UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CARRERA DE TELECOMUNICACIONES

Tema:

EVALUACIÓN DE RIESGOS PARA UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN BASE A LA NORMA ISO/IEC 27001 APLICADO A UN PROVEEDOR DE SERVICIOS DE INTERNET

Trabajo de titulación modalidad Proyecto de Investigación, presentado previo a la obtención del título de Ingeniero en Telecomunicaciones.

ÁREA: Comunicaciones

LÍNEA DE INVESTIGACIÓN: Tecnologías de comunicación

AUTOR: William David Hidalgo Martinez

TUTOR: Ing. Andrea Patricia Sánchez Zumba, Mg.

Ambato – Ecuador

agosto – 2023

APROBACIÓN DEL TUTOR

En calidad de tutor del trabajo de titulación con el tema EVALUACIÓN DE RIESGOS PARA UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN BASE A LA NORMA ISO/IEC 27001 APLICADO A UN PROVEEDOR DE SERVICIOS DE INTERNET , desarrollado bajo la modalidad Proyecto de Investigación por el señor William David Hidalgo Martinez, estudiante de la Carrera de Telecomunicaciones, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, me permito indicar que el estudiante ha sido tutorado durante todo el desarrollo del trabajo hasta su conclusión, de acuerdo a lo dispuesto en el Artículo 17 del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato y el numeral 6.3 del instructivo del reglamento referido.

Ambato, agosto 2023.

……..

Ing. Andrea Patricia Sánchez Zumba, Mg.

TUTOR

AUTORÍA

El presente trabajo de titulación titulado: EVALUACIÓN DE RIESGOS PARA UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN BASE A LA NORMA ISO/IEC 27001 APLICADO A UN PROVEEDOR DE SERVICIOS DE INTERNET es absolutamente original, auténtico y personal y ha observado los preceptos establecidos en la Disposición General Quinta del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato. En tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, agosto 2023.

William David Hidalgo Martinez

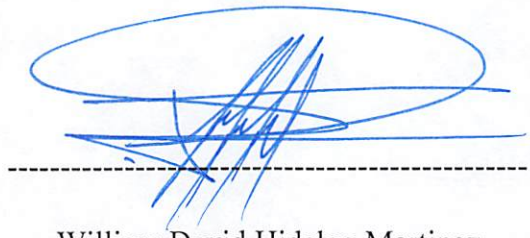
C.C. 1804894937

AUTOR

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato para que reproduzca total o parcialmente este trabajo de titulación dentro de las regulaciones legales e institucionales correspondientes. Además, cedo todos mis derechos de autor a favor de la institución con el propósito de su difusión pública, por lo tanto, autorizo su publicación en el repositorio virtual institucional como un documento disponible para la lectura y uso con fines académicos e investigativos de acuerdo con la Disposición General Cuarta del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato.

Ambato, agosto 2023.



William David Hidalgo Martinez

C.C. 1804894937

AUTOR

APROBACIÓN DEL TRIBUNAL DE GRADO

En calidad de par calificador del informe final del trabajo de titulación presentado por el señor William David Hidalgo Martinez, estudiante de la Carrera de Telecomunicaciones, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, bajo la Modalidad Proyecto de Investigación, titulado EVALUACIÓN DE RIESGOS PARA UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN BASE A LA NORMA ISO/IEC 27001 APLICADO A UN PROVEEDOR DE SERVICIOS DE INTERNET, nos permitimos informar que el trabajo ha sido revisado y calificado de acuerdo al Artículo 19 del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato y el numeral 6.4 del instructivo del reglamento referido. Para cuya constancia suscribimos, conjuntamente con la señora Presidente del Tribunal.

Ambato, agosto 2023.

Firmado electrónicamente por:
ELSA PILAR URRUTIA URRUTIA

Ing. Elsa Pilar Urrutia Urrutia, Mg.
PRESIDENTE DEL TRIBUNAL

Firmado electrónicamente por:
VICTOR SANTIAGO MANZANO VILLAFUERTE

Ing. Mg. Víctor Santiago Manzano Villafuerte.
PROFESOR CALIFICADOR

Firmado electrónicamente por:
JOSE VICENTE MORALES LOZADA

Dr. PhD José Vicente Morales Lozada.
PROFESOR CALIFICADOR

DEDICATORIA

Dedicado a Dios en primer lugar y luego "A mi padre, quien siempre fue mi fuente de inspiración y motivación en la vida. Aunque ya no está físicamente conmigo, su amor, sabiduría y coraje siguen viviendo en mí. Esta tesis no habría sido posible sin el apoyo y aliento que me brindó durante toda mi vida, y aunque no esté aquí para ver este logro, sé que está orgulloso de mí desde donde quiera que esté.

Te extraño tanto papá, pero sé que me guías desde arriba, y que siempre estás presente en mis pensamientos y acciones. Agradezco profundamente todo lo que me enseñaste y los valores que me inculcaste, los cuales me han guiado en este camino de la vida.

Esta tesis es para ti, papá, en honor a tu memoria y legado. Gracias por ser mi modelo a seguir y mi mayor héroe. Te amo y siempre te llevaré en mi corazón."

William David Hidalgo Martinez

AGRADECIMIENTO

"A Dios, quien es mi guía y protector en todo momento, le agradezco por darme la fortaleza y sabiduría para llevar a cabo este trabajo. A mi familia, quienes han sido mi mayor apoyo y fuente de inspiración en la vida, les doy las gracias por su amor incondicional y confianza en mí. En especial, quisiera agradecer a mi tía Miriam, quien siempre ha estado a mi lado, apoyándome incondicionalmente. Ella ha sido mi ángel en la tierra y sin ella no habría sido posible lograr este sueño, no obstante, a mi tía Crys de igual manera ya que en todo momento estuvo presente y fue mi voz de aliento.

A la Ingeniera Andrea Sánchez, quien me brindó su tiempo, conocimiento y paciencia para ayudarme a completar este trabajo. Sus consejos fueron esenciales para lograr los objetivos establecidos, y siempre estuvo dispuesta a ayudarme en todo momento.

Este logro no es solo mío, sino de todas aquellas personas que me han apoyado y alentado en este camino. Espero poder retribuirles de alguna manera en el futuro."

William David Hidalgo Martinez

ÍNDICE GENERAL DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN EJECUTIVO

La ciberdelincuencia es una amenaza constante para individuos y organizaciones a nivel mundial, porque utiliza técnicas expuestas para robar información confidencial, dañar sistemas y causar graves daños financieros y reputacionales. La importancia de la ciberseguridad es evidente a raíz de la pandemia del COVID-19, ya que los ciberdelincuentes buscan nuevas formas de explotar vulnerabilidades en sistemas y redes. Una de las principales preocupaciones es proteger los datos sensibles de empresas y usuarios. En la era digital actual, es fundamental protegerse contra amenazas y ataques cibernéticos, resguardar información y garantizar la integridad de los sistemas y la infraestructura crítica.

En el caso de un ISP, la Evaluación de Riesgos es importante debido a la naturaleza crítica de los datos que manejan. Los riesgos pueden incluir el acceso no autorizado a la información de los usuarios, la pérdida de datos, el fraude en línea y el daño a la reputación de la organización. Esta evaluación es exhaustiva, considerando factores como la confidencialidad, integridad y disponibilidad de la información, así como los riesgos asociados con los procesos y la tecnología utilizada basado en la norma ISO/IEC 27001. Ya que un ISP, maneja grandes cantidades de datos de clientes y usuarios, esta normativa proporciona un marco para el establecimiento, implementación, mantenimiento y mejora continua contra amenazas, la evaluación de la vulnerabilidad y la probabilidad de ocurrencia de cada riesgo, además de medidas de mitigación.

Mediante tecnología Open Source, se identifican los activos de información, la evaluación de las amenazas y vulnerabilidades a los que están expuestos. Adicionalmente, la determinación del impacto potencial de una amenaza en la empresa. Con esta información, se efectúan medidas adecuadas de seguridad de la información para mitigar los riesgos identificados.

Palabras clave: Open Source, Riesgo, vulnerabilidad, amenaza, mitigación, ISP.

ABSTRACT

Cybercrime is a constant threat to individuals and organizations worldwide, as it utilizes exposed techniques to steal confidential information, damage systems, and cause significant financial and reputational harm. The importance of cybersecurity is evident in the wake of the COVID-19 pandemic, as cybercriminals seek new ways to exploit vulnerabilities in systems and networks. One of the primary concerns is protecting sensitive data of companies and users. In today's digital age, it is crucial to safeguard against cyber threats and attacks, secure information, and ensure the integrity of systems and critical infrastructure.

In the case of an ISP, Risk Assessment is important due to the critical nature of the data they handle. Risks may include unauthorized access to user information, data loss, online fraud, and damage to the organization's reputation. This assessment is comprehensive, considering factors such as confidentiality, integrity, and availability of information, as well as risks associated with processes and technology used based on the ISO/IEC 27001 standard. Since an ISP manages large amounts of customer and user data, it provides a framework for the establishment, implementation, maintenance, and continuous improvement against threats, vulnerability assessment, and the likelihood of occurrence for each risk, along with mitigation measures.

Through Open Source technology, information assets are identified, and the evaluation of threats and vulnerabilities to which they are exposed is conducted. Additionally, the potential impact of a threat on the company is determined. With this information, appropriate information security measures are implemented to mitigate the identified risks.

Keywords: Open Source, risk, vulnerability, threat, mitigation, ISP.

CAPÍTULO I

MARCO TEÓRICO

1.1 Tema de investigación

Plan de Evaluación y Tratamiento de riesgos para un Sistema de Gestión de Seguridad de la Información en base a la norma ISO/IEC 27001 aplicado a un Proveedor de Servicios de Internet

1.1.1 Planteamiento del problema

Desde hace algunos años, muchas organizaciones a nivel mundial han comenzado a implementar un proceso de transformación digital que requiere del uso de nuevas tecnologías y almacenamiento de la información en la nube así como en diferentes dispositivos electrónicos, que conlleva a tener un especial cuidado con la evaluación y tratamiento de riesgos cibernéticos, por eso cada vez es más importante contar con un sistema de gestión de seguridad de la información basado en la norma ISO 27001 para proteger los datos y prevenir las consecuencias que traería la materialización de un riesgo de este tipo, lo que denota la necesidad de iniciar con la planificación de un SGSI [1].

Por otra parte, la seguridad de la información, es una escena de constante cambio, y de acuerdo con una investigación reciente de Check Point, proveedor global de soluciones de seguridad informática, los ciberataques a empresas han aumentado un 59% en 2022 [1], y es pertinente señalar que la empresa de ciberseguridad Kaspersky publicó un impactante informe de una operación global que infiltró bancos en Rusia, Estados Unidos, Alemania, China y Ucrania, donde alrededor de 100 bancos en 30 países diferentes fueron robados y se sustrajeron cientos de millones de dólares [2].

Karpersky se negó a nombrar bancos específicos fuera de los acuerdos de confidencialidad con los clientes, como estrategia de protección de datos. Los piratas informáticos utilizaron enjambres de spam para infectar las computadoras mediante el envío de una ola de correos electrónicos (SPAM) infectados con malware, y por la falta de conocimiento en este tipo de ataques, los empleados de las entidades financieras abrieron los correos electrónicos y dieron paso para que los ciberdelincuentes tengan acceso y control total de sus computadoras, y también del

sistema con credenciales de empleados obtenidas por ingeniería social. Utilizaron la red interbancaria SWIFT (Society for Worldwide Interbank Financial Telecommunication) para mover fondos de un lugar a otro, señaló Kaspersky [3]

Además, según el Informe de Riesgos Globales 2022 del Foro Económico Mundial, en diciembre de 2022, se descubrió una falla critica de seguridad en un software muy utilizado. Los datos reflejaban que más de 100 intentos de explotar la vulnerabilidad fueron detectados cada minuto, ilustrando la vulnerabilidad de los sistemas informáticos [3].

El delito cibernético aumentó en un 600 % como resultado de la pandemia de COVID 19 (SARS-CoV-2) desde robo y malversación hasta piratería y corrupción de datos. La Mayor parte de las industrias tuvieron que adoptar nuevas soluciones, y de acuerdo con estadísticas del Índice Global de Ciberseguridad de la Unión Internacional de Telecomunicaciones, agencia de la Organización de las Naciones Unidas; los ataques cibernéticos han aumentado entre un 30 y 40% en los últimos 3 años en América Latina, sobre todo en las zonas urbanas donde, según un estudio publicado a meses del inicio de la pandemia por el IICA, el BID y Microsoft, el 71% de la población ya cuenta con acceso a Internet. En las zonas rurales, no obstante, existe un notorio rezago con menos de un 37% de acceso [4].

Como consecuencia, los Estados miembros de la Organización de Estados Americanos (OEA), aprobaron un marco regional coordinado denominado “Estrategia Interamericana Integral para Combatir las Amenazas a la Seguridad Cibernética”. Con estos lineamientos se genera una instancia de cooperación internacional que promueve el intercambio de información, la protección de infraestructura tecnológica y la capacidad de respuesta y resiliencia de los Estados pertenecientes [4].

Un panorama que no es ajeno en Latinoamérica es Perú, sumándose a Brasil, Argentina, Colombia, México y Ecuador, como uno de los países más golpeados por los delitos informáticos, colocándose en el puesto 119 de 182 países en vulnerabilidad por los ciberdelincuentes. En cuanto a detecciones de phishing, Ecuador ocupó la séptima posición (5,1%), después de Brasil (26,4%), Perú (22,8%), México (12%), Colombia (9,1%), Argentina (7,1%) y Chile (6,5%) [5].

En lo referente a la ciudad de Ambato, algunas empresas implementan acciones para mitigar riesgos de ataques informáticos, sin embargo, estos procesos no son habituales en el sector empresarial. No obstante, los incidentes de ciberseguridad en infraestructuras ISP (internet Service Provider) han crecido de manera significativa, por lo que, se hace necesario implementar actividades que cooperen con la identificación de las prácticas de seguridad con el fin de salvaguardar la información personal e institucional de los principales ataques como ransomware, phishing, malware, inyección SQL, entre otros, que pueden poner en riesgo tanto la reputación de la empresa como la continuidad de la misma [1].

"CONCRELTEC" es una empresa que se dedica a proveer servicios de internet, incluyendo el servicio de fibra óptica, con más de mil usuarios del sur de Ambato, ubicada en la parroquia Picaihua en las calles Galo Vela y Platón sector el Calvario, en los últimos meses, esta entidad ha sufrido alertas de amenazas en cuanto al intento de robo y malversación de sus datos [6].

1.2 Antecedentes investigativos

La investigación presentada fue realizada partiendo de la información procesada de los distintos repositorios de las entidades educativas de nivel superior, tanto nacionales como internacionales, de la misma manera se ha procesado información proveniente de artículos científicos, informes de trabajos de investigación y reportes referentes a la seguridad de la información.

En el año 2020, Allaica Caranqui Joel Franklin, de la Universidad Técnica de Ambato realizó una "AUDITORÍA DE LA SEGURIDAD INFORMÁTICA SIGUIENDO LA METODOLOGÍA OPEN SOURCE SECURITY TESTING METHODOLOGY MANUAL (OSSTMM) PARA LA EMPRESA MEGAPROFER S.A." en donde el proyecto de investigación desarrollado tiene como objetivo ejecutar una Auditoría de la Seguridad Informática con el fin de determinar las posibles falencias o vulnerabilidades que puede tener la infraestructura de red y posterior explotación de las debilidades mediante el uso de las herramientas informáticas adecuadas para determinar los riesgos que tiene la empresa en lo referente a la red y activos informáticos, el nivel de acceso que podría tener una persona o un agente externo dentro de la empresa al pretender producir algún tipo de perjuicio en los servicios o

equipos tecnológicos y, a su vez al intentar substraer datos sensibles; tomando como fundamento los resultados conseguidos, para así plantear medidas y recomendaciones apropiadas que puedan garantizar la integridad, confidencialidad y disponibilidad de la información, así como posibles soluciones para mitigar a los inconvenientes encontrados. Para llegar al propósito planteado en el tema, se utiliza el Manual de la Metodología Abierta de Testeo de Seguridad (OSSTMM). los módulos de la metodología OSSTMM fueron seleccionados de manera acertada, ya que se pudo cumplir con los objetivos del proyecto, teniendo éxito y llegando a detectar vulnerabilidades existentes en los servidores de la empresa; mediante estos resultados se pudo plantear medias y políticas de seguridad acordes a la necesidad de la empresa en lo referente a seguridad informática [7].

Por otro lado, en el año 2020 el autor Lituma Briones Linda Carolina de la Universidad Estatal Península de Santa Elena realiza una investigación titulada "LABORATORIO VIRTUAL DE ANÁLISIS Y COMPORTAMIENTO DE MALWARE BASADO EN TÉCNICAS Y MÉTODOS DE SEGURIDAD INFORMÁTICA PARA LOS LABORATORIOS EN LA FACULTAD DE SISTEMAS Y TELECOMUNICACIONES", donde se implementó un laboratorio virtual de análisis y comportamiento de malware para mejorar la seguridad y protección de datos de la red en los laboratorios de la Facultad de Sistemas y Telecomunicaciones (FACSISTEL), debido a que en los mismos no existía un control en el tráfico de red que se generaba, lo que causaba una red inestable e insegura, provocando difusión de software malicioso (malware), infiltraciones de seguridad e incluso llegando a atentar contra la integridad de los datos que fluyen a través de las redes, anomalías que fueron motivos de análisis. Para lograr este análisis, el laboratorio virtual se implementó en los servidores de FACSISTEL y se utilizaron herramientas de código abierto que coadyuvaron en las fases del análisis estático y dinámico, constituyéndose en una poderosa herramienta que permite realizar el estudio de las máquinas infectadas dentro de en un entorno controlado los mismos que serán insumos válidos y confiables para la toma de decisiones en la creación de medidas de contención, mitigación y remediación de daños [8].

A continuación, en el año 2020 los autores: Liset Sulay Rodriguez Baca, Francisco Cruzado, Carolina Mejía y Mitchell Alarcón, realizan un artículo científico en la revista Propósitos y Representaciones Vol.8 no.3 publicado también en Scielo titulado "APLICACIÓN DE ISO 27001 Y SU INFLUENCIA EN LA SEGURIDAD DE LA INFORMACIÓN DE UNA EMPRESA PRIVADA PERUANA" donde el manejo de importante información puede considerarse como fundamental para los intereses estratégicos de las empresas. La investigación tuvo como objetivo el analizar la influencia de la aplicación del ISO 27001 en la seguridad de la información de una empresa privada de Lima (Perú). A partir de la aplicación de una metodología cuantitativa, se empleó un estudio pre-experimental en el que se determinó la influencia de la aplicación de la normativa ISO 27001.Para ello se consideró una muestra de 30 colaboradores de la empresa. La conclusión cuantitativa muestra que si existe una influencia de la aplicación del ISO en la seguridad de la información y en las dimensiones confidencialidad, integridad y disponibilidad. Los resultados muestran que en todos los casos se hallaron mejoras porcentuales después de aplicada la intervención, en relación a la integridad de la seguridad de la información, si una organización no implementa políticas o normas para el desarrollo de sus procesos, éstos marcharán a la deriva y expuestos a altos riesgos. Asimismo, se menciona que la aplicación de la normativa ISO 27001 influye en la integridad de la información porque permite evaluar que estrategias, políticas, directivas se están aplicando para evitar que la información sea alterada sin autorización [9].

Mayra Elizabeth Aillon Carrasco en el año 2021, en la Universidad Técnica de Ambato (UTA), presenta una AUDITORÍA DE SEGURIDAD DE LA INFORMACIÓN APLICANDO LA NORMA ISO/IEC 27001 EN EL GOBIERNO AUTÓNOMO DESCENTRALIZADO SAN PEDRO DE PELILEO, el cual tuvo como finalidad la mitigación de riesgos y protección de la información manejada diariamente en el Gobierno Autónomo Descentralizado Municipal San Pedro de Pelileo, por medio de la aplicación de políticas que se basan en la norma ISO 27001 en el ámbito de seguridad en cuanto al control de accesos gestión de activos, seguridad física, restricciones del personal, entre otros análisis, el cual busca satisfacer las necesidades de una entidad pública respecto al resguardo de información y a la par que funcionarios den cumplimiento a las políticas establecidas para que exista un control estricto en las áreas que existen falencias en cuanto a seguridad siempre buscando la mejora continua

con la aplicación de monitoreo constante de todas las áreas existentes, Después de haber realizado un análisis riguroso de las vulnerabilidades y riesgos existentes dentro del Gobierno Autónomo Descentralizado Municipal de San Pedro de Pelileo al aplicar el estándar ISO/EC 27001 se pudo determinar que no se cumplen con las respectivas normativas de seguridad en determinadas áreas, por ende es necesaria la implementación de políticas de seguridad que ayuden en la gestión adecuada de la información que se maneja dentro de la municipalidad, es obligatorio que estos estándares sean aprobados y puestos en marcha por la Unidad de Gestión Tecnológica [10].

De igual manera en el año 2021 los autores: Erick Guerra, Harol Neira, Jorge Diaz y Janns Patiño, publican un artículo científico en base a su investigación titulada "DESARROLLO DE UN SISTEMA DE GESTIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN BASADO EN METODOLOGÍA DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGO EN BIBLIOTECAS UNIVERSITARIAS", donde la investigación tuvo como objetivo la aplicación de un sistema de gestión de la información basado en la metodología de identificación y análisis de riesgos para los procesos de bibliotecas universitarias, Este además se adapta la norma ISO/IEC 27001:2013 combinado con la metodología MARGERIT en una biblioteca universitaria. Los resultados obtenidos de los cálculos de riesgos intrínseco y efectivo demostraron la presencia de salvaguardas y la evaluación de los impactos. Se estableció el porcentaje de afectación en cada riesgo por proceso de calidad, se identificó la medida correctiva, y se incorporaron formatos de registros. Se concluyó que la incorporación de los formatos propuestos para desarrollar el control y auditorías a los indicadores de calidad permite la optimización del sistema de gestión de la seguridad de la información (SGSI) para los procesos de la biblioteca universitaria [11].

Este proyecto, además tiene como respaldo los sitios web, La Ley Orgánica de protección de datos personales y su Reglamento, además de los requisitos principales que disponen la Agencia de Regulación y Control de las Telecomunicaciones ARCOTEL, a más de estar basado en la normativa ISO/IEC 27001, sobre todo en el Sistema de Gestión de Seguridad de la información y demás documentos que de una u

otra manera son de gran ayuda para el desarrollo de la investigación, obteniendo así información de las dos variables a utilizarse.

Una vez que se ha recopilada la información obtenida de los antecedentes investigativos y como aporte al proyecto se concluye que para llevar a cabo la evaluación de riesgos es necesario definir el alcance y límites de este, pues la puesta en marcha de este plan da como resultado las vulnerabilidades y elementos críticos del sistema, por lo que al desarrollar una correcta relación con la norma ISO/IEC 27001 se logra tener a buen recaudo la información sensible de la empresa.

1.3 Fundamentación teórica

En el presente punto se pretende fundamentar científicamente las variables de la investigación de la normativa ISO/IEC 27001 para plasmar el conocimiento fundamental con respecto a un sistema de gestión de seguridad aplicado a un proveedor de servicios de internet.

1.3.1. ISP (Internet Services Provider)

La evolución constante de la tecnología de comunicaciones ha llevado a una definición más amplia el concepto de un Proveedor de Servicios de Internet (ISP), pues ya no se limita simplemente a proporcionar acceso a Internet a los usuarios, sino que su función principal es permitir a los clientes obtener e intercambiar información a través de Internet. Además, los ISPs se encargan de ofrecer acceso a una variedad de servicios disponibles en la red, asegurando calidad, conectividad e inmediatez, independientemente del medio utilizado para la conexión a la red. En resumen, un ISP se define como una empresa que facilita a sus clientes el acceso y la interacción con información en Internet, al mismo tiempo que brinda una amplia gama de servicios en línea, garantizando una experiencia de calidad, conectividad y rapidez [12].

1.3.2. Características de un ISP

A fin de que un proveedor de servicios de Internet (ISP) pueda satisfacer las diversas necesidades de los usuarios, resulta imprescindible que cuente con características específicas que le posibiliten desenvolverse con eficacia y destreza ante los constantes requerimientos que enfrenta en su quehacer diario [12]:

- **Disponibilidad.** Es la capacidad del ISP para proporcionar una conexión a Internet estable y sin interrupciones [13].
- **Eficiencia.** Se refiere a su capacidad para obtener servicios de Internet de alta calidad de gestión y rentable [14].
- **Redundancia.** Capacidad de la infraestructura de red para mantener la conectividad y el servicio en caso de fallas o interrupciones en los sistemas principales [15].
- **Escalabilidad.** Con la escalabilidad la ISP tiene la habilidad de crecer y adaptarse a medida que aumenta la demanda de sus servicios [16].
- **Flexibilidad.** Ajusta sus servicios y características para satisfacer las necesidades específicas de los clientes [17].
- **Seguridad.** Protege la información, los datos de los clientes, garantizando la privacidad y la confidencialidad de posibles amenazas externas [18].
- **Soporte Técnico.** Brinda asistencia técnica y resolver los problemas técnicos de los clientes [14].
- **Preventa, Venta y Postventa.** Capacidad para brindar un servicio completo y satisfactorio a los clientes, desde el momento en que se interesan por el servicio hasta después de haberlo adquirido [14].
- **Call Center.** Habilidad para establecer conversaciones a través de llamadas telefónicas o canales digitales con los clientes y potenciales clientes de una empresa y brindarles información, soporte y asistencia [19].
- **Mercadeo.** Permite atraer y retener a los clientes a través de estrategias de marketing efectivas para promocionar y vender sus servicios de Internet a los clientes y potenciales clientes [14].
- **Protección de la inversión.** Se debe garantizar que la inversión realizada en la infraestructura y los servicios de Internet sea segura y rentable [20].

1.3.3. Arquitectura básica de un ISP

La arquitectura de un ISP puede dividirse en tres redes principales [21]:

- Red de acceso al cliente
- Red del ISP
- Red Troncal

La Figura 1. representa la estructura fundamental de un ISP, donde se ilustra la disposición básica de la arquitectura. Esta estructura incluye la red de acceso al cliente, que establece la conexión entre el usuario y la red interna del proveedor. Asimismo, se encuentra la red del ISP, que consta de múltiples redes locales (LAN) y un conjunto de servidores. Por último, está presente la red troncal, encargada de enlazar al ISP con el backbone de Internet o con un proveedor de servicios de Internet de nivel superior [21].

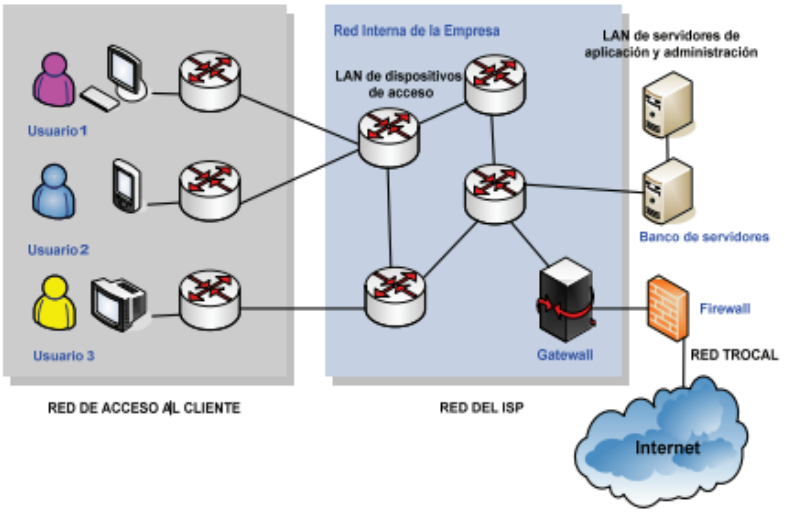


Figura 1. Arquitectura de un ISP *[21]*.

1.3.4. Open source

Es un software de código abierto con una forma de programación que se crea con la intención de ser accesible para el público en general. Esto implica que cualquier persona tiene la capacidad de visualizar, modificar y distribuir dicho código de acuerdo con sus propias necesidades y preferencias. El desarrollo del software se lleva a cabo de forma descentralizada y colaborativa, dependiendo de la revisión y aportes de los colegas y de la comunidad en general [22].

Igualmente, es común que el software sea más asequible, adaptable y perdurable en comparación con las alternativas propietarias, debido a que su desarrollo recae en comunidades y no en un único autor o empresa. Open source se ha convertido en un movimiento y en un enfoque laboral que va más allá de la creación de software. Adopta los valores y el modelo de producción descentralizada para descubrir nuevas formas de abordar problemas en comunidades y sectores diversos [22].

1.3.5. Riesgo

El término "riesgo" hace referencia a la posibilidad de que se produzcan eventos o situaciones que puedan afectar la seguridad de la información de la organización. La norma ISO/IEC 27001 establece que las organizaciones deben llevar a cabo una evaluación de riesgos para identificar y evaluar los riesgos de seguridad de la información, y luego implementar controles adecuados para mitigar o tratar esos riesgos. Algunos ejemplos de riesgos de seguridad de la información que pueden afectar a un proveedor de servicios de Internet incluyen el acceso no autorizado, la pérdida o robo de información, la interrupción del servicio, los errores humanos, el malware o virus informáticos, y las vulnerabilidades de seguridad [23].

La evaluación de riesgos es un proceso clave para garantizar que se identifiquen y aborden los riesgos de seguridad de la información de manera efectiva, y es un requisito fundamental para llevar a cabo la implantación de un sistema de gestión de seguridad de la información conforme a la norma ISO/IEC 27001 [24].

1.3.6. Amenaza

El término "amenaza" se define como cualquier evento o situación que pueda causar daño o perjuicio a la seguridad de la información de la organización. En cuanto a la ciberseguridad, existen dos enfoques distintos. El primero sostiene que es importante considerar las vulnerabilidades y trabajar en su mitigación, ya que se argumenta que una vez que existe una vulnerabilidad, en algún momento será explotada mediante un ataque. Por otro lado, el segundo enfoque, propone centrar los esfuerzos en identificar las amenazas en lugar de enfocarse únicamente en las vulnerabilidades, es necesario priorizar los ataques que tengan una mayor probabilidad de ocurrir y tener éxito. Las amenazas pueden provenir de fuentes internas o externas y pueden ser intencionales o accidentales. Algunos ejemplos de amenazas de seguridad de la información que pueden afectar a un proveedor de servicios de Internet incluyen [25]:

- Ataques de hackers o ciberdelincuentes que intentan acceder a la información confidencial de los clientes o interrumpir los servicios de Internet [23].
- Errores humanos, como la eliminación accidental de datos importantes o la divulgación no autorizada de información confidencial [23].

- Desastres naturales, como terremotos, incendios o inundaciones, que pueden dañar los equipos y sistemas de red y afectar la disponibilidad de los servicios de Internet [26].
- Fallos técnicos, como la interrupción de la energía eléctrica o la falla de los sistemas de refrigeración, que pueden afectar el funcionamiento de los equipos y sistemas de red [26].
- Vulnerabilidades de seguridad en los sistemas y aplicaciones de software utilizados por el proveedor de servicios de Internet, que pueden ser explotadas por atacantes para acceder a la información confidencial o interrumpir los servicios de Internet [27].

La identificación y evaluación de las amenazas es un paso importante en la evaluación de riesgos para un sistema de gestión de seguridad de la información según la norma ISO/IEC 27001, ya que permite a la organización desarrollar medidas de seguridad adecuadas para mitigar o tratar los riesgos identificados [23].

1.3.7. Vulnerabilidad

El término "vulnerabilidad" se define como una debilidad o fallo en los sistemas, aplicaciones o procesos que pueden ser explotados por atacantes para comprometer la seguridad de la información. Las vulnerabilidades pueden surgir debido a fallos en el diseño, falta de actualizaciones de seguridad, configuraciones inadecuadas, y otros factores similares. Algunos ejemplos de vulnerabilidades de seguridad de la información que pueden afectar a un proveedor de servicios de Internet incluyen [25]:

- Fallos de seguridad en el software utilizado por el proveedor de servicios de Internet, como sistemas operativos, aplicaciones web, bases de datos, entre otros [28].
- Configuraciones incorrectas de los sistemas y aplicaciones que pueden permitir el acceso no autorizado a la información confidencial [28].
- Falta de actualizaciones de seguridad para los sistemas y aplicaciones que pueden dejarlos expuestos a vulnerabilidades conocidas [26].
- Fallos en los procesos de gestión de la seguridad de la información, como la falta de políticas y procedimientos claros, la falta de capacitación del personal, entre otros [26].

1.3.8. Contramedidas

Son las medidas de seguridad que se implementan para reducir o eliminar los riesgos identificados, se utilizan para mitigar los riesgos de seguridad de la información y proteger los activos críticos de la organización. Las amenazas se valen de las vulnerabilidades existentes, mientras que las contramedidas se encargan de eliminar dichas amenazas. Las contramedidas se clasifican en [29]:

Tabla 1. Clasificación de contramedidas

Tipo	Descripción
Físicas	Todos aquellos mecanismos que protejan al sistema informático de entradas no deseables o de robos.
Lógicas	Con el fin de gestionar los accesos a los recursos, se aplican medidas de control como la criptografía y la realización de copias de seguridad.
Administrativas	Medidas tomadas por las personas responsables de la seguridad. Definición de una política de seguridad.
Legales	Medidas que se aplican después de ocurrir un suceso.

Elaborado por: El investigador basado en [29].

La implementación de contramedidas es un paso importante en la evaluación de riesgos para un sistema de gestión de seguridad de la información según la norma ISO/IEC 27001, ya que permite a la organización reducir o eliminar los riesgos identificados y proteger los activos críticos de la organización [28].

1.3.9. Sistema de gestión de seguridad de la información (SGSI)

Un Sistema de Gestión de Seguridad de la Información (SGSI) abarca el conjunto de políticas, procedimientos, directrices, recursos y actividades que se administran en relación con la seguridad de la información de manera colectiva por una organización con el fin de proteger sus activos. Según el estándar internacional ISO/IEC 27001, un SGSI es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información en una organización, con el fin de alcanzar los objetivos comerciales y/o de servicio establecidos. Esto aplica tanto a empresas públicas como a organizaciones sin fines de lucro y otros tipos de entidades [30].

En general, el concepto de seguridad de la información se basa en reconocer que la información es un activo de valor que requiere una protección adecuada. Esto implica salvaguardarla contra posibles pérdidas de disponibilidad, confidencialidad e integridad. Cada organización tiene la capacidad de ampliar e integrar en su Sistema de Gestión de Seguridad de la Información (SGSI), y además se puede considerar la autenticidad, trazabilidad y no repudio, según sea necesario para cumplir con los requisitos internos y/o externos aplicables a cada actividad [31].

1.3.10. Fundamentos de la seguridad de la información

A fin de asegurar una correcta gestión, es necesario identificar el ciclo de vida del Sistema de Gestión de Seguridad de la Información, el cual se fundamenta en una serie de principios clave que se describen en la figura 2.

Figura 2. Triángulo CIA Seguridad Información *[32]*.

- **Confidencialidad:** Se persigue restringir el acceso a la información, asegurando que solo las personas autorizadas puedan utilizarla. El objetivo es preservar la privacidad y evitar la divulgación no autorizada de información sensible [33].
- **Integridad:** Describe la protección de la información en términos de su almacenamiento, gestión y administración. Implica garantizar que la información no sea modificada o alterada de manera no autorizada, manteniendo su exactitud y confiabilidad [33].
- **Disponibilidad:** La disponibilidad es esencial para la productividad de las organizaciones, asegurando que los recursos y sistemas estén disponibles y funcionando adecuadamente en todo momento [30].

1.3.11. Fallo de seguridad

Se entiende como cualquier evento o suceso que compromete alguno de los aspectos evaluados en términos de seguridad. Dado el creciente número de usuarios que manejan sistemas de información cada vez más complejos y que intercambian información constantemente, resulta todo un desafío evitar la aparición de diversos tipos de fallos, entre los cuales se pueden mencionar [33]:

- Fallo en las comunicaciones.
- Fallos en el suministro eléctrico.
- Fallos humanos de usuarios internos, usuarios externos, administradores, etc.
- Fallos en los sistemas de información: redes, aplicaciones, equipos, etc.
- Virus informáticos, gusanos, troyanos, etc., que inundan la red.
- Accesos no autorizados a los sistemas o a la información.
- Incumplimiento de una ley o reglamento.

En ocasiones, los fallos de seguridad se producen debido a una percepción errónea de que, si se garantiza la seguridad física, no habrá problemas, o de que la protección de las aplicaciones y bases de datos es suficiente para garantizar la seguridad. Sin embargo, esta perspectiva deja desprotegidas muchas áreas de la organización o activos de información, lo que los expone a daños o destrucción. Es necesario considerar tanto la seguridad física como la seguridad lógica y las medidas organizativas para evitar estos fallos y proteger de manera integral los activos de información [33].

1.3.12. Escáner de vulnerabilidades

Las empresas de todos los tamaños tienen algún tipo de información que un atacante podría explotar. Incluso es posible que un ciberdelincuente invada la red disponible de una empresa con el único propósito de causar problemas de testeo de la Seguridad de la web. Ya se trate de historiales médicos de pacientes, datos de tarjetas de crédito, historiales de transacciones de consumidores o secretos comerciales, si una empresa utiliza la tecnología para transmitir o almacenar información sensible, tiene la responsabilidad de protegerse contra la vulnerabilidad de los ciberataques. Existen herramientas de escaneo y comprobación de vulnerabilidades que son necesarias para proteger un sistema de ataques o amenazas [34].

Desafortunadamente, no todas las organizaciones hacen lo suficiente para escanear y bloquear las medidas de Seguridad de su red para evitar las vulnerabilidades. Los escáneres de vulnerabilidades son herramientas imprescindibles para proteger sus valiosos activos digitales sin agotar los recursos de IT [34].

1.3.13. Aplicaciones de escaneo de vulnerabilidades

Los escáneres de vulnerabilidades son herramientas y aplicaciones fáciles de usar que las empresas grandes y pequeñas utilizan para proporcionar y evaluar la eficacia y la Seguridad de sus sistemas, redes y aplicaciones web.

Con las herramientas de escaneo de vulnerabilidades, también conocidas como aplicaciones de evaluación de vulnerabilidades, los equipos de Seguridad pueden detectar brechas, puntos débiles o una vulnerabilidad en cualquier parte del sistema, la red o las aplicaciones web como:

- Firewalls
- Impresoras
- Máquinas de fax
- Routers
- Un servidor web
- Sistemas operativos
- Vulnerabilidad en la nube
- Componentes de herramientas de código abierto
- Testeo de seguridad de aplicaciones.

Un escaneo o evaluación de vulnerabilidades puede encontrar estas debilidades de Seguridad en la web, que pueden ser vistas como los puntos de entrada vulnerables disponibles que los usuarios no autorizados utilizan para infiltrarse en las aplicaciones del sistema, y que explotan viendo el tráfico de entrada y salida de las aplicaciones de la red. Muchos pueden hacerlo liberando datos sensibles (causando así una filtración) y tomando el control de las aplicaciones de la red, bloqueando al equipo de Seguridad de la organización, líderes y empleados [34].

Las herramientas de escaneo de vulnerabilidades utilizan un proceso de evaluación sistemático y automatizado que agiliza la capacidad de exploración de:

- Lagunas en la comprobación de Seguridad de las aplicaciones
- Brechas de vulnerabilidades
- Aplicaciones web antiguas
- Otras vulnerabilidades del Sistema Operativo
- Otras vulnerabilidades de la aplicación web
- Una vulnerabilidad basada en la web de código abierto [34].

Reducen significativamente el riesgo de vulnerabilidad al acceso no autorizado disponible en muchos sistemas y aplicaciones (aplicación web, redes, empresa basada en la nube, software, herramienta de código abierto, servidor web, etc.) comprobando regularmente las aplicaciones para preservar la integridad y confidencialidad de la empresa y sus sistemas [34].

Hay muchas herramientas, aplicaciones y software de vulnerabilidades disponibles que pueden ayudar en el escaneo de vulnerabilidades. Todos ellos cubren activos específicos para ayudar a las empresas a desarrollar un programa de gestión de vulnerabilidades. Con esto la organización tendrá un conocimiento claro y general de lo débiles o robustas que son sus redes, y la ayuda disponible para mejorarlas [34].

El uso de una herramienta de software de escaneo de vulnerabilidades ofrece diversos beneficios a las organizaciones, entre los que se incluyen los siguientes [34]:

Los escáneres de vulnerabilidades son herramientas automatizadas, por lo que el margen de error humano disminuye drásticamente. A los profesionales de la Seguridad les llevaría una cantidad de tiempo considerable comprobar manualmente cada componente del sistema, por lo que una evaluación de las vulnerabilidades mediante la automatización es más rápida y eficaz en el tiempo. Las personas siguen siendo necesarias para el proceso general de escaneo de la red, porque es importante asegurarse de que ninguna vulnerabilidad sea un falso positivo [34].

Las herramientas de escaneo de vulnerabilidades reducirán el tiempo y el coste de la limpieza del sistema tras una amenaza o un ciberataque y, al mismo tiempo, reforzarán la organización y evitarán cualquier riesgo de Seguridad durante la evaluación [34].

La evaluación de las vulnerabilidades tiene un rendimiento de calidad y solo tarda unas horas en completarse [34].

1.3.14. Causas de las vulnerabilidades de Seguridad

Aunque los hackers pueden infiltrarse en los sistemas de muy diversas formas, las empresas deben tener en cuenta varios puntos débiles de Seguridad en particular. Las herramientas de escaneo de vulnerabilidades por sí solas no serán suficientes para abordar cada uno de estos puntos débiles, pero puede utilizar muchas herramientas de software disponibles para ayudarle a priorizar los riesgos de amenaza que plantea cada uno [34].

1.3.14.1. Abuso de cuentas

Una formación inadecuada en materia de Seguridad, la falta de políticas y la mala intención son las formas más comunes de desarrollar vulnerabilidades en la red de una organización y sus dispositivos [34].

Los siguientes factores pueden contribuir a una debilidad:

- Problemas de configuración del servidor
- Filtraciones de datos
- Incumplimiento de los protocolos de seguridad
- Credenciales predeterminadas
- No eliminar los usuarios antiguos de los sistemas
- Errores en la configuración web:
- Las aplicaciones web mal configuradas o anticuadas pueden contribuir a una vulnerabilidad de la aplicación web [34].

Algunos ejemplos de casos de uso de aplicaciones web mal configuradas son:

- Certificación SSL (Secure Sockets Layer, Capa de sockets seguros) caducada
- Configuración HTTP incorrecta
- Codificación no segura [34].

Otros casos de uso incluyen aplicaciones de terceros:

Añadir demasiadas aplicaciones o complementos de terceros en los dispositivos de red los deja expuestos a brechas de Seguridad. No todas las aplicaciones disponibles están al día con su software y muchas pueden quedar obsoletas. Los delincuentes utilizarán las brechas de estos complementos como otra puerta trasera en los sistemas de su organización [34].

1.3.14.2. Mala estructura de red:

Dejar las redes abiertas al no requerir contraseñas o credenciales de usuario personalizadas puede ser conveniente para los trabajadores y clientes, pero puede ser desastroso para la empresa. Las redes abiertas tienen una Seguridad mínima y son objetivos fáciles para los usuarios no autorizados. Se puede hacer frente a esta vulnerabilidad segmentando el sistema y dando solo los privilegios suficientes a los usuarios finales para que realicen el trabajo que se les ha asignado [34].

1.3.15. Escaneo de vulnerabilidades

Los procedimientos exactos que utiliza la herramienta de software de escaneo de vulnerabilidades dependerán del departamento de IT y del equipo de Seguridad de la organización, ya que hay muchas herramientas y funciones a su disposición. Este software elegirá la mejor herramienta de escaneo de vulnerabilidades para la organización [34].

Independientemente de la elección, los miembros del equipo utilizarán escáneres de vulnerabilidades junto con otras tácticas para generar una respuesta de los dispositivos de la red. Compararán las respuestas que reciban con vulnerabilidades conocidas dentro de una base de datos para determinar la gravedad de la brecha de Seguridad [34].

Los pasos para que una herramienta de software de escaneo de vulnerabilidades pueda identificar y ayudar a los profesionales de IT son:

- Identificación de vulnerabilidades
- Identificación de valoraciones de riesgos
- Tratamiento de vulnerabilidades identificadas
- Informe de vulnerabilidades [34].

1.3.15.1. Identificación de vulnerabilidades

El descubrimiento de vulnerabilidades mediante herramientas de escaneo de vulnerabilidades se basa en tres factores:

1) La capacidad del escáner de vulnerabilidades para localizar e identificar dispositivos de red, puertos abiertos y software.
2) La capacidad del escáner de vulnerabilidades para identificar y recopilar datos del sistema y de la base de datos de vulnerabilidades conocidas.
3) La capacidad del escáner para correlacionar los datos que identifica con al menos una base de datos de vulnerabilidades conocidas [34].

Los administradores de IT pueden configurar la herramienta de software de escaneo de vulnerabilidades para que sea más o menos agresiva en sus escaneos, lo que a veces es necesario porque puede ser lo suficientemente intrusiva como para afectar a la estabilidad de la red durante el proceso de escaneo. Los escaneos también pueden reducir el ancho de banda, pero ninguno de estos problemas es permanente en los escaneos [34].

Para reducir o eliminar este problema, los equipos de seguridad pueden programar las herramientas de escaneo de vulnerabilidades para que funcionen fuera de horario. El equipo debe asegurarse de escanear todos los portátiles de la empresa y cualquier otro dispositivo que se conecte a la red [34].

1.3.15.2. Evaluación de riesgos

Los servicios de escaneo de vulnerabilidades suelen utilizar una extensa lista generada de vulnerabilidades identificadas. Intentar mitigar toda la lista, si es demasiado larga, puede consumir demasiados recursos informáticos y no es práctico mitigar algunas vulnerabilidades de la red les costará a las empresas menos que no hacer nada y permitir que un delincuente explote los puntos débiles [34].

La evaluación de los riesgos de todas las vulnerabilidades alertará a los equipos de Seguridad sobre las que suponen las mayores amenazas y las menos problemáticas. Durante esta fase, los profesionales de IT pueden determinar:

- La gravedad de las brechas de Seguridad y cómo podrían afectar a la organización si se manipulan con éxito [34];

La facilidad con la que un atacante podría explotar la vulnerabilidad, incluyendo si pudiese hacerlo desde Internet o si debe estar físicamente presente para acceder a un dispositivo de red conectado directamente al sistema [34];

- Si pueden reconfigurar los controles de Seguridad actuales.
- Si las vulnerabilidades son falsos positivos.
- Mediante la evaluación de riesgos, el equipo puede determinar qué puntos débiles necesitan una atención más urgente y cuáles pueden ignorar [34].

1.3.15.3. Tratamiento de vulnerabilidades identificadas

El objetivo final de los servicios de evaluación de vulnerabilidades es parchear o reparar una vulnerabilidad conocida de la red, y eliminar los riesgos existentes para la empresa. Lamentablemente, no todas las vulnerabilidades de Seguridad disponen de soluciones inmediatas, por lo que los administradores de IT suelen mitigar la vulnerabilidad añadiendo más protecciones para dificultar la explotación por parte de un delincuente. La mitigación no es una solución permanente, pero es una forma efectiva de reducir una amenaza potencial hasta que un parche viable pueda asegurar la brecha en la Seguridad de la red [34].

Durante esta fase, la organización puede aceptar la vulnerabilidad y no hacer nada para prevenir un ataque. Esta suele ser la mejor opción para las vulnerabilidades, pero es importante asegurarse de que el riesgo de peligro para la empresa sea bajo y los costes para solucionar el problema sean mayores que el daño que podría causar [34].

1.3.15.4. Informe de vulnerabilidades

Después de que el equipo de IT aborde todas las vulnerabilidades identificadas, debe cumplir con las normas que rigen la organización documentando lo que encuentran y tratan.

Una herramienta de software de escaneo de vulnerabilidades puede generar y proporcionar informes personalizables, que ayudan al equipo a entender qué tratamientos funcionan mejor para vulnerabilidades específicas sin requerir demasiados recursos. Los informes también permiten al departamento de IT controlar el flujo y reflujo de las tendencias de vulnerabilidades a lo largo del tiempo. Cuantos más conocimientos tenga sobre las vulnerabilidades específicas, más éxito tendrá la protección de los sistemas [34].

1.3.15.5. Técnicas de gestión de vulnerabilidades

El uso de una herramienta de software de escaneo de vulnerabilidades en sus sistemas y redes proporcionará a los departamentos de IT y a los administradores de la organización una valiosa información sobre los puntos fuertes y las vulnerabilidades de su infraestructura. La inclusión de técnicas adicionales de gestión de vulnerabilidades en la estrategia de la empresa proporcionará más información sobre la red [34]:

1.3.16. Pentesting:

Los test de penetración y los escáneres de vulnerabilidades trabajan juntos para permitir al personal de Seguridad de gestión de vulnerabilidades ver la red desde la perspectiva de un hacker. El pentesting es un procedimiento de gestión en el que los expertos en Seguridad simulan un hackeo en una red de forma controlada [34].

Los test de penetración permiten utilizar métodos de hackeo bien conocidos para identificar la amplia gama de formas en que un atacante podría ingresar en el sistema. Los test de penetración pueden proporcionar una visión general de las consecuencias reales que las vulnerabilidades podrían tener en la empresa si se explotara con éxito el punto débil [34].

1.3.16.1. Escaneo de Internet o aplicaciones web:

Las aplicaciones web necesitan tanta protección como las redes internas, pero las empresas suelen pasar por alto los testeos de Seguridad de las aplicaciones web. Una herramienta de software de escaneo de Seguridad de vulnerabilidades de aplicaciones web es similar a los escáneres de vulnerabilidades y puede detectar las vulnerabilidades basadas en la web que existan. Los escáneres de vulnerabilidades de Internet o de aplicaciones web son herramientas que ayudan a detectar diversos problemas en línea, como la inyección SQL, la inyección de comandos, los problemas de configuración no segura del servidor, el cross-site scripting y más. Por lo tanto, garantizan la Seguridad de las aplicaciones web testeando y detectando las configuraciones, inyección SQL y cross-site scripting de estas [34].

1.3.16.2. Configuración de la gestión:

Las malas configuraciones de la gestión y la falta de gestión de los parches son algunas de las razones más comunes de las vulnerabilidades. Los testeos de Seguridad y los escaneos de las aplicaciones pueden sacar a la luz estos riesgos de gestión, aun cuando hayan pasado desapercibidos durante meses o años. Solucionar estos problemas de configuración mediante escaneos a menudo crea coherencia en toda la red y aumenta su Seguridad. Estas técnicas adicionales de gestión de vulnerabilidades proporcionarán información sobre la red en la estrategia de mitigación de vulnerabilidades de la empresa [34].

1.3.16.3. Tipos de escaneo de vulnerabilidades

Los profesionales de IT que planifican su enfoque de escaneo de vulnerabilidades tienen varias opciones a su disposición. Pueden optar por combinar varios tipos de estrategias para descubrir qué versión funciona mejor o pueden ceñirse al método preferido por la organización. Los escaneos de vulnerabilidades internos y externos cubren dos tipos distintos de ubicaciones de red, mientras que los escaneos de vulnerabilidades autenticados y no autenticados dividen el alcance del escaneo [34].

1.3.16.4. Escaneo de vulnerabilidades externo

El escaneo de vulnerabilidades externo se realiza fuera de la red de la empresa. Este escaneo de detección de vulnerabilidades externo busca cualquier posible intruso o problema de seguridad a lo largo del perímetro de la red, incluso dentro de las diversas defensas que proporciona, como firewalls de Seguridad de la red o de aplicaciones web [34].

La forma en que un hacker o intruso intenta invadir los sistemas es similar a la forma en que un ladrón entra en una casa. Intentan entrar por las entradas conocidas, como puertas y ventanas, pero si el propietario las cierra con llave, al intruso le resulta más difícil robar la casa [34].

Los escaneos de vulnerabilidades externos son como cerrar todas las puertas y ventanas de una casa para comprobar su perímetro. Estos escaneos de detección externos son herramientas valiosas que comprueban las direcciones IP externas y los límites del sistema para que el departamento de IT pueda parchear cualquier debilidad que encuentren para mantener a un intruso fuera [34].

1.3.16.5. Escaneo de vulnerabilidades interno

La mayoría de las empresas entienden que los atacantes tratarán de encontrar y obtener acceso a sus sistemas desde fuera del perímetro de su red, pero la red interna de la organización también está en riesgo de sufrir ciberataques. Utilice los escaneos de vulnerabilidades internos para combatir estas amenazas [34].

Las amenazas de Seguridad dentro de una red incluyen:

- Empleados descontentos con acceso a un dispositivo de red o información de usuario
- Malware descargado en un portátil de la empresa
- Un intruso que tiene acceso a una estación de trabajo desatendida dentro de las instalaciones.

Cualquiera de estas amenazas puede dar lugar a sistemas con datos borrados, exportados o alterados, lo que puede ser devastador para la organización al salir de sus parámetros de Seguridad. Se pueden implementar herramientas de detección para buscar vulnerabilidades en una red [34].

El escaneo de vulnerabilidades interno y las herramientas de detección de vulnerabilidades buscan vulnerabilidades dentro de la red interna. Encontrar y parchear los puntos débiles de la Seguridad dentro del sistema, o «amenazas internas», es tan necesario como cerrar las brechas en el perímetro de la red. Si los hackers descubren y explotan una vulnerabilidad interna en sus escaneos, pueden moverse rápidamente de forma lateral dentro del sistema hacia sus servidores [34].

1.3.16.6. Escaneos de vulnerabilidades autenticados y no autenticados

Los escaneos de vulnerabilidades autenticados utilizan credenciales de acceso para encontrar información detallada sobre el Sistema Operativo de la red, cualquier aplicación web y una herramienta de software dentro de la máquina. No todos los programas son accesibles a través de los dispositivos de red, pero aun así pueden suponer un riesgo para la Seguridad. Por ejemplo, se podría encontrar que la vulnerabilidad es un sitio web malicioso, cuidadosamente elaborado, en el que un usuario podría hacer click, confundiéndolo con una página legítima [34].

Las soluciones de evaluación de vulnerabilidades pueden incluir agentes de software que acceden a los dispositivos de la red, como los ordenadores, y una herramienta de software de escaneo de la red para conocer la postura de Seguridad completa de la empresa. Es importante conocer la postura de Seguridad completa para reunir más información para los agentes de la red [34].

Los escaneos no autenticados tienen el mismo propósito que los escaneos de vulnerabilidades autenticados, pero no utilizan credenciales de acceso. En su lugar, los servicios abiertos en un ordenador conectado a la red reciben paquetes en sus puertos abiertos. Este tipo de escaneo obtiene información específica del ordenador, incluyendo la versión del Sistema Operativo de los servicios, herramienta de software, capacidad de abrir archivos compartidos y otros datos que no necesitan credenciales de la empresa [34].

La herramienta de software de escaneo de vulnerabilidades puede encontrar y utilizar esta información para determinar qué versión o tipos de vulnerabilidades pueden tener los sistemas [34].

1.3.17. Kali Linux:

Kali Linux es una distribución de Linux especializada en seguridad informática y pruebas de penetración. Es una herramienta diseñada para profesionales y entusiastas de la seguridad cibernética que ofrece una amplia gama de herramientas y programas preinstalados para realizar pruebas de seguridad en redes, sistemas y aplicaciones, es un software bastante potente y con multitud de usos avanzados para que un administrador pueda aprovecharla a fondo. Se destacan algunas de sus principales características [35]:

- Es gratis, no tiene coste ninguno para usarlo tanto personal como profesionalmente.
- Cuenta con más de 600 herramientas para trabajar todo lo mencionado en el punto anterior.
- Cuenta con un soporte magnífico, en varios lenguajes y muy bien atendido.
- No hace falta instalarlo para usarlo, ya que tiene un modo live que permite utilizarlo desde dispositivos portátiles en casi cualquier sistema.

- Está desarrollado en un entorno seguro, lo que ofrece muchas garantías acerca de datos y fallos.
- Usa el estándar de jerarquía de sistema de archivos (FHS) que permite bibliotecas, archivos de soporte, etc [35].

Se basa en Debian y está desarrollado por Offensive Security. Su objetivo principal es proporcionar un entorno de pruebas completo y seguro para evaluar la seguridad de los sistemas y redes, así como para realizar auditorías de seguridad y análisis forense digital, esta distribución incluye una amplia variedad de herramientas, desde exploradores de vulnerabilidades y herramientas de hacking ético hasta utilidades de análisis de protocolos y herramientas de recuperación de datos. Además, se actualiza regularmente para incluir las últimas herramientas y mantenerse al día con las últimas técnicas de seguridad, igualmente es utilizado por profesionales de la seguridad, investigadores de seguridad y expertos en pruebas de penetración para llevar a cabo pruebas éticas y mejorar la seguridad de los sistemas. Su enfoque en la seguridad y su conjunto de herramientas hacen de Kali Linux una opción popular para aquellos que buscan una plataforma confiable y completa para fines de seguridad informática [36].

1.3.17.1. Funciones de Kali Linux

- Recopilación de información: herramientas para obtener todos los datos posibles sobre el sistema objetivo.
- Análisis de vulnerabilidades: escaneo e identificación de fallos de seguridad, los cuales pueden ser aprovechados para iniciar un ciberataque.
- Análisis de aplicaciones web: herramientas especiales para escanear sitios web en búsqueda de vulnerabilidades.
- Evaluación de bases de datos: encuentra vulnerabilidades de forma automática en bases de datos.
- Ataques de contraseñas: ataques de diccionario, tablas y fuerza bruta para encontrar contraseñas fáciles de descubrir.
- Ataques Wireless: herramientas para ejecutar ciberataques por medio de redes inalámbricas.
- Ingeniería inversa: herramientas para descubrir el código fuente de una aplicación. Por ejemplo, de un malware.

- Herramientas de explotación: sirven para aprovechar las fallas de seguridad de un sistema con el fin de infiltrarse en él.
- Sniffing and Spoofing: robo de datos y suplantación de identidad.
- Postexplotación: escalada de privilegios, establecimiento de persistencia y entrega del payload en el sistema. Es decir, ejecución de tareas dañinas como tal.
- Análisis forense: estudio de las huellas dejadas por un ciberatacante.
- Herramientas de reporte: especiales para diseñar informes de ciberseguridad, después de ejercicios de pentesting.
- Herramientas de ingeniería social: para simular campañas de phishing, spear phishing y más [36].

1.3.17.2. Algunas herramientas

Algunos de los programas más famosos que incluye Kali y cuáles son sus funciones:

- Nmap: este es uno de los programas de hacking más famosos y se utiliza para escanear redes, dispositivos y puertos abiertos. Nmap revela información sobre los dispositivos conectados a una red y sus fallos de seguridad.

- John The Ripper: es un programa de código abierto que se especializa en ejecutar técnicas para descubrir contraseñas. Por medio de esta herramienta puedes realizar ataques de fuerza bruta y de diccionario, para «romper» contraseñas (sobre todo las más fáciles).

- Metasploit: se trata de un framework de código abierto que contiene miles de herramientas para explotar vulnerabilidades conocidas en un sistema [36].

1.3.18. Cómo elegir un software para la gestión de vulnerabilidades

Un ***vulnerability management software*** de alta calidad debe ayudar a realizar un escaneo completo y continuo de tus plataformas. Para ello, es imperativo que el programa cuente con tecnología multifuncional. Asimismo, es necesario asegurarse de que haga uso de integraciones como la Inteligencia Artificial para detectar contenido malicioso y mantener al mínimo los falsos positivos. Aunado a esto, el sistema necesita ser automático y de fácil implantación para completar todas las exigencias de una herramienta realmente preparada para las amenazas en continua evolución [37].

Por último, que el software tenga su propio sistema de reporting es de vital importancia. Solo así, se podrá analizar la seguridad de la compañía a través del tiempo, y conocer en detalle los puntos vulnerables; así como seguir la ruta de actividades en la red corporativa por parte de los empleados, en la figura 3 se observa el logo de un escáner de vulnerabilidades [37].

1.3.19. Rapid7

Figura 3. Rapid7 Logo *[37]*.

Rapid7 es una empresa líder en seguridad cibernética y análisis de datos, que proporciona soluciones y servicios para ayudar a las organizaciones a gestionar y reducir los riesgos de seguridad en sus entornos digitales. Ofrece una amplia gama de productos y servicios diseñados para ayudar a identificar vulnerabilidades, detectar y responder a amenazas, y fortalecer la postura de seguridad de una organización [37].

En particular, se especializa en el desarrollo de herramientas y plataformas de seguridad cibernética que permiten a las organizaciones evaluar su postura de seguridad, realizar pruebas de penetración, detectar y responder a incidentes de seguridad, y administrar la exposición de vulnerabilidades. Sus soluciones abarcan áreas clave de seguridad, como gestión de vulnerabilidades, detección y respuesta de amenazas, orquestación y automatización de seguridad, y análisis de seguridad [37].

Además de sus productos, también ofrece servicios de consultoría y capacitación en seguridad cibernética para ayudar a las organizaciones a fortalecer sus capacidades y conocimientos en materia de seguridad. Su enfoque se basa en el uso de tecnología avanzada, análisis de datos y conocimientos especializados para proporcionar a las organizaciones la inteligencia y las herramientas necesarias para proteger sus activos digitales y responder eficazmente a las amenazas de seguridad [37].

En resumen, Rapid7 es una empresa de seguridad cibernética que ofrece soluciones y servicios para ayudar a las organizaciones a gestionar y mitigar los riesgos de seguridad, mediante el uso de tecnología, análisis de datos y consultoría especializada. Su enfoque integral abarca desde la evaluación de vulnerabilidades hasta la detección y respuesta de amenazas, brindando a las organizaciones una mayor visibilidad y control sobre su postura de seguridad cibernética. Ayuda a gestionar la vulnerabilidad de la red a través del análisis y la supervisión del comportamiento malicioso. Esto, con el fin de atacarlo, reducir los riesgos y optimizar la seguridad de los canales. Por otro lado, con esta herramienta se deben crear políticas y credenciales por separado, lo cual ralentiza el chequeo, su inclusión en la nube es parcial, pues solo se alojan allí los tableros de información [37].

Aun así, su agente de monitoreo continuo simplifica el trabajo de gestión de vulnerabilidad. Sin duda, la simplicidad es un punto a su favor, pues mantiene un proceso activo, que permite saber qué pasa en la red en tiempo real [37].

1.3.20. Herramienta de gestión de seguridad informática

Una buena herramienta de seguridad informática cuenta con los siguientes puntos:

1.3.20.1. Cobertura de activos

Para que la herramienta sea completa, es necesario que esta cuente con mecanismos que permitan ver de manera integral los activos.

Esto se logra combinando diagnósticos de aplicaciones conectadas a la red y la seguridad de los contenedores, de manera centralizada.

Rapid7 permite el escaneo general de los activos digitales como aplicaciones web y sistemas locales. Asimismo, ejecuta la remediación de agujeros de seguridad y mantiene bajo llave los contenedores. Por otro lado, sus conectores de nube se basan en una conexión API; lo que requiere de la implementación local de Nexpose a un entorno cloud.

1.3.20.2. Detección de vulnerabilidades

En la figura 4, hay un ejemplo de cómo sería detectar alguna vulnerabilidad mediante un equipo.

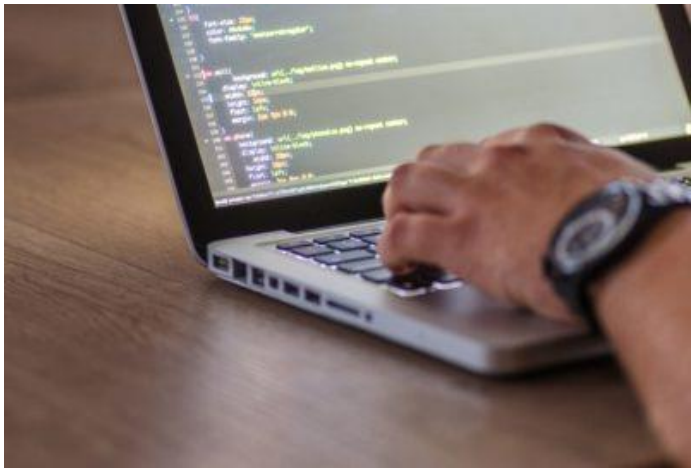


Figura 4. Detección de vulnerabilidades *[37]*.

La detección de amenazas es el centro de todo vulnerability management software. En este sentido, una herramienta fuerte cuenta con un análisis activo y otro basado en agente, apoyado en dispositivos de IO, lo cual reduce la generación de vulnerabilidades.

Además, se recomienda elegir soluciones con escaneo pasivo y continuo, que puedan proteger todo tu entorno de forma no intrusiva y sin generar interrupciones. Aunado a esto, el software debe contar con políticas de auditoría y configuración para distintos activos e inteligencia de amenazas; pues permite rastrear las últimas debilidades de Internet para salvaguardar tus datos [37].

Rapid7 cuenta con escaneos activos y agent based potenciados con Inteligencia de Amenazas.

1.3.20.3. Automatización

La automatización reduce la carga de trabajo en los departamentos de TI y Soporte. Es imperativo escoger una herramienta de seguridad informática capaz de realizar análisis programados e inteligentes. Pues estos se basan en el contexto donde se desenvuelven tus recursos tecnológicos para arrojar resultados más precisos [37].

De igual forma, debe incluir integraciones que muestren en tiempo real lo que pasa en el host, llevando así la protección al siguiente nivel. Por otro lado, se recomienda herramientas con parámetros de escaneo personalizados que ayuden a atacar las vulnerabilidades prioritarias.

- **Rapid7**

También ofrece módulo de información contextual. Sin embargo, esta integración solo puede ser utilizada con un etiquetado manual [37].

1.3.20.4. Gestión de resultados

Para medir la eficiencia de la gestión de resultados, se utilizan equipos de igual forma, como se observa en la figura 5.

Figura 5. Gestión de resultados *[37]*.

También se puede medir la eficiencia de las herramientas de seguridad informática a través de su flexibilidad y facilidad de adaptación a la empresa. En otras palabras: Debe contar con una licencia flexible capaz de trabajar perfectamente en software in-house y cloud.

Una gestión de reporting idónea cuenta con análisis especializados en protocolos de calidad y de seguridad [37].

Estos análisis permiten a los distintos departamentos tener el control de las operaciones de producción y ejecución de actividades online [37].

1.3.21. Nessus

Nessus es una herramienta ampliamente utilizada en el campo de la ciberseguridad que permite identificar y evaluar posibles debilidades y vulnerabilidades en sistemas informáticos, redes y aplicaciones. Desarrollada por Tenable, esta herramienta de escaneo de vulnerabilidades y evaluación de seguridad realiza un análisis exhaustivo de los sistemas y dispositivos objetivo para detectar posibles riesgos de seguridad, en la figura 6, se aprecia su logo [38].

Figura 6. Nessus Logo *[38]*.

Al utilizar una base de datos de vulnerabilidades conocidas y pruebas de seguridad, Nessus compara la configuración y el estado de los sistemas escaneados para identificar posibles vulnerabilidades y brechas de seguridad. A través de escaneos activos y exhaustivos, proporciona informes detallados que resumen los hallazgos de seguridad, incluyendo la gravedad de las vulnerabilidades encontradas y recomendaciones para solucionar los problemas identificados.

Esta herramienta es ampliamente utilizada para escanear redes empresariales y evaluar la seguridad de aplicaciones web. Su capacidad de generar informes personalizados y su amplia base de datos de vulnerabilidades la convierten en una herramienta poderosa para la identificación y mitigación de riesgos de seguridad [38].

Es importante destacar que el uso ético y el cumplimiento de las regulaciones y leyes aplicables son fundamentales al utilizar esta herramienta. Se recomienda que su implementación sea realizada por profesionales con conocimientos técnicos en ciberseguridad, ya que su interpretación adecuada y la implementación de las recomendaciones requerirán experiencia en el campo [38].

1.3.21.1. Información relevante sobre Nessus:

Funcionalidad: Nessus escanea activamente sistemas en busca de vulnerabilidades conocidas y posibles riesgos de seguridad. Utiliza una amplia base de datos de vulnerabilidades y pruebas de seguridad para identificar cualquier debilidad o brecha de seguridad en los sistemas objetivo.

Escaneo de red y de aplicaciones: Nessus es capaz de realizar escaneos tanto en redes como en aplicaciones. Los escaneos de red evalúan los sistemas y dispositivos conectados a una red en busca de vulnerabilidades, mientras que los escaneos de aplicaciones se centran en las aplicaciones web para identificar posibles problemas de seguridad [38].

Base de datos de vulnerabilidades: Nessus utiliza una base de datos actualizada constantemente que contiene información sobre miles de vulnerabilidades conocidas. Esto permite que la herramienta compare la configuración y los sistemas escaneados con esta base de datos para identificar posibles riesgos de seguridad [38].

Generación de informes: Nessus genera informes detallados y personalizables que resumen los hallazgos de seguridad. Estos informes proporcionan una visión general de las vulnerabilidades encontradas, su gravedad y recomendaciones para solucionar los problemas identificados [38].

Integración con otras herramientas: Nessus se puede integrar con otras herramientas y sistemas de gestión de seguridad para facilitar la correlación de datos y la administración de vulnerabilidades en un entorno empresarial [38].

Actualizaciones y soporte: Tenable, la empresa desarrolladora de Nessus, proporciona actualizaciones periódicas para mantener la herramienta al día con las últimas amenazas y vulnerabilidades. También ofrece soporte técnico a sus usuarios para resolver cualquier problema o duda que puedan surgir [38].

Es importante destacar que Nessus es una herramienta de seguridad avanzada y su uso requiere conocimientos técnicos sólidos en el ámbito de la ciberseguridad. Se recomienda utilizar Nessus de manera ética y cumpliendo con las regulaciones y leyes aplicables [38].

1.3.21.2. Cómo utilizar Nessus

Para utilizar Nessus es necesario descargar e instalar el software en un ordenador. Una vez instalado, se puede acceder a la consola web de Nessus a través de un navegador de Internet.

El primer paso es configurar el escaneo. Para ello, se debe seleccionar el tipo de escaneo que se desea realizar (por ejemplo, un escaneo de red, de web, de base de datos, etc.). Además, es necesario definir las opciones de escaneo, como el rango de direcciones IP que se desean escanear, las credenciales de acceso para el escaneo, etc.

Una vez configurado el escaneo, se puede iniciar el proceso de escaneo. Nessus examinará cada dispositivo de la red y buscará vulnerabilidades conocidas en su sistema operativo, aplicaciones y servicios. Los resultados del escaneo se presentan en

un informe detallado que indica las vulnerabilidades encontradas, su nivel de gravedad y la recomendación para corregirlas [38].

Para descargar Nessus, puedes seguir los siguientes pasos:

1) Visita el sitio web de Tenable, la empresa detrás de Nessus: https://www.tenable.com/downloads/nessus
2) Selecciona la versión de Nessus que deseas descargar. Hay versiones para diferentes sistemas operativos, incluyendo Windows, Linux y macOS.
3) Completa el formulario de registro y haz clic en «Descargar».
4) Después de descargar Nessus, instálalo en tu sistema. El proceso de instalación varía según el sistema operativo, pero generalmente es un proceso sencillo.
5) Una vez que hayas instalado Nessus, deberás configurarlo antes de poder comenzar a utilizarlo. Aquí hay algunos pasos básicos para implementar Nessus:
6) Abre Nessus y conéctate a través de tu navegador web.
7) Crea una política de escaneo. La política de escaneo establece cómo se llevará a cabo el escaneo de vulnerabilidades.
8) Crea un escaneo. Los escaneos se basan en las políticas de escaneo que has creado previamente.
9) Inicia el escaneo y espera a que se complete. Después de que el escaneo se complete, podrás ver un informe de vulnerabilidades encontradas [38].

1.3.21.3. Ejemplos de uso de Nessus

A continuación, se presentan algunos ejemplos de uso de Nessus en la práctica:

Escaneo de red: Una organización desea saber si su red corporativa está segura frente a posibles ataques externos. Para ello, utiliza Nessus para escanear todos los dispositivos conectados a la red en busca de vulnerabilidades. Nessus identifica una serie de vulnerabilidades críticas en el firewall, en algunos servidores y en los equipos de los empleados. La organización corrige las vulnerabilidades detectadas y mejora su postura de seguridad [38].

Auditoría de cumplimiento: Una organización debe cumplir con ciertos requisitos de seguridad impuestos por la normativa de la industria en la que opera. Nessus escanea la red y se asegura que cumple con los requisitos de seguridad, este encuentra algunas vulnerabilidades que la organización no había detectado previamente, lo que permite corregirlas y cumplir con los requisitos de seguridad necesarias [38].

Penetration testing: Una empresa de seguridad desea probar la seguridad de los sistemas informáticos de una organización mediante la simulación de un ataque. Nessus identifica vulnerabilidades que podrían ser explotadas por un atacante real y simula un ataque para probar la efectividad de las defensas de la organización [38].

Evaluación de proveedores: si se desea evaluar la seguridad de los proveedores con los que trabaja para asegurarse de que cumplen con los estándares de seguridad necesarios. Nessus escanea los sistemas informáticos de los proveedores y determinar si tienen vulnerabilidades que podrían poner en riesgo la información de la organización [38].

Seguimiento de la postura de seguridad: Nessus de forma regular escanea la red y se asegura que no hay nuevas vulnerabilidades. Si se detectan nuevas vulnerabilidades, se toman medidas inmediatas para corregirlas y mejorar la postura de seguridad de la organización [38].

Finalmente se puede decir que esta herramienta es fundamental para cualquier organización que busque mejorar su postura de seguridad y proteger su información de posibles amenazas. Con su capacidad de escanear redes y sistemas informáticos en busca de vulnerabilidades, Nessus permite identificar los riesgos y tomar medidas para corregirlos. Además, se utiliza para realizar pruebas de penetración, evaluaciones de proveedores y auditorías de cumplimiento. En resumen, Nessus es un instrumento imprescindible para cualquier equipo de seguridad informática que busque mejorar la seguridad de su organización [38].

1.3.22. Importancia y beneficios de la seguridad en las organizaciones

La seguridad de la información guarda una estrecha relación con la supervivencia de un negocio, sus actividades y procesos. Incluso pequeños fallos pueden ocasionar pérdidas significativas para una organización, mientras que eventos graves o catastróficos pueden llevar al cierre de la empresa con pérdidas irreparables en términos de información [39].

En vista de ello, las organizaciones están adoptando una mayor conciencia sobre la implementación de controles y el cumplimiento de regulaciones legales. El objetivo principal es proteger la información mediante la aplicación de sistemas de gestión que permitan organizar y dirigir las actividades hacia el logro de los objetivos de la organización [39].

La implementación de un sistema de gestión de seguridad tiene como propósito evitar tener que reaccionar ante situaciones que podrían haberse previsto o gestionado con anterioridad. De esta manera, se busca evitar que los problemas se conviertan en costosos desafíos, ya que prevenir los problemas resulta ser una forma económica de ahorrar [39].

1.3.23. Normas ISO

ISO (International Organization for Standardization) es una red global que identifica las normas internacionales necesarias para el comercio, los gobiernos y la sociedad en general. Estas normas son desarrolladas en colaboración con los sectores que las utilizarán y son adoptadas a través de procesos transparentes que se basan en aportes nacionales provenientes de múltiples partes interesadas. Las normas ISO se ofrecen para su utilización a nivel mundial y se fundamentan en un consenso internacional logrado a partir de la amplia participación de grupos de partes interesadas. La contribución de expertos en la elaboración de las normas proviene de aquellos que están más familiarizados con las necesidades relacionadas con las normas y de los resultados obtenidos a través de su implementación [40].

1.3.24. Norma ISO/IEC 27001

La norma internacional ISO/IEC 27001 fue aprobada en octubre de 2005 por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC), que son los organismos especializados en normalización a nivel mundial. Este estándar se basa en los requisitos para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI) utilizando el enfoque del "Ciclo de Deming" (Planificar, Hacer, Verificar, Actuar), que se utiliza con la finalidad de alcanzar la mejora continua [41].

El concepto central de un SGSI es el diseño, implementación y mantenimiento de un conjunto de procesos para gestionar de manera eficiente la accesibilidad de la información, asegurando la confidencialidad, integridad y disponibilidad de los activos de información, al mismo tiempo que se minimizan los riesgos de seguridad. Al igual que cualquier proceso de gestión, un SGSI debe mantener su eficiencia a lo largo del tiempo, ajustándose a las modificaciones internas y externas de la organización y su contexto. La norma establece que la organización debe evaluar el desempeño y la eficacia del SGSI (cláusula 9.1 de la norma ISO/IEC 27001). Esta evaluación es un componente fundamental del sistema de gestión, ya que sin ella no es posible validar si la organización ha logrado o está logrando sus objetivos, y si los procesos y controles implementados son efectivos [41].

1.3.24.1. Requisitos

La norma ISO/IEC 27001 es la más relevante y fundamental dentro de la familia ISO/IEC 27000, ya que establece los requisitos para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en las organizaciones. Su origen se remonta a la norma británica BS 7799-2:2002. En el **Anexo A de la norma ISO/IEC 27001** se encuentran los objetivos de control y los controles que se basan en la gestión de riesgos y promueven la mejora continua de los procesos. Esta norma se publicó como estándar internacional en octubre de 2005 y se revisó en septiembre de 2017. En la Figura 7. se muestra la estructura de la norma ISO/IEC 27001 [41].

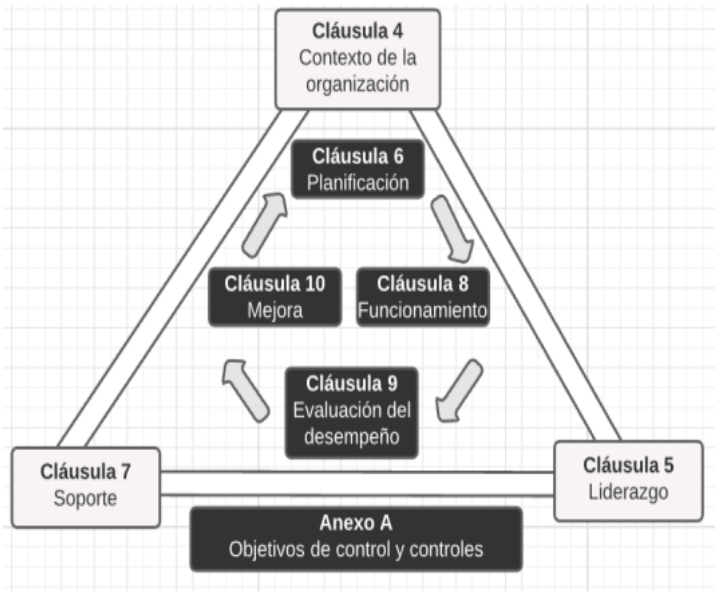


Figura 7. Estructura de la norma ISO 27001 *[41]*.

1.3.24.2. Amenazas y Vulnerabilidades en ISO 27001

Las amenazas y vulnerabilidades son abordadas en el capítulo 8 de la norma ISO 27001. La correcta identificación de estas es un aspecto crucial en un sistema de seguridad de la información durante el proceso de evaluación de riesgos. En ISO 27001, las amenazas y vulnerabilidades van de la mano y, por lo tanto, se tratan en el mismo capítulo y deben ser consideradas en conjunto. Sin embargo, puede existir una confusión entre ambos conceptos, especialmente para aquellos que son nuevos en el tema [42].

Es de suma importancia diferenciar claramente estos dos atributos de un riesgo, ya que la existencia del riesgo depende de la coexistencia de una amenaza y una vulnerabilidad. En primer lugar, las vulnerabilidades se refieren a fallos o debilidades presentes en un activo, por otro lado, las amenazas son situaciones que pueden desencadenar o aprovechar una vulnerabilidad para comprometer algún aspecto del activo [42].

Tabla 2. Amenazas y Vulnerabilidades en ISO 27001

Amenazas	Vulnerabilidades
● Acceso a la red o al sistema de información por personas no autorizadas. ● Amenaza o ataque con bomba. ● Incumplimiento de relaciones contractuales. ● Infracción legal ● Comprometer información confidencial. ● Ocultar la identidad de un usuario. ● Daño causado por un tercero. ● Daños resultantes de las pruebas de penetración. ● Destrucción de registros. ● Desastre natural, incendio, inundación, rayo. ● Revelación de información. ● Divulgación de contraseñas. ● Malversación y fraude. ● Errores en mantenimiento. ● Fallo de los enlaces de comunicación. ● Falsificación de registros. ● Espionaje industrial. ● Fuga de información. ● Interrupción de procesos de negocio. ● Pérdida de electricidad. ● Pérdida de servicios de apoyo. ● Mal funcionamiento del equipo. ● Código malicioso. ● Uso indebido de los sistemas de información. ● Errores de software. ● Instalación no autorizada de software.	● Interfaz de usuario complicada. ● Contraseñas predeterminadas no modificadas. ● Eliminación de medios de almacenamiento sin eliminar datos. ● Inadecuada seguridad del cableado. ● Inadecuada gestión de capacidad del sistema. ● Clasificación inadecuada de la información. ● Control inadecuado del acceso físico. ● Mantenimiento inadecuado. ● Inadecuada gestión de red. ● Respaldo inapropiado o irregular. ● Especificación incompleta para el desarrollo de software. ● Falta de política de acceso o política de acceso remoto. ● Falta de control sobre los datos de entrada y salida. ● Carencia o mala implementación de la auditoría interna. ● Falta de políticas para el uso de la criptografía. ● Desprotección en equipos móviles. ● Falta de redundancia, copia única. ● Ausencia de sistemas de identificación y autenticación. ● No validación de los datos procesados. ● Ubicación vulnerable a inundaciones. ● Mala selección de datos de prueba. ● Descarga no controlada de Internet. ● Uso incontrolado de sistemas de información. ● Software no documentado. ● Conexiones a red pública desprotegidas.

Elaborado por: El investigador basado en [42]

Las amenazas representan situaciones que dan lugar a incidentes en una empresa, causando daños materiales o pérdidas inmateriales en sus activos de información. El Sistema de Gestión de Seguridad de la Información basado en ISO 27001 ayuda a controlar las amenazas que pueden desencadenar estos incidentes. Como consecuencia de las amenazas, se produce un incidente que altera el estado de seguridad de los activos afectados, pasando de un estado anterior al evento a otro posterior. La forma en que se manejen las amenazas o las agresiones materializadas determinará si las amenazas son potenciales o materializadas. La medida de la distancia entre una amenaza potencial y su manifestación como una agresión real se basa en la frecuencia o probabilidad de que ocurra dicha manifestación. Cuando se produce una agresión materializada, se determina si las amenazas son potenciales o ya se han manifestado [42].

1.3.25. Ley orgánica de protección de datos personales del Ecuador

1.3.25.1. Protección de Datos Personales del Ecuador

El propósito de esta legislación es asegurar el derecho de todos los ciudadanos ecuatorianos a la protección de sus datos personales, así como a acceder a dicha información y tener control sobre ella. Con este fin, la ley establece y desarrolla principios, derechos, obligaciones y mecanismos de protección. El 26 de mayo de 2021 se promulgó la Nueva Ley Orgánica de Protección de Datos Personales de Ecuador. Esta medida permite que las empresas se adapten a los requisitos establecidos por la normativa. El objetivo principal de esta ley es mejorar la seguridad de la información en lo que respecta a los datos personales de las organizaciones. Busca proteger las bases de datos que las empresas manejan en relación con sus clientes, asegurando la confidencialidad de los datos personales y evitando su uso para otros fines. La ley es aplicable a todas las empresas, tanto públicas como privadas, que accedan al tratamiento de datos en Ecuador, ya sea a través de la oferta de bienes o servicios, o mediante contratos o regulaciones internacionales vigentes [43].

1.3.25.2. Principios de la Ley Orgánica de Protección de Datos Personales del Ecuador

La Ley cuenta con 13 Principios, que constituyen los fundamentos de las medidas implementadas para prevenir el manejo indebido de datos personales en los ámbitos [44]:

1. Juridicidad
2. Lealtad
3. Transparencia
4. Finalidad (explícitas, legítimas y comunicadas la titular)
5. Pertenencia y minimización
6. Proporcionalidad
7. Confidencialidad
8. Calidad y exactitud
9. Conservación (durante un tiempo no mayor al necesario)
10. Seguridad
11. Responsabilidad proactiva y demostrada
12. Aplicación favorable al titular (Interpretación de la norma)
13. Independencia del control (Autonomía e independencia del ente regulador)

1.3.25.3. Nuevos derechos presentes en la nueva ley

Esta ley presenta también nuevos derechos entre los cuales se tiene los siguientes [44]:

- Derecho a la información.
- Derecho de acceso.
- Derecho de rectificación y actuación.
- Derecho de eliminación.
- Derecho de oposición.
- Derecho a la portabilidad.
- Derecho a la suspensión del tratamiento.
- Derecho a la suspensión del tratamiento (limitación de uso).
- Derecho a no ser sujeto de una determinación basada exclusiva o parcialmente en evaluaciones automatizadas.
- Derecho de consulta en el registro nacional de protección de datos personales.
- Derecho a la educación digital.

1.3.25.4. Medidas de seguridad a implementar

La ley establece que las organizaciones deben adoptar medidas de seguridad para garantizar un nivel apropiado de protección de los datos personales, teniendo en cuenta aspectos como el anonimato, la integridad, la confidencialidad, la resiliencia técnica, física, administrativa y legal. Además, se requiere la implementación de un proceso de verificación, evaluación y valoración continua y constante de la eficacia a más de efectividad de las medidas técnicas [10].

En caso de producirse una violación de datos, la entidad encargada del tratamiento de datos personales debe informar al titular si ello implica un riesgo para sus derechos fundamentales y libertades individuales, en un plazo de 3 días a partir de la fecha en que tuvo conocimiento del riesgo. Además, debe notificar a la autoridad de protección de datos personales y a la agencia de regulación y control de telecomunicaciones en un plazo de 5 días después de confirmar la violación [10].

1.3.25.5. Sanciones y multas con la nueva ley de protección de datos personales del Ecuador

La Ley de protección de datos personales contempla medidas punitivas y sanciones para los servidores públicos, responsables y encargados del tratamiento de datos en caso de incumplimiento de la normativa. Estas sanciones van desde 1 hasta 20 salarios unificados en el caso de faltas graves por parte de servidores públicos, y para los responsables o encargados, las multas varían entre el 0.7% y el 1% del volumen de negocios en caso de faltas graves [22].

1.4. Objetivos

1.4.1. Objetivo general

Evaluar riesgos para un Sistema de Gestión de Seguridad de la Información en base a la norma ISO/IEC 27001 aplicado al Proveedor de Servicios de Internet “CONCRELTEC”.

1.4.2. Objetivos específicos

- Analizar el estado del sistema de comunicación y resguardo de información en la empresa proveedora de servicios de internet.

- Identificar riesgos, vulnerabilidades y amenazas existentes en la empresa proveedora de servicios de internet por medio de la norma ISO/IEC 27001.
- Seleccionar controles de seguridad informática para el manejo de riesgos de la empresa proveedora de servicios de internet.
- Generar un manual de políticas de seguridad para el manejo de la información de clientes de la empresa proveedora de servicios de internet "CONCRELTEC" con la finalidad de garantizar la integridad, confidencialidad y disponibilidad de la información en base a las vulnerabilidades detectadas.

CAPÍTULO II

METODOLOGÍA

2.1 Materiales

Para llevar a cabo la evaluación de riesgos para un Sistema de Gestión de Seguridad de la Información (SGSI) en base a la norma ISO/IEC 27001 aplicado a un Proveedor de Servicios de Internet (ISP), se realiza una identificación sistemática de los activos de información, las amenazas y vulnerabilidades que pueden afectarlos y el impacto que tendría en la organización y en sus clientes. Se utilizan metodologías y técnicas adecuadas para valorar el riesgo, y definir medidas de seguridad y controles apropiados para mitigar los riesgos identificados. La norma ISO/IEC 27001 establece un marco de trabajo para la implementación de un SGSI, que permite a las organizaciones gestionar y proteger su información de forma efectiva, mediante la identificación, evaluación y tratamiento de los riesgos que puedan afectarla. En el caso de un ISP, la evaluación de riesgos es crucial para garantizar la continuidad de los servicios y la confidencialidad, integridad y disponibilidad de la información de sus clientes.

2.2 Métodos

2.2.1 Modalidad de la Investigación

A continuación, se describen los diferentes tipos de investigación que se aplicarán para la ejecución de este proyecto.

2.2.1.1 Investigación Aplicada

El presente proyecto utilizo una investigación aplicada, porque se empleó los conocimientos ya adquiridos durante la carrera estudiantil para solucionar los problemas existentes de acuerdo con el manejo de información y a su vez satisfacer las necesidades latentes de la demanda actual en la empresa antes mencionada.

2.2.1.2 Investigación Bibliográfica

La investigación fue bibliográfica, porque el proyecto de investigación se sustentó mediante la recopilación de información de revistas técnicas, libros, artículos científicos, publicaciones en internet de fuentes confiables y tesis, relacionadas al

sistema de gestión de seguridad de la información, la norma ISO/IEC 27001 y la ley orgánica de protección de datos personales.

2.2.1.3 Investigación Experimental

El proyecto también empleó una modalidad de Investigación Experimental ya que se realizaron pruebas en los servidores para medir y garantizar la fiabilidad del resguardo de información en base a las categorías de la norma mencionada.

2.2.1.4 Investigación de Campo

El proyecto fue una investigación de campo, debido a que se recopiló información y se implementó el sistema en donde se origina el problema. Factores como la exigencia gubernamental y sobre todo el mismo cliente de la empresa al momento de resguardar su información personal sirvieron de base para plantear una solución factible que contribuyo el análisis y tratamiento de riesgos.

2.2.2 Recolección de Información

Para lograr la recolección de información se emplearon libros, revistas, fuentes online y proyectos desarrollados, así como guías prácticas y manuales de construcción, por lo que, se tomaron en cuenta bases de datos confiables que permitieron el desarrollo del proyecto.

2.2.3 Procesamiento y Análisis de Datos

Una vez recopilada la información, se llevó a cabo una selección de los datos más importantes, descartando aquellos que resultaron irrelevantes o redundantes para el proyecto. A partir de ahí, se procedió a realizar las siguientes actividades pertinentes al proyecto.

Para el procesamiento y análisis de datos se realizarán los siguientes pasos:

- Revisión de la información recopilada.
- Estudio de las propuestas de solución planteadas para mitigar riesgos existentes
- Planteamiento de la propuesta de solución.
- Interpretación de la información relevante que contribuya al desarrollo del proyecto de investigación que lleve a la solución de la propuesta.
- Validación del plan y tratamiento de los riesgos existentes

2.2.4 Propuesta de Solución

El plan de evaluación y tratamiento de riesgos considerando los conceptos base de un SGSI y la norma ISO/IEC 27001, aplicado a la empresa "CONCRELTEC", podrá garantizar que la información existente en la empresa se encuentre a buen recaudo pues se analizará y evaluará los riesgos, vulnerabilidades y amenazas existentes para de esta manera mitigar las inseguridades en cuanto a estructura y manejo de información, llevando a cabo un compromiso con la seguridad de los datos ya que incipientemente se identifican los activos y se recopila la información de seguridad para luego determinar y evaluar el peligro, se establecen además los requisitos de seguridad informática para dar paso a la selección de controles desarrollando un manual de seguridad que avale la integridad y confidencialidad de las políticas adoptadas mediante la remediación de las vulnerabilidades detectadas con el fin de alertar y prevenir futuros ataques por lo que la empresa estará prevenida y tomara las medidas necesarias evitando el robo y malversación de su información

2.2.5 Desarrollo del Proyecto

El proceso para la evaluación y tratamiento de riesgos para un Sistema de Gestión de Seguridad de la Información en base a la norma ISO/IEC 27001, aplicado a un proveedor de servicios de internet tendrá las siguientes actividades:

1. Revisión del estado actual del sistema de comunicación y resguardo de datos en la empresa "CONCRELTEC".
2. Levantamiento de información inicial
3. Análisis de información recopilada en la empresa
4. Establecimiento de criterios básicos para la gestión del riesgo
5. Determinación del alcance y límites de la Gestión de Riesgo
6. Identificación Activos de Información, riesgos, amenazas y vulnerabilidades mediante software Open Source.
7. Aplicación de parámetros de la Norma ISO/IEC 27001 en el análisis de datos.
8. Identificación de los controles existentes
9. Determinación y evaluación del nivel de estimación del riesgo.
10. Selección de controles.
11. Aceptación y comunicación del riesgo
12. Monitoreo y revisión de los riesgos

13. Implementación un manual de políticas de seguridad para el manejo de la información garantizando la integridad, confidencialidad y disponibilidad de la información en base a las vulnerabilidades detectadas
14. Elaboración del informe final.

CAPÍTULO III

RESULTADOS Y DISCUSIONES

3.3. Análisis y discusión de los resultados

La correcta puesta en marcha de un escaneo de vulnerabilidades en un proveedor de servicios de internet en base a la norma ISO/IEC 27001 fue una fase clave para poder establecer un sistema de gestión de seguridad de la información eficiente ya que este se enfoca en el resguardo de información crítica para la empresa "CONCRELTEC" y por ende de todos sus clientes, es decir más de mil usuarios, poniéndolo a buen recaudo de los piratas informáticos, basado en una evaluación de riegos eficaz y orientado a acciones para mitigar cualquier tipo de vulnerabilidad y prevenir ataques futuros

3.4. Análisis de Factibilidad

3.4.1. Factibilidad Económica

El presente proyecto es económicamente factible, ya que el investigador cuenta con los recursos necesarios para su ejecución. Además, la empresa se beneficiará al obtener la protección necesaria contra riesgos de seguridad y garantizará la seguridad de la información de la empresa y sus usuarios. Esto se logrará a través del cumplimiento de la norma ISO/IEC 27001, lo que representa una inversión con amplios beneficios

3.4.2. Factibilidad Bibliográfica

Existen diversas fuentes de información accesibles y abundantes sobre ciberseguridad, incluyendo la norma ISO/IEC 27001. Estas fuentes incluyen libros, artículos científicos, tesis, proyectos, revistas académicas, foros y bases de datos confiables, entre otros, que proporcionan amplio acceso a información relevante en el campo de la ciberseguridad

3.5. Desarrollo de la propuesta

3.5.1. Evaluación del servicio de ISP con normativa ISO/IEC 27001

Este estudio de investigación se clasifica como cualitativo debido a que, se fundamenta en la recopilación de datos a partir de un caso de estudio específico. Por lo tanto, se lleva a cabo, una evaluación del servicio de ISP en la empresa CONCRELTEC, con el objetivo de analizar la viabilidad de implementar una metodología que garantice el

cumplimiento de los requisitos de seguridad establecidos por los entes reguladores en el país. Para alcanzar este propósito, se ha estructurado la metodología en diferentes etapas, las cuales permiten realizar la evaluación, implementación de las medidas correctivas necesarias y realizar una comparación de resultados para determinar la validez de la metodología en el contexto de este trabajo. En total, la metodología se compone de 7 etapas, que se describen detalladamente a continuación. Es de enorme importancia tener en cuenta que este proceso, se encuentra fundamentado en la normativa ISO/IEC 27001:2013 [45].

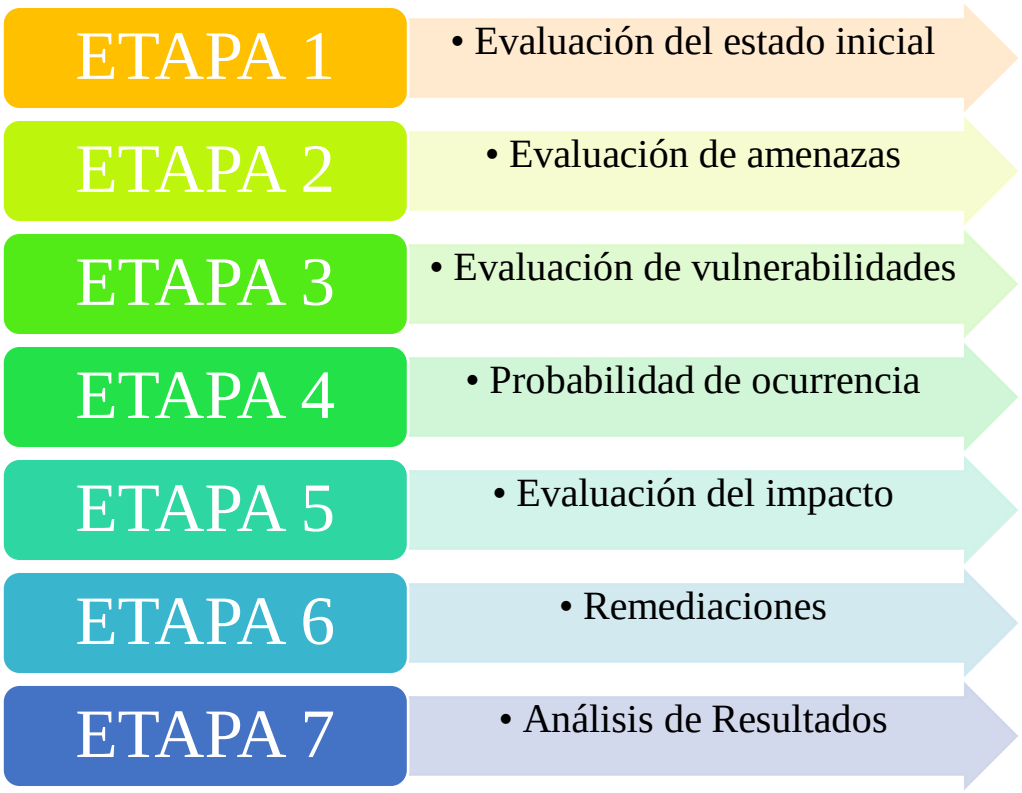


Figura 8. Metodología para la evaluación de servicio ISP

Elaborado por: el investigador basado en [45]

Para realizar la evaluación de riesgos para un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001 aplicado a un Proveedor de Servicios de Internet (ISP), se deben tener en cuenta los siguientes criterios básicos:

Tabla 3. Criterios básicos para una evaluación de riesgos

1.	Identificación de activos: Identificar y clasificar los activos de información relevantes para el ISP. Esto incluye datos sensibles de los clientes, información financiera, propiedad intelectual y otros datos críticos para la operación del ISP.
2.	Evaluación de amenazas: Identificar y evaluar las posibles amenazas que podrían afectar la seguridad de los activos de información. Esto implica analizar factores internos y externos que puedan representar una amenaza, como ataques cibernéticos, malware, intrusiones físicas, desastres naturales, entre otros.
3.	Evaluación de vulnerabilidades: Identificar y evaluar las vulnerabilidades existentes en los sistemas y redes del ISP. Esto implica analizar las brechas de seguridad y las debilidades que podrían ser explotadas por posibles ataques.
4.	Determinación de la probabilidad de ocurrencia: Evaluar la probabilidad de que una amenaza específica explote una vulnerabilidad y cause un impacto en los activos de información. Esto implica considerar factores como la exposición de los activos, la eficacia de los controles de seguridad existentes y otros factores relevantes.
5.	Evaluación del impacto: Determinar el impacto potencial que podría tener una amenaza en los activos de información del ISP. Esto incluye evaluar las consecuencias financieras, operativas y reputacionales de un posible incidente de seguridad.
6.	Valoración del riesgo: Calcular el nivel de riesgo asociado a cada amenaza identificada, considerando la probabilidad de ocurrencia y el impacto potencial. Esto permite priorizar y clasificar los riesgos para establecer medidas de mitigación.
7.	Determinación de medidas de mitigación: Identificar y establecer medidas de seguridad adecuadas para mitigar los riesgos identificados. Esto incluye implementar controles y salvaguardas de seguridad, como firewalls, sistemas de detección de intrusiones, políticas de acceso, respaldos de datos, entre otros.

Elaborado por: el investigador basado en [45]

Estos criterios básicos ayudan a realizar una evaluación de riesgos integral y efectiva, en línea con los requisitos de la norma ISO/IEC 27001, para garantizar la seguridad de la información en un Proveedor de Servicios de Internet.

Para realizar una revisión del estado actual del sistema de comunicación en la empresa "CONCRELTEC", se llevaron a cabo los siguientes pasos basados en la norma ISO/IEC27001 [45]:

1. Recopilación de información: Obtención de todos los documentos, políticas, procedimientos y registros relacionados con el sistema de comunicación y seguridad de datos en la empresa. Esto incluyo manuales de políticas de seguridad (hay que tener en cuenta que la empresa no contaba con estos), informes de incidentes, registros de auditorías, entre otros.
2. Análisis de políticas y procedimientos: se revisó detalladamente las políticas y procedimientos existentes relacionados con la comunicación y protección de datos, donde se evalúo su ajuste, aplicabilidad y eficacia en el contexto actual.
3. Evaluación de la infraestructura de comunicación: Análisis de la infraestructura de comunicación de la empresa, como redes, servidores, dispositivos de seguridad, etc., simultáneamente, se llevó a cabo la identificación de las tecnologías utilizadas y su respectiva configuración, es decir, se identificó si cumplen o no, con los estándares de seguridad y la existencia de vulnerabilidades o puntos débiles.
4. Análisis de controles de seguridad: se examinaron los controles de seguridad implementados en la empresa, como cortafuegos, sistemas de detección de intrusiones, cifrado de datos, políticas de acceso, entre otros. Se determinó si estos controles son suficientes y adecuados para proteger los datos y prevenir ataques.
5. Evaluación de la gestión de datos: Análisis de la gestión de los datos en la empresa, revisión de los procesos de almacenamiento, respaldo, recuperación y eliminación de datos, al mismo tiempo se evaluó si se siguen las mejores prácticas de seguridad de la información, si se cumplen los requisitos legales y normativas aplicables.
6. Revisión de incidentes de seguridad: Examen de los incidentes de seguridad que han ocurrido en la empresa: las causas, impacto y medidas tomadas para solucionarlos.
7. Evaluación del cumplimiento normativo: Verificación para identificar si la empresa cumple con los requisitos legales y normativos aplicables en materia

de comunicación y garantía de datos. Esto incluyó normas de privacidad, protección de datos, retención de información, entre otros.

8. Identificación de áreas de mejora: Basado en los resultados de la revisión, se llevó a cabo la identificación de las áreas de mejora y los puntos críticos que requieren atención. Priorizando las acciones que deben tomarse para fortalecer la seguridad y mejorar el sistema de comunicación y resguardo de datos.
9. Elaboración de un informe: Resumen de hallazgos y recomendaciones claras y concretas, en un informe detallado que proporciona una visión general del estado actual del sistema de comunicación y aseguramiento de datos, destacando los puntos fuertes y las áreas de mejora

Este proceso de revisión se debe realizar de manera periódica para garantizar que el sistema de comunicación esté actualizado y protegido contra las amenazas cibernéticas en constante evolución.

Es importante tener en consideración los siguientes aspectos:

a) **Activos:** Se realiza una validación del estado de los activos, configuraciones de acuerdo con las mejores prácticas, aplicación de parches de seguridad y endurecimiento de cada activo, así como su ubicación física.
b) **Vulnerabilidades:** Mediante el uso de herramientas de seguridad de software, se lleva a cabo un análisis de las vulnerabilidades para cada uno de los activos y/o servicios del proveedor de Internet. Además, con el fin de evaluar el nivel de exposición del servicio de ISP, se realiza un análisis de riesgos inicial siguiendo la norma ISO 27001 Sistema de Gestión de Riesgos de Seguridad de la Información. Como resultado de esta evaluación, se establecen recomendaciones adecuadas teniendo en cuenta los riesgos identificados, las vulnerabilidades, el nivel de exposición y los posibles fallos en las configuraciones, entre otros aspectos.
c) **Aplicación de Remediaciones:** Una vez finalizada la evaluación inicial, se procede a aplicar las medidas correctivas a las vulnerabilidades detectadas en cada etapa correspondiente. Es importante considerar que en este punto se deben aplicar los ajustes necesarios al presupuesto y las necesidades tecnológicas de la empresa, teniendo en cuenta que la metodología se enfoca en proveedores de tamaño pequeño.

d) **Valoración Final del Servicio:** Después de aplicar las remediaciones en cada etapa, se establece un período de pruebas para evaluar el correcto funcionamiento del servicio y verificar las mejoras implementadas en términos de operatividad y seguridad.

3.5.2. Identificación de Requisitos

En el Ecuador, la seguridad informática en los proveedores de servicios de Internet (ISP) presenta numerosos desafíos. Sin embargo, este trabajo se centra específicamente en la empresa CONCRELTEC y el desarrollo de una metodología para abordar estos problemas.

Con el objetivo de identificar las principales dificultades que ocurren en la empresa, se lleva a cabo una evaluación inicial de la topología de red. Esto permite identificar los activos comunes y abordarlos de manera eficiente y efectiva. Es decir, se obtiene acceso a la infraestructura de la empresa, lo que permitió evaluar la red utilizada tanto para la conexión internacional como para el acceso de los usuarios al servicio.

La identificación precisa de la topología de red implica obtener acceso al hardware, software y personal involucrado. De esta manera, se pudo comprender claramente la estructura y composición de la red utilizada para brindar los servicios de Internet. Es fundamental identificar y cuantificar adecuadamente todo el hardware para determinar si se están utilizando los equipos adecuados y evitar su sobreutilización. Además, se realiza una verificación exhaustiva del software instalado y en funcionamiento en los equipos para identificar posibles vulnerabilidades o fechas de finalización de soporte.

Asimismo, es importante considerar al personal encargado de administrar la red, ya que esto permite identificar posibles deficiencias o áreas de oportunidad que puedan aprovecharse.

Para llevar a cabo una identificación precisa de las vulnerabilidades en los equipos de red, la metodología se basa en los manuales de identificación, manejo y priorización de vulnerabilidades proporcionados por la ARCOTEL [46]. Esto no solo ayuda a mantener a los proveedores de Internet en cumplimiento con los requisitos estatales actuales, sino que también permite analizar y remediar las vulnerabilidades mediante la aplicación de parches o configuraciones. En este proceso, se utilizan herramientas

de análisis de vulnerabilidades, tanto de código abierto como comerciales con limitaciones de tiempo, para evitar gastos adicionales para los proveedores de Internet. Estas herramientas facilitan la identificación y evaluación de las diversas vulnerabilidades.

En resumen, la metodología desarrollada se basa en la norma ISO/IEC 27001 y está diseñada para ser aplicable a una amplia variedad de proveedores de servicios de Internet en el Ecuador.

3.5.3. Descripción de la metodología.

Con el objetivo de lograr un enfoque metodológico exitoso y aplicable en múltiples áreas de la empresa proveedora de servicios de internet CONCRELTEC, se ha elegido fundamentarlo en la norma ISO/IEC 27001, adaptándola específicamente para abordar las deficiencias de seguridad identificadas en el proveedor analizado [45].

La metodología se fundamenta en el empleo de los procedimientos de análisis de vulnerabilidades como el PTES (Penetration Testing Execution Standard) y el OSSTM (Open Source Security Test Methodology). Asimismo, se emplea la norma ISO/IEC-27001 para llevar a cabo la evaluación de los riesgos. Además, tomar en cuenta los requisitos técnicos que actualmente solicitan las entidades gubernamentales de Ecuador, como la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) [46].

3.5.3.1. Etapa 1: Evaluación del estado inicial.

En esta etapa, se toma como referencia los formularios de los entes gubernamentales del estado ecuatoriano, en este caso ARCOTEL, para posteriormente dar cumplimento a los mismos en la empresa Concreltec, en los pasos siguientes:

Paso 1: Definición del alcance

En esta etapa, es necesario establecer claramente el alcance de la organización. En el caso de los pequeños proveedores de servicios de Internet en Ecuador, el alcance se refiere a los mecanismos de seguridad que deben implementarse.

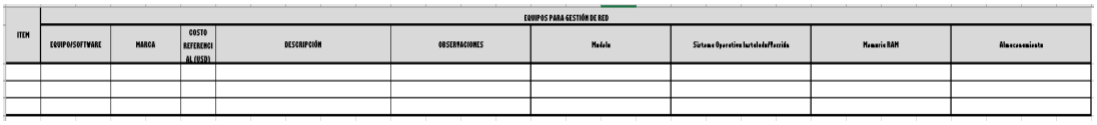
El objetivo de aplicar esta metodología en la empresa Concreltec, es garantizar que los equipos que brindan el servicio de Internet cumplan con altos estándares de seguridad, asegurando así la provisión de un servicio de calidad sin interrupciones ni retrasos que

puedan afectar a los usuarios. Además, se busca mantener todos los documentos exigidos por las autoridades ecuatorianas actualizados y en concordancia con la situación actual de la empresa.

Paso 2: Identificación de activos

Se procede a identificar los activos más importantes en la empresa proveedora de servicios de Internet. En este apartado se manifiesta una muestra de las tablas que son necesarias para llevar a cabo el presente trabajo, esto implica realizar un inventario de los equipos utilizados para la gestión de los servicios de Internet, es decir, los equipos de red empleados para ofrecer el servicio a los usuarios o abonados.

El inventario incluye información como el ítem, equipo/software, marca, costo referencial, descripción, observaciones, modelo, sistema operativo instalado/versión, memoria RAM y almacenamiento. Un formato en Excel puede utilizarse para llevar a cabo este inventario, como se muestra en la Figura 9.



ITEM	EQUIPOS PARA GESTIÓN DE RED								
	EQUIPO/SOFTWARE	MARCA	COSTO REFERENCIAL (USD)	DESCRIPCIÓN	OBSERVACIONES	Modelo	Sistema Operativo instalado/Versión	Memoria RAM	Almacenamiento

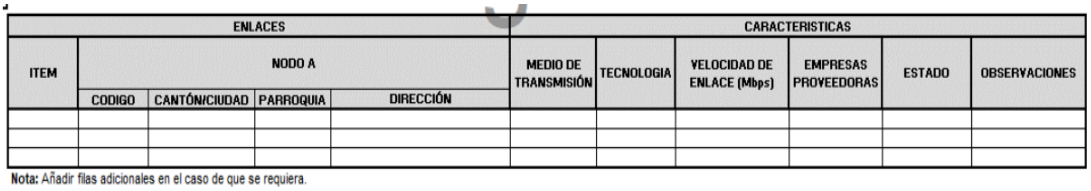
Figura 9. Formato para el registro de activos [46]

Una vez que se hayan identificado los activos de la organización, se procede a analizar la estructura de la topología de red. Para ello, se utiliza la información proporcionada por el administrador de la red. En caso de que esta información no esté disponible en formato digital, hay realiza un bosquejo de la topología que posteriormente se transfiere a un sistema de diseño de gráficos o diagramas, como Visio, Google Draw, Lucidchart u otros. Es importante considerar los siguientes aspectos al diseñar la topología de red de manera precisa:

- Identificar las salidas internacionales.
- Identificar las conexiones entre los nodos de la red.
- Identificar los routers utilizados tanto para la salida internacional como para la interconexión entre los nodos.
- Identificar las conexiones entre los equipos de la red interna (switches).
- Identificar los servidores o equipos de gestión de la red.

Además de obtener la topología de red a través del recurso humano, se debe analizar los equipos y sus interfaces para identificar las conexiones entre las redes internas y externas. También se verifican cada una de las interfaces de red, las direcciones IP, las VLAN y las rutas de los equipos que operen en la capa 3 o enrutamiento

Además de plasmar la topología en un diagrama, esta hay que documentarla en tablas que describan los enlaces de conexión internacional, los enlaces de red de transporte, los tipos de medios físicos utilizados en la red de transporte y los enlaces físicos de la red de acceso tal cual se puede apreciar en las figuras 10, 11 y 12.



ENLACES					CARACTERISTICAS					
ITEM	NODO A				MEDIO DE TRANSMISIÓN	TECNOLOGIA	VELOCIDAD DE ENLACE (Mbps)	EMPRESAS PROVEEDORAS	ESTADO	OBSERVACIONES
	CODIGO	CANTÓN/CIUDAD	PARROQUIA	DIRECCIÓN						

Nota: Añadir filas adicionales en el caso de que se requiera.

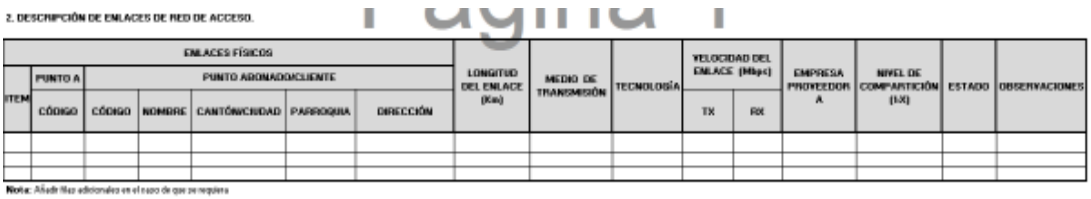
Figura 10. Descripción de enlaces de conexión internacional. [46].

2. DESCRIPCION DE ENLACES DE RED DE TRANSPORTE:

ENLACES FÍSICOS									LONGITUD DEL ENLACE (Km)	MEDIO DE TRANSMISIÓN	TECNOLOGIA	VELOCIDAD DEL ENLACE (Mbps)	EMPRESA PROVEEDORA	ESTADO	OBSERVACIONES
ITEM	PUNTO A				PUNTO B										
	CODIGO	CANTÓN/CIUDAD	PARROQUIA	DIRECCIÓN	CODIGO	CANTÓN/CIUDAD	PARROQUIA	DIRECCIÓN							

Nota: Añadir filas adicionales en el caso de que se requiera.

Figura 11. Descripción de enlaces de red-transporte [46].



2. DESCRIPCIÓN DE ENLACES DE RED DE ACCESO.

ENLACES FÍSICOS							LONGITUD DEL ENLACE (Km)	MEDIO DE TRANSMISIÓN	TECNOLOGÍA	VELOCIDAD DEL ENLACE (Mbps)		EMPRESA PROVEEDORA	NIVEL DE COMPARTICIÓN (1:X)	ESTADO	OBSERVACIONES
ITEM	PUNTO A	PUNTO ABONADO/CLIENTE								TX	RX				
	CÓDIGO	CÓDIGO	NOMBRE	CANTÓN/CIUDAD	PARROQUIA	DIRECCIÓN									

Nota: Añadir filas adicionales en el caso de que se requiera

Figura 12. Descripción de enlaces de red de acceso [46].

a. Identificación de activos en la empresa CONCRELTEC

Para validar la eficacia de la metodología propuesta, se ha contado con la colaboración de CONCRELTEC Cía. Ltda., una empresa con sede en Ambato que opera un servicio de Internet con desafíos de seguridad. La disposición de esta empresa para participar en el desarrollo y evaluación de la metodología ha sido invaluable, permitiendo así analizar y aplicar las medidas en sus equipos de telecomunicaciones y servidores encargados de proporcionar el servicio de Internet.

A la fecha de presentación de este proyecto, Concreltec Cia. Ltda. Cuenta con los siguientes equipos:

- 2 Routers
- 2 Servidores
- 1 Switch.
- 1 OLT.

Activos existentes en la empresa Concreltec.

En el proceso de identificación de activos, se contó con la colaboración del personal de Concreltec que se encarga de administrar los equipos que ofrecen el servicio de Internet a los usuarios o abonados. El Ing. Mauricio Romo, responsable de las redes de la empresa, junto con Magaly Ortega, asistente administrativo, fueron los encargados de proporcionar un bosquejo la información necesaria para este trabajo.

Una vez con el esquema de red en bosquejo, se procede con este en formato digital, como se aprecia en la figura 13.

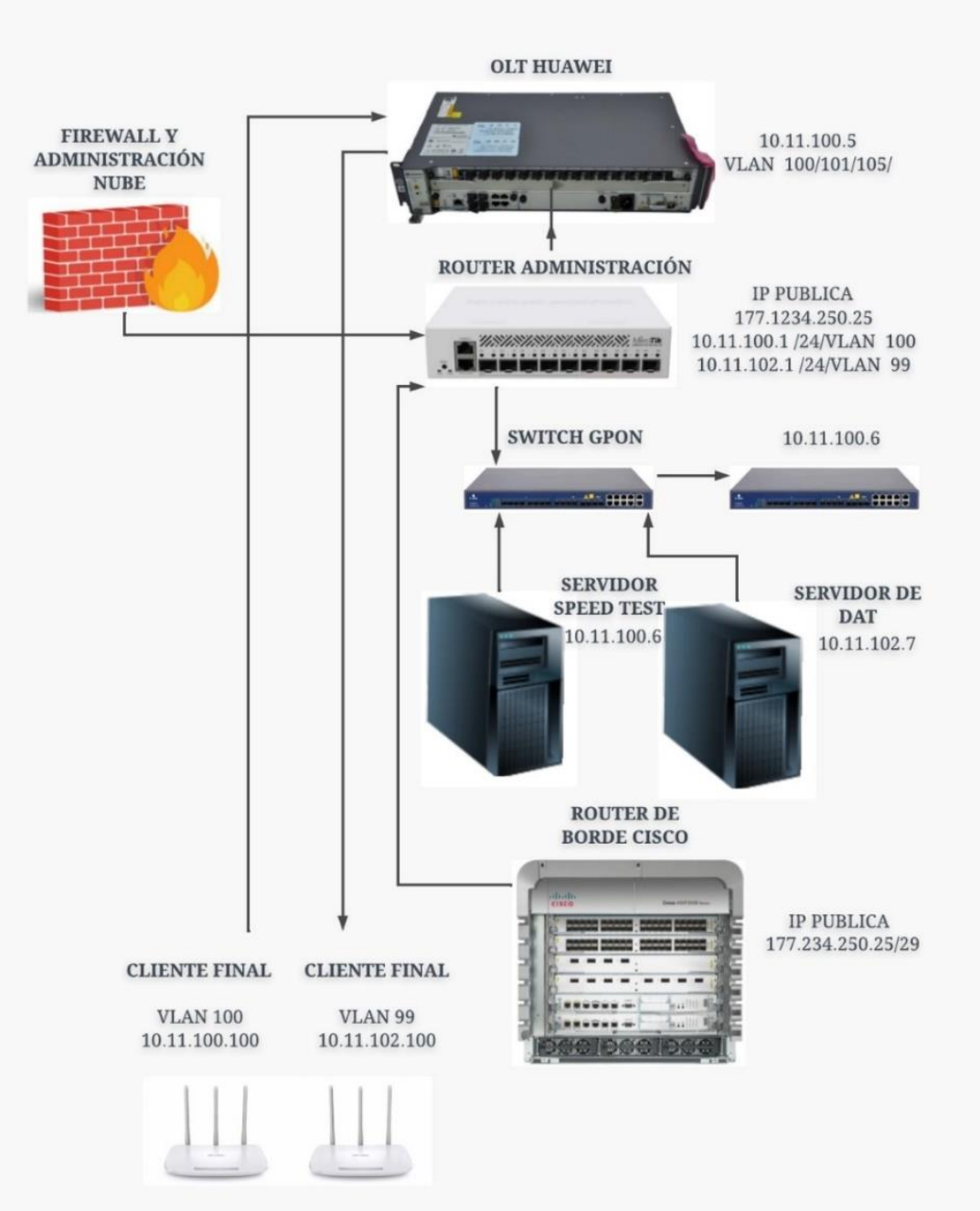


Figura 13. Diagrama de red Concreltec.

Elaborado por: El investigador.

Asimismo, se realiza un cuadro de equipos para la gestión de red, como se observa en las siguientes tablas.

- **Identificación de nodos**

Tabla 4. Tabla de nodos Concreltec

NODOS PRINCIPALES										
INFORMACION DEL NODO			UBICACIÓN GEOGRAFICA							
ITEM	CODIGO	NOMBRE DEL NODO	PROVINCIA	CIUDAD	PARROQUIA	DIRECCION	LATITUD	LONGITUD	ESTADO	OBSERVACIONES
1	00100101	Matriz	Tungurahua	Ambato	Picaihua	Av. Galo vela s/n y Platón	1 15 19.9 S	78 34 51.80 W	Registrado	

Elaborado por: El investigador.

- **Identificación de activos**

Tabla 5. Activos Principales Concreltec

EQUIPOS PARA LA GESTION DE RED									
ITEM	EQUIPO/SOFTWARE	MARCA	COSTO REFERENCIAL (USD)	DESCRIPCION	OBSERVACIONES	MODELO	SISTEMA OPERATIVO INSTALADO/VERSION	MEMORIA RAM	ALMACENAMIENTO
1	Router salida internacional/MIKROTIK	MIKROTIK	450	Router para salida internacional	4 FastEthernet interfaces 4 Serial(sync/async) interfaces 1 ATM interface	RB 3011	RouterOS 6.1	1GB	ROM
2	Switch de interconexión/ MIKROTIK	MIKROTIK	600	Switch para interconexión de equipos	48 puertos	CRS354-48G	ISO 12.2	64MB	ROM
3	Router conexión interna con clientes-abonados/CISCO IOS	CISCO	200	Router de interconexión con clientes-abonados	38 FastEthernet interfaces	3745	IOS 12.2	512MB	ROM
4	SERVIDOR DNS-DATOS/LINUX	DELL	350	Servidor DNS		DELL T30	Linux CentOS 6.10	8 GB	Disco Duro 1TB

				primario y datos					
5	SERVIDOR PROXY	DELL	350	Servidor proxy para brindar servicio de Internet		DELL T30	Linux CentOS 6.10	4 GB	Disco Duro 1TB
6	OLT	HUAWEI	600	Dispositivo terminal para conexión de fibra		MA560 8t			

Elaborado por: El investigador.

- **Identificación de enlaces**

Tabla 6. Enlaces Concreltec

ENLACES											
NODO A							CARACTERISTICAS				
ITEM	CODIGO	CANTON/ CIUDAD	PARROQUIA	DIRECCION	PARROQUIA	DIRECCION	MEDIO DE TRANSMISION	TECNOLOGIA	VELOCIDAD DE ENLACE	EMPRESA PROVEDORA	ESTADO
1	00100101	Ambato	Picaihua	Av. Galo vela s/n y Platón	Picaihua	Av. Galo vela s/n y Platón	Fibra Óptica	Clear Channel	25 Mbps	NEDETEL	REGISTRAD0

Elaborado por: El investigado

3.5.3.2. Etapa 2: Evaluación de amenazas

Con el fin de identificar las posibles amenazas a los activos mencionados en la etapa anterior, se proporciona a continuación una tabla que detalla las amenazas más relevantes a las que puede estar expuesto un proveedor de servicios de Internet. Es importante tener en cuenta que se pueden seleccionar o agregar otras amenazas según corresponda a cada activo:

En la tabla 7, se listan las amenazas relevantes para el proveedor de Internet, permitiendo su selección o inclusión adicional según sea necesario para cada activo, todo aquello basado en la normativa que se lleva a cabo en este trabajo.

Tabla 7. Cuadro de posibles amenazas consideradas en un proveedor de Internet.

Causas	**Escenario**
- Terremoto (evento sísmico) **- Evento destructivo** **- Cortocircuito** **-Deflagración**	Inaccesibilidad total de nodos (Destrucción del Nodo)
Falla de equipos de comunicación - Routers - Switches - Radios - Fibra óptica -Fallas en software en servidores -Perdida de comunicación con los portadores	Pérdida parcial de servicios de Internet
-Interrupción del suministro eléctrico	Interrupción del servicio de Internet por sectores
- Accidente del personal técnico **- Renuncia inesperada del personal del técnico**	Ausencia parcial o permanente del personal encargado de administrar el ISP
- Infección por Virus/Malware **- Sobrecarga de capacidad de procesamiento de servidores** **-Sobrecarga de capacidad de almacenamiento de servidores**	Fallas lógicas en servidores, puede causar lentitud o ausencia del servicio
Fallas en cableado estructurado del nodo principal o secundarios - Fallas en la asignación de direcciones IP - Falla puerto del patch panel	Fallas de conectividad limitada o nula entre usuarios y los servidores, causando ausencia del servicio.

Elaborado por: El investigador basado en [45].

3.5.3.3. Etapa 3: Evaluación de vulnerabilidades

La evaluación de vulnerabilidades en el ámbito de la seguridad informática desempeña un papel crucial, ya que permite reducir costos a largo plazo, aumentar la conciencia sobre la seguridad, prevenir incidentes de ciberseguridad y cumplir con los requisitos legales establecidos por el gobierno ecuatoriano. Con el objetivo de tomar decisiones que ayuden a mitigar los riesgos presentes en los activos tecnológicos en la empresa CONCRELTEC, se lleva a cabo un análisis cualitativo. En este análisis, se utiliza una matriz en la que se asigna una calificación del 1 al 4 a cada riesgo, en función de su nivel de criticidad, como se observa en la figura 14.

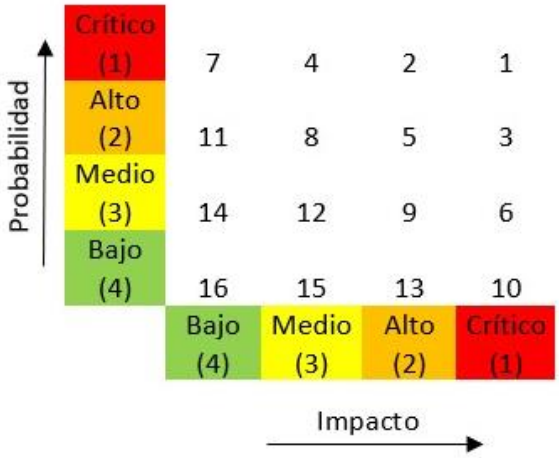


Figura 14. Cuadro para medir nivel de riesgo y prioridades

Elaborado por: El investigador basado en [45]

Con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información gestionada por un proveedor de servicios de Internet, es crucial establecer una política de seguridad fundamentada en estándares, procedimientos y controles. El objetivo principal es crear una arquitectura de seguridad que proteja los activos de información de la organización. Para llevar a cabo un análisis de vulnerabilidades efectivo, se emplean las siguientes metodologías:

- PTES (Penetration Testing Execution Standard)
- OSSTMM (Open Source Security Test Methodology)

A continuación, se detalla el procedimiento recomendado para desarrollar el análisis de vulnerabilidades de los activos que conforman el servicio.

a. Herramientas utilizadas

- Sistemas Operativos

Es crucial elegir un sistema operativo adecuado para iniciar el análisis de los activos, ya que esto juega un papel fundamental en el éxito de la prueba de penetración. Los sistemas operativos más ampliamente utilizados son: Linux y Windows. Es importante destacar que Linux es la elección preferida por la mayoría de los consultores de seguridad.

- Software

Para la elección de la herramienta adecuada de escaneo de vulnerabilidades hay que priorizar las necesidades específicas y los requerimientos de la empresa. Cada herramienta tiene sus propias características y ventajas, por lo que es importante evaluar cuidadosamente cuál se adapta de mejor manera a los objetivos planteados y recursos disponibles. A continuación, una tabla comparativa entre Nessus, Rapid7, OpenVAS y Qualys en función de ciertos criterios clave, como se observa en la siguiente tabla:

Tabla 8. Tabla comparativa entre Nessus, Rapid7, OpenVas y Qualys

Criterios	Nessus	Rapid7	OpenVAS	Qualys
Tipo de licencia	Comercial y gratuita	Comercial y gratuita	Código abierto	Comercial
Escaneo de red	Sí	Sí	Sí	Sí
Escaneo de aplicaciones	Sí	Sí	No	Sí
Gestión de vulnerabilidades	Sí	Sí	Sí	Sí
Integración de API	Sí	Sí	Sí	Sí
Reporting avanzado	Sí	Sí	No	Sí
Compatibilidad	Multiplataforma	Multiplataforma	Multiplataforma	Multiplataforma
Base de datos de vulnerabilidades	Sí	Sí	Sí	Sí
Soporte técnico	Sí	Sí	Comunidad y comercial	Sí
Escaneo en la nube	Sí	Sí	No	Sí

Elaborado por: El investigador basado en [37] y [47].

Para el presente trabajo, Nessus y Rapid7 fueron seleccionadas como las herramientas principales para el escaneo de vulnerabilidades, debido a sus reconocidas capacidades y amplia funcionalidad en la detección de vulnerabilidades en sistemas y redes. Nessus es conocido por su exhaustividad en la detección y su extensa base de datos de vulnerabilidades, lo que permite identificar amenazas de manera efectiva. Por otro lado, Rapid7 ofrece una interfaz amigable y potentes funciones de análisis, facilitando la identificación y mitigación de riesgos. Ambas herramientas proporcionan un enfoque integral para el análisis de vulnerabilidades, lo que las convierte en una opción sólida y confiable para garantizar la seguridad de la información en el proyecto de investigación. Ambas plataformas trabajan en Linux y Windows, la herramienta Rapid7 permite investigar vulnerabilidades, analizar su explotación, estudiar el comportamiento de atacantes, recopilar datos de escaneo en Internet, realizar análisis de exposición y generar informes en tiempo real con un periodo gratuito de 30 días, por otro lado Nessus tiene como objetivo identificar y documentar vulnerabilidades, centrándose especialmente en aquellas que pueden surgir dentro de una red interna teniendo un periodo Gratis para hasta 16 activos.

Considerando el alcance de la prueba de penetración y los recursos disponibles, se proporciona una lista de software comercial y de código abierto que puede ser útil en este proceso. Para el sistema operativo Linux, se sugieren distribuciones como Kali Linux o Parrot, que ofrecen herramientas específicamente diseñadas para llevar a cabo análisis de vulnerabilidades y pruebas de penetración.

b. Reconocimiento de información

Durante la etapa de Reconocimiento de Información, se recopila datos relevantes sobre los activos en evaluación que rinden muestra de ser los más críticos para la empresa, como información de los administradores del servicio, instalaciones y equipamiento. Para cumplir con los requisitos de los entes gubernamentales ecuatorianos, se realiza un reconocimiento externo de los activos con mayor índice de vulnerabilidad utilizando fuentes de información de acceso público en la web, como Cisco Talos Intelligence, Shodan y Whois, entre otros, en la tabla 9 se realiza una comparación de estas.

Tabla 9.Comparacion Entre Cisco Talos Intelligence, Shodan y Whois

Software	Cisco Talos Intelligence	Shodan	Whois
Descripción	Servicio de inteligencia de amenazas	Motor de búsqueda IoT	Base de datos de dominios
Funcionalidad	Identificación y análisis de amenazas	Escaneo de dispositivos	Información de registro de dominios
Enfoque	Amenazas de seguridad informática	Dispositivos conectados	Registro de nombres de dominio
Información	Inteligencia sobre amenazas	Información sobre dispositivos conectados	Información sobre propietarios de dominios
Aplicaciones	Seguridad de redes y sistemas	Monitoreo de dispositivos IoT	Búsqueda y registro de dominios
Acceso	Suscripción y acceso a la plataforma	Pública y gratuita	Pública y gratuita
Fuente de datos	Propia base de datos y fuentes externas	Escaneo de Internet	Registros de dominios y registradores
Ventajas	Amplia cobertura de amenazas	Identificación de dispositivos vulnerables	Información detallada de propietarios de dominios
Limitaciones	Acceso restringido y de pago	Enfoque limitado a dispositivos IoT	Limitado a información de dominios y registradores

Elaborado por: El investigador basado en [48].

Para la elaboración de este trabajo, se seleccionaron específicamente Shodan.io y Cisco Talos Intelligence como herramientas clave, debido a su destacada capacidad para identificar vulnerabilidades y amenazas en sistemas de red, además de proporcionar una valiosa inteligencia sobre ciberseguridad. Shodan.io, con su capacidad de búsqueda y monitoreo en tiempo real de dispositivos conectados a Internet, permite un análisis profundo de las vulnerabilidades expuestas, brindando una visión clara de los riesgos a los que se enfrenta una organización. Por otro lado, Cisco Talos Intelligence, al ser un reconocido proveedor de inteligencia de seguridad, ofreció información precisa y actualizada sobre amenazas emergentes, ayudando a evaluar los riesgos asociados y adoptar estrategias efectivas de mitigación. Ambas herramientas demostraron ser fundamentales para el éxito de la investigación al proporcionar una visión integral y precisa de la seguridad de la información en el entorno digital actual.

c. Shodan.Io

A continuación, se presenta una descripción del proceso general de Shodan y algunos parámetros que se configuran al utilizarlo:

1. **Acceso a Shodan:** Para utilizar Shodan, se debe acceder al sitio web oficial de Shodan en https://www.shodan.io/ . Allí se puede crear una cuenta y obtener una clave de API para acceder a las funcionalidades avanzadas de la plataforma, como se puede observar en la figura 15.

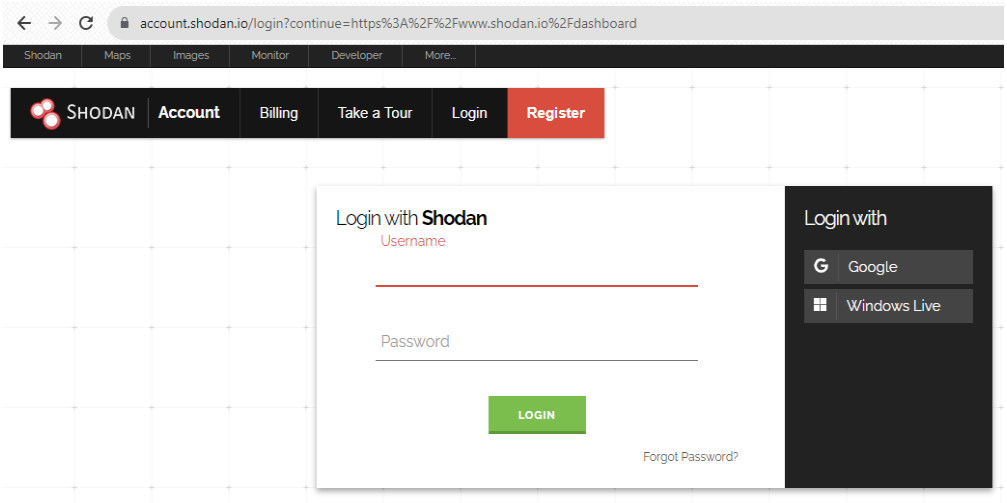


Figura 15. Creación de cuenta en Shodan.io

Elaborado por: El investigador

2. **Configuración de parámetros:** Una vez obtenida la clave de API, se la puede utilizar para realizar consultas avanzadas en Shodan. Algunos parámetros para configurar son:

    - *Query*: Especifica los términos de búsqueda para buscar dispositivos o servicios específicos. Por ejemplo, puedes buscar "Apache" para encontrar servidores web Apache.
    - *Filters*: Permite refinar la búsqueda utilizando filtros como país, puerto, protocolo, organización, etc. Se especificar los filtros que se desea para obtener resultados más específicos.
    - *Facets*: Proporciona opciones para agrupar y filtrar los resultados. Se puede utilizar los facets para mostrar resultados basados en el país, la

ciudad, el puerto, el sistema operativo, entre otros, como se visualiza en la figura 16.

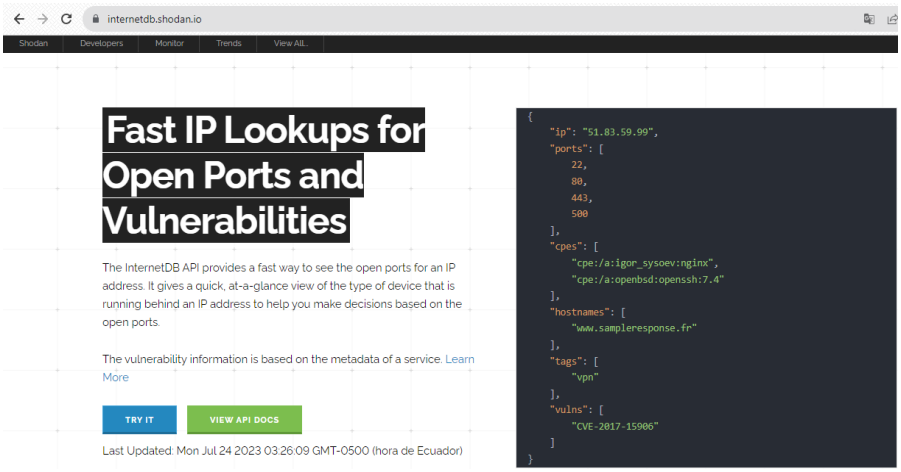


Figura 16. Configuración de parámetros en shodan.io

Elaborado por: El investigador

3. **Inicialización de la búsqueda:** Una vez que se han configurado los parámetros deseados, se debe iniciar la búsqueda haciendo clic en el botón de búsqueda, o utilizando la API de Shodan para realizar consultas programáticas, tal cual se observa en la figura 17.

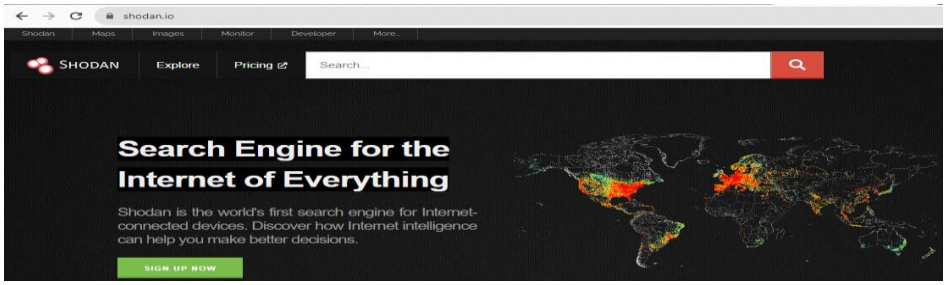


Figura 17. Inicialización de la búsqueda en shodan.io

Elaborado por: El investigador

4. **Análisis de los resultados:** Shodan proporciona una lista de dispositivos y servicios que coinciden con los parámetros de búsqueda. Se puede examinar los resultados para obtener información detallada sobre los dispositivos, como dirección IP, puertos abiertos, banners, información de la organización propietaria, entre otros, en la figura 18, se identifica el análisis de puertos realizado.

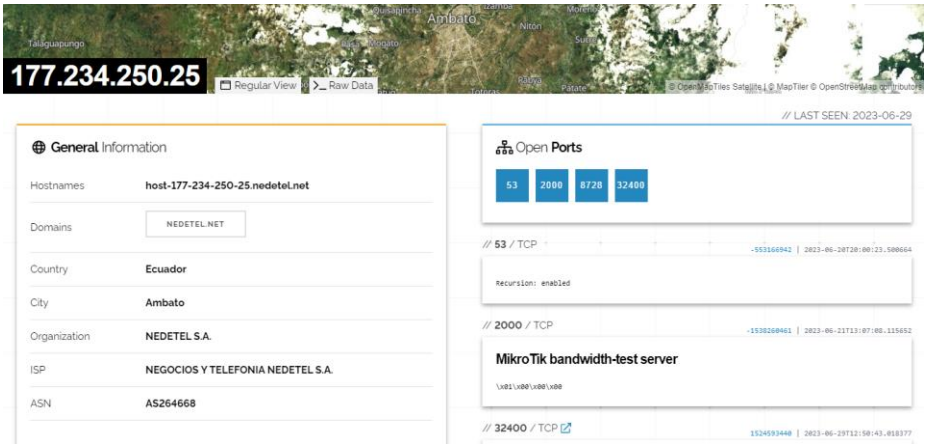


Figura 18. Revisión de puertos en Shodan.

Elaborado por: El investigador

d. Cisco Talos Intelligence

A continuación, se presenta una descripción del proceso general para realizar una validación de IPs en Cisco Talos Intelligence, incluyendo la configuración de parámetros y la inicialización:

1. **Acceso a Cisco Talos Intelligence:** Para utilizar Cisco Talos Intelligence, hay que acceder al sitio web oficial de Talos Intelligence en https://talosintelligence.com/. Se debe crear una cuenta para acceder a las funcionalidades avanzadas de la plataforma, como se aprecia en la figura 19.

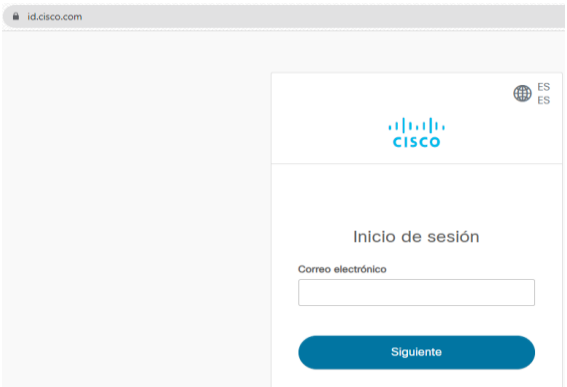


Figura 19. Creación de cuenta en Cisco Talos Intelligence

Elaborado por: El investigador

2. **Configuración de parámetros:** Una vez ingresado a Cisco Talos Intelligence, se puede configurar los parámetros para la validación de IPs. Algunos de los parámetros comunes que se pueden configurar incluyen:

- *IP Address*: Especifica la dirección IP a validar. Se puede ingresar una única dirección IP o un rango de direcciones IP.
- *Reputation Threshold*: Permite establecer un umbral de reputación para filtrar los resultados. Se puede ajustar este valor según las necesidades y criterios de evaluación.
- *Query Options*: Proporciona opciones adicionales para refinar la búsqueda, como la inclusión de información de geolocalización, detalles de WHOIS, entre otros, estos se parámetros se pueden observar en las figuras 20 y 21.

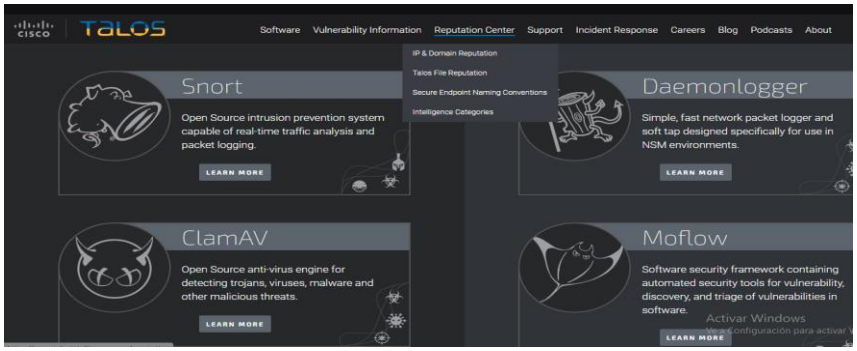


Figura 20. Interfaz de validación de Cisco Talos Intelligence

Elaborado por: El investigador

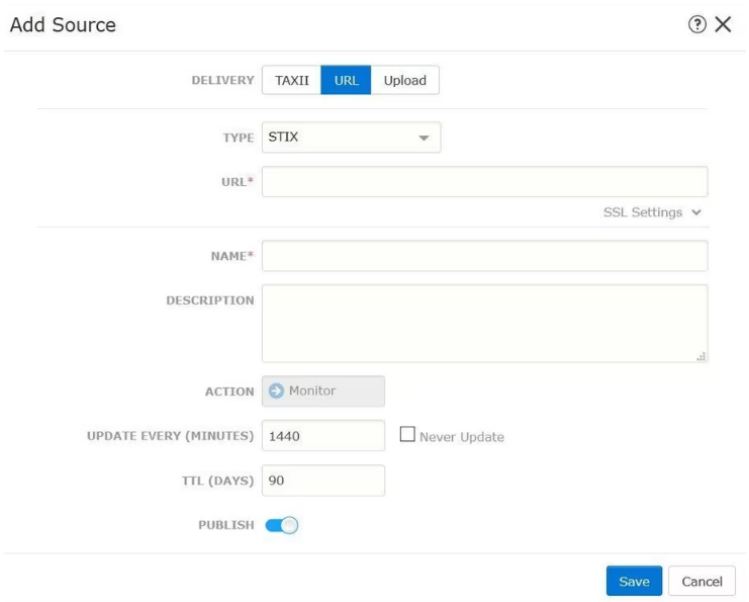


Figura 21. Configuración de parámetros en Cisco Talos Intelligence

Elaborado por: El investigador

3. **Inicialización de la validación:** Una vez configurado los parámetros deseados, se puede iniciar la validación haciendo clic en el botón de búsqueda o en la opción correspondiente. Cisco Talos Intelligence realiza una consulta utilizando los parámetros configurados, como se observa en la figura 22.

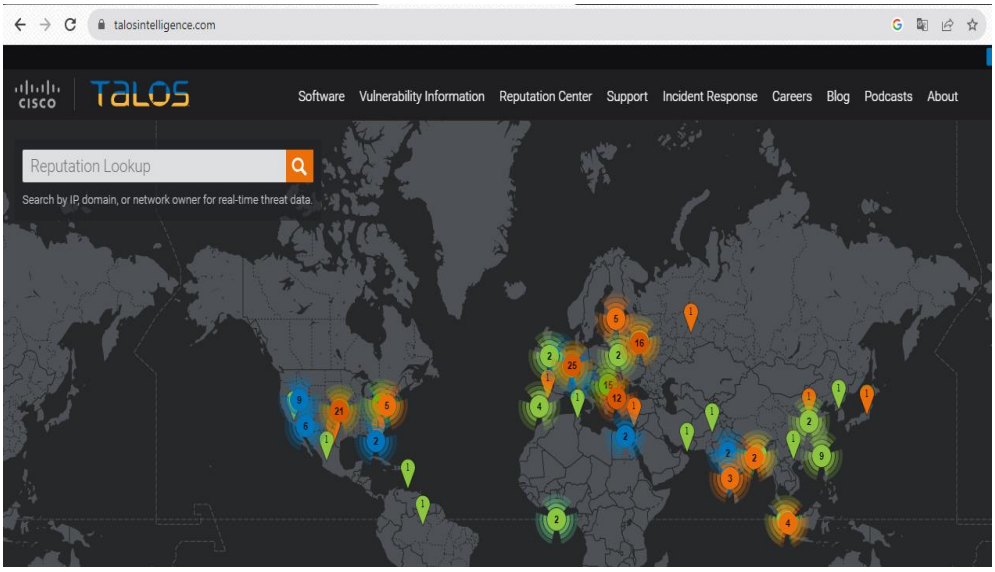


Figura 22. Configuración de la validación en Cisco Talos Intelligence

Elaborado por: El investigador

4. **Análisis de los resultados:** Cisco Talos Intelligence muestra los resultados de la validación de la IP o IPs especificadas. Se puede examinar los resultados para obtener información detallada sobre la IP, como la clasificación de reputación, información de categorías de amenazas, detalles de geolocalización, entre otros, tal cual se aprecian en la figura 23.

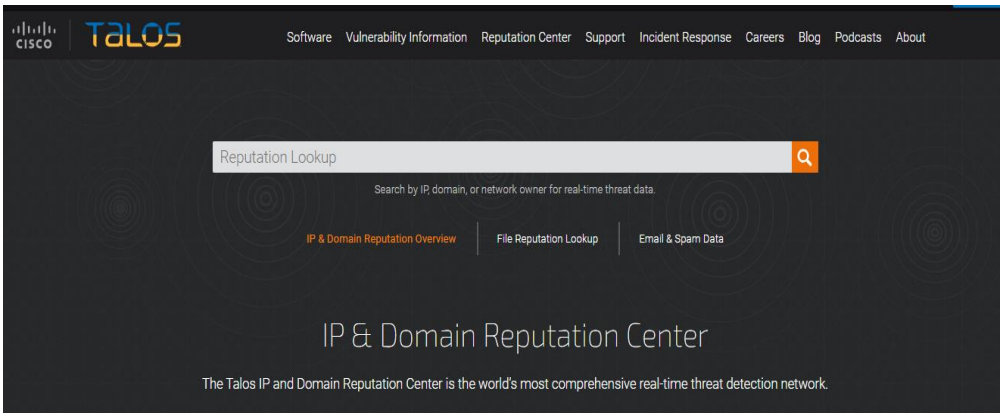


Figura 23, Ingreso de Ips en Cisco Talos Intelligence

Elaborado por: El investigador.

Es importante recalcar que Cisco Talos Intelligence, es una herramienta de inteligencia de amenazas y seguridad cibernética que proporciona información actualizada sobre la reputación de las direcciones IP [48]. En la figura 24, se observa el resultado de la validación de direcciones IP planteada.

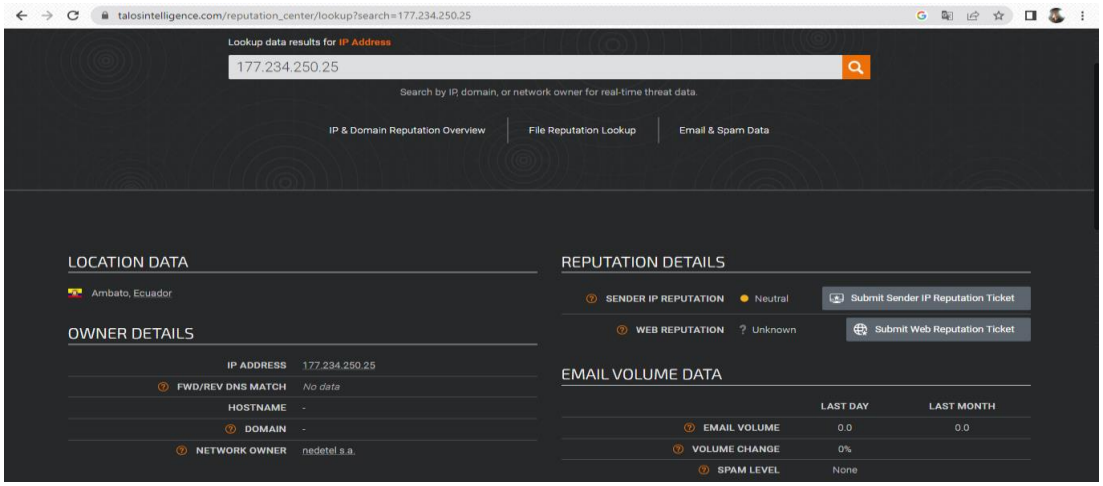


Figura 24. Validación de reputación de direcciones IP

Elaborado por: El investigador

Existen herramientas disponibles, como Rapid7 y Nessus, que permiten automatizar la identificación de vulnerabilidades. Estas herramientas pueden ser instaladas en equipos y desempeñar esta función de manera eficiente. Además, Shodan.IO puede ser utilizada como una estrategia complementaria para la identificación inicial de vulnerabilidades. En el proyecto, se emplean estas tres herramientas para cumplir con este propósito.

e. Rapid7

Cabe destacar que el desarrollo del presente trabajo no está enmarcado en la instalación y administración del software, sin embargo, se detallan algunos pasos clave necesarios para la correcta puesta en marcha del mismo.

Primero, descargar el software y llenar los datos necesarios, como se observa en la figura 25.

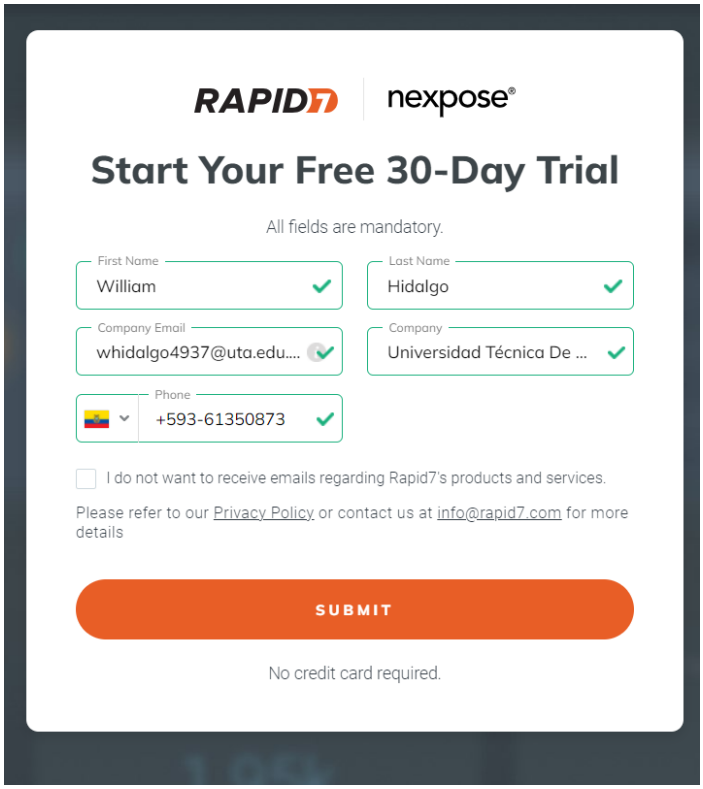


Figura 25. Ingreso de datos inicial en Rapid7

Elaborado por: El investigador

Rápidamente hay que priorizar la instalación, tal cual se muestra en la figura 26.

Figura 26. Instalación de Rapid 7

Elaborado por: El investigador

Una vez instalado, confirmar la información de la cuenta, como se detalla en la figura 27.

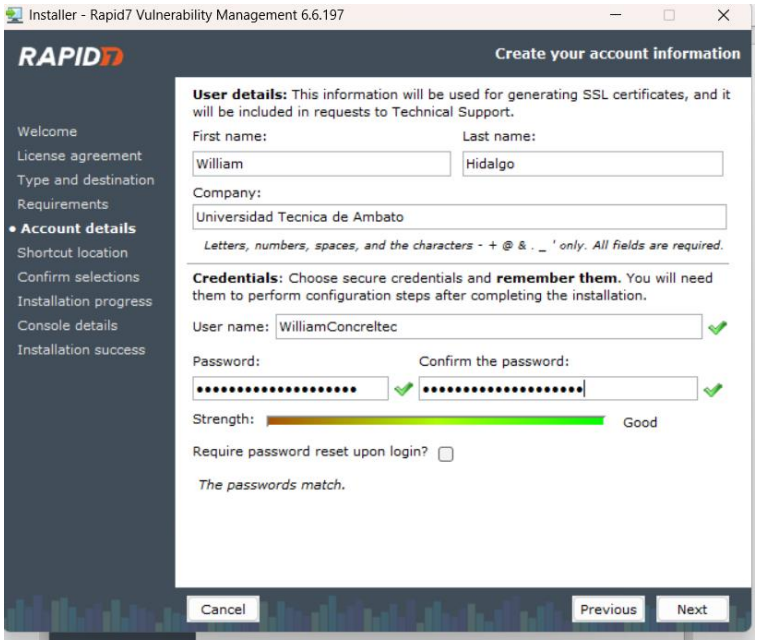


Figura 27. Confirmación de la información de la cuenta

Elaborado por: El investigador

Seguidamente, se debe activar la misma cuenta con el código de autenticación que llega al email, como se identifica en la figura 28.

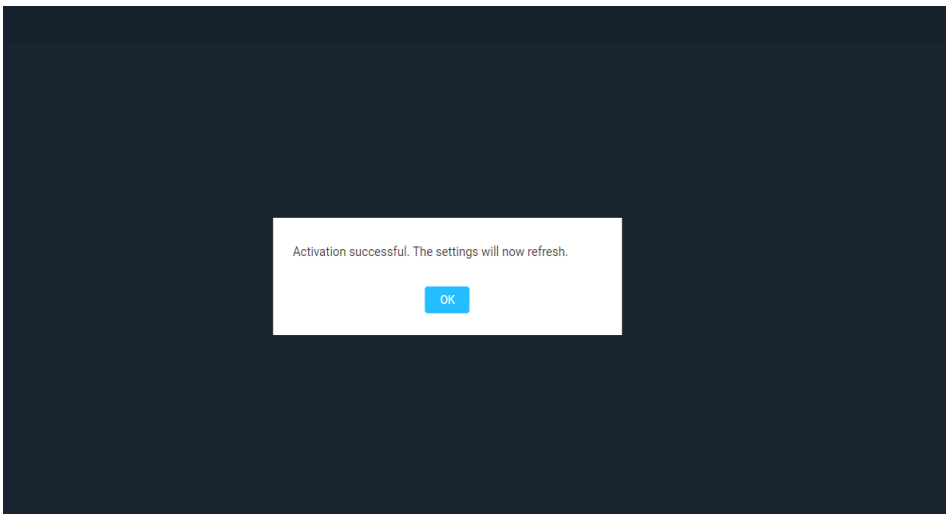


Figura 28. Activación de la cuenta en Rapid7

Elaborado por: El investigador.

Una vez que se ha familiarizado con la interfaz del programa, empezar con la puesta en marcha del análisis de vulnerabilidades, siguiendo la estructura que se observa en la figura 29.

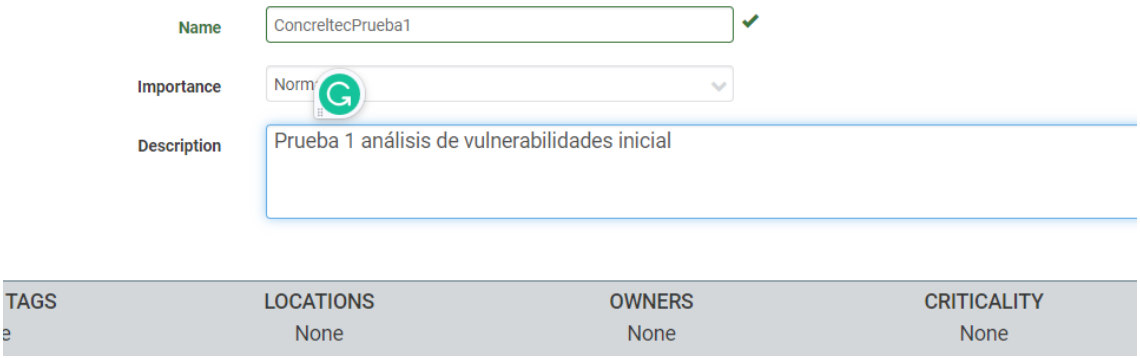


Figura 29. Inicio del análisis de vulnerabilidades.

Elaborado por: El investigador

Seguidamente, añadir al sitio los activos que serán escaneados, para posteriormente identificar y procesar vulnerabilidades existentes, como se detalla en la figura 30.

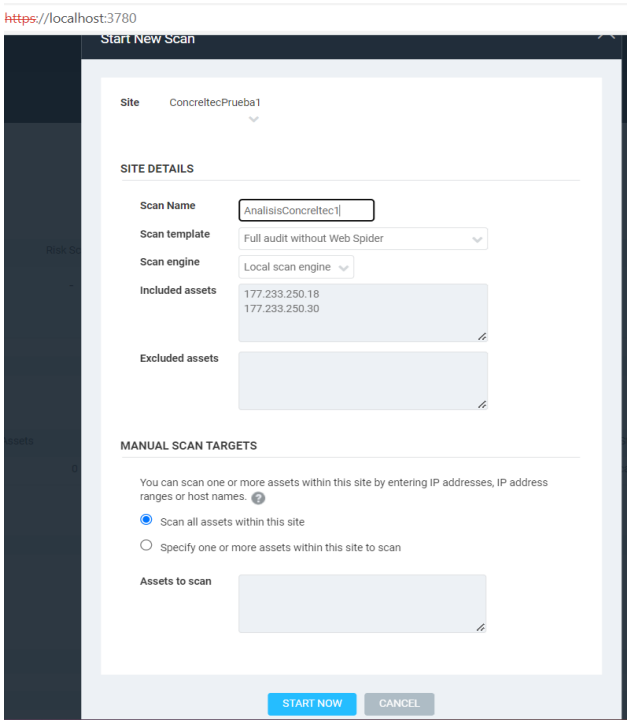


Figura 30. Ingreso de activos.

Elaborado por: El investigador

El escaneo, se puede realizar paso a paso, gracias a la propia interfaz del programa, como se visualiza en la figura 31.

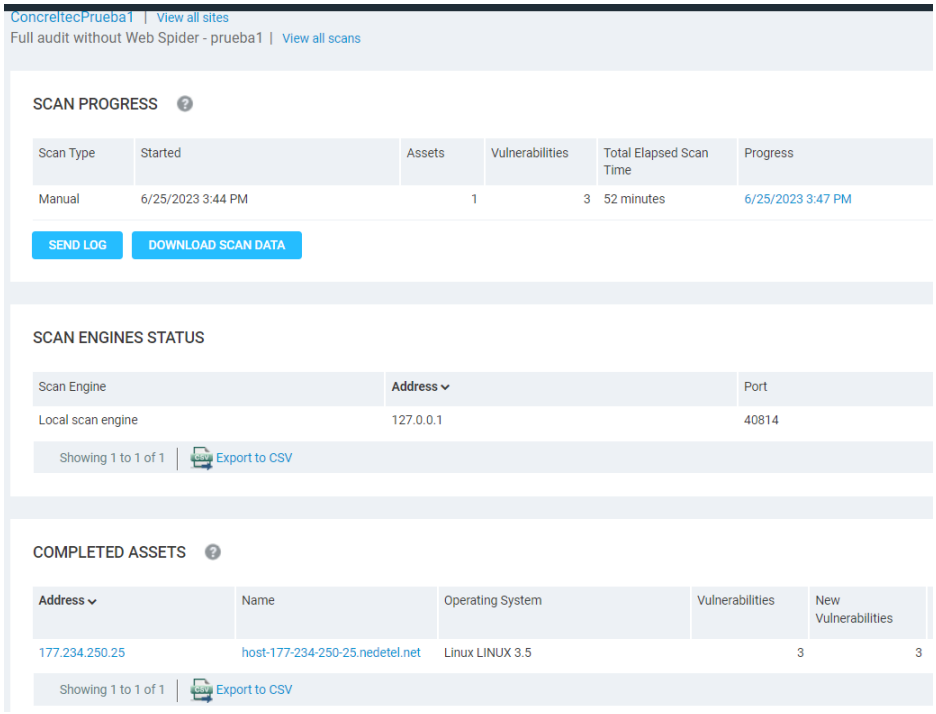


Figura 31. Escaneo paso a paso.

Elaborado por: El investigador

Al agregar los activos de la empresa de dos en dos, se agiliza el proceso, como se aprecia en la figura 32.

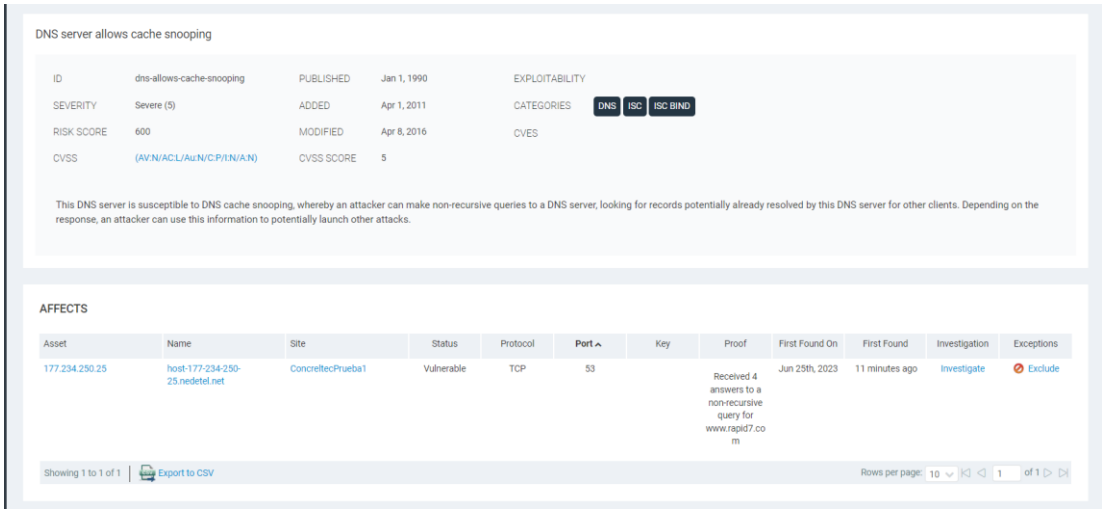


Figura 32. Ingreso de activos de par en par.

Elaborado por: El investigador

Repetir el mismo proceso con todos los activos de la empresa CONCRELTEC, como se puede ver en las figuras 33, 34 y 35.

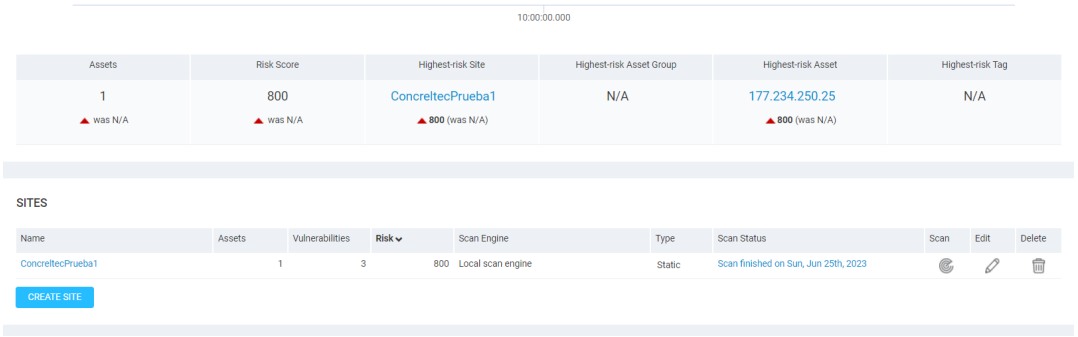


Figura 33. Activo con índice más alto de vulnerabilidad.

Elaborado por: El investigador

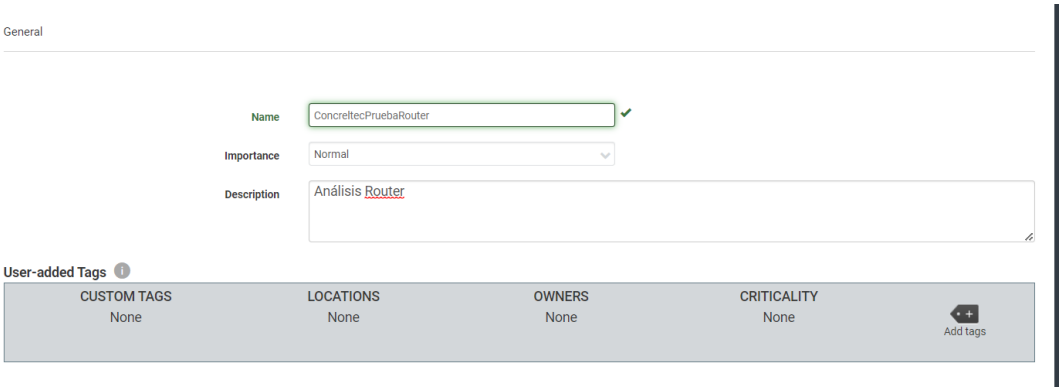


Figura 34. Prueba Router.

Elaborado por: El investigador

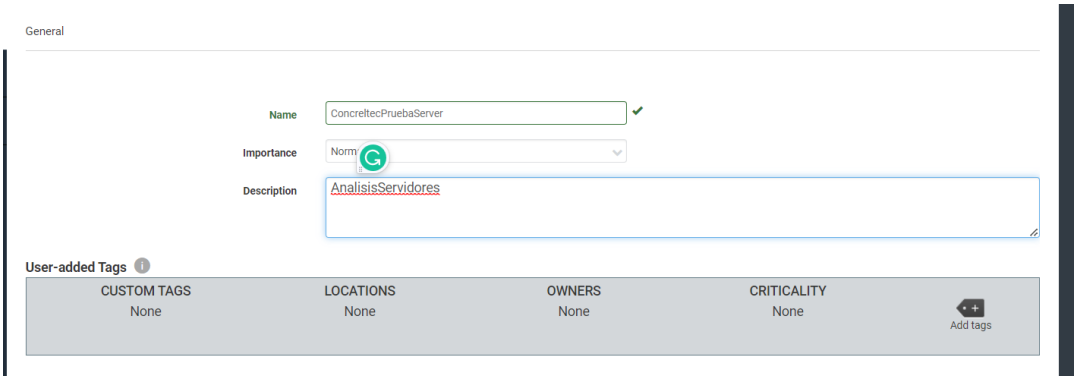


Figura 35. Análisis servidores.

Elaborado por: El investigador

f. Análisis del Router de borde.

En la figura 36, se aprecia el análisis del router de borde.

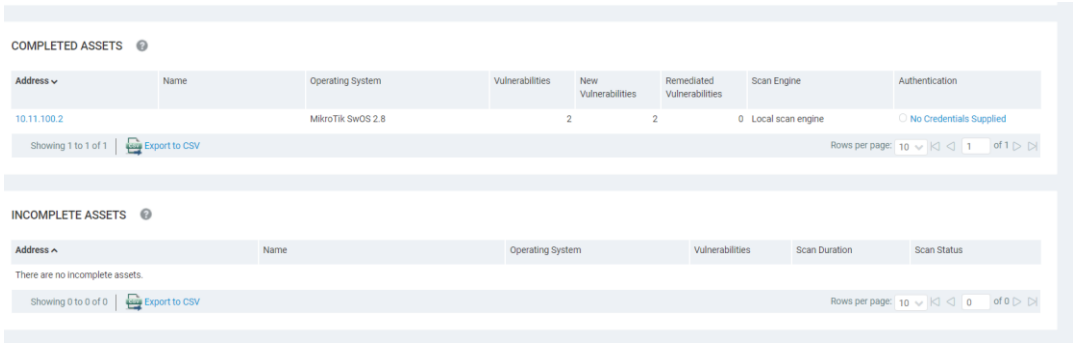


Figura 36. Análisis de router de borde.

Elaborado por: El investigador

Al seguir utilizando el programa, se visualizan todas las pruebas realizadas, así como los activos, cada uno con el número de vulnerabilidades totales, como se observa en la figura 37.

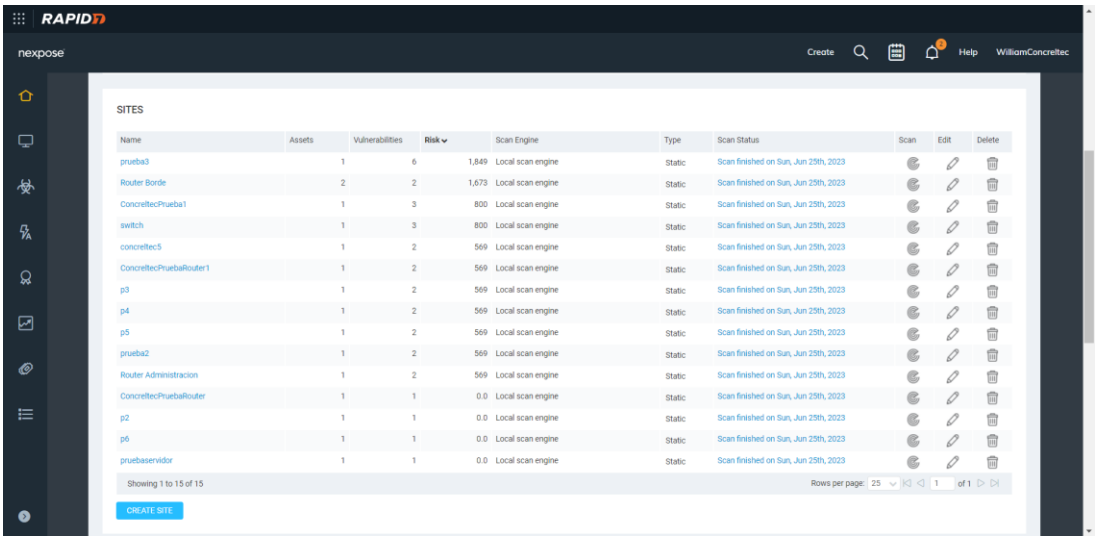


Figura 37. Lista de pruebas realizadas.

Elaborado por: El investigador

Además, se puede identificar el activo con mayor amenaza, en este caso es el servidor de datos con la dirección IP 10.11.102.7 con un valor de 9,105 tal cual se muestra en la figura 38.

Assets	Risk Score	Highest-risk Site	Highest-risk Asset Group	Highest-risk Asset	Highest-risk Tag
13 ▲ was N/A	9,105 ▲ was N/A	prueba3 ▲ 1,849 (was N/A)	N/A	10.11.102.7 ▲ 1,849 (was N/A)	N/A

SITES

Name	Assets	Vulnerabilities	Risk	Scan Engine	Type	Scan Status	Scan	Edit	Delete
prueba3	1	6	1,849	Local scan engine	Static	Scan finished on Sun, Jun 25th, 2023			
Router Borde	2	2	1,673	Local scan engine	Static	Scan finished on Sun, Jun 25th, 2023			
ConcreltecPrueba1	1	3	800	Local scan engine	Static	Scan finished on Sun, Jun 25th, 2023			
switch	1	3	800	Local scan engine	Static	Scan finished on Sun, Jun 25th, 2023			
concreltec5	1	2	569	Local scan engine	Static	Scan finished on Sun, Jun 25th, 2023			
ConcreltecPruebaRouter1	1	2	569	Local scan engine	Static	Scan finished on Sun, Jun 25th, 2023			
p3	1	2	569	Local scan engine	Static	Scan finished on Sun, Jun 25th, 2023			
p4	1	2	569	Local scan engine	Static	Scan finished on Sun, Jun 25th, 2023			
p5	1	2	569	Local scan engine	Static	Scan finished on Sun, Jun 25th, 2023			
prueba2	1	2	569	Local scan engine	Static	Scan finished on Sun, Jun 25th, 2023			
Router Administracion	1	2	569	Local scan engine	Static	Scan finished on Sun, Jun 25th, 2023			
ConcreltecPruebaRouter	1	1	0.0	Local scan engine	Static	Scan finished on Sun, Jun 25th, 2023			
p2	1	1	0.0	Local scan engine	Static	Scan finished on Sun, Jun 25th, 2023			

Figura 38. Lista de pruebas realizadas y activo más crítico.

Elaborado por: El investigador

En la figura 39, se identifica la lista de activos analizados y las pruebas aplicadas. Un punto importante a destacar es que el mismo programa permite visualizar el sistema operativo del activo analizado, el número de vulnerabilidades y sobre todo el nivel de riesgo.

Address	Name	Site	Operating System			Vulnerabilities	Risk	Assessed ▲
10.11.102.7		prueba3	Linux LINUX 3.5	0	1	6	1,849	Yes
10.11.100.2		Router Borde	MikroTik SwOS 2.8	0	0	2	1,673	Yes
10.11.100.1		switch	Linux LINUX 3.5	0	0	3	800	Yes
177.234.250.25	host-177-234-250-25.nedetel.net	ConcreltecPrueba1	Linux LINUX 3.5	0	0	3	800	Yes
10.11.100.4		ConcreltecPruebaRouter1	Synology SYNOLOGY DISKSTATION MANAGER 5 (LINUX) 5.X	0	0	2	569	Yes
10.11.100.6		Router Administracion	Linux LINUX 3.5	0	0	2	569	Yes
10.11.100.8		prueba2	Linux LINUX 3.6	0	0	2	569	Yes
10.11.102.2		p5	Linux LINUX 3.4	0	0	2	569	Yes
10.11.102.3		concreltec5	Linux LINUX 3.4	0	0	2	569	Yes
10.11.102.4		p4	Linux LINUX 3.5	0	0	2	569	Yes
10.11.102.6		p3	Linux LINUX 3.6	0	0	2	569	Yes
10.11.100.7		Global	Linux LINUX 3.6	0	0	1	0	Yes
10.11.102.1		Global		0	0	1	0	Yes

Showing 1 to 13 of 13 Export to CSV Rows per page: 25

Figura 39. Lista de activos analizados y nivel de riesgo.

Elaborado por: El investigador

Adicionalmente, con las herramientas y a través de gráficos, se puede apreciar el nivel de riesgo, en este caso el índice de vulnerabilidad CVSS, manifestando el número total de vulnerabilidades ya sean estas de nivel crítico con un valor de entre (8 y 10), nivel medio (6 a 7.9) o nivel bajo (4 a 5.9) como se observa en la figura 40.

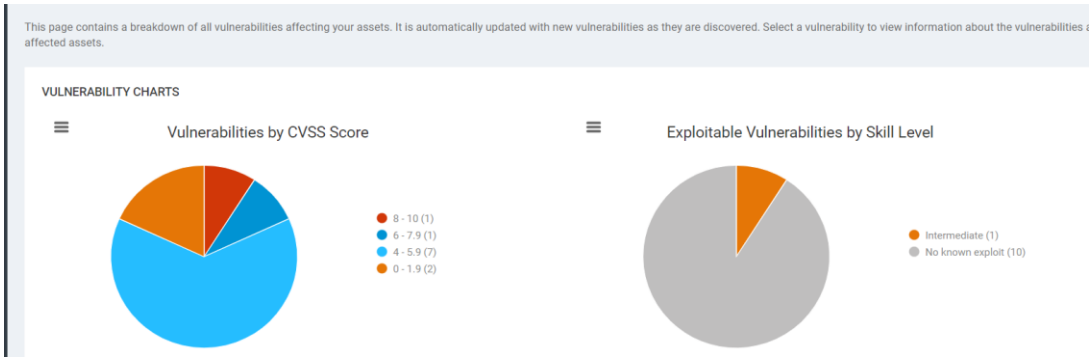


Figura 40. Nivel de riesgo mediante gráficos.

Elaborado por: El investigador

En la figura 41, se visualiza el nivel de riesgo de acuerdo con el sistema operativo, de igual forma el número de activos evaluados y las vulnerabilidades por cada uno, rindiendo muestra que Linux es el principal a sistema a ser atacado con un valor de 10, seguido de mikrotik.

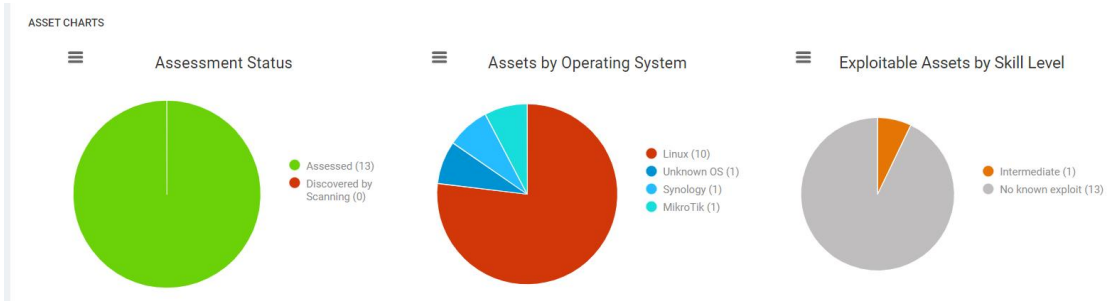


Figura 41. Nivel de riesgo de acuerdo con el sistema operativo.

Elaborado por: El investigador

Las vulnerabilidades totales detectadas se las puede observar en la figura 42.

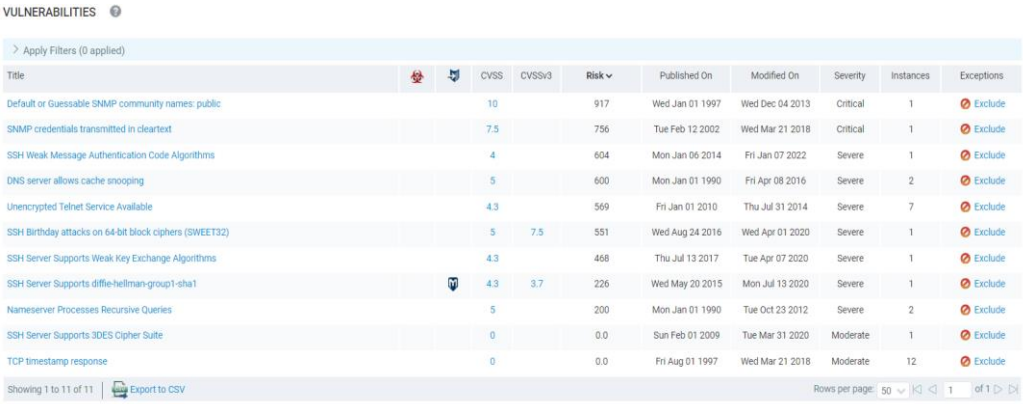


Figura 42. Vulnerabilidades totales detectadas.

Elaborado por: El investigador

Los hallazgos más importantes, es decir las vulnerabilidades criticas encontradas, de acuerdo a la figura anterior según el software fueron:

- Fallos en servicio DNS
- Conexión remota a la base de datos
- Versiones de php obsoletas.
- Fallos de software en servidores
- Sobrepasar cantidad de procesamiento del servidor
- Ataques de Denegación de Servicio por ejecución de datos inesperados. CVE-2015-4602
- Consultas recursivas al servicio de DNS

Hay que tener en cuenta que el software, pone en marcha un plan de remediación para cada tipo de vulnerabilidad detectada, como el ejemplo de la figura 43.

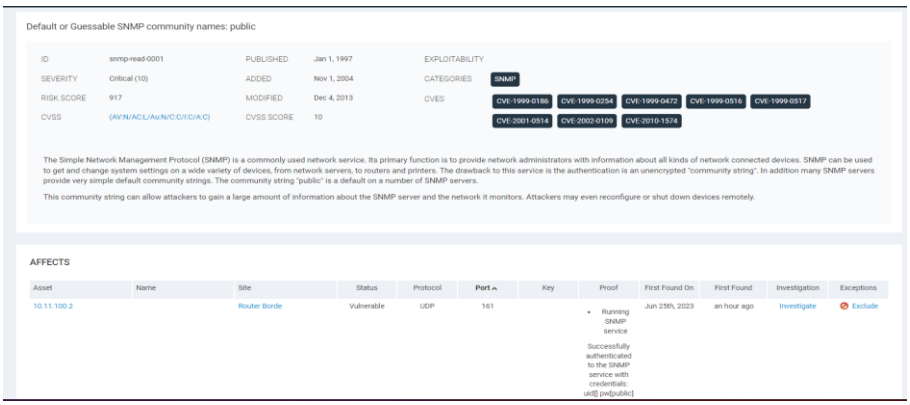


Figura 43. Detalle de vulnerabilidad.

Elaborado por: El investigador

En la figura 44, se puede apreciar que la remediación para la vulnerabilidad detectada se centra en la revisión de la documentación para la obtención de instrucciones para deshabilitar cualquier algoritmo inseguro.

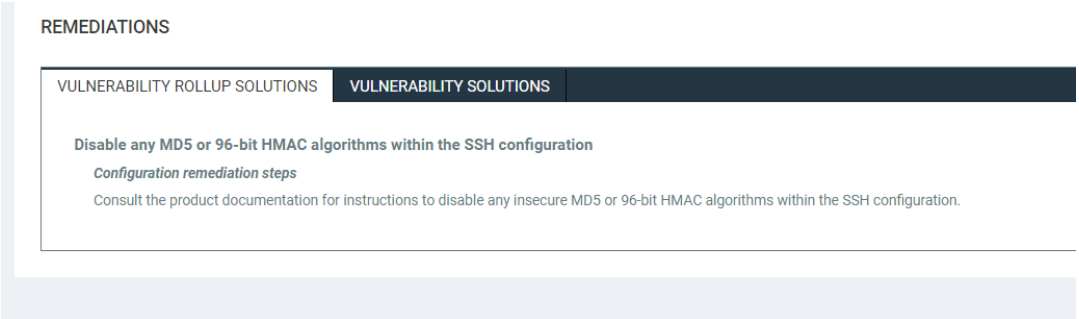


Figura 44. Remediación para la vulnerabilidad detectada.

Elaborado por: El investigador

A continuación, en la figura 45, de igual manera se puede observar que la remediación, para la vulnerabilidad detectada, en este caso recalcando que no es critica se centra en la des habilitación del soporte del puerto SSH.

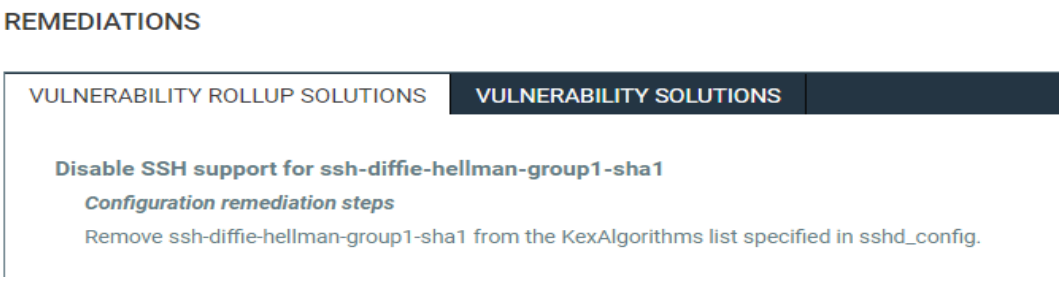


Figura 45. Remediación para la vulnerabilidad detectada.

Elaborado por: El investigador

Una vez concluido el proceso, la información obtenida permitió tomar decisiones relacionadas con las acciones correctivas para abordar cada una de las vulnerabilidades identificadas.

g. Nessus

Esta herramienta de análisis de vulnerabilidades ha ganado popularidad entre varias empresas debido a su capacidad para presentar resultados de manera sencilla y comprensible ya que Nessus es una potente herramienta de escaneo de vulnerabilidades que ayuda a identificar y evaluar posibles debilidades en sistemas, redes y aplicaciones, además proporciona informes detallados sobre las vulnerabilidades encontradas, permitiendo a los administradores de seguridad tomar

medidas para fortalecer la postura de seguridad de su infraestructura. Existen tres opciones disponibles para utilizar Nessus [47]:

- Nessus Essentials, que permite el análisis de hasta 16 activos de forma gratuita;
- Nessus PRO, adecuado para consultores y expertos en seguridad;
- Tenable.io, diseñado para empresas y gestión de vulnerabilidades [47].

Para este trabajo o similares, se sugiere Nessus Essentials, ya que no requiere la compra de licencias o suscripciones y permite escanear hasta 16 activos tecnológicos de la empresa sin costo.

Nessus Essentials, es una herramienta que se lo puede descargar de manera gratuita, además es compatible con sistemas operativos como Linux o Windows.

El primer paso al igual que el scanner de vulnerabilidades anterior, consiste en descargar e instalar el software, como se puede ver en la figura 46.

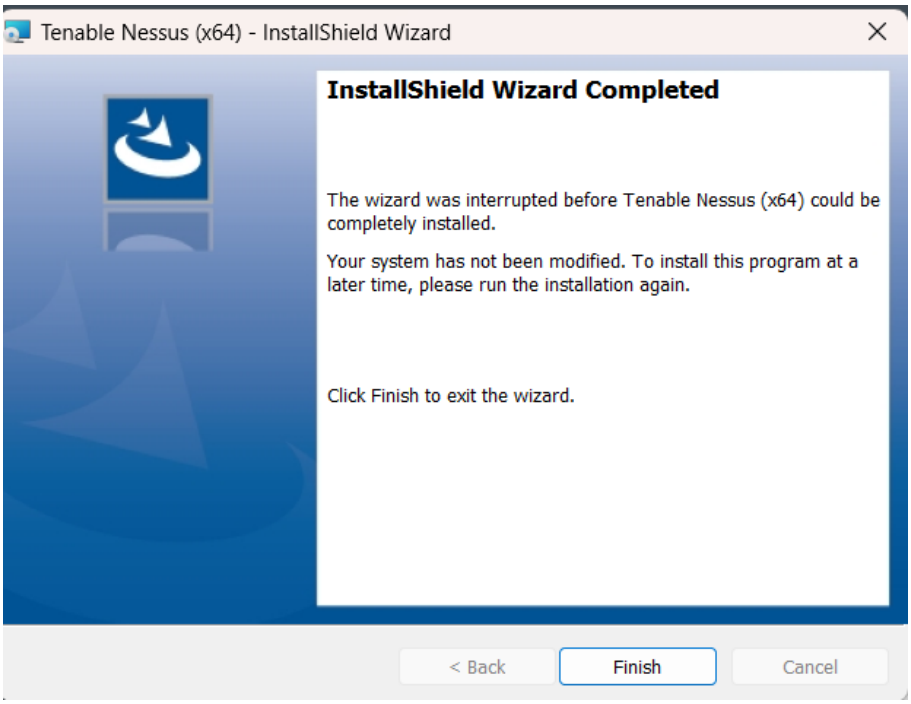


Figura 46. Descarga e instalación de nessus.

Elaborado por: El investigador

Seguidamente, registrarse y crear una cuenta, tal cual la figura 47.

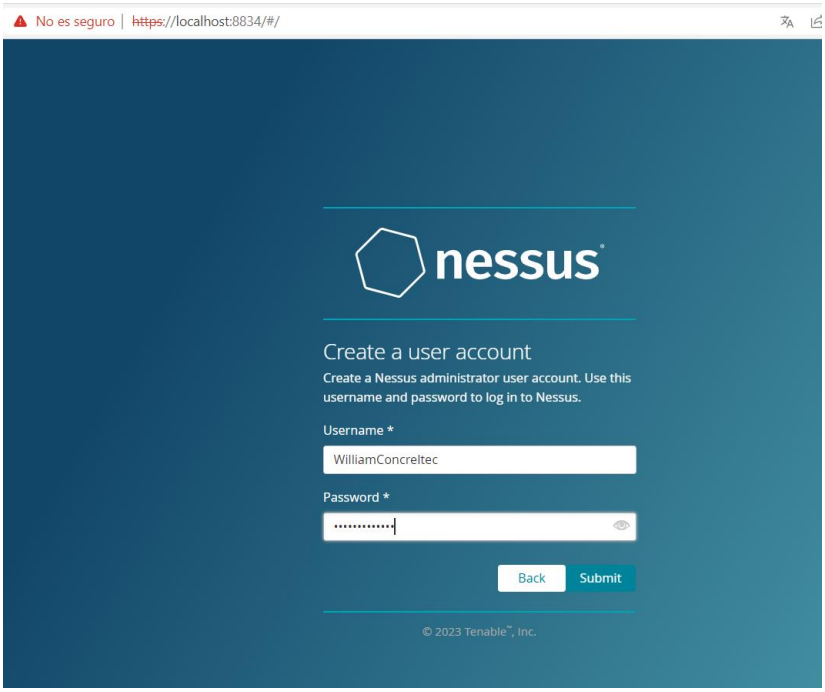


Figura 47. Registro y creación de cuenta en nessus.

Elaborado por: El investigador

Seguidamente, esperar la descarga de *plugins* para extender funcionalidades y capacidades del software, de igual manera que se muestra en la figura 48.

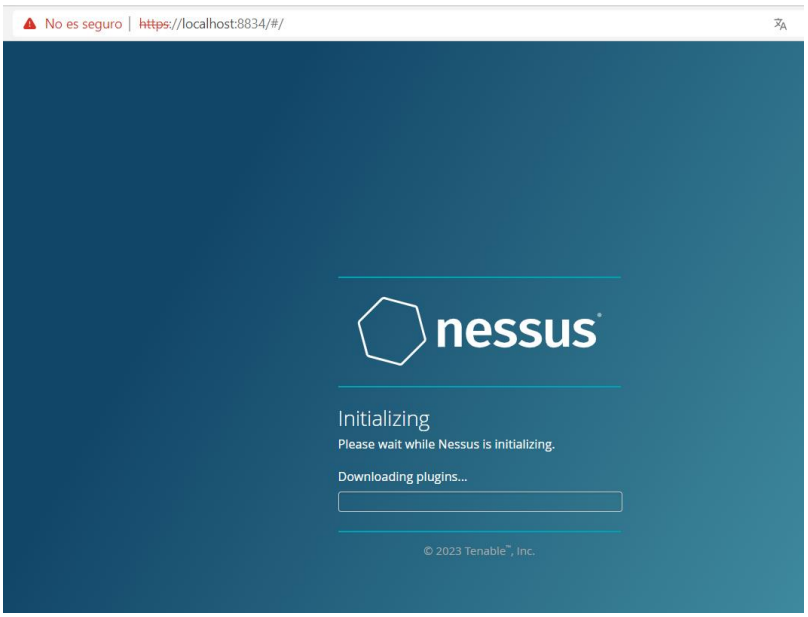


Figura 48. Descarga de complementos en nessus.

Elaborado por: El investigador

Una vez iniciado el software de Nessus Essentials, este permite interactuar rápidamente con la interfaz , al mismo tiempo solicita el primer lote de activos para iniciar con el escaneo de vulnerabilidades, el cual puede ser modificado cuando el usuario lo desee, como se puede observar en la figura 49.

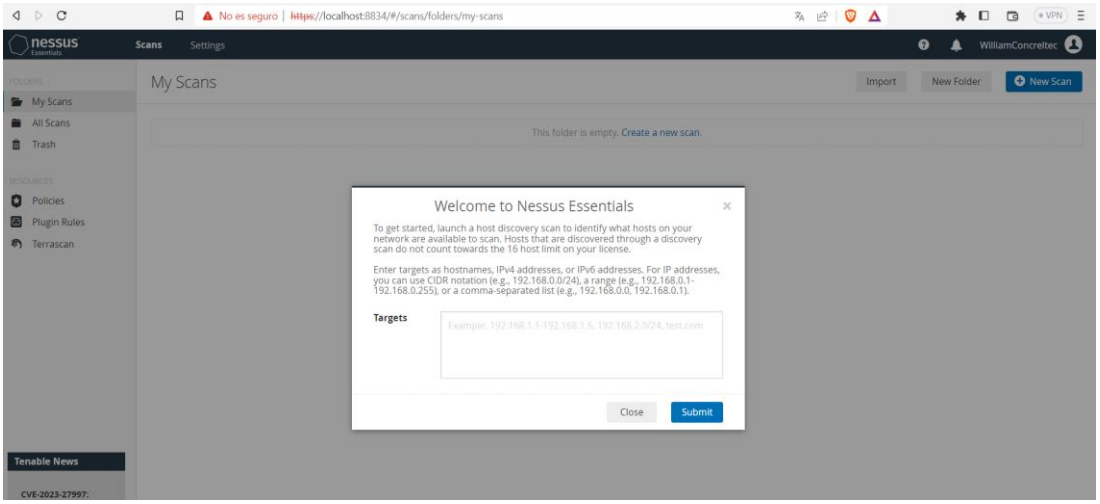


Figura 49. Datos iniciales para el escaneo de vulnerabilidades.

Elaborado por: El investigador

Como segundo paso, ingresar los activos a ser analizados, en este las direcciones IP de la empresa Concreltec, como se aprecia en la figura 50.

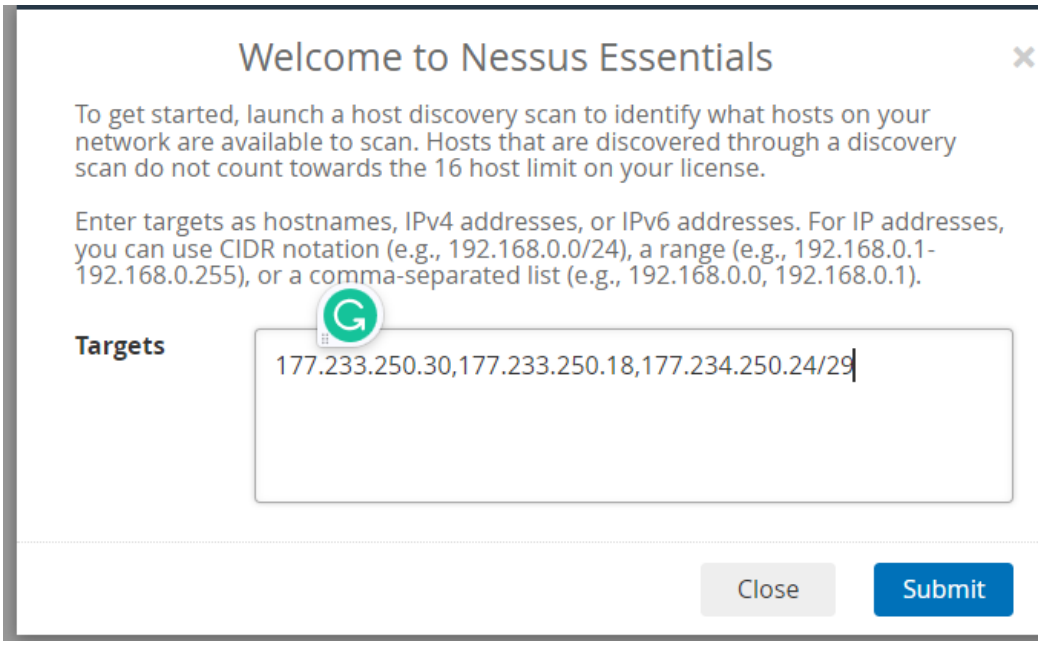


Figura 50. Ingreso de direcciones IP para el primer escaneo de vulnerabilidades.

Elaborado por: El investigador

De igual forma, continuar ingresando los activos y proseguir con las pruebas de reconocimiento, como se observa en la figura 51.

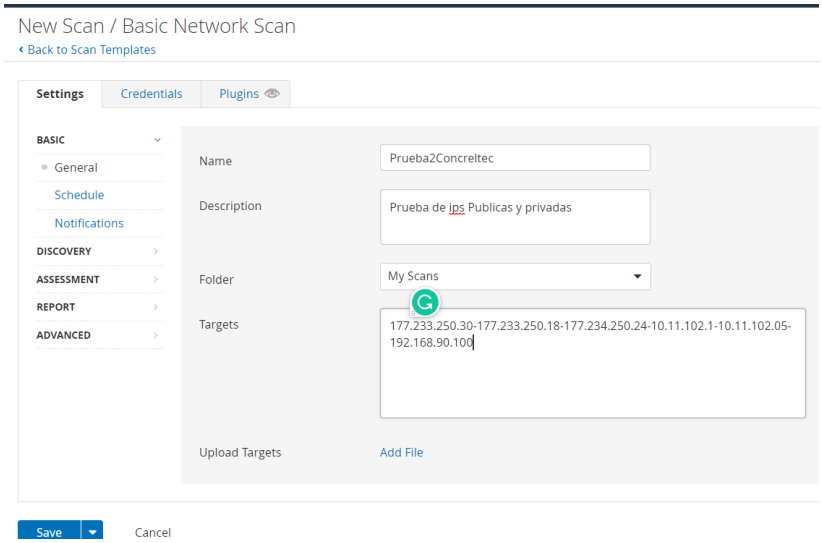


Figura 51. Ingreso de lote de activos para su respectivo análisis.

Elaborado por: El investigador

Posteriormente, el software aporta un resumen de los activos y las vulnerabilidades detectadas, se puede apreciar esta información en la figura 52, en donde se observa que el activo con mayor amenaza, es decir con nivel crítico, es el servidor de datos, seguido de los demás, de igual forma de acuerdo a la cantidad de vulnerabilidades detectadas.

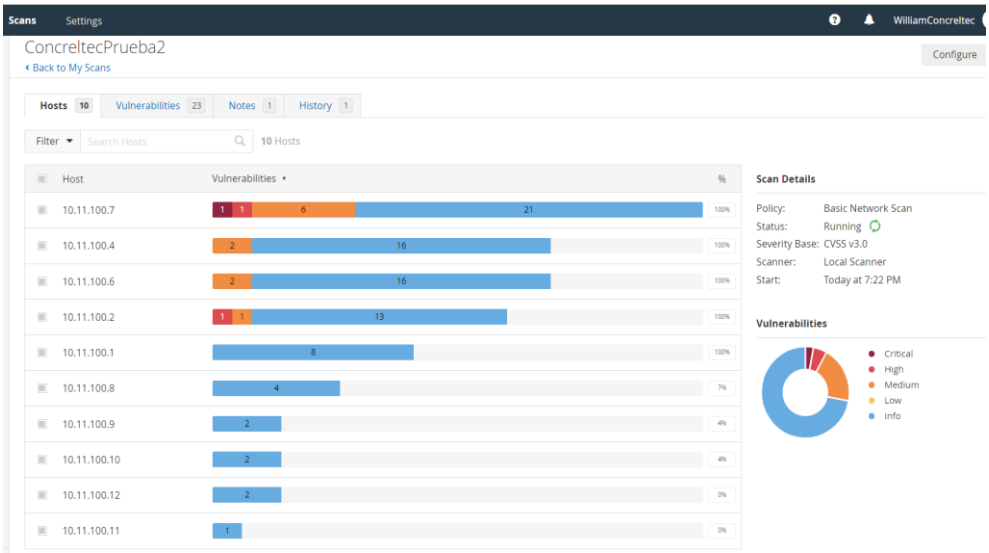


Figura 52. Resumen de activos y vulnerabilidades detectadas.

Elaborado por: El investigador

Así mismo, al navegar por la interfaz y evaluar cada una de las direcciones IP analizadas, se encuentra un resumen sobre las vulnerabilidades detectadas y los activos a los cuáles se relacionan, al igual que el nivel de riesgo, detallados en la figura 53.

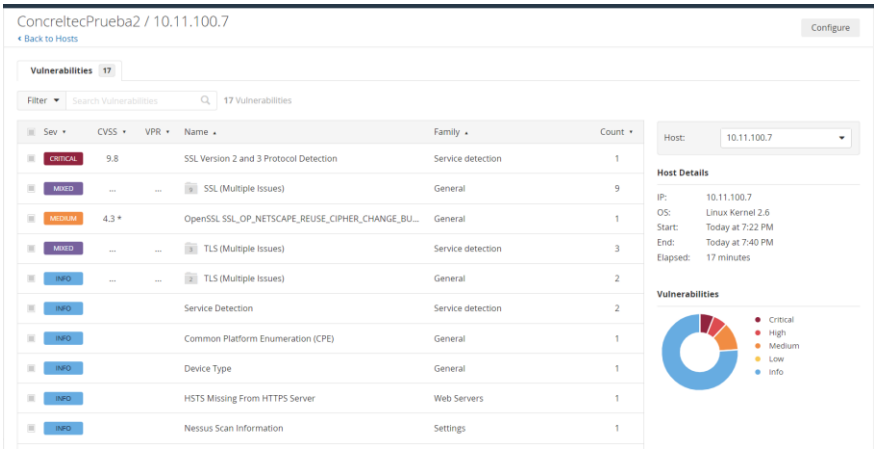


Figura 53. Resumen de vulnerabilidades y nivel de riesgo.

Elaborado por: El investigador

A continuación, se puede apreciar un resumen de cada prueba realizada, en donde se detalla la cantidad de vulnerabilidades detectadas por activo, dando un total de 8, de igual forma que la figura 54, en esta se puede observar a detalle cada prueba de penetración realizada y el número total de amenazas detectadas ordenadas por colores refiriéndose a estas como rojo (criticas), amarillo (amenaza nivel medio), y azul (amenaza de nivel bajo o información) de mayor a menor.

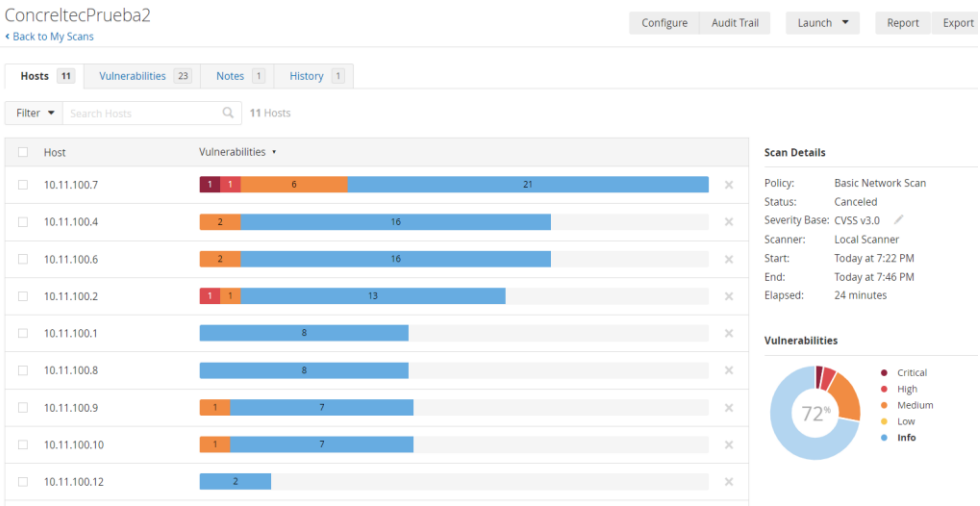


Figura 54. Cantidad de vulnerabilidades por activo.

Elaborado por: El investigador

Adicionalmente, se aprecia el tipo de vulnerabilidad detectada, sus detalles y las contramedidas, la clasificación de prioridad de la vulnerabilidad (VPR) y la historia de escaneos, como se observa en la figura 55, donde se detalla cual fue la vulnerabilidad detectada y sus características.

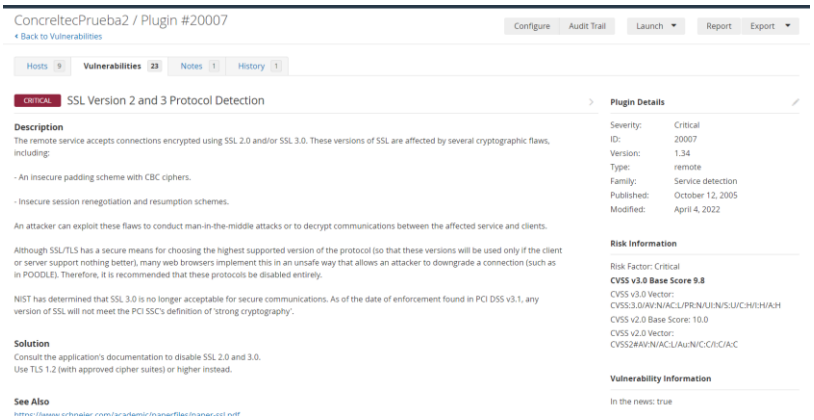


Figura 55. Vulnerabilidad detectada, detalles y remediaciones

Elaborado por: El investigador

A continuación, en la figura 56, se puede observar una amenaza de nivel medio, su descripción, así como la posible remediación.

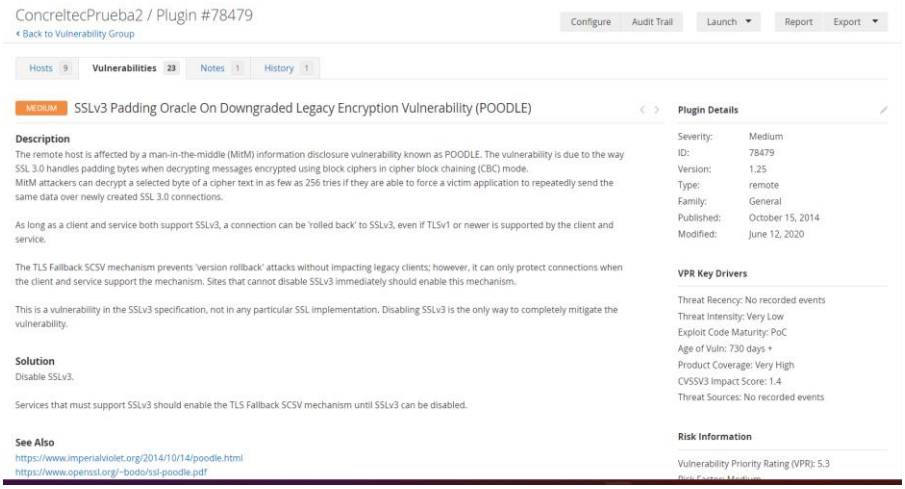


Figura 56. Vulnerabilidad detectada, detalles, remediaciones, VPR, historial de escaneos.

Elaborado por: El investigador

Finalmente, el mismo software presenta un resumen de las vulnerabilidades identificadas en la empresa CONCRELTEC, mediante un gráfico expresado en la figura 57, en donde el 5% de los activos analizados presentan amenazas de nivel alto, el 3% nivel crítico, 25% nivel medio y el resto son vulnerabilidades de índice bajo o de información.

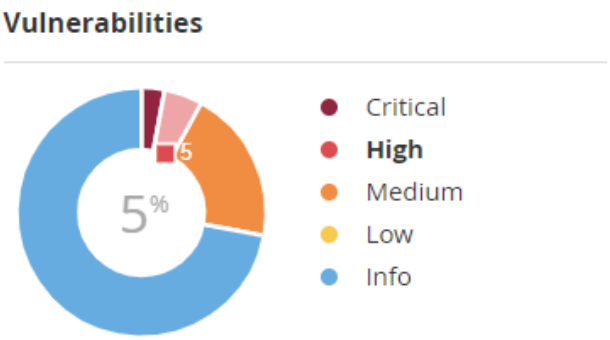


Figura 57. Resumen de las vulnerabilidades detectadas.

Elaborado por: El investigador

Esta información es clave para establecer las contramedidas de seguridad que se deben llevar a cabo. Una vez que se han identificado las vulnerabilidades en todos los activos de la empresa proveedora de servicios de internet CONCRELTEC, se procede a completar una tabla con la siguiente información:

- Nombre del equipo (según la topología de red)
- Detalles de la vulnerabilidad
- Prioridad (CRÍTICA, ALTA, MEDIA O BAJA)
- Tipo de usuario (ABONADO, CLIENTE O INFRAESTRUCTURA PROPIA)
- Dirección IP del equipo reportado
- Estado de la gestión (EN ANÁLISIS, PENDIENTE O ATENDIDO)
- Fecha de la gestión
- Hora de la gestión
- Acción (describe cómo se resolvió la vulnerabilidad)
- Observación (si hay alguna observación sobre la vulnerabilidad o la gestión realizada)

Es de enorme importancia recalcar que esta información se encuentra enmarcada y detallada, en la etapa 7, en el periodo de aplicación de remediaciones, bajo el nombre de “Tabla 24 de controles y remediaciones para los riesgos identificados en Concreltec”

3.5.3.4.Etapa 4. Probabilidad de ocurrencia.

Para calcular la probabilidad de ocurrencia en una evaluación de riesgos para un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001 aplicado a un Proveedor de Servicios de Internet (ISP), se debe seguir los siguientes pasos:

1. Identificar los posibles eventos o amenazas que pueden afectar la seguridad de la información en el ISP. Por ejemplo, ataques cibernéticos, fallas de hardware, errores humanos, desastres naturales, etc.
2. Para cada evento o amenaza identificado, determinar la frecuencia o la cantidad de veces que podría ocurrir en un período específico (por ejemplo, por año).
3. Asignar un valor numérico a la frecuencia, por ejemplo, si una amenaza ocurre con frecuencia mensual, el valor numérico sería 12 veces al año.
4. Luego, considerar la magnitud o impacto que tendría cada evento o amenaza si ocurriera. Por ejemplo, evaluar el impacto en términos de pérdida de datos, daño a la reputación, pérdida financiera, tiempo de inactividad del servicio, etc.
5. Asignar un valor numérico a la magnitud o impacto, por ejemplo, en una escala del 1 al 10, donde 1 es un impacto menor y 10 es un impacto catastrófico.
6. Finalmente, multiplica el valor numérico de la frecuencia por el valor numérico del impacto para obtener la probabilidad de ocurrencia para cada evento o amenaza.
7. Se puede representar la probabilidad de ocurrencia en una escala numérica (por ejemplo, del 1 al 100) o en una escala cualitativa (por ejemplo, baja, media o alta) [45].

Es importante tener en cuenta que la evaluación de riesgos es un proceso continuo y dinámico, por lo que es importante revisar y actualizar regularmente los resultados para mantener la seguridad de la información en el ISP.

Para calcular esta probabilidad de ocurrencia, se tomó en cuenta la guía: NIST SP 800-30: Guía del National Institute of Standards and Technology (NIST) para realizar

evaluaciones de riesgos de tecnologías de la información, teniendo en cuenta que se proporciona en formato PDF y no tiene una versión en línea específica.

Determinación de la probabilidad de ocurrencia.

Cálculo de la probabilidad de ocurrencia en una evaluación de riesgos para un Sistema de Gestión de Seguridad de la Información (SGSI) aplicado a la empresa CONCRELTEC, según información de las bases de datos proporcionados por el Ing. Mauricio Romo (Director de Redes de Concreltec cia Ltda.) [6]:

1. Identificación de amenazas potenciales:

    a) Ataque de malware.
    b) Error humano que lleva a la filtración de información.
    c) Corte de energía.

2. Determinación de la frecuencia de ocurrencia, se describe en la tabla 10:

Tabla 10. Determinación de la probabilidad de ocurrencia

Amenazas	**Probabilidad**
Ataque de malware	Ocurrió 8 veces en el último año.
Error humano	Ocurrió 4 veces en el último año.
Corte de energía:	Ocurrió 2 veces en el último año

Elaborado por: El investigador basado en [6].

3. Asignación de valores numéricos a la frecuencia, como se visualiza en la tabla 11:

Tabla 11. Asignación de valores numéricos a la frecuencia

Amenazas	**Probabilidad**
Ataque de malware	8 veces al año.
Error humano	4 veces al año.
Corte de energía	2 veces al año.

Elaborado por: El investigador basado en [6].

4. Valoración del impacto basado en la evaluación de riesgos para un Sistema de Gestión de Seguridad de la Información aplicado a la empresa Concreltec, de igual forma que en la tabla 12:

Tabla 12. Evaluación del impacto

Amenazas	**Impacto**
Ataque de malware	Daño moderado a la reputación y pérdida de datos.
Error humano	Pérdida moderada de datos y tiempo de recuperación.
Corte de energía	Pérdida moderada de servicios y tiempo de inactividad.

Elaborado por: El investigador basado en [6].

5. Asignación de valores numéricos al impacto (en una escala del 1 al 10, donde 1 es considerado el impacto más bajo y 10 el mas alto), como se observa en la siguiente tabla:

Tabla 13. Asignación de valores numéricos al impacto

Amenaza	**Impacto**
Ataque de malware	Impacto 7.
Error humano	Impacto 6.
Corte de energía	Impacto 5.

Elaborado por: El investigador basado en [6].

6. Cálculo de la probabilidad de ocurrencia para cada amenaza:

Probabilidad de ocurrencia de ataque de malware:

$$Frecuencia(8) \times Impacto(7) = 56$$

Probabilidad de ocurrencia de error humano:

$$Frecuencia(4) \times Impacto(6) = 24$$

Probabilidad de ocurrencia de corte de energía:

$$Frecuencia(2) \times Impacto(5) = 10$$

En este caso, el ataque de malware tiene la mayor probabilidad de ocurrencia con un valor de 56, seguido del error humano con un valor de 24, y finalmente, el corte de energía con un valor de 10. Esto proporciona una idea general de qué amenazas tienen más probabilidad de ocurrir, lo que permite priorizar las acciones para mitigar los riesgos de manera efectiva.

3.5.3.5.Etapa 5. Evaluación del impacto

La Evaluación del Impacto es una parte crucial del proceso de evaluación de riesgos, ya que permite determinar las consecuencias potenciales que podrían surgir si una amenaza se materializa en un activo de información.

A continuación, se describen los pasos para realizar la Evaluación del Impacto:

1. Identificación de activos: Enumera todos los activos de información del ISP que están involucrados en la prestación de servicios, como servidores, bases de datos, sistemas de red, datos de clientes, etc.
2. Identificación de amenazas: Identifica las posibles amenazas que podrían afectar a estos activos. Pueden ser amenazas físicas, tecnológicas o humanas, como desastres naturales, ataques cibernéticos, fallos de hardware, etc.
3. Evaluación de la probabilidad de ocurrencia: Determina la probabilidad de que cada amenaza ocurra y afecte un activo. Se puede utilizar una escala numérica o de categorías (alta, media, baja) para calificar la probabilidad.
4. Evaluación del impacto: Para cada amenaza, evalúa el impacto que tendría si se materializa en un activo. El impacto puede ser en términos de pérdida de confidencialidad, integridad o disponibilidad de la información.
5. Calificación del impacto: Utiliza una escala numérica o de categorías (alto, medio, bajo) para calificar el impacto en cada activo en caso de que la amenaza se materialice.
6. Cálculo del riesgo: Combina la probabilidad de ocurrencia y el impacto para calcular el nivel de riesgo de cada amenaza sobre cada activo.
7. Priorización de riesgos: Prioriza los riesgos según su nivel de gravedad. Los riesgos con una alta probabilidad de ocurrencia y un alto impacto deben recibir una atención prioritaria.

8. Implementación de medidas de control: Desarrolla e implementa medidas de control para mitigar los riesgos identificados. Estas medidas pueden incluir políticas, procedimientos, controles tecnológicos, entre otros.
9. Monitoreo y revisión: El proceso de evaluación de impacto es continuo. Se debe monitorear y revisar regularmente los riesgos y las medidas de control implementadas para asegurarse de que sigan siendo efectivas y adecuadas [45].

Evaluación del Impacto para un Proveedor de Servicios de Internet (ISP) CONCRELTEC basado en la norma ISO/IEC 27001:

Paso 1: Identificación de activos

- Servidores de red
- Bases de datos de clientes
- Equipos de comunicación
- Información de clientes (nombres, direcciones, datos personales)
- Sistemas de facturación

Paso 2: Identificación de amenazas

- Ataque cibernético (malware)
- Interrupción del suministro eléctrico
- Robo de información confidencial
- Error humano (borrado accidental de datos)

Paso 3: Evaluación de la probabilidad de ocurrencia, como se observa en la tabla 14.

Tabla 14. Evaluación de la probabilidad de ocurrencia

Ataque cibernético	Media
Interrupción del suministro eléctrico	Baja
Robo de información confidencial	Baja
Error humano	Alta

Elaborado por: El investigador basado en [45].

Paso 4: Evaluación del impacto, como se describe en la siguiente tabla:

Tabla 15. Evaluación del impacto Concreltec.

Ataque cibernético	Alta (pérdida de confidencialidad y disponibilidad de datos)
Interrupción del suministro eléctrico	Media (interrupción temporal de servicios)
Robo de información confidencial	Alta (pérdida de confidencialidad y posible daño a la reputación)
Error humano	Media (pérdida de datos y tiempo para recuperación)

Elaborado por: El investigador basado en [45].

Paso 5: Calificación del impacto, como se observa en la tabla 16:

Tabla 16. Calificación del impacto en Concreltec.

Alta	4
Media	3
Baja	2

Elaborado por: El investigador basado en [45].

Paso 6: Cálculo del riesgo

- Riesgo = Probabilidad de ocurrencia x Impacto
- Riesgo del ataque cibernético:

$$Media(2) \times Alta(4) = 8$$

- Riesgo de interrupción del suministro eléctrico:

$$Baja(1) \times Media(3) = 3$$

- Riesgo del robo de información confidencial:

$$Baja(1) \times Alta(4) = 4$$

- Riesgo del error humano:

$$Alta(4) \times Media(3) = 12$$

Paso 7: Priorización de riesgos

- Los riesgos se ordenan de mayor a menor valor, tal cual la tabla 17:

Tabla 17. Priorización de riesgos Concreltec

1	Error humano	(Riesgo 12)
2	Ataque cibernético	(Riesgo 8)
3	Robo de información confidencial	(Riesgo 4)
4	Interrupción del suministro eléctrico	(Riesgo 3)

Elaborado por: El investigador basado en [45].

Paso 8: Implementación de medidas de control

- Para mitigar el riesgo del error humano, se implementa una capacitación y concientización regular para el personal.
- Para reducir el riesgo del ataque cibernético, se instalan firewalls y se actualizarán regularmente los sistemas de seguridad.
- Para proteger contra el robo de información, se implementan medidas de cifrado y autenticación de usuarios.
- Para disminuir el riesgo de interrupción eléctrica, se instalan sistemas de respaldo de energía.

Paso 9: Monitoreo y revisión

- Se realizan auditorías periódicas para asegurarse de que las medidas de control sean efectivas y se mantengan actualizadas en función de los cambios en el entorno de riesgo.

3.5.3.6.Etapa 6. Remediaciones

Paso 1: Remediación de Vulnerabilidades

En el presente estudio, se abordaron las correcciones de las vulnerabilidades con impacto "Crítico" y "Medio", priorizando aquellas calificadas con valores del 1 al 6. Estas correcciones se basan en las recomendaciones que se describen a continuación, las cuales se enfocan en las distintas áreas que pueden ser consideradas puntos vulnerables desde la perspectiva de un atacante:

Vulnerabilidades de Software

Estas vulnerabilidades se refieren a los fallos presentes en los programas instalados en los dispositivos de red y seguridad que conforman la arquitectura de la empresa CONCRELTEC, objeto de este estudio. En caso de que estos fallos sean explotados, podrían provocar degradación o indisponibilidad del servicio. A continuación, en la tabla 18 se presentan las recomendaciones que deben aplicarse para este tipo de fallos:

Tabla 18. Errores que provocan vulnerabilidades de software.

Amenazas	**Recomendaciones**
Errores en la configuración del sistema.	1. Ajustar la configuración de los sistemas siguiendo las directrices del fabricante. 2. Realizar mantenimientos preventivos de carácter lógico al menos dos veces al año para detectar posibles errores o necesidades de configuración adicional. 3. Mantener el software actualizado con las últimas actualizaciones y parches disponibles. 4. Evitar el uso de software no autorizado o pirata.
Recursos mal gestionados	Planificar y asignar con antelación los recursos necesarios para asegurar la efectividad del sistema, considerando las tareas que serán ejecutadas, con el fin de prevenir posibles ataques que afecten el rendimiento del activo.
Gestión inadecuada de Accesos y permisos	Administrar los accesos y establecer los permisos según el rol de cada empleado o persona encargada de administrar los programas o dispositivos del servicio.
Vulnerabilidades detectadas CVE	1. Aplicar las actualizaciones o parches correspondientes, siguiendo las referencias de soluciones y el número de identificación de vulnerabilidad (CVE). 2. Realizar actualizaciones de software a versiones más recientes.

Elaborado por: El investigador

Vulnerabilidades de hardware

El equipo tecnológico utilizado por las empresas de servicios de Internet puede enfrentar diversas vulnerabilidades físicas, incluyendo posibles fallas de hardware y riesgos asociados a desastres naturales. A continuación, se describen algunas de estas situaciones:

Tabla 19. Errores que causan vulnerabilidades de hardware.

Amenazas	Recomendaciones
Acceso no autorizado	1.- Implementar una política de control de acceso para proteger los equipos de la red del servicio. 2.- Emplear dispositivos biométricos para autorizar el acceso y registrar las personas que interactúan con los equipos.
Catástrofes Naturales	1.- Evitar ubicar equipos en áreas elevadas para prevenir posibles caídas. 2.- No poner objetos móviles sobre los equipos para evitar que puedan caer sobre ellos. 3.- Mantener una distancia segura entre los equipos y las ventanas para evitar caídas o daños causados por objetos externos. 4.- Utilizar fijaciones adecuadas para asegurar los elementos críticos. 5.- Colocar los equipos sobre plataformas de goma para absorber las vibraciones y reducir riesgos.
Riesgos asociados a posibles fallos en los componentes de hardware.	1.- Es importante reemplazar el hardware antes de que alcance el final de su vida útil. 2.- Realizar mantenimientos periódicos para prevenir problemas con la memoria RAM debido a la soldadura cercana. 3.- Monitorear la tecnología Smart de los discos duros para anticiparse y prevenir fallos.

	4.- Se recomienda cerrar los puertos USB o aplicar filtrado MAC para limitar el acceso a dispositivos autorizados.

Elaborado por: El investigador basado en [45]

Vulnerabilidades Humanas

La empresa proveedora de servicios de internet CONCRELTEC, aunque cuenta con un equipo reducido de empleados, es esencial aplicar las siguientes recomendaciones para mitigar las vulnerabilidades relacionadas con recursos humanos:

1. Implementar sistemas de registros y auditorías para rastrear las acciones de los empleados.
2. Realizar charlas de concientización para prevenir estafas mediante ingeniería social, como solicitar contraseñas por medios falsos, correos electrónicos fraudulentos o robo de información a través de anuncios web, entre otros.
3. Al inicio de la relación laboral, establecer acuerdos de confidencialidad firmados para proteger la información sensible de la empresa.
4. Definir las responsabilidades de los empleados en materia de seguridad informática dentro del marco del contrato laboral.

Asimismo, se llevaron a cabo las acciones correctivas necesarias para cumplir con los objetivos de control identificados en la fase inicial tras el análisis de riesgos. Estas medidas son aplicadas a los activos que conforman el servicio, tomando en cuenta los objetivos tecnológicos de la empresa y los recursos disponibles para abordar y mitigar todos los riesgos.

Las acciones correctivas se fundamentaron en los controles establecidos en el Anexo A de la norma ISO 27001, aplicando cada uno de ellos a los siguientes activos del sistema con certificación ISO 27001:

Políticas de seguridad de la información: Establecer directrices para garantizar la protección de la información.

Seguridad de los recursos humanos: Definir políticas y directrices para que los empleados eviten ataques de ingeniería social.

Gestión de activos: Realizar inventarios detallados de cada activo que forma parte del servicio de Internet.

Controles de acceso: Auditar los accesos a cada dispositivo y consola de administración de los activos de la red.

Gestión de claves: Asignar accesos y privilegios a los usuarios según sus funciones.

Seguridad física y ambiental: Colocar los dispositivos en lugares seguros para prevenir daños por desastres naturales y controlar el acceso físico a dichos lugares.

Seguridad de las comunicaciones: Implementar dispositivos de seguridad, como IPS, IDS, Firewalls, Antivirus y cifrado para mantener la seguridad en las comunicaciones remotas, entre otros.

Adquisición, desarrollo y mantenimiento del sistema: Implementar un programa de mantenimientos periódicos tanto físicos como lógicos a lo largo del año para garantizar el óptimo funcionamiento del sistema.

Gestión de incidentes de seguridad de la información: Asignar responsabilidades claras para el tratamiento de eventos de seguridad y crear bases de conocimiento específicas para cada tipo de incidente.

Cumplimiento: Establecer roles y responsabilidades para asegurar el cumplimiento de los requisitos de los organismos reguladores de Ecuador, que constituyen el objetivo central de este proyecto.

3.5.3.7. Etapa 7. Pruebas y análisis de resultados.

Periodo de pruebas:

Después de implementar las acciones correctivas, se lleva a cabo un monitoreo exhaustivo del servicio durante 7 días, donde las primeras 72 horas fueron clave para verificar su correcto funcionamiento. Estas remediaciones fueron realizadas en horarios fuera del horario laboral para evitar posibles impactos en la operación. Los detalles específicos de las actividades de monitoreo se registraron en la siguiente tabla.

Tabla 20. Detalle monitoreo del servicio.

Servicio	Dirección IP	Tiempo	Herramienta	Afectación SI/NO	Rollback SI/NO	Tiempo Rollback	Observación

Elaborado por: El investigador

Actividades de validación:

Dentro del período designado para las tareas, se llevaron a cabo las siguientes pruebas para asegurar la eficacia de las acciones correctivas implementadas.

Tabla 21. Checklist de pruebas

Pruebas realizadas	Funcionalidad	Observaciones	Herramientas
Monitoreo de los servicios			OPEN NMS
Resolución DNS			Windows: NSLOOKUP Linux: HOST o DIG
Acceso Web			GT METRIX
Uso de Recursos			Linux: Top Windows: Administrador de Tareas
Tiempos de respuesta			Ping
Logs de registro para verificar errores			Archivos de registro de los servicios Linux: /var/log Windows: Visor de Eventos
Validaciones de usuario final			Acceso al servicio mediante Navegadores: Chrome, Firefox, Edge, IE.

Elaborado por: El investigador

Análisis de resultados

Para llevar a cabo un correcto análisis de resultados, a continuación, se presenta un cuadro resumen de amenazas de cada activo que dispone la empresa CONCRELTEC.

Tabla 22. Identificación de Amenazas Concreltec

Identificador de Riesgo	Activo	Amenaza
1	Servidor DNS - DATOS (10.11.102.7)	Eventos naturales como incendios, sismos y desbordamientos de agua.
2	Servidor DNS - DATOS (10.11.102.7)	Interrupciones del suministro eléctrico.
3	Servidor DNS - DATOS (10.11.102.7)	Errores en los programas de los servidores.
4	Servidor DNS - DATOS (10.11.102.7)	Contaminación del servidor por virus o software malicioso.
5	Servidor DNS - DATOS (10.11.102.7)	Problemas en el servicio DNS.
6	Servidor DNS - DATOS (10.11.102.7)	Acceso remoto a la base de datos SQL.
7	Servidor Proxy (10.11.100.6)	Errores en los programas de los servidores.
8	Servidor Proxy (10.11.100.6)	Exceso de carga en el servidor.
9	Servidor Proxy (10.11.100.6)	Infección del servidor por virus o software malicioso.
10	Servidor Proxy (10.11.100.6)	Errores en los programas de los servidores.
11	Router de Borde (Salida Internacional) (177.234.250.25)	Fallos en software de servidores

12	Router de Borde (Salida Internacional) (177.234.250.25)	Fallos en software de servidores
13	Router de Borde (Salida Internacional) (177.234.250.25)	Fallos en software de servidores
14	Switch de conexión interna (10.11.100.2)	Errores en los programas de los servidores.
15	Switch de conexión interna (10.11.100.2)	Errores en los programas de los servidores.
16	Router conexión interna con clientes-abonados (177.234.250.24)	Fallos en software de servidores
17	Router conexión interna con clientes-abonados (177.234.250.24)	Eventos naturales como incendios, sismos y desbordamientos de agua.
18	Router conexión interna con clientes-abonados (177.234.250.24)	Interrupciones del suministro eléctrico.
19	Router conexión interna con clientes-abonados (177.234.250.24)	Fallos en software de servidores
20	Olt (10.11.100.5)	Eventos naturales como incendios, sismos y desbordamientos de agua.
21	Personal técnico	Escape de Información
22	Cableado	Fallas en cables
23	Equipos de red	Acceso no autorizado

Elaborado por: El investigador

Análisis de Riesgos.

Para llevar a cabo el análisis de riesgos, se utilizaron los datos de la Figura 39 para evaluar la probabilidad frente al impacto. En la siguiente fase, se buscaron las estrategias de mitigación para los riesgos más críticos y se identificaron las vulnerabilidades que fueron sometidas a escaneo en el próximo paso.

Tabla 23. Evaluación de riesgos Concreltec

Identificador de Riesgo	Activo	Amenaza	Vulnerabilidad	Probabilidad	Impacto	Prioridad
1	Servidor DNS - DATOS (10.11.102.7)	Eventos naturales como incendios, sismos y desbordamientos de agua.	No se utiliza la infraestructura de servicios en la nube.	Baja	Alto	11
2	Servidor DNS - DATOS (10.11.102.7)	Interrupciones del suministro eléctrico.	No se dispone de un sistema de respaldo, como un generador o UPS, para hacer frente a los cortes de energía.	Alta	Crítico	2
3	Servidor DNS - DATOS (10.11.102.7)	Errores en los programas de los servidores.	El certificado del servidor ha expirado, lo cual afecta a los servicios de IMAP, POP, IMAPS y POPS.	Baja	Bajo	16
4	Router de Borde (Salida Internacional) (177.234.250.25)	Eventos naturales como incendios, sismos y desbordamientos de agua.	No se utiliza la infraestructura de servicios en la nube.	Baja	Alto	11
5	Router de Borde (Salida Internacional) (177.234.250.25)	Interrupciones del suministro eléctrico.	No se dispone de un sistema de respaldo, como un generador o UPS, para hacer frente a los cortes de energía.	Alta	Crítico	2

6	Personal técnico	Escape de Información.	La empresa carece de una política que establezca la eliminación y cambio regular de claves para salvaguardar la información en caso de despidos repentinos.	Media	Crítico	6
7	Cableado	Fallas en cables.	No se dispone del cable con certificación correspondiente.	Media	Alto	9
8	Equipos de Red	Acceso no autorizado.	La protección física para los equipos de red no ha sido implementada de manera específica.	Media	Crítico	6

Elaborado por: El investigador.

Aplicación de remediaciones.

A continuación, se proporciona una tabla que resume las acciones correctivas llevadas a cabo para abordar las vulnerabilidades y riesgos más significativos detectados. Para esta sección, se siguió el **Anexo A de la norma ISO 27001** para aplicar los controles correspondientes en función de los riesgos y vulnerabilidades identificados.

Tabla 24. Tabla de controles y remediaciones para los riesgos identificados en Concreltec

Sección Norma ISO 27001:2013	ID Control	Objetivo del Control	Control	Activo	Amenaza	Vulnerabilidad	Remediación
A.11 Seguridad física y medioambiental	A.11.2 Equipos	Prevenir la pérdida, daño, hurto o cualquier acción que pueda afectar los activos y provocar interrupciones en las operaciones de la organización.	A.11.2.2. Es importante salvaguardar los equipos ante posibles interrupciones de energía y otras perturbaciones que puedan surgir debido a fallas en los servicios públicos de soporte.	Servidor DNS - DATOS (10.11.102.7)	Interrupciones del suministro eléctrico.	No se dispone de un sistema de respaldo, como un generador o UPS, para hacer frente a los cortes de energía.	La compra de un generador o UPS para evitar que los equipos se apaguen durante una interrupción del suministro eléctrico.

A.12 Seguridad de las Operaciones	A.12.6 Gestión de las vulnerabilidades técnicas	Prevenir la explotación de debilidades técnicas.	A.12.6.1. Es importante obtener de forma oportuna información sobre las vulnerabilidades técnicas presentes en los sistemas de información a utilizar. Luego, se debe evaluar cómo afectarían estas vulnerabilidades a la organización y tomar las medidas necesarias para gestionar los riesgos asociados de manera adecuada.	Servidor DNS - DATOS (10.11.102.7)	Interrupciones en servicio DNS	Solicitudes de búsqueda recursiva al servidor DNS.	Limitar o restringir el procesamiento de solicitudes de búsqueda recursiva mediante el uso de una lista de permisos.
A.12 Seguridad de las Operaciones	A.12.6 Gestión de las vulnerabilidades técnicas	Prevenir la explotación de debilidades técnicas.	A.12.6.1. Es importante obtener de forma oportuna información sobre las vulnerabilidades técnicas presentes en los sistemas de información a utilizar. Luego, se debe evaluar cómo afectarían estas vulnerabilidades a la organización y tomar las medidas necesarias para gestionar los riesgos asociados de manera adecuada.	Servidor DNS - DATOS (10.11.102.7)	Acceso remoto a la base de datos SQL.	Permisos sin restricciones para acceder a la Base de Datos.	Isolar el servicio de Base de Datos de la zona de Demilitarización (DMZ).
A.12 Seguridad de las Operaciones	A.12.6 Gestión de las vulnerabilidades técnicas	Prevenir la explotación de debilidades técnicas	A.12.6.1. Es importante obtener de forma oportuna información sobre las vulnerabilidades técnicas presentes en los sistemas de	Servidor Proxy (10.11.100.6)	Incidencias en el funcionamiento del software de los servidores.	La versión de PHP utilizada está desactualizada.	Realizar la actualización de la versión actual de PHP (5.3.25) a una versión

			información a utilizar. Luego, se debe evaluar cómo afectarían estas vulnerabilidades a la organización y tomar las medidas necesarias para gestionar los riesgos asociados de manera adecuada.				recomendada igual o superior a 7.
A.12 Seguridad de las Operaciones	A.12.1 Procedimientos y responsabilidades operaciones	Manejo de recursos y capacidad del sistema.	A.12.1.3. Es necesario supervisar y optimizar la utilización de recursos, así como realizar proyecciones de los requisitos futuros de capacidad, con el fin de asegurar el rendimiento óptimo del sistema.	Servidor Proxy (10.11.100.6)	Evitar exceder la capacidad de procesamiento del servidor.	Se deben prevenir los ataques de denegación de servicio que puedan ocurrir debido a la ejecución de datos inesperados. También, es importante tomar medidas específicas para mitigar la vulnerabilidad conocida como CVE-2015-4602.	Realizar la actualización de la versión actual de PHP (5.3.25) a una versión recomendada igual o superior a 7.
A.11 Seguridad Física y Ambiental	A.11.2. Equipos	Prevenir la pérdida, daño, hurto o cualquier acción que pueda afectar los activos y provocar interrupciones en las operaciones de la organización.	A.11.2.2. Es importante salvaguardar los equipos ante posibles interrupciones de energía y otras perturbaciones que puedan surgir debido a fallas en los servicios públicos de soporte.	Router de Borde (Salida Internacional) (177.234.250. 25)	Interrupciones del suministro eléctrico.	No se dispone de un sistema de respaldo, como un generador o UPS, para hacer frente a los cortes de energía.	La compra de un generador o UPS para evitar que los equipos se apaguen durante una interrupción del suministro eléctrico.
A.7 Seguridad de los recursos humanos	A.7.3 Término y cambio de empleo	Asegurar la salvaguardia de los intereses de la organización durante los procesos de cambio o finalización de empleo.	A.7.3.1. Es necesario establecer, comunicar y reforzar entre todos los empleados y contratistas las responsabilidades y tareas	Personal técnico	Escape de Información.	La empresa carece de una política que establezca la eliminación y cambio regular de claves para salvaguardar la	Crear un protocolo que permita eliminar los accesos de usuarios una vez que hayan sido

			relacionadas con la seguridad de la información, que seguirán siendo vigentes incluso después de finalizar su empleo.			información en caso de despidos repentinos.	dados de baja de la empresa.
A.11 Seguridad física y medioambiental	A.11.1. Áreas Seguras	Prevenir el acceso físico no autorizado, daños e interferencias a la información y a las instalaciones de procesamiento de datos de la organización.	A.11.1.3. Se debe diseñar y aplicar mecanismos de seguridad física a las salas, oficinas e instalaciones.	Equipos de Red	Acceso no autorizado	La protección física para los equipos de red no ha sido implementada de manera específica.	Crear un ambiente físico destinado específicamente para la ubicación y protección de los equipos.

Elaborado por: El investigador

Periodo de pruebas:

Después de implementar las medidas correctivas para las vulnerabilidades críticas identificadas en los activos de la empresa evaluada, se llevó a cabo un seguimiento continuo durante un período de 72 horas. Durante este tiempo, no se registraron informes de interrupciones del servicio por parte de los clientes de Concreltec. A continuación, en la figura 58, se presenta un informe que muestra el porcentaje de disponibilidad de los equipos de red.

Figura 58. Reporte de disponibilidad de activos Concreltec

Elaborado por: El investigador

Tabla 25. Detalle monitoreo y observaciones de activos Concreltec

Servicio	Dirección IP	Tiempo	Herramienta	Afectación	Rollback SI/NO	Tiempo Rollback	Observación
Correo IMAP-POP-SMTP	10.11.102.7	3 días	OPEN NMS	NO	NO	N/A	
DNS BIND Primario	10.11.102.7	3 días	OPEN NMS	SI	SI	10 min	Listas de hosts inseguras con configuración incorrecta para la recursión. Se llevó a cabo una nueva sesión de trabajo para corregir y aplicar adecuadamente las medidas correctivas.
DATOS APACHE-MYSQL	10.11.102.7	3 días	OPEN NMS	NO	NO	N/A	
DNS BIND Secundario	10.11.100.6	3 días	OPEN NMS	NO	NO	N/A	
Proxy Squid	177.234.250.25	3 días	OPEN NMS	NO	NO	N/A	

Elaborado por: El investigador

Luego del periodo de aplicación de las remediaciones, se puede observar en la figura 59 el reporte de disponibilidad:

Figura 59. Reporte de disponibilidad de activos con remediaciones aplicadas Concreltec.

Elaborado por: El investigador

A continuación, se presenta el Checklist de pruebas:

Tabla 26. Checklist de pruebas Concreltec

Pruebas realizadas	Funcionalidad	Observaciones	Herramientas
Monitoreo de los servicios	Operativo	Ninguna	OPEN NMS
Resolución DNS	Operativo	El problema se solucionó después de corregir la configuración incorrecta que había sido aplicada previamente.	Windows: NSLOOKUP Linux: HOST ó DIG
Acceso Web	Operativo	Ninguna	GT METRIX
Uso de Recursos	Normal	Ninguna	Linux: Top Windows: Administrador de Tareas
Tiempos de respuesta	Normal	Los tiempos de respuesta se registran por debajo de 100 ms desde ubicaciones externas y por debajo de 30 ms en la red local.	Ping o MTR
Logs de registro para verificar errores	Sin errores		Archivos de registro de los servicios Linux: /var/log Windows: Visor de Eventos
Validaciones de usuario final	Operativo	Acceso al servicio sin problemas	Acceso al servicio mediante Navegadores: Chrome, Firefox, Edge, Brave.

Elaborado por: El investigador

Análisis de resultados:

Después de realizar nuevamente el escaneo en uno de los activos de Concreltec, en este caso el router de borde con la IP 177.234.250.25 se observó que el nivel de riesgo disminuyó significativamente de su valor inicial de 800, como se muestra en la figura 60. Esta reducción del nivel de riesgo y la eliminación de las mismas vulnerabilidades detectadas demuestran la efectividad de la metodología desarrollada en este informe.

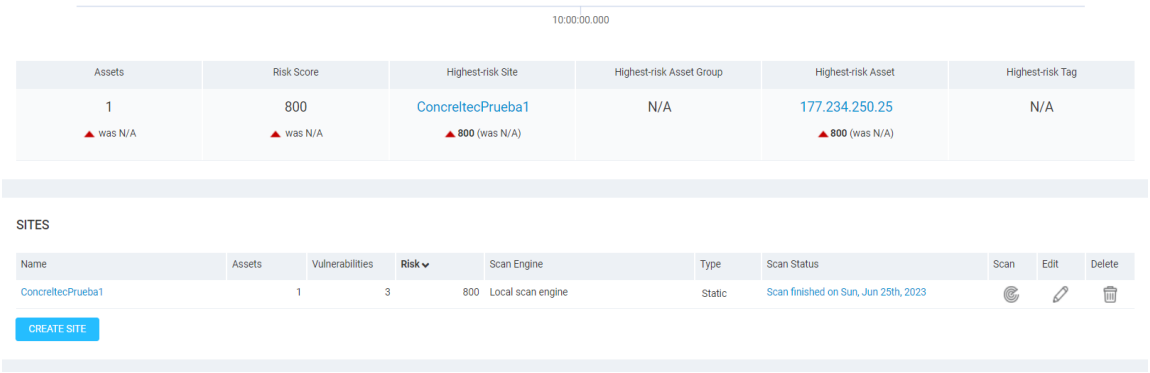


Figura 60. Puntaje de riesgo concreltec.

Elaborado por: El investigador

Como se puede apreciar en la figura 61, las vulnerabilidades del activo escaneado se redujeron, dejando atrás las de tipo critico (color rojo), y medio (color amarillo).

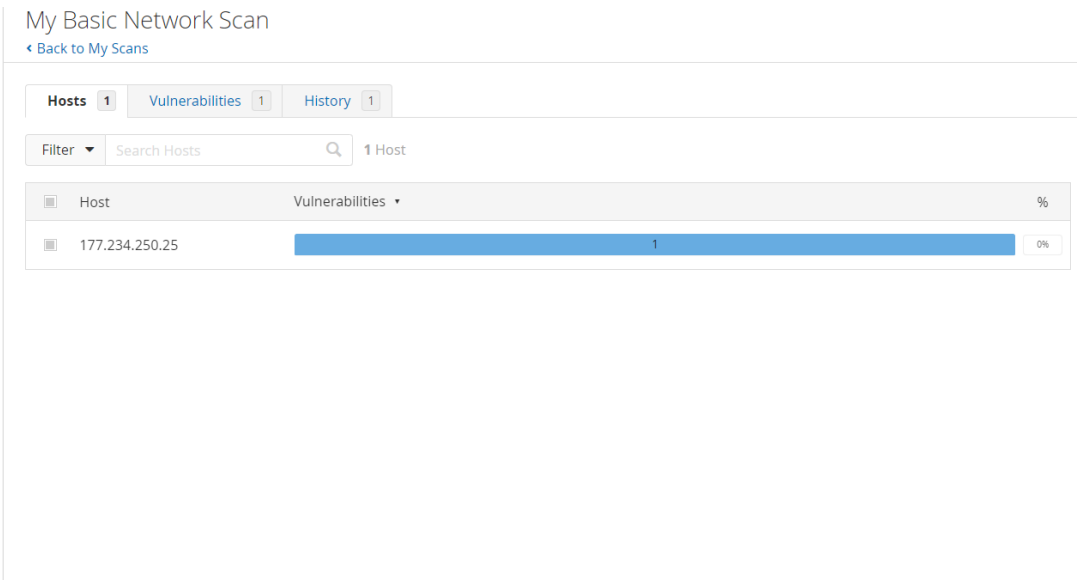


Figura 61. Escaneo de vulnerabilidad final del activo con mayor riesgo en Concreltec

Elaborado por: El investigador

De igual al realizar el escaneo de vulnerabilidades de los siguientes activos con mayor índice de vulnerabilidad y luego de aplicar las remediaciones como se observa en la figura 62 se obtiene lo siguiente:

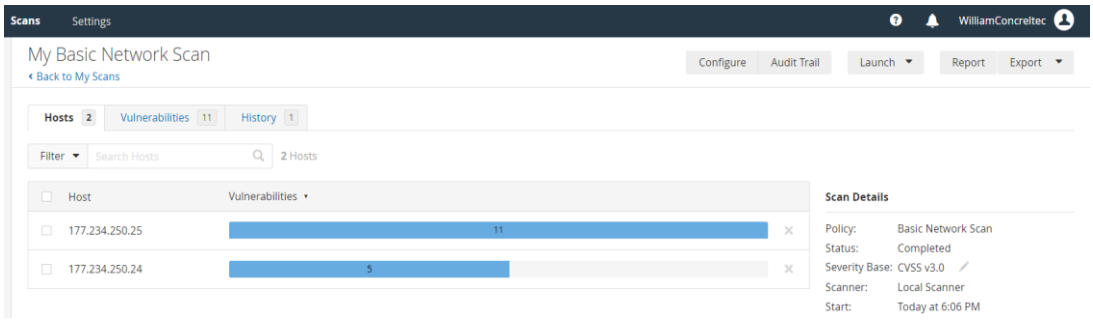


Figura 62. Escaneo final luego de las remediaciones Concreltec

Elaborado por: El investigador

Finalmente, en base a las remediaciones aplicadas, se logró una significativa disminución de las vulnerabilidades identificadas en el sistema de seguridad de CONCRELTEC. Las medidas implementadas demostraron ser efectivas para mitigar los riesgos detectados, asegurando la integridad, confidencialidad y disponibilidad de la información.

Además, el manual de políticas de seguridad desarrollado durante este estudio ha sido incluido como **Anexo 1**, del presente trabajo, proporcionando una guía detallada y completa para el manejo seguro de la información y el mantenimiento de un entorno protegido, no obstante, a la par de este, como **Anexo 2**, se encuentra el protocolo TLP (Traffic Light Protocol), también conocido como "Protocolo de semáforos", en último lugar se encuentra la administración y configuración del software utilizado.

.

CAPÍTULO IV

CONCLUSIONES Y RECOMENDACIONES

Con la puesta en marcha de la evaluación de riesgos para un sistema de gestión de seguridad de la información en base a la norma ISO/IEC 27001 aplicado a un proveedor de servicios de internet, se obtuvieron las siguientes conclusiones y recomendaciones:

4.1. Conclusiones

- Tras el análisis detallado del sistema de comunicación y resguardo de información en CONCRELTEC, se identificaron áreas de mejora y fortalezas en cuanto a la seguridad de la información. Se detectaron algunos puntos vulnerables en la infraestructura de comunicaciones de la empresa como la falta de respaldo para enfrentar cortes de energía, uso de versiones desactualizadas de software como PHP 5.3.25 en el servidor proxy, accesos no autorizados a archivos críticos, no utilizar una infraestructura de servicios en la nube, entre otros, los cuales requirieron medidas de mitigación y actualización para garantizar la integridad, confidencialidad y disponibilidad de los datos.
- El proceso de evaluación de riesgos ISO/IEC 27001 identificó con precisión los riesgos, vulnerabilidades y amenazas en CONCRELTEC. Proporcionó una visión completa de la seguridad de la información, priorizando controles y medidas de mitigación. Se abordaron riesgos significativos como eventos naturales, interrupciones del servicio DNS, accesos no autorizados y fallas en programas. La implementación de controles específicos, basados en la norma, redujo efectivamente los riesgos y protegió la información sensible de los clientes.
- La selección cuidadosa de controles de seguridad informática como realizar análisis de vulnerabilidades y pruebas de penetración periódicamente, la capacitación habitual a los empleados en seguridad informática y buenas prácticas, además de mantener el software y los sistemas actualizados, ha permitido mitigar efectivamente los riesgos en CONCRELTEC. Los controles técnicos, organizativos y de gestión implementados abordan específicamente

vulnerabilidades y amenazas, como la limitación de solicitudes recursivas en el servicio DNS y la actualización de versiones de software críticas. Estos controles han demostrado ser efectivos para mantener un ambiente seguro y cumplir con los requisitos de seguridad de la norma ISO/IEC 27001.

- La elaboración del manual de políticas de seguridad ha sido una herramienta fundamental para establecer lineamientos claros y prácticos en la gestión de la información de los clientes de CONCRELTEC. El manual proporciona directrices específicas para garantizar la integridad, confidencialidad y disponibilidad de la información, abordando de manera proactiva las vulnerabilidades identificadas durante la evaluación de riesgos La implementación de estas políticas de seguridad contribuye a crear un entorno confiable para los clientes de la empresa, generando confianza en la protección de sus datos y asegurando el cumplimiento de las regulaciones y normativas aplicables.
- La evaluación de riesgos basada en la norma ISO/IEC 27001 ha brindado a CONCRELTEC una visión integral de los riesgos y una base sólida para la toma de decisiones en materia de seguridad de la información. La implementación de las medidas de mitigación y el desarrollo del manual de políticas de seguridad han mejorado de manera significativa la protección de la información de los clientes y han fortalecido la posición competitiva de la empresa en el mercado de servicios de internet. Este estudio sienta las bases para una gestión proactiva y continua de la seguridad de la información en CONCRELTEC, asegurando la confianza y satisfacción de sus clientes.

4.2. Recomendaciones:

- Realizar auditorías periódicas del sistema de comunicación y resguardo de información mediante herramientas avanzadas de escaneo y análisis, como Cisco Talos Intelligence y Shodan, para detectar posibles vulnerabilidades y asegurar el cumplimiento de los estándares de seguridad. Implementar sistemas de monitoreo y registro de eventos de seguridad, como SIEM (Security Information and Event Management), para identificar cualquier actividad sospechosa o anómala en la red y tomar acciones inmediatas ante posibles intrusiones o ataques.
- Establecer un sistema de gestión de incidentes de seguridad de la información, con protocolos claros y específicos para responder de manera efectiva ante cualquier evento o brecha de seguridad. Capacitar regularmente al personal en técnicas de respuesta a incidentes y realizar ejercicios de simulación para mejorar la preparación ante situaciones de crisis. Mantener un registro detallado de cada incidente, las medidas tomadas y las lecciones aprendidas para mejorar continuamente la capacidad de respuesta.
- Definir una estructura organizativa clara en relación con la gestión de la seguridad de la información. Designar a un equipo especializado en seguridad de la información con roles y responsabilidades bien definidos, incluyendo un responsable de seguridad de la información, para coordinar y supervisar las actividades de seguridad. Implementar controles técnicos robustos, como firewalls, sistemas de prevención de intrusiones (IPS) y sistemas de detección de intrusiones (IDS), para proteger los activos de información crítica contra amenazas internas y externas.
- Desarrollar un manual de políticas de seguridad de la información que aborde de manera específica las vulnerabilidades y amenazas identificadas durante la evaluación de riesgos. El manual debe contener directrices claras y prácticas para proteger la información de los clientes, incluyendo el uso de cifrado de datos, autenticación de múltiples factores y políticas de contraseñas robustas. Asimismo, establecer políticas de acceso y control de

privilegios para garantizar que solo el personal autorizado pueda acceder a la información confidencial.

- Realizar revisiones periódicas del manual de políticas de seguridad y actualizarlo según sea necesario para reflejar los cambios en el entorno tecnológico y las mejores prácticas de seguridad. Además, llevar a cabo sesiones de capacitación y concientización de seguridad de manera regular para todo el personal de la organización, con énfasis en la importancia de la seguridad de la información y la responsabilidad individual en la protección de los activos y datos de la empresa.
- Considerar la implementación de nuevas tecnologías y soluciones de seguridad avanzadas, como sistemas de prevención y detección de amenazas basados en inteligencia artificial y aprendizaje automático. Evaluar constantemente el rendimiento y la efectividad de los controles de seguridad implementados y ajustarlos según sea necesario para mantener un nivel óptimo de protección.

BIBLIOGRAFÍA

[1] J. M. María, «Pirani,» 31 agosto 2022. [En línea]. Available: https://www.piranirisk.com/es/blog/ciberataques-empresas-en-2022#:~:text=Por%20otro%20lado%2C%20seg%C3%BAn%20Fortinet,el%20que%20hubo%2091.000%20millones.. [Último acceso: 15 01 2023].

[2] N. Cabrera, «Expansion,» Business/Finance, 2020. [En línea]. Available: https://expansion.mx/tecnologia/2015/02/17/que-sabemos-del-multimillonario-ciberasalto-bancario. [Último acceso: 15 01 2023].

[3] KASPERKY, «KASPERKY STATUS,» 2023. [En línea]. Available: https://cybermap.kaspersky.com/es/stats. [Último acceso: 20 01 2023].

[4] Iniseg, «Ciberseguridad al dia,» 2021. [En línea]. Available: https://www.iniseg.es/blog/ciberseguridad/ciberseguridad-en-america-latina-analisis-y-perspectiva/#:~:text=Algunos%20expertos%20distinguen%20tres%20debilidades,y%203)%20la%20falta%20de. [Último acceso: 15 01 2023].

[5] N. Guitierrez, «Fundamentos de ciberseguridad,» 17 02 2022. [En línea]. Available: https://preyproject.com/es/blog/30-estadisticas-seguridad-informatica. [Último acceso: 5 01 2023].

[6] M. Romo, «Concreltec,» 2023. [En línea]. Available: https://www.concreltec.net/#testimonials. [Último acceso: 15 01 2023].

[7] A. C. J. Franklin, «AUDITORÍA DE LA SEGURIDAD INFORMÁTICA SIGUIENDO LA METODOLOGÍA OPEN SOURCE SECURITY TESTING METHODOLOGY MANUAL (OSSTMM) PARA LA EMPRESA MEGAPROFER S.A.,» UTA, Ambato, 2020.

[8] L. B. L. CAROLINA, «“LABORATORIO VIRTUAL DE ANÁLISIS Y COMPORTAMIENTO DE MALWARE BASADO EN TÉCNICAS Y MÉTODOS DE SEGURIDAD INFORMÁTICA PARA LOS

LABORATORIOS EN LA FACULTAD DE SISTEMAS Y TELECOMUNICACIONES,» UNIVERSIDAD ESTATAL DE SANTA ELENA , Santa Elena, 2020.

[9] F. C. C. M. y. M. A. Liset Sulay Rodriguez Baca, «Aplicación de ISO 27001 y su influencia en la seguridad de la información de una empresa privada peruana,» *Scielo,* vol. 8, nº 5, 2020.

[10] M. E. A. Carrasco, «AUDITORÍA DE SEGURIDAD DE LA INFORMACIÓN APLICANDO LA NORMA ISO/IEC 27001 EN EL GOBIERNO AUTÓNOMO DESCENTRALIZADO SAN PEDRO DE PELILEO,» UTA, Ambato, 2021.

[11] Erick Guerra, Harol Neira, Jorge Diaz, Janns Patiño , «Desarrollo de un sistema de gestión para la seguridad de la información basado en metodología de identificación y análisis de riesgo en bibliotecas universitarias,» *Scielo, Informacion Tecnologica* , vol. 32, nº 5, 2021.

[12] D. G. M. Hernandez, «Estudio tecnico, economico y legal para la implementacion de un ISP en la zona de Quitumbe para la empresa GLOBAL TELNET,» Escuela Politecnica Nacional, Quito, 2010.

[13] «NETWORKING,» 15 junio 2023. [En línea]. Available: https://network-king.net/es/herramientas-de-supervision-de-proveedores-de-servicios-de-internet-isp/. [Último acceso: 28 junio 2023].

[14] «BANDALIBRE Comunicaciones,» 15 septiembre 2020. [En línea]. Available: https://bandalibre.es/por-que-es-importante-hacer-un-analisis-dafo-para-un-isp/. [Último acceso: 28 junio 2023].

[15] A. P. y. F. Guerrero, «Esquema de redundancia y distribucion de carga de alta disponibilidad para la prestación de telefonia IP usando SIP,» *Scielo,* 28 mayo 2009.

[16] «Estándares y guías para la digitalización,» Gob.pe, [En línea]. Available: https://guias.servicios.gob.pe/creacion-servicios-digitales/tecnologias-accesibilidad/escalabilidad. [Último acceso: 05 05 2023].

[17] «AXESS Networks,» 23 03 2023. [En línea]. Available: https://axessnet.com/que-es-un-isp-proveedor-de-servicios-de-internet/. [Último acceso: 07 05 2023].

[18] T. López, «INNEVO,» 03 02 2023. [En línea]. Available: https://blog.innevo.com/politica-de-seguridad-de-la-informacion. [Último acceso: 23 05 2023].

[19] M. Uriarte, «OMNIA,» 2020. [En línea]. Available: https://omniawfm.com/blog/call-center-que-es.php. [Último acceso: 23 05 2023].

[20] J. A. P. Hernandéz, PROYECTO DE INVERSIÓN PARA LA IMPLEMENTACIÓN DE UN ISP EN LA RIVERA DEL RÍO HONDO, México, 2016.

[21] P. A. Racines Medina, « Diseño de un ISP considerando criterios de calidad de servicio para la transmisión de voz, datos y video utilizando el estándar IEEE 802.16 (WIMAX) para cubrir el área norte de la ciudad de Quito,» Escuela Politécnica Nacional. , Quito, 2007.

[22] M. Sevillano, «ISOtols,» PLATAFORMA TECNOLÓGICA PARA LA GESTIÓN DE LA EXCELENCIA, [En línea]. Available: https://www.isotools.org/2022/11/17/ley-organica-de-proteccion-de-datos-personales-del-ecuador/. [Último acceso: 15 01 2023].

[23] I. Excellence, «Seguridad de la Información,» 1 junio 2023. [En línea]. Available: https://www.pmg-ssi.com/2023/06/riesgos-en-iso-iec-270012022/. [Último acceso: 29 junio 2023].

[24] T. López, «INNEVO,» 10 marzo 2023. [En línea]. Available: https://blog.innevo.com/evaluacion-de-riesgos-iso27001. [Último acceso: 29 06 2023].

[25] S. T. Ottati, «IMF(UNIVERSIDAD DE LOS HEMISFERIOS),» [En línea]. Available: https://globalimf.com.ec/uhemisferios/blog/gestion-de-riesgos-informaticos/. [Último acceso: 15 01 2023].

[26] D. J. A. M. Sánchez., «NORMA ISO/IEC 27001 APLICADA A UNA CARRERA UNIVERSITARIA,» Santiago de Chile, 2017.

[27] «Normas ISO,» [En línea]. Available: https://www.normas-iso.com/iso-27001/. [Último acceso: 29 junio 2023].

[28] M. Z. G. G. Navira Angulo, «PROPUESTA METODOLÓGICA DE SEGURIDAD DE INFORMACIÓN PARA PROVEEDORES DE SERVICIOS DE INTERNET EN ECUADOR,» *Revista Científica Multidisciplinaria ISSN 2528-7842,* 10 08 2018.

[29] «Introducción a la problemática de la seguridad informatica,» [En línea]. Available: http://www.spi1.nisu.org/recop/al02/charly/tema1.html#:~:text=Contramedida%3A%20T%C3%A9cnicas%20de%20protecci%C3%B3n%20especificas%20contra%20amenazas.&text=contramedidas.,las%20contramedidas%20eliminan%20las%20amenazas.&text=F%C3%ADsica%3A%20Acciones%20f. [Último acceso: 15 01 2023].

[30] P. Dirección General de Modernización Administrativa, MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información., Madrid: Ministerio de Hacienda y Administraciones Públicas, 2012.

[31] L. N. &. Ruiz, «SGSI Blog especializado en Sistemas de Gestión de,» Excellence, I, 28 julio 2015. [En línea]. Available: https://www.pmgssi.com/2015/07/que-es-sgsi/. [Último acceso: 25 01 2023].

[32] D. O. P. SOLANO, «ANÁLISIS DE VULNERABILIDADES Y ACCIONES CORRECTIVAS SOBRE UN SISTEMA WEB,» ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL, Guayaquil, 2017.

[33] M. G. P. Cuenca, «Modelo de Gestión de Seguridad de la Información para la Universidad Nacional de Loja basado en la norma ISO/IEC 27001,» Loja, 2015.

[34] FORTRA COMPANY, «FORTRA Help Systems,» HelpSystems, 25 07 2022. [En línea]. Available: https://www.fortra.com/es/blog/escaneo-vulnerabilidades. [Último acceso: 17 05 2023].

[35] R. Altuve, «OpenWebinars,» 11 05 2021. [En línea]. Available: https://openwebinars.net/blog/kali-linux-que-es-y-caracteristicas-principales/. [Último acceso: 17 05 2023].

[36] F. Rodriguez, «Keepcoding,» 06 01 2023. [En línea]. Available: https://keepcoding.io/blog/que-es-kali-linux/. [Último acceso: 17 05 2023].

[37] GB Advisors, «GB advisors,» 19 03 2019. [En línea]. Available: https://www.gb-advisors.com/es/herramientas-de-seguridad-informatica-tenable-vs-rapid7/. [Último acceso: 17 05 2023].

[38] Keepcoding Tech School, «Keepcoding,» Tech School, 12 01 2023. [En línea]. Available: https://keepcoding.io/blog/que-es-nessus/#Que_es_Nessus_y_para_que_sirve. [Último acceso: 17 05 2023].

[39] A. P, «SEGURIDAD INFORMÁTICA,» [En línea]. Available: http://books.google.com.ec/books?id=Mgvm3AYIT64C&lpg=PP1&hl=es&pg=PP1#v=onepage&q&f=false. [Último acceso: 15 01 2023].

[40] S. G. d. ISO, «Organismos Nacionales de Normalización en Países en,» 2010. [En línea]. Available: http://www.iso.org/iso/fast_forwardes.pdf. [Último acceso: 25 01 2023].

[41] M. A. O. TOLEDO, «ELABORACION DE UNA GUIA DE IMPLEMENTACION DE UN SGSI PARA LA CORPORACION

ECUATORIANA PARA EL DESARROLLO DE LA INVESTIGACION Y LA ACADEMIA - CEDIA,» CUENCA, 2022.

[42] «Escuela Europea de la excelencia,» 13 11 2019. [En línea]. Available: https://www.escuelaeuropeaexcelencia.com/2019/11/listado-de-amenazas-y-vulnerabilidades-en-iso-27001/. [Último acceso: 25 01 2023].

[43] J. E. A. CHANG, «ANÁLISIS DE ATAQUES CIBERNÉTICOS HACIA EL ECUADOR,» *Revista Científica Aristas.* , pp. 18-34, 2020.

[44] «LEY ORGANICA DE PROTECCION DE DATOS PERSONALES,» Quito, 2021.

[45] G. Disterer, «ISO/IEC 27001:2013 Scientific Reserch and academic publisher,» Department of Business Administration and Computer Science, University of Applied Sciences and Arts, Hannover, Germany., 2019. [En línea]. Available: https://www.scirp.org/journal/paperinformation.aspx?paperid=30059. [Último acceso: 13 05 2023].

[46] «ARCOTEL,» [En línea]. Available: https://www.arcotel.gob.ec/. [Último acceso: 22 06 2023].

[47] Tenable, «Nessus,» 2023. [En línea]. Available: https://es-la.tenable.com/products/nessus. [Último acceso: 13 05 2023].

[48] Cisco Talos Intelligence, «Cisco Talos Intelligence,» Cisco Systems, Inc. and/or its affiliates, 2023. [En línea]. Available: https://www.talosintelligence.com/. [Último acceso: 13 05 2023].

[49] «BANDALIBRE Comunicaciones,» 11 02 2020. [En línea]. Available: https://bandalibre.es/conoce-todos-los-problemas-que-resuelves-con-un-servicio-de-soporte-tecnico-avanzado-para-isps/. [Último acceso: 22 05 2023].

ANEXOS

ANEXO 1: Manual de políticas de seguridad en la empresa CONCRELTEC.

Manual de Políticas de Seguridad de la Información

Versión: 1.0

Autor: William Hidalgo

Revisado por: Ing. Mauricio Romo.

Fecha de Publicación: 10/07/2023

ÍNDICE

1. Introducción

El Manual de Políticas de Seguridad de la Información tiene como objetivo establecer los lineamientos y procedimientos necesarios para garantizar la integridad, confidencialidad y disponibilidad de la información en Concreltec. Este manual define las políticas y medidas de seguridad que deben seguirse por todo el personal de la organización.

2. Objetivos del Manual

- Establecer un marco de referencia para la gestión de la seguridad de la información.
- Identificar y abordar las vulnerabilidades y amenazas existentes en los activos de la empresa.
- Definir las medidas de remediación y las buenas prácticas para mitigar los riesgos identificados.
- Promover una cultura de seguridad de la información entre los empleados y contratistas.
- Cumplir con los requisitos legales y reglamentarios relacionados con la seguridad de la información.

3. Alcance

Este manual se aplica a todos los empleados, contratistas y terceros que interactúan con los activos de información de Concreltec. Es responsabilidad de todos los usuarios cumplir con las políticas y procedimientos establecidos en este manual.

4. Responsabilidades

- La alta dirección tiene la responsabilidad de establecer una cultura de seguridad de la información y asignar recursos adecuados para implementar las políticas y medidas de seguridad.

- El Equipo de Seguridad de la Información será responsable de monitorear y evaluar continuamente los riesgos y vulnerabilidades, así como de implementar las medidas de remediación adecuadas.

- Todos los empleados y contratistas son responsables de seguir las políticas y procedimientos establecidos en este manual y de informar cualquier incidente de seguridad de la información.

5. Políticas de Seguridad de la Información

En esta sección, se detallarán las políticas y medidas de seguridad específicas basadas en las vulnerabilidades detectadas en los activos de la empresa. A continuación, se presenta un resumen de las políticas relacionadas con las vulnerabilidades mencionadas:

Política 1: Infraestructura en la Nube

- Descripción: Se debe utilizar la infraestructura de servicios en la nube para garantizar la disponibilidad de los activos de información en caso de eventos naturales.

- Área de Aplicación: Servidores DNS - DATOS (10.11.102.7)

- Impacto: Alto

- Remediación: Implementar servicios en la nube para garantizar la continuidad del servicio en caso de eventos naturales.

Esta política tiene como objetivo garantizar la disponibilidad y seguridad de la información mediante la utilización de servicios en la nube. Se recomienda migrar los activos críticos, como el Servidor DNS, a una infraestructura en la nube para mitigar los riesgos asociados a eventos naturales, como incendios, sismos y desbordamientos de agua.

Política 2: Restricción de Búsqueda Recursiva en el Servidor DNS

- Descripción: Se deben limitar o restringir las solicitudes de búsqueda recursiva en el servidor DNS para prevenir interrupciones en el servicio.

- Área de Aplicación: Servidores DNS - DATOS (10.11.102.7)
- Impacto: Alto
- Remediación: Establecer una lista de permisos para limitar el procesamiento de solicitudes de búsqueda recursiva.

Esta política tiene como objetivo proteger el Servidor DNS de posibles interrupciones en el servicio causadas por solicitudes de búsqueda recursiva. Se recomienda limitar o restringir el procesamiento de estas solicitudes mediante el uso de una lista de permisos.

Política 3: Protección ante Eventos Naturales

- Descripción: Esta política tiene como objetivo proteger los activos de la empresa contra eventos naturales como incendios, sismos y desbordamientos de agua.
- Procedimiento de Seguridad:
    - Realizar una evaluación de riesgos y establecer medidas preventivas específicas para cada tipo de evento natural.
    - Implementar sistemas de detección temprana de incendios y sistemas de extinción automática.
    - Realizar copias de seguridad regulares de los datos y almacenarlas en un lugar seguro fuera del sitio.
    - Establecer un plan de contingencia y recuperación ante desastres.

Política 4: Control de Acceso a DNS

- Descripción: Esta política tiene como objetivo proteger el servidor DNS contra interrupciones y solicitudes de búsqueda no autorizadas.
- Procedimiento de Seguridad:

- Limitar o restringir el procesamiento de solicitudes de búsqueda recursiva mediante el uso de una lista de permisos.
- Configurar correctamente las reglas de firewall para controlar el acceso al servidor DNS.
- Implementar sistemas de detección de intrusos y monitoreo de actividad sospechosa en el servidor DNS.

Política 5: Acceso Remoto a la Base de Datos

- Descripción: Esta política tiene como objetivo proteger el acceso remoto a la base de datos SQL del servidor DNS.
- Procedimiento de Seguridad:
  - Isolar el servicio de Base de Datos de la zona de Demilitarización (DMZ) para limitar el acceso remoto.
  - Establecer políticas de autenticación fuertes y restricciones de acceso basadas en roles.
  - Monitorear y auditar los accesos remotos a la base de datos para detectar actividades sospechosas.

Política 6: Respaldo de Energía para el Servidor DNS

- Descripción: Esta política tiene como objetivo garantizar la disponibilidad del servidor DNS durante interrupciones del suministro eléctrico.
- Procedimiento de Seguridad:
  - Adquirir un generador o UPS (sistema de alimentación ininterrumpida) para respaldar el suministro eléctrico del servidor DNS.
  - Realizar pruebas periódicas del generador o UPS para asegurar su correcto funcionamiento.

- Establecer un plan de contingencia para la gestión de energía durante cortes prolongados.

Política 7: Certificados de Servidor

- Descripción: Esta política tiene como objetivo garantizar la validez de los certificados utilizados por el servidor DNS.
- Procedimiento de Seguridad:
    - Establecer un proceso de seguimiento y renovación regular de los certificados del servidor.
    - Implementar un sistema de alertas para notificar sobre la expiración inminente de los certificados.
    - Mantener un registro actualizado de los certificados utilizados y sus fechas de vencimiento.

Política 8: Actualización de PHP en el Servidor Proxy

- Descripción: Esta política tiene como objetivo mantener la versión de PHP actualizada en el servidor proxy.
- Procedimiento de Seguridad:
    - Realizar la actualización de la versión actual de PHP (5.3.25) a una versión recomendada igual o superior a 7.
    - Establecer un proceso periódico de monitoreo y actualización de las versiones de software utilizadas.

Política 9: Prevención de Ataques de Denegación de Servicio en el Servidor Proxy

- Descripción: Esta política tiene como objetivo prevenir los ataques de denegación de servicio en el servidor proxy.
- Procedimiento de Seguridad:

- Implementar medidas de protección contra ataques de denegación de servicio, como el filtrado de tráfico sospechoso y la limitación de conexiones simultáneas.
- Actualizar regularmente las soluciones de seguridad y aplicar los parches correspondientes.
- Monitorear de forma proactiva el tráfico de red y utilizar sistemas de detección de intrusos para identificar posibles ataques.

Política 10: Protección ante Eventos Naturales para el Router de Borde

- Descripción: Esta política tiene como objetivo proteger el router de borde contra eventos naturales como incendios, sismosy desbordamientos de agua.
- Procedimiento de Seguridad:
  - Realizar una evaluación de riesgos específica para el router de borde y establecer medidas preventivas para cada evento natural identificado.
  - Implementar sistemas de detección temprana de incendios y sistemas de extinción automática cerca del router de borde.
  - Garantizar que el router de borde esté ubicado en un área segura y protegida de posibles inundaciones.
  - Realizar copias de seguridad regulares de la configuración del router y almacenarlas en un lugar seguro fuera del sitio.

Política 11: Respaldo de Energía para el Router de Borde

- **Descripción**: Esta política tiene como objetivo garantizar la disponibilidad del router de borde durante interrupciones del suministro eléctrico.
- Procedimiento de Seguridad:

- Adquirir un generador o UPS (sistema de alimentación ininterrumpida) para respaldar el suministro eléctrico del router de borde.
- Realizar pruebas periódicas del generador o UPS para asegurar su correcto funcionamiento.
- Establecer un plan de contingencia para la gestión de energía durante cortes prolongados.

Política 12: Control de Acceso para el Personal Técnico

- Descripción: Esta política tiene como objetivo prevenir el escape de información confidencial por parte del personal técnico.
- Procedimiento de Seguridad:
  - Establecer una política de eliminación y cambio regular de claves de acceso para salvaguardar la información en caso de despidos repentinos.
  - Revocar los accesos y credenciales de los empleados dados de baja de la empresa de manera oportuna.
  - Realizar sesiones de capacitación y concientización sobre la importancia de la confidencialidad de la información y las consecuencias del incumplimiento.

Política 13: Certificación del Cableado

- Descripción: Esta política tiene como objetivo garantizar que el cableado utilizado cumpla con los estándares de certificación correspondientes.
- Procedimiento de Seguridad:
  - Verificar y asegurar que todo el cableado utilizado esté certificado y cumpla con los estándares necesarios.

- Realizar inspecciones periódicas del cableado para detectar posibles fallas o deterioro.
- Mantener registros actualizados de las certificaciones del cableado utilizado.

Política 14: Protección Física para los Equipos de Red

- Descripción: Esta política tiene como objetivo proteger físicamente los equipos de red contra acceso no autorizado y daños.
- Procedimiento de Seguridad:
    - Crear un ambiente físico designado específicamente para la ubicación y protección de los equipos de red.
    - Implementar sistemas de control de acceso físico, como cerraduras, tarjetas de acceso y cámaras de seguridad.
    - Establecer políticas de seguridad que regulen el acceso y la manipulación de los equipos de red por parte del personal autorizado.

Este manual de políticas de seguridad proporciona un marco de referencia para asegurar la integridad, confidencialidad y disponibilidad de la información en base a las vulnerabilidades detectadas. Cada política incluye los procedimientos detallados que se deben seguir para implementar las medidas de seguridad correspondientes.

ANEXOS DEL MANUAL

Glosario de Términos

Este anexo contiene una lista de términos y definiciones utilizados en el manual. El glosario proporciona una referencia rápida y clara para asegurar que todos los lectores comprendan el significado de los términos técnicos y de seguridad utilizados en el contexto del manual.

Ejemplo de términos incluidos en el glosario:

1. Amenaza: Cualquier evento o circunstancia que tiene el potencial de causar daño a los activos de información.
2. Vulnerabilidad: Una debilidad en un sistema o proceso que podría ser explotada por una amenaza para comprometer la seguridad de la información.
3. Remediación: Acción tomada para eliminar o mitigar una vulnerabilidad o riesgo de seguridad.
4. Política de seguridad de la información: Conjunto de principios y directrices establecidos por una organización para proteger la confidencialidad, integridad y disponibilidad de la información.

Referencias y Recursos Adicionales

Este anexo proporciona una lista de referencias y recursos adicionales que pueden ser útiles para aquellos que deseen obtener más información sobre la seguridad de la información y las mejores prácticas relacionadas. Incluye enlaces a estándares de seguridad, sitios web, libros recomendados y otras fuentes de información relevante.

Ejemplo de recursos adicionales incluidos en el anexo:

1. ISO/IEC 27001: Norma internacional que establece los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información.

2. OWASP (Open Web Application Security Project): Organización dedicada a mejorar la seguridad de las aplicaciones web mediante el suministro de herramientas, documentación y recursos.

3. Libro recomendado: "The Art of Information Security" por Kevin D. Mitnick.

ANEXO 2: Guía TLP.

El Protocolo TLP (Traffic Light Protocol), también conocido como "Protocolo de semáforos", es una guía de uso comúnmente utilizada para clasificar y compartir información sensible relacionada con la seguridad cibernética. El TLP se utiliza para asegurar que la información se comparta de manera adecuada y controlada entre diferentes organizaciones y equipos de seguridad.

El Protocolo TLP clasifica la información en cuatro niveles o colores, cada uno de los cuales representa un nivel de restricción diferente:

1. TLP: ROJO (Red): La información marcada con este nivel está restringida y solo puede ser compartida con personas y equipos específicos que estén directamente involucrados en la respuesta a incidentes o en la solución del problema. No debe compartirse fuera de ese grupo cerrado de personas.

2. TLP: AMARILLO (Yellow): La información marcada con este nivel es sensible y está destinada a un público limitado. Puede ser compartida con socios de confianza que tengan la necesidad de conocerla, pero debe evitarse su distribución más amplia.

3. TLP: VERDE (Green): La información marcada con este nivel es ampliamente difundible y puede compartirse de manera abierta dentro de la comunidad de seguridad. Sin embargo, aún se deben tomar precauciones para evitar su distribución pública generalizada.

4. TLP: BLANCO (White): La información marcada con este nivel no está sujeta a restricciones y puede compartirse libremente con cualquier persona o grupo, incluso fuera de la comunidad de seguridad.

El Protocolo TLP es una herramienta valiosa para asegurar que la información sensible relacionada con la seguridad se comparta de manera responsable y controlada, ayudando así a mejorar la cooperación y la colaboración entre diferentes entidades para proteger mejor los sistemas y datos contra amenazas cibernéticas [46].

AGENCIA DE REGULACIÓN Y CONTROL DE LAS TELECOMUNICACIONES

EL GOBIERNO DE TODOS

Libre difusión. Sujeto a las normas de protección intelectual, puede distribuirse sin restricciones.

GUÍA DE USO DEL PROTOCOLO TLP

TLP (Traffic Light Protocol o Protocolo de Semáforos)

Es un protocolo de comunicación que proporciona un esquema simple e intuitivo, para que quien origina la información, indique cuándo y cómo se puede compartir información sensible y confidencial; y, cuán ampliamente quiere que su información se distribuya más allá del destinatario inmediato.

Está diseñado para mejorar el flujo de información entre individuos, organizaciones o comunidades de forma controlada y confiable. Es importante entender y respetar las reglas del protocolo, ya que sólo entonces se puede establecer la confianza entre los involucrados.

El TLP se basa en el concepto de etiquetado, con el cual quien comparte la información, utiliza uno de los cuatro (4) colores definidos por este protocolo, para indicar el alcance de la difusión que el destinatario deberá dar a la información. La información de etiquetado consiste simplemente en agregar "TLP: COLOR" a un documento o parte de él.

A continuación se detalla los cuatro (4) colores utilizados en este protocolo:

Color	¿Cuándo utilizar?	¿Cómo debe ser compartida la información?	Ejemplo
TLP:ROJO	DIFUSIÓN RESTRINGIDA Cuando la información está limitada a personas concretas, debido a que su difusión a terceras personas podría tener un impacto en la privacidad, reputación u operaciones si es mal utilizada.	Los destinatarios no pueden compartir información de TLP: ROJO con nadie fuera del intercambio, reunión o conversación específica en la que se reveló originalmente. En caso de que se necesite dar a conocer a otra persona se deberá pedir autorización al emisor de la información. En la mayoría de los casos, TLP:ROJO debe intercambiarse de manera verbal o en persona. Los destinatarios no pueden compartir información con nadie, incluso en un nivel jerárquico superior.	1. Información compartida en una reunión o conversación. 2. Correo electrónico directo. (Con etiqueta TLP:ROJO)

Página 1 de 3

Figura 1.Guía de uso del protocolo TLP-1 *[46]*

Elaborado por: El investigador

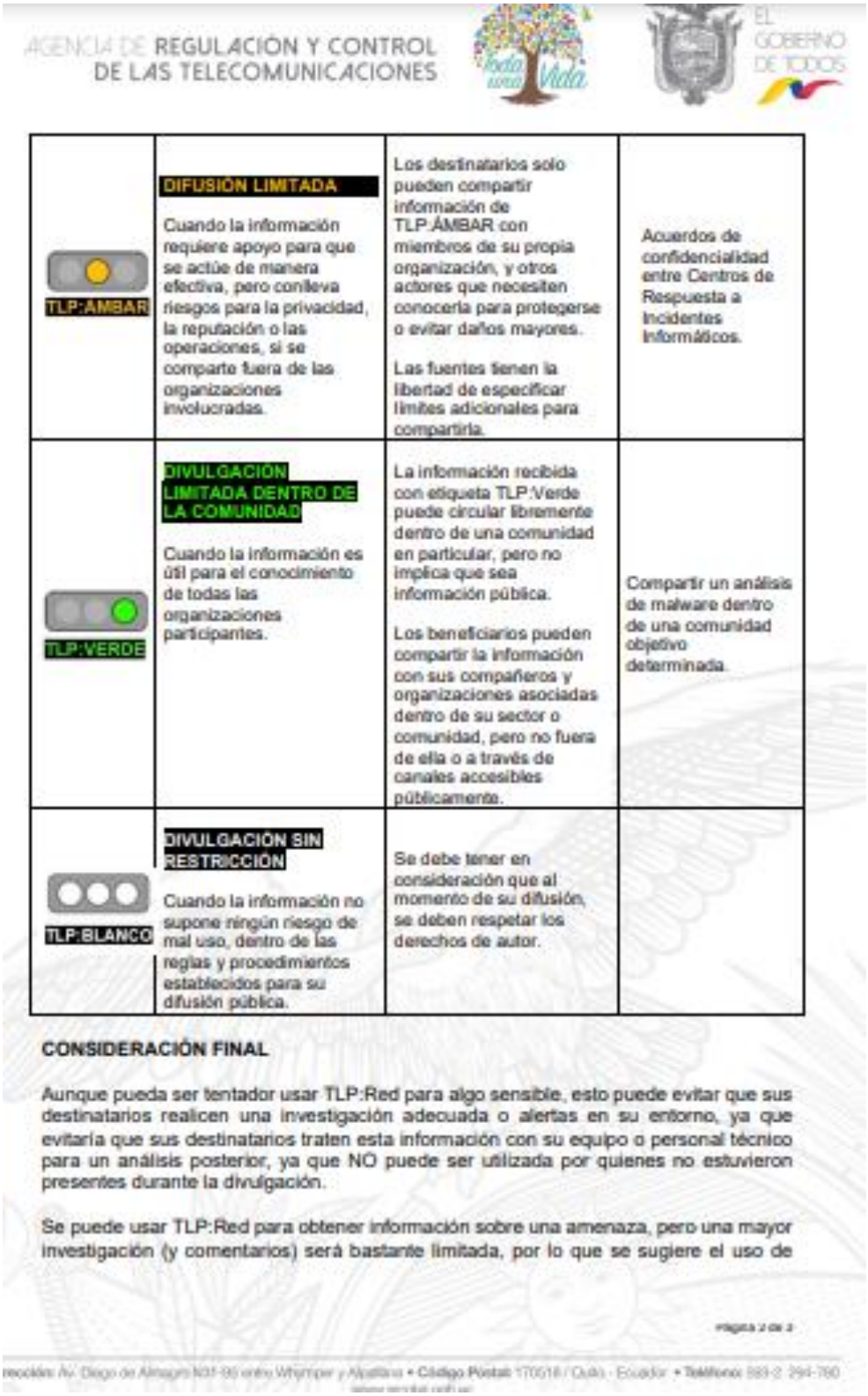


Figura 2.Guía de uso del protocolo TLP-2 *[46]*

Elaborado por: El investigador

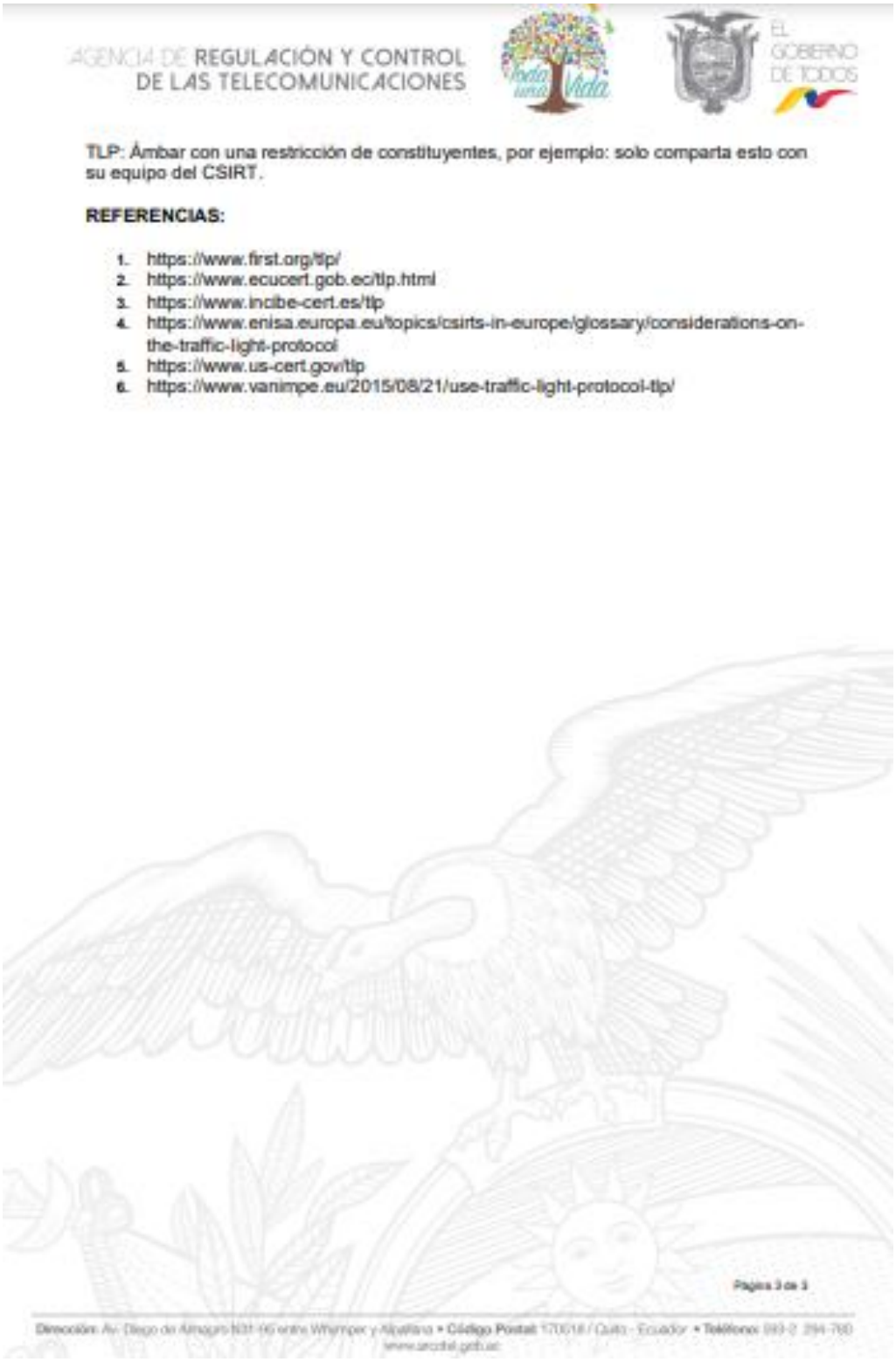


Figura 3.Guía de uso del protocolo TLP-3. *[46]*

Elaborado por: El investigador

ANEXO 3: Administración y configuración de software

Rapid7:

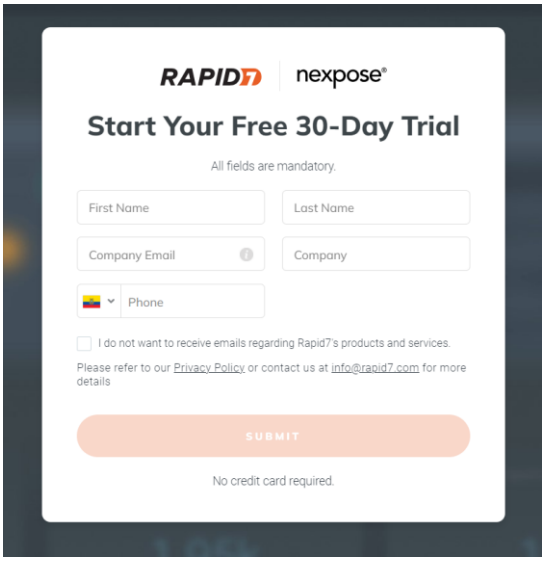


Figura 4. Página Inicial para ingreso de datos en rapid7

Elaborado por: El investigador

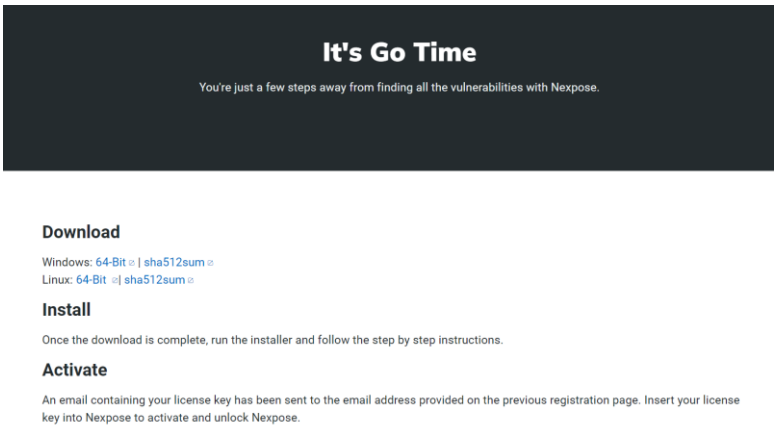


Figura 5. Descarga de Rapid 7 de acuerdo al sistema operativo

Elaborado por: El investigador

Figura 6. Instalación paso 1 de Rapid 7

Elaborado por: El investigador

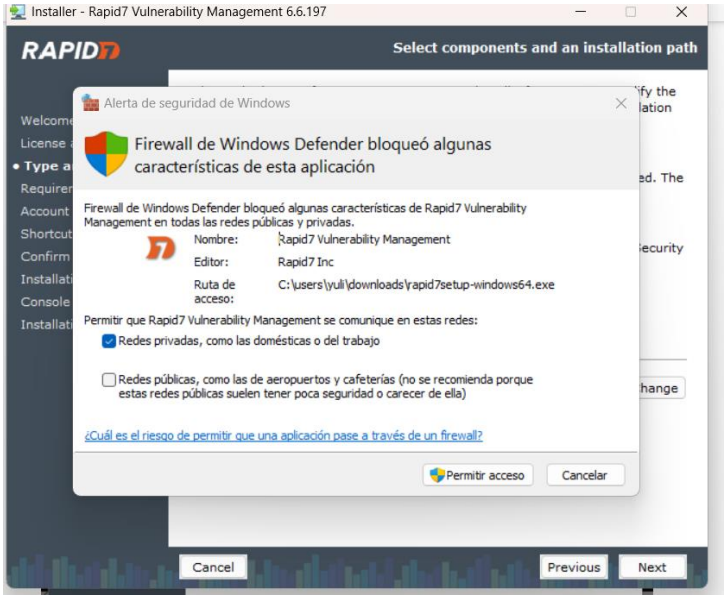


Figura 7. Instalación paso 2 de Rapid7

Elaborado por: El investigador

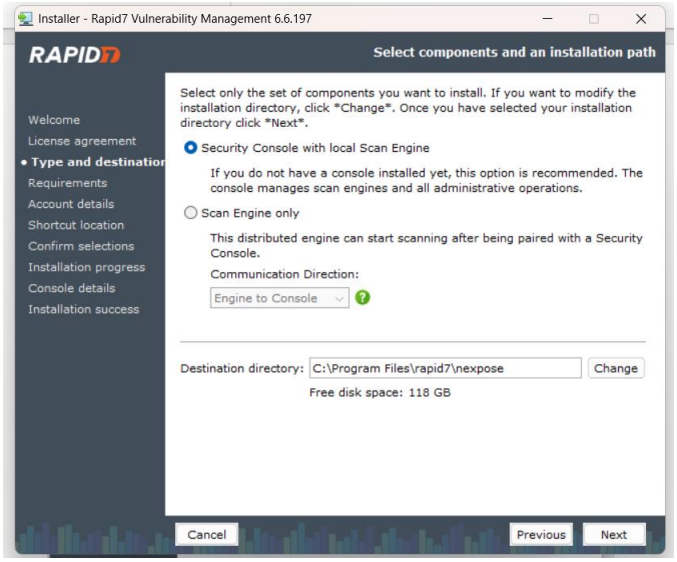


Figura 8. Instalación paso 3 de Rapid7

Elaborado por: El investigador

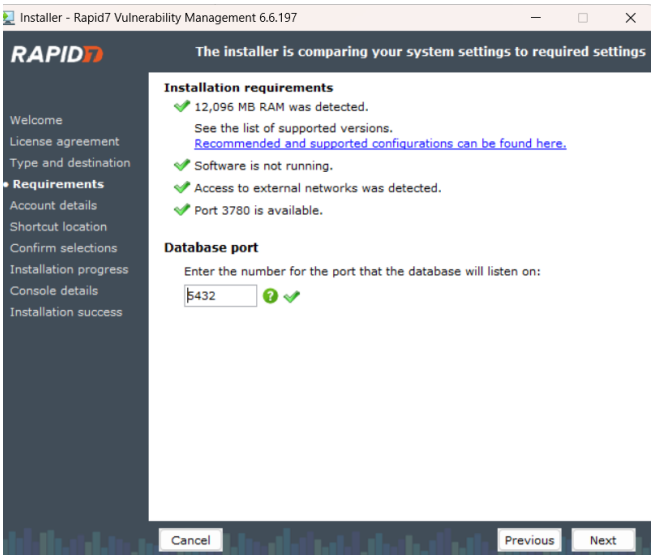


Figura 9. Instalación paso 4 de Rapid7

Elaborado por: El investigador

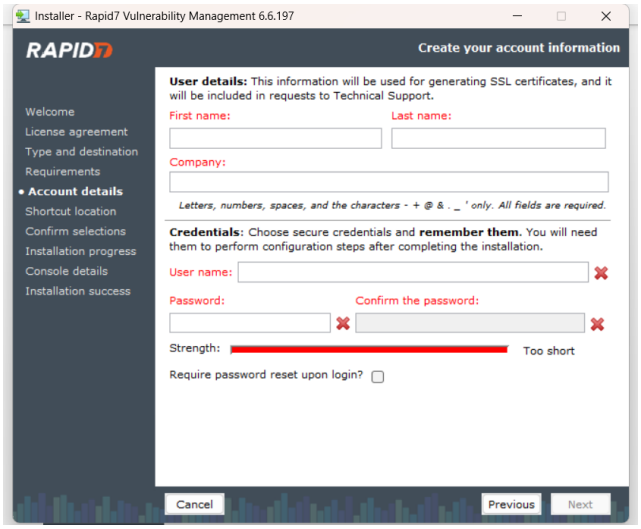


Figura 10. Ingreso de datos en Rapid7

Elaborado por: El investigador

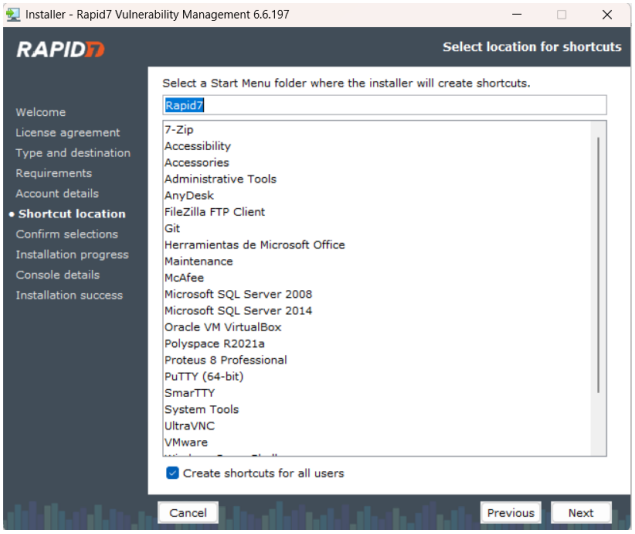


Figura 11. Selección de ubicación de Rapid7

Elaborado por: El investigador

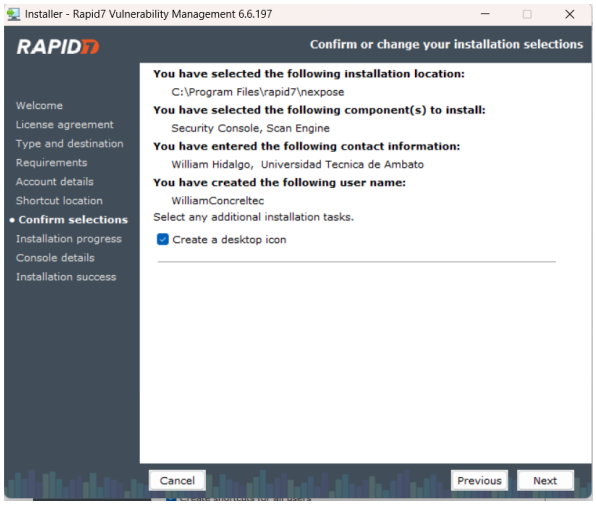


Figura 12. Confirmación de selecciones en Rapid7

Elaborado por: El investigador

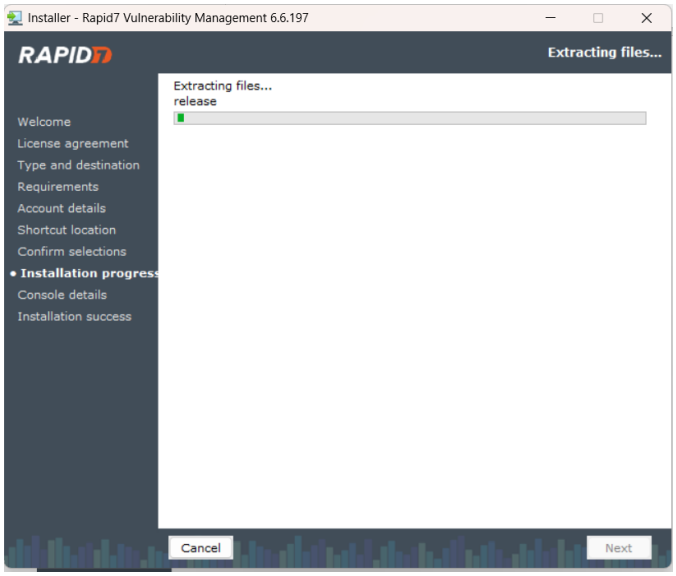


Figura 13. Instalación de Rapid7 paso final

Elaborado por: El investigador

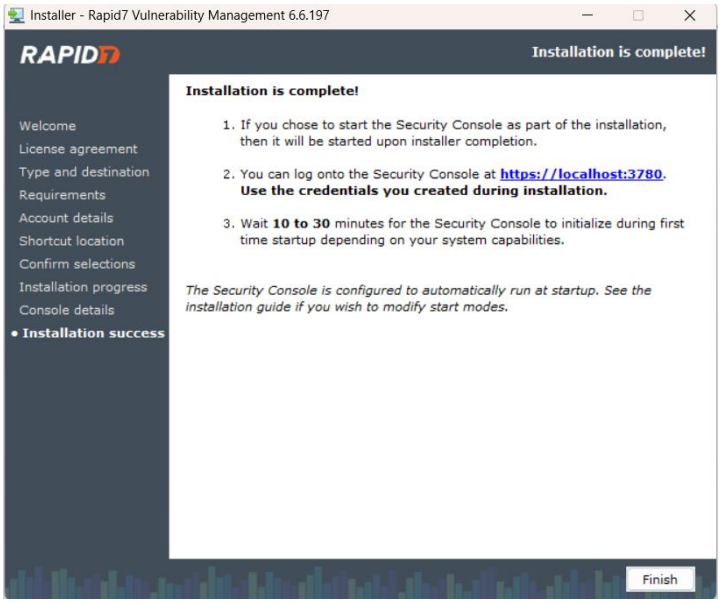


Figura 14. Instalación Completa de Rapid7

Elaborado por: El investigador

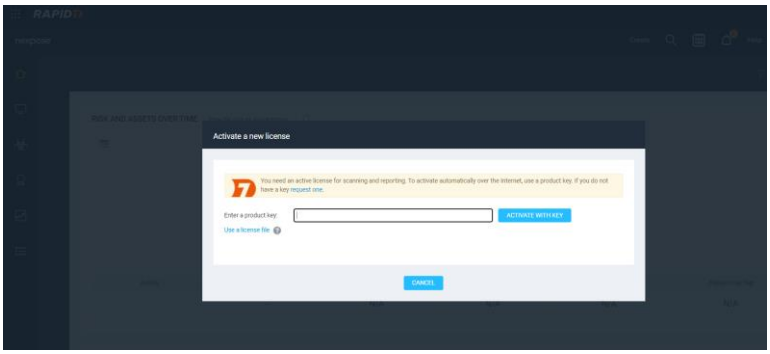


Figura 15. Ingreso de clave de activación

Elaborado por: El investigador

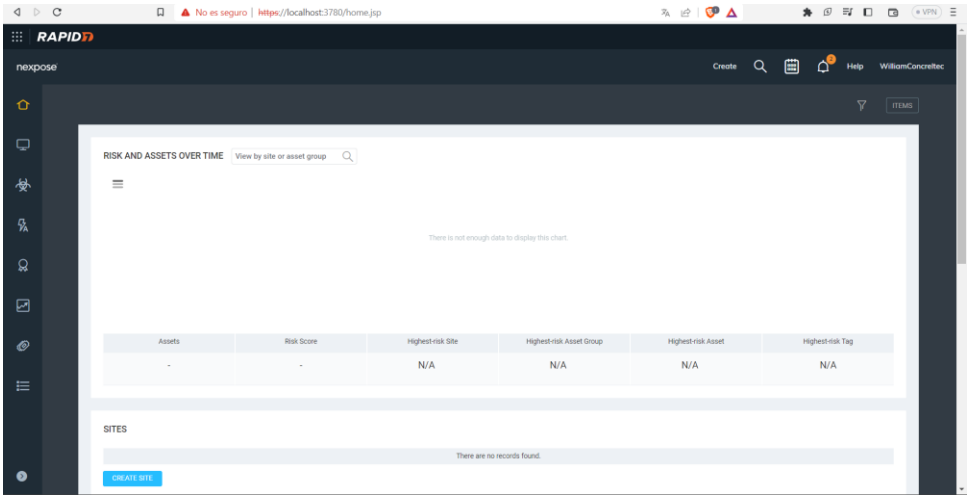


Figura 16. Interfaz de usuario de rapid7

Elaborado por: El investigador

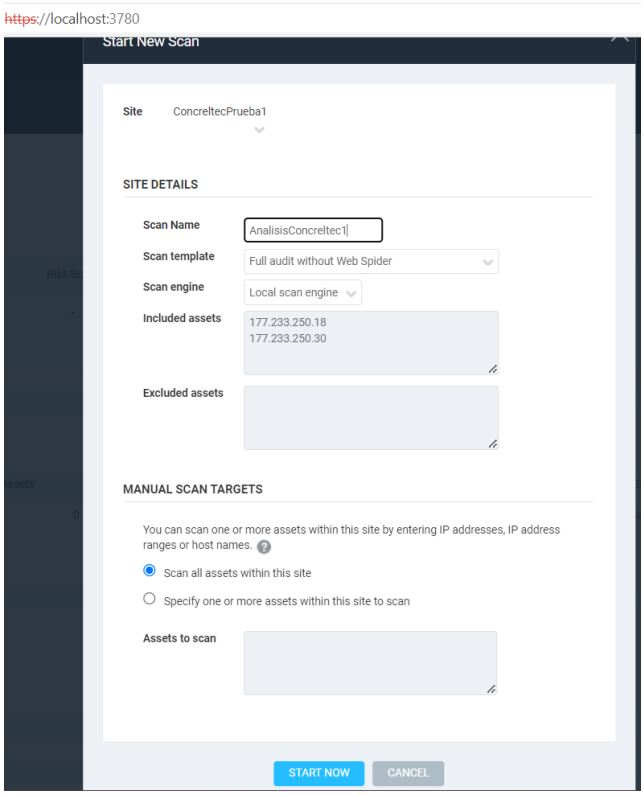


Figura 17. Ejemplo de cómo realizar un análisis en rapid7

Elaborado por: El investigador

NESSUS

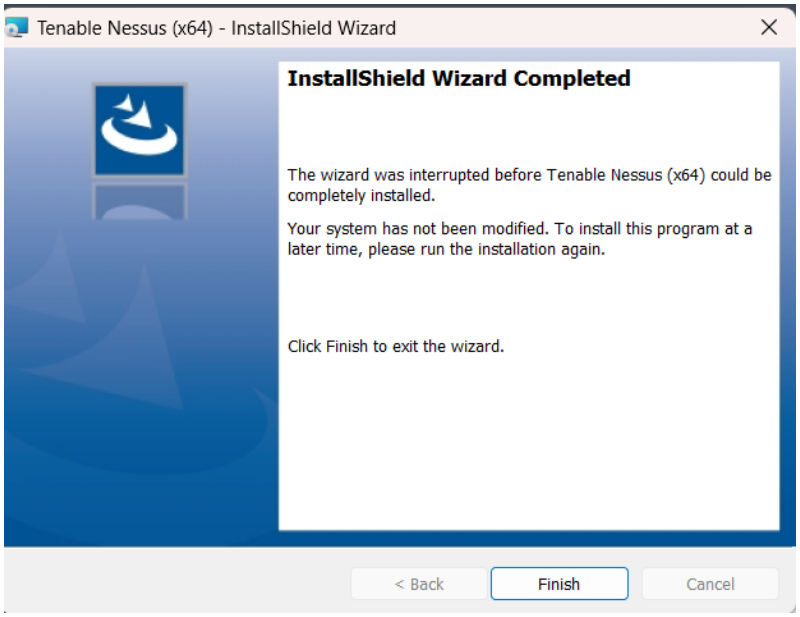


Figura 18. Paso final para la instalación de nessus

Elaborado por: El investigador

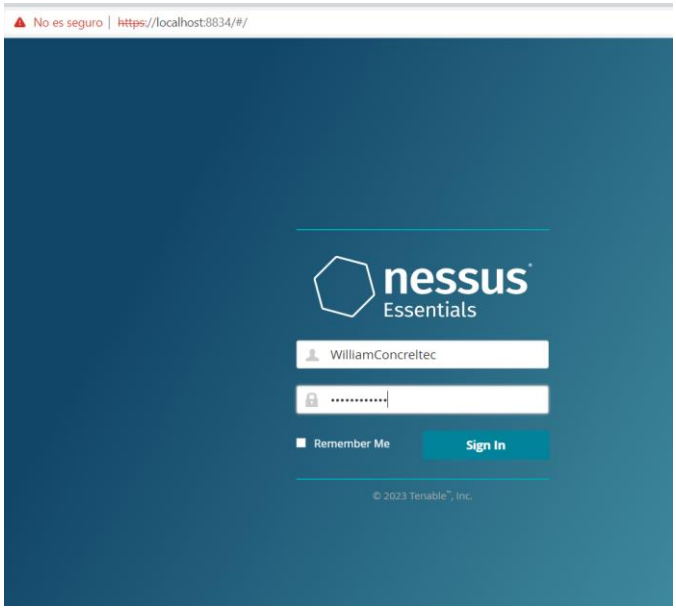


Figura 19. Inicio de sesión en nessus

Elaborado por: El investigador

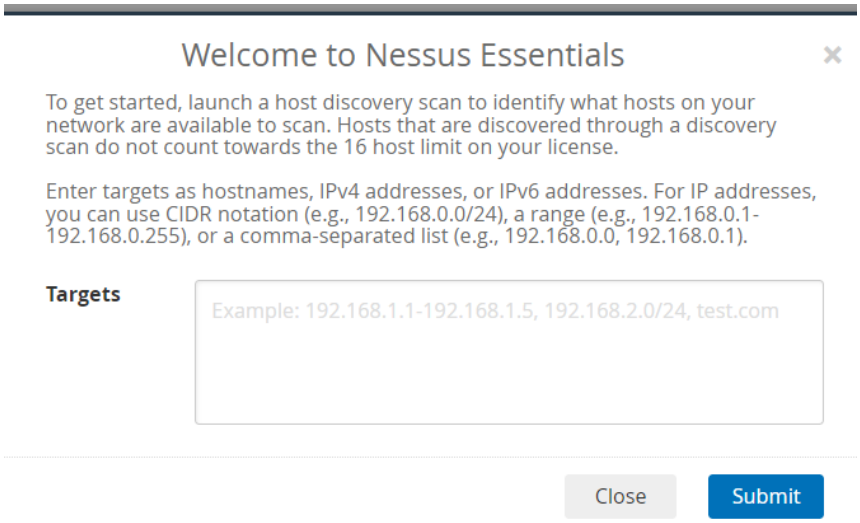


Figura 20. Interfaz inicial de nessus

Elaborado por: El investigador

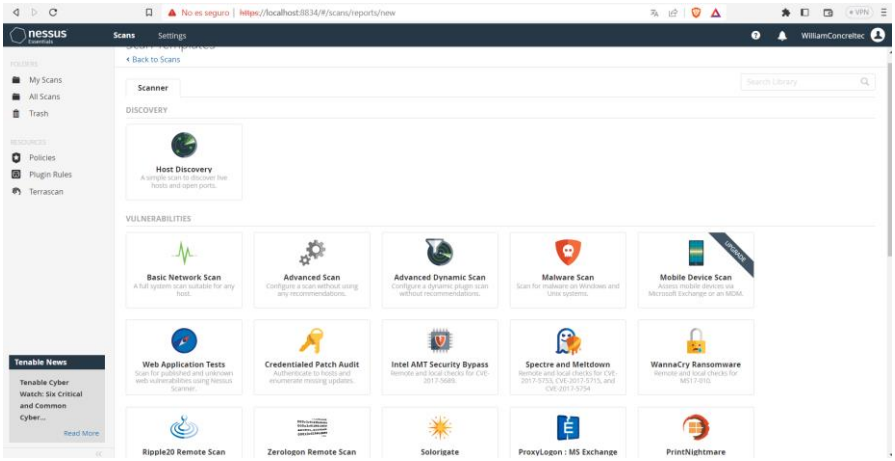


Figura 21. Página principal de nessus

Elaborado por: El investigador

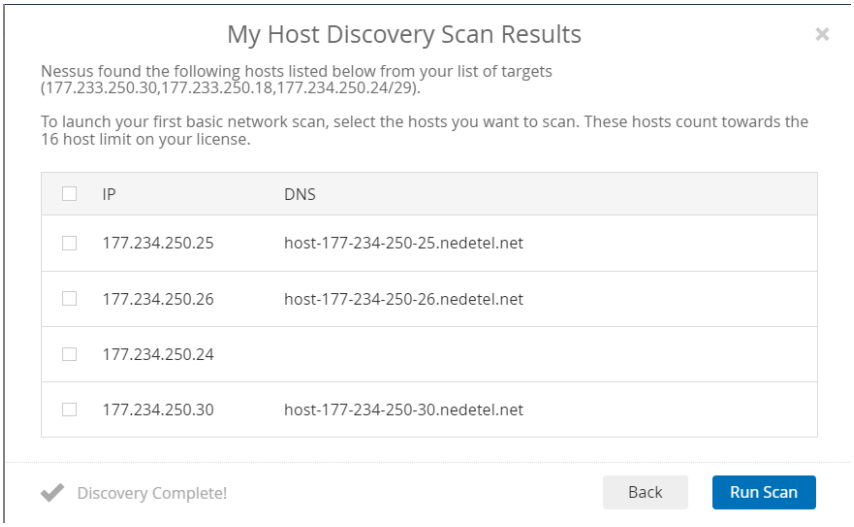


Figura 22. Escaneo inicial

Elaborado por: El investigador

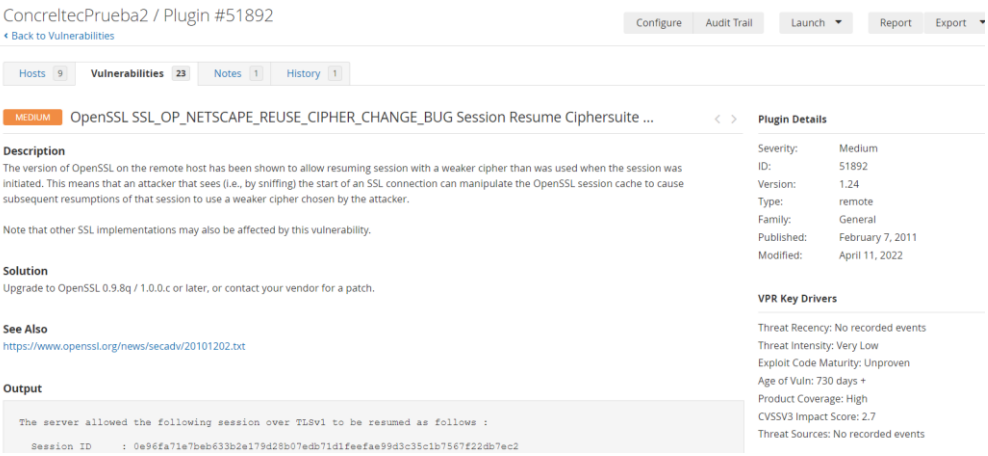
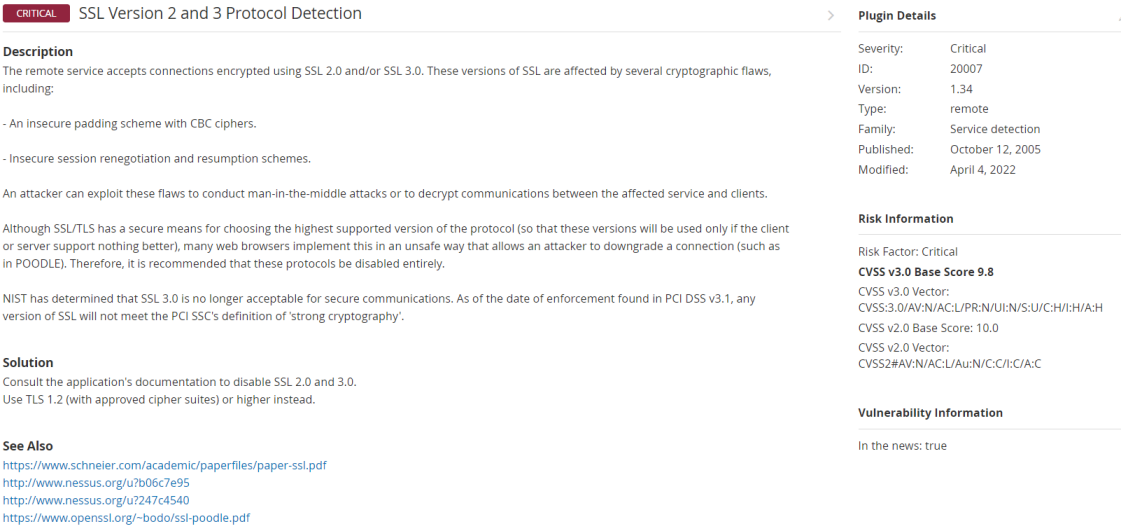


Figura 23. Ejemplo de vulnerabilidad detectada

Elaborado por: El investigador



CRITICAL SSL Version 2 and 3 Protocol Detection

Description
The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.

- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

Solution
Consult the application's documentation to disable SSL 2.0 and 3.0.
Use TLS 1.2 (with approved cipher suites) or higher instead.

See Also
https://www.schneier.com/academic/paperfiles/paper-ssl.pdf
http://www.nessus.org/u?b06c7e95
http://www.nessus.org/u?247c4540
https://www.openssl.org/~bodo/ssl-poodle.pdf

Plugin Details

Severity:	Critical
ID:	20007
Version:	1.34
Type:	remote
Family:	Service detection
Published:	October 12, 2005
Modified:	April 4, 2022

Risk Information

Risk Factor: Critical
CVSS v3.0 Base Score 9.8
CVSS v3.0 Vector:
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS v2.0 Base Score: 10.0
CVSS v2.0 Vector:
CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Vulnerability Information

In the news: true

Figura 24. Ejemplo de vulnerabilidad detectada

Elaborado por: El investigador

10.11.100.6

0	0	2	0	14
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS v3.0	VPR Score	Plugin	Name
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	42263	Unencrypted Telnet Server
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	84502	HSTS Missing From HTTPS Server
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	10919	Open Port Re-check
INFO	N/A	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	10863	SSL Certificate Information
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	10281	Telnet Server Detection
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	10386	Web Server No 404 Error Code Check

* indicates the v3.0 score was not available;
the v2.0 score is shown

Figura 25. Reporte de vulnerabilidad detectada en nessus activo 10.11.100.6

Elaborado por: El investigador

10.11.100.7

1	1	6	0	20
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS v3.0	VPR Score	Plugin	Name
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
HIGH	7.5	6.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	6.8	5.3	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	157288	TLS Version 1.1 Protocol Deprecated
MEDIUM	5.9	3.6	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	4.3*	2.7	51892	OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	84502	HSTS Missing From HTTPS Server
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	10919	Open Port Re-check
INFO	N/A	-	66334	Patch Report
INFO	N/A	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	10863	SSL Certificate Information
INFO	N/A	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	58768	SSL Resume With Different Cipher Issue

Figura 26. Reporte de vulnerabilidad detectada en nessus activo 10.11.100.7

Elaborado por: El investigador

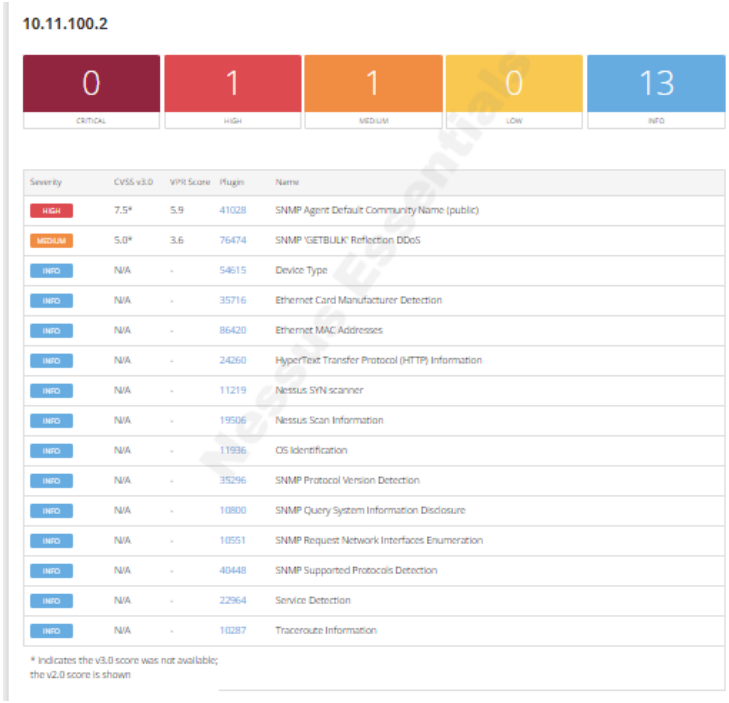


Figura 27. Reporte de vulnerabilidad detectada en nessus activo 10.11.100.2

Elaborado por: El investigador

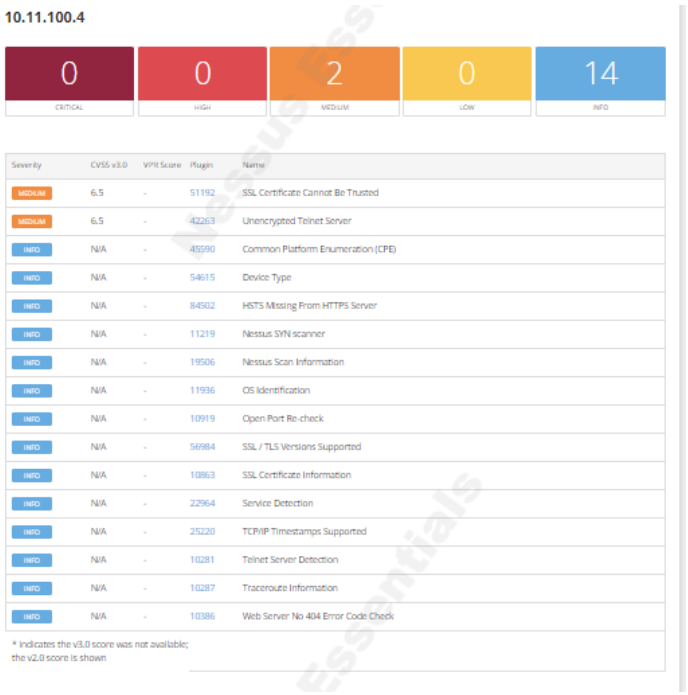
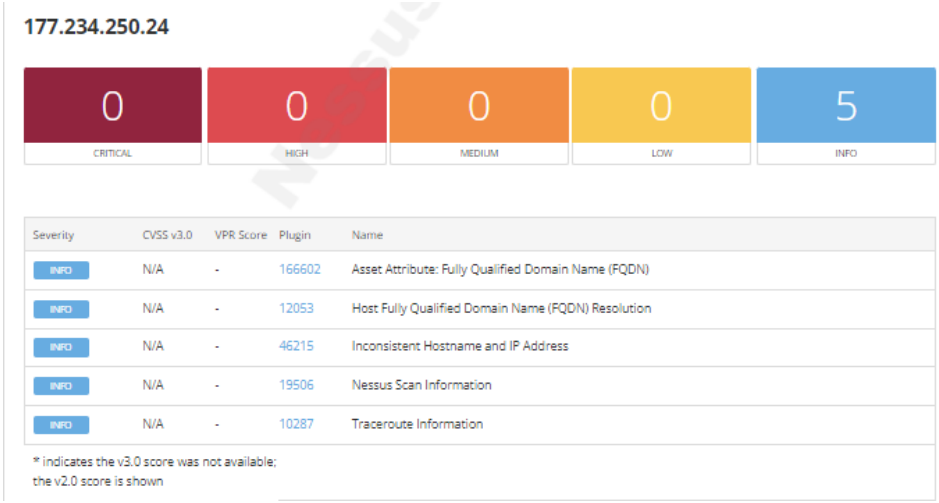


Figura 28. Reporte de vulnerabilidad detectada en nessus activo 10.11.100.4

Elaborado por: El investigador



177.234.250.24

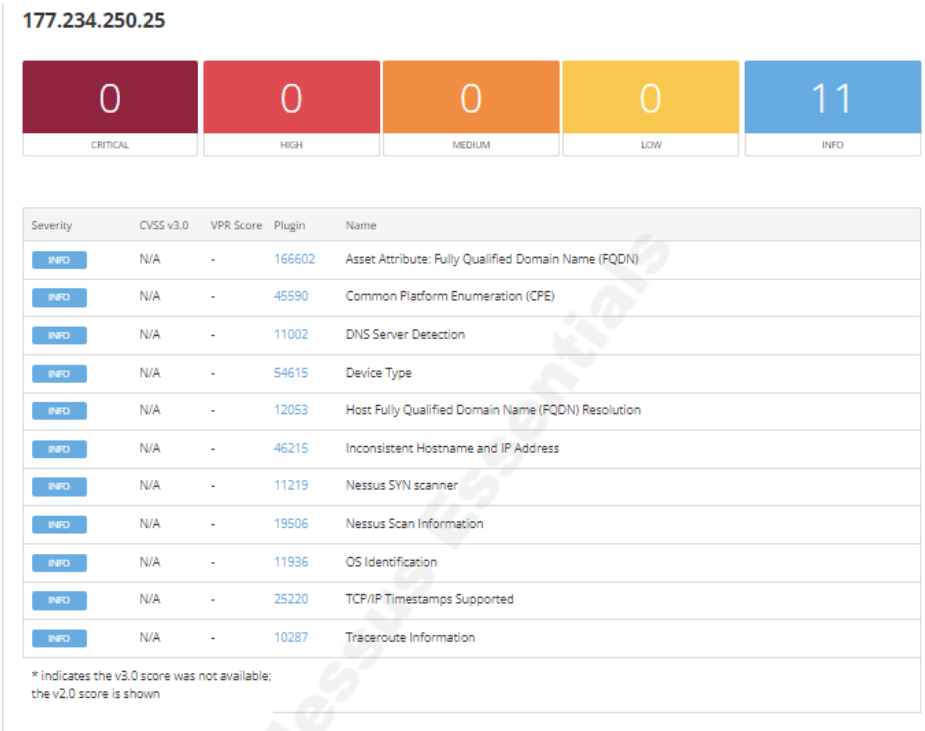
CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	0	0	5

Severity	CVSS v3.0	VPR Score	Plugin	Name
INFO	N/A	-	166602	Asset Attribute: Fully Qualified Domain Name (FQDN)
INFO	N/A	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	46215	Inconsistent Hostname and IP Address
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	10287	Traceroute Information

* indicates the v3.0 score was not available; the v2.0 score is shown

Figura 29. Reporte de vulnerabilidad luego de aplicación de remediaciones activo 177.234.250.24

Elaborado por: El investigador



177.234.250.25

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	0	0	11

Severity	CVSS v3.0	VPR Score	Plugin	Name
INFO	N/A	-	166602	Asset Attribute: Fully Qualified Domain Name (FQDN)
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	11002	DNS Server Detection
INFO	N/A	-	54615	Device Type
INFO	N/A	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	46215	Inconsistent Hostname and IP Address
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	10287	Traceroute Information

* indicates the v3.0 score was not available; the v2.0 score is shown

Figura 30. Reporte de vulnerabilidad luego de aplicación de remediaciones activo 177.234.250.25

Elaborado por: El investigador