender la máquina remota de usuarios y aplicaciones peligrosos.	
Solución:	
En el servidor RDP remoto, active la autenticación a nivel de red (NLA). En Windows, esto suele hacerse en la pestaña "Remoto" de la configuración "Sistema".	
Referencias adicionales:	
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732713(v=ws.11)	
http://www.nessus.org/u?e2628096	

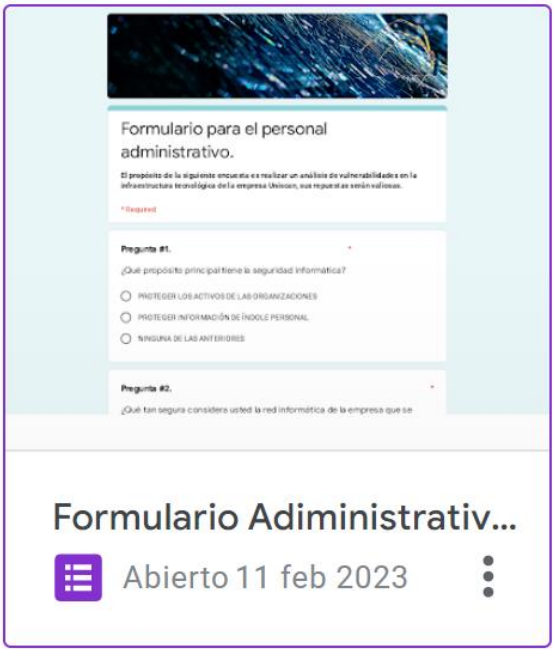
Vulnerabilidad #16	
Nombre:	Terminal Services Encryption Level is Medium or Low
Gravedad:	Media
Detalles de vulnerabilidad:	
La criptografía fuerte no está configurada para ser utilizada por el servicio remoto Terminal Services. Un cifrado débil en este servicio podría facilitar que un atacante espíe conversaciones y capture capturas de pantalla y/o pulsaciones de teclas.	
Solución:	
Establezca uno de los siguientes niveles de cifrado RDP: 3. Alto 4. Conforme a FIPS	

Vulnerabilidad #17	
Nombre:	mDNS Detection (Remote Network)
Gravedad:	Media
Detalles de vulnerabilidad:	
El servicio remoto conoce el protocolo Bonjour, a menudo denominado ZeroConf o mDNS, que permite a cualquiera conocer detalles sobre el host remoto, incluido su tipo de sistema operativo y versión precisa, nombre de host y la lista de servicios que está utilizando en ese momento. Este complemento busca hosts que utilicen mDNS y que no estén en el segmento de red en el que se encuentra Nessus.	
Solución:	
Si lo desea, filtre el tráfico entrante al puerto UDP 5353.	

Vulnerabilidad #18	
Nombre:	Terminal Services Encryption Level is not FIPS-140 Compliant
Gravedad:	Baja
Detalles de vulnerabilidad:	
La configuración de cifrado del servicio de Terminal Services remoto no es compatible con FIPS-140.	
Solución:	
Nivel de cifrado RDP cambiar a: 4. Conforme a FIPS	

ANEXO 10. FORMULARIOS DISEÑADOS EN GOOGLE PARA REALIZAR LAS ENCUESTAS AL PERSONAL TÉCNICO Y ADMINISTRATIVO DE LA EMPRESA UNISCAN.

Enlace de ingreso al formulario para el personal técnico: https://forms.gle/sZHZ1yKQFWv4EjX76



Enlace de ingreso al formulario para el personal administrativo: https://forms.gle/Av5nmV5bJaA62iZj8

ANEXO 11. DESARROLLO DE LA METODOLOGÍA MAGERIT DENTRO DE LA ORGANIZACIÓN UNISCAN.

Link de descarga del documento:

https://docs.google.com/spreadsheets/d/1PsUJpHb3CQK6Ckg1qUzsA0jLM1PPgrxU/edit?usp=share_link&ouid=113909454238408380337&rtpof=true&sd=true

ANEXO 12.PLAN DE TRATAMIENTO DE VULNERABILIDADES PARA LA ORGANIZACIÓN UNISCAN.

Link de descarga del documento:

https://drive.google.com/file/d/1T6X-G93c264RU_cqbUugsXykIAiDJhWJ/view?usp=share_link

ANEXO 13. CARTA DE ACEPTACIÓN DE REALIZACIÓN DE PROYECTO DE TESIS POR PARTE DE LA ORGANIZACIÓN UNISCAN.

Uniscan
Equipos y suministros para identificación Automática y Códigos de barras

Quito, a 19 de Julio de 2022.

Uniscan CIA. LTDA.
Gerente Técnico
Presente. -

Estimado Ing. José Luis Trujillo, quien suscribe Luis Omar Villacrés Túqueres, estudiante de la Maestría en Seguridad de la Información, me dirijo a usted para solicitarle el auspicio de su prestigiosa empresa Uniscan para la realización del proyecto intitulado como "Análisis de vulnerabilidad en la infraestructura tecnológica de la organización Uniscan en el área funcional de frontera de la empresa."

El proyecto que voy a llevar a cabo, tiene los siguientes objetivos:

- Analizar la infraestructura tecnológica en la empresa Uniscan en busca de los riesgos en la seguridad de la información dentro de la frontera de acción de la empresa.
- Identificar las vulnerabilidades en activos como, software y equipos de cómputo que se requiere que mantengan la integridad, confidencialidad, autenticidad y disponibilidad de los datos.
- Determinar las principales amenazas, al momento de realizar el análisis de las vulnerabilidades, en los activos que constituyen la infraestructura de la empresa.
- Proponer un plan de tratamiento para los riesgos de nivel inaceptable detectados durante el análisis de riesgos de seguridad de la información para obtener nociones básicas de cómo prevenir dichos ataques informáticos.

Para llevar a cabo con éxito los objetivos, es imprescindible realizar una auditoría de la infraestructura, que permita realizar el análisis e identificación de los activos, amenazas y vulnerabilidades en la infraestructura de la empresa para determinar los riesgos en los procesos que se vienen realizando en las diferentes actividades dentro de la organización y que en especial involucra el área de tecnologías de la información.

Me permito, por ello, acogerme a su amabilidad para solicitar la colaboración de su empresa en esta importante actividad que consiste en el análisis de vulnerabilidad en la infraestructura tecnológica de la organización aplicando y desarrollando los objetivos planteados en la parte superior del documento.

Si bien el alcance está limitado a la infraestructura de la empresa, durante el levantamiento de información será necesario revisar el servidor en el que se almacena todos los datos de clientes y de las transacciones comerciales que realiza la empresa, revisar la infraestructura de red de la organización, y demás actividades que involucran software y hardware que en conjunto forman parte de infraestructura de la empresa, al momento de analizar y dar tratamiento a la información se tomará las medidas necesarias para en todo momento proteger la confidencialidad, integridad y disponibilidad de la información, cuidando siempre de los pilares fundamentales se los sistemas de seguridad de la información mencionados anteriormente.

En espera de sus noticias le saluda atentamente.

Luis Omar Villacres Túqueres
C.C: 0919653170

Aprobado por:

Ing. José Luis Trujillo
Gerente Departamento Técnico Uniscan

Quito: Calle de los Perales N47-164 y Eloy Alfaro.
Telfs: (+593) 02 2245919 / 4614 /4643 / 4640 / 998087942
Guayaquil: Km 5.5 vía Daule entre Av. 4ta y Av. 5ta C.C. Big Outlet
Local 35. Telfs: (+593) 04 5 051-416 04 5 109-352 / 0984618315.