ANÁLISIS Y RECOMENDACIONES DE SEGURIDAD DE LA INFORMACIÓN PARA LA EMPRESA ALIMENTOS PHD

PRESENTADO POR:
ARIEL FERNANDO RODRÍGUEZ
CRISTIAN CAMILO MUÑOZ
MAURICIO JIMÉNEZ

ASESOR TÉCNICO DE PROYECTO:
Ingeniero Jairo García

UNIVERSIDAD EL BOSQUE
FACULTAD DE INGENIERÍA ELECTRÓNICA
ESPECIALIZACIÓN EN SEGURIDAD DE REDES TELEMATICAS
BOGOTÁ, COLOMBIA
05 JULIO

Resumen

Este trabajo se ha realizado con el propósito de realizar un análisis de vulnerabilidades a la infraestructura tecnológica, fisca, lógica y personal humano de la empresa ALIMENTOS PHD utilizando herramientas como NESSUS, NMAP y metodología MAGERIT.

El objetivo principal de este proyecto es escanear los activos, analizar vulnerabilidades y de acuerdo a los resultados obtenidos generar recomendaciones y controles a la organización, dado que las herramientas que se utilizaran en el desarrollo del trabajo proporcionan métricas e información actualizada permite tomar decisiones ágiles con la finalidad de priorizar e implementar en corto, mediano o largo plazo, remediaciones que permiten conformar una línea base que definirá la implementación de las políticas de seguridad de la información, basados en la disponibilidad, confidencialidad e integridad.

Palabras clave

Hardening, Seguridad de la información, Seguridad informática, Análisis de vulnerabilidades, Riesgo informático, Protocolo RDP, VPN, Router, MAGERIT, Nessus, Nmap, SSH, Hackers, denegación de servicios, Malware, Equipos informáticos, redes de comunicaciones, Confidencialidad, Integridad, Disponibilidad.

Abstract

This work has been done with de objective of perform a vulnerability analysis of the technological, physical, logical and human personnel infrastructure using tools like as NESSUS, NMAP and the MAGERIT methodology.

The main objective of this project is to scan the assets, analyze vulnerabilities and according to the results obtained, generate recommendations and controls to the organization, given that the tools used in the development of the work provide metrics and updated information to make agile decisions with the purpose of prioritizing and implementing, in the short, medium or long term, remediations that allow us to form a baseline that will define the implementation of information security policies, based on availability, confidentiality and integrity.

Keywords

Hardenning, Information security, Computer security, Vulnerability analysis, Computer risks, RDP(Remote Desktop Protocol) , VPN(Virtual Network Private), Router, MAGERIT, Nessus, Nmap, SSH, Hackers, denial of services, Malware, Computer equipment , communications networks, confidentiality, integrity, availability.

Tabla de contenido

Tabla de ilustraciones

Lista de Tablas

1. Título

ANÁLISIS Y RECOMENDACIONES DE SEGURIDAD DE LA INFORMACIÓN PARA LA EMPRESA ALIMENTOS PHD

2. Introducción

En la actualidad los sistemas de información se han convertido en parte primordial de las empresas, es por eso que los activos de información como los equipos de cómputo, red de comunicaciones y seguridad en donde se almacena o se transmite esta información, forman parte de la actividad cotidiana de todas las organizaciones.

Así como los sistemas facilitan el acceso a la información y brindan facilidades a los usuarios, también se requiere concientizar y preparar al personal de las organizaciones para proteger la información, actualmente existen organizaciones que desconocen cómo asegurar o no están preparadas para salvaguardar su activo más valioso que es la información, es por esto que se quiere mostrar con este proyecto independientemente de la industria en la que se desenvuelva la empresa es posible cuidar sus activos e incluso con recursos existentes de manera eficiente lograr llevar a cabo planes de contingencia y de seguridad.

La empresa ALIMENTOS PHD es una empresa dedicada a la venta de productos de alimentación saludable, cuenta con información sensible que debe almacenar y proteger, entre ellos el registro de proveedores, ventas, marketing, sin embargo, desconoce los riesgos existentes que pueden llegar a materializarse si no se cuenta con protección en sus equipos y concientización del personal que utiliza a diario la información.

A lo largo de este proyecto veremos que asegurar una red y todos los equipos asociados a ella requiere limitar y bloquear características que puede ser usada para acceder a la información por personas no autorizadas, por tal razón el resultado de este proyecto consiste en entregar a la empresa ALIMENTOS PHD recomendaciones que ayuden a tomar medidas para proteger su información y de la mano trabajar con los empleados concientizándolos y sensibilizándolos en la seguridad de la información y buen manejo de los recursos basados en buenas prácticas bajo los tres pilares de la seguridad de la información.

3. Descripción general del proyecto

En la actualidad, la Internet es para las organizaciones una herramienta fundamental de comunicación, e investigación. Cuando se habla de la seguridad de la información y la informática es relevante la situación de la protección y la vulnerabilidad de su información y sus redes de datos, por consiguiente, las empresas requieren de una buena y robusta infraestructura tecnológica, para no verse afectados en temas de pérdidas o vulnerabilidades de su información, es aquí donde surge la necesidad de realizar un análisis profundo de las redes de datos de la organización con el objetivo de escanear y analizar la seguridad actual en los activos y de acuerdo a resultados, proponer recomendaciones de mejora para lograr un buen aseguramiento de su infraestructura tecnológica y de su información.

3.1 Definición del problema

ALIMENTOS PHD es una empresa especializada en la venta de alimentos funcionales y saludables, esta empresa cuenta con una sede principal y cuatro sedes remotas las cuales realizan todos sus procesos y almacena la información en un servidor ubicado en la sede principal, como tal está categorizada como una empresa PYME no mayor a 50 empleados la cual tiene definidas áreas de gerencia, contables y de producción de alimentos.

En la actualidad la compañía cuenta con una infraestructura básica adecuada a su necesidad, se identifican falencias a nivel de seguridad de la información y de su infraestructura de red lo cual surge la necesidad de realizar un análisis profundo de la red local (LAN) y sus conexiones (WAN).

El desarrollo de este proyecto se basa en realizar un análisis de vulnerabilidades sobre la red de datos y a la infraestructura existente con herramientas como Nessus, NMap para gestionar y proponer a la empresa recomendaciones que sean línea base para remedir amenazas futuras.

3.2 Aspectos a solucionar

La compañía ALIMENTOS PHD requiere a nivel de seguridad incrementar y fortalecer la conexión hacia el servidor desde las sedes remotas con las que cuenta a la fecha; Durante la visita realizada a la sede principal se identifica la necesidad de asegurar el intercambio de información entre las sedes remotas y su sede principal, este intercambio o almacenamiento de información de una u otra manera viaja por sistemas intermedios que se desconocen y no se tiene control de estos, lo que implicaría que se desconoce en algún momento lo que pudiesen hacer con la información, dado que hoy en día existen herramientas diversas para suplantar un sistema. Por tanto, se pretende entregar un documento con recomendaciones y controles que la organización debe implementar para mitigar los riesgos encontrados en sus activos de información, mejorando la seguridad actual, garantizando una infraestructura acorde a sus necesidades y continuidad del negocio.

3.3 Solución propuesta

Se propone con este proyecto gestionar un modelado de aseguramiento de la red y de la información que sea lo más recomendable y a bajo coste asegurando la continuidad del negocio. Sin embargo, para llegar a esto es necesario realizar las recomendaciones pertinentes de seguridad informática y de la información que permitan asegurar la sede principal y sus sedes remotas con un mínimo coste de inversión mitigando que esta esté expuesta a delincuentes o ataques cibernéticos.

Se requiere por parte de la empresa realizar, gestionar y administrar un firewall existente con las políticas adecuadas a la necesidad del negocio con el fin de mitigar y exponer su información sensible que se publica hacia internet desde el servidor y el protocolo RDP. Las amenazas incluyen ransomware como CrySiS, que se dirige a las empresas a través de puertos RDP abiertos; CryptON, que usa ataques de fuerza bruta para obtener acceso a las sesiones de RDP; y Samsam, que utiliza una amplia gama de ataques, incluidos los que atacan a máquinas habilitadas para RDP, para realizar ataques de fuerza bruta.

4. Estado del arte

Hemos basado el desarrollo de este proyecto en investigaciones y/o artículos más recientes que nos permiten ilustrar y obtener herramientas de trabajo y así poder generar de acuerdo a resultados soluciones óptimas y viables en la organización. En la actualidad en un mundo cibernético tan cambiante y evolucionado es importante concientizarnos en utilizar buenas prácticas existentes para asegurar nuestra información la cual podría llegar a verse vulnerada o manipulada si no contamos con medidas preventivas. Es por esto, que se hace necesario realizar un análisis de vulnerabilidad el cual nos permitirá ajustar y validar las configuraciones necesarias para evitar debilidades en los sistemas que puedan estar expuestos a riesgos informáticos.

Resaltamos el artículo Metodología de Análisis de Vulnerabilidades para Empresas de Media y Pequeña Escala, como base de investigación de este trabajo“ Con el fin incrementar tal seguridad, se hace necesario realizar un análisis de vulnerabilidades, para identificar aquellas brechas de seguridad que se encuentran expuestas hacia el exterior o el interior de la organización, así como facilitar la toma de decisiones sobre las formas de proteger sus bienes y los servicios que prestan a la comunidad. De este modo, el estudio de estas vulnerabilidades debe abarcar varios frentes de seguridad, reduciendo al mínimo la efectividad de los ataques que pueden aprovechar las mismas. Estos frentes son Seguridad Lógica, donde se aplican barreras y se elaboran procedimientos que ayuden a proteger la información; Seguridad Física, la cual aplica defensas físicas y procedimientos de control; Políticas y Estándares, que son los documentos que utiliza una organización para administrar y proteger la información; y finalmente Auditoría de Sistemas, que es la revisión y la evaluación de los controles, sistemas y procedimientos de informática.

Asimismo, se deben identificar y mitigar los riesgos a los que se encuentra expuesta la empresa, de tal modo que cada uno de estos frentes identifique, administre y mitigue cada uno de los mismos, basados en las necesidades y requerimientos de la empresa.”. (Documentos de Metodología de Análisis de vulnerabilidad, Fase 5, p. 66).

Para lograr tener nuestra información segura es necesario realizar un análisis de vulnerabilidades, identificar los riesgos y posibles amenazas con el fin de definir controles que permitan mejorar la seguridad de los equipos que contienen el activo más importante de toda

organización, la información.

4.1 Marco de referencia teórico

Para el desarrollo de este proyecto es necesario indagar qué, cómo, y dónde se presentan estos grandes problemas de vulnerabilidades y una posible solución para dichas amenazas o vulnerabilidades, basados en referencias de otros documentos como herramientas para la realización de nuestro proyecto, en donde el objetivo es mantener nuestra información segura, y tratar que los pilares de la seguridad de la información la disponibilidad, la integridad y la confidencialidad se logren cumplir a satisfacción.

Es necesario saber a qué nos exponemos como usuarios cada vez que navegamos en internet sin ningún tipo de defensa, esto no quiere decir que toda la navegación sea critica, si no que se debe tener prevención al navegar en sitios desconocidos y también al gestionar nuestro correo electrónico ya que el correo también es un punto de acceso de malware a nuestra organización. para esto es necesario abordar el tema de la seguridad de la información y un paralelo como lo es la seguridad informática. Con este proyecto se pretende identificar, analizar, buscar y corregir las brechas de seguridad que pueden ser aprovechadas de forma automatizada por virus y malware utilizados por los cibercriminales que pueden afectar nuestra información e infraestructura tecnológica.

Una vulnerabilidad hace referencia a una debilidad informática que podría ser utilizada para causar cualquier tipo de daño cibernético pone en riesgo la seguridad de la información. Dichas falencias pueden aparecer en cualquier sistema o elemento de nuestra red tecnológica y de la información, tanto en hardware como en software. Y por otro lado una amenaza es toda acción aprovechada en una vulnerabilidad para atentar contra un sistema informático.

Un sistema informático se puede ver expuesto a un ataque o una amenaza en cualquier momento, por eso es necesario saber cómo abordarlo, y para ello vamos a entrar a conocer los tipos de atacantes y herramientas que se conocen en la actualidad, con esto se pueden prevenir y evitar ser víctima de un ataque cibernético. Se encuentran numerosos tipos de atacantes a los que se puede

estar expuesto como lo son: **Hackers, Crackers, Phreaks, Lammers, Ciberterrorista.** Estos se consideran en la actualidad los atacantes más conocidos, como se pueden observar bastantes perfiles, esto no quiere decir que todos los hagan con ánimo de robo o maldad, todo lo contrario, en la mayoría de los casos las empresas los contratan para saber qué tan vulnerables son y así mismo tener una buena seguridad de sus equipos de cómputo y su información relevante.

A continuación, se pudo recolectar una información relevante de los ataques críticos a lo que puede ser expuesto un sistema al que se le puedan explotar y aprovechar sus vulnerabilidades ocasionando así una **Interrupción, Interceptación, Modificación**, sin duda dentro de estas técnicas se puede mencionar una que está cogiendo fuerza durante los últimos la cual es nombrada como la fabricación.

Se debe tener en cuenta que cualquier equipo conectado a una red se encuentra expuesto a ser atacado, ya que a diario se encuentran expertos informáticos en la búsqueda de vulnerabilidades, para esto es necesario utilizar herramientas que nos mantengan informados de posibles ataques o amenazas.

4.2 Marco de referencia tecnológico

En la actualidad las organizaciones realizan sus operaciones a través de internet, y es por esto que es importante contar con seguridad robusta en la infraestructura tecnológica, aunque existe otra opción que toma la mayoría de las organizaciones, la cual consiste en tercerizar sus procesos tecnológicos, esto con el fin de tener una infraestructura segura y estable. Las herramientas tecnológicas que se encuentran disponibles permiten realizar un análisis de vulnerabilidades, las cuales permiten explorar puertos y aplicaciones y por medio de una métrica ofrecen posibles soluciones.

4.2.1 Herramientas para el escaneo de vulnerabilidades

"La variedad de herramientas de Software para realizar el escaneo y explotación de vulnerabilidades; es amplia, ya es cuestión de elegir cuál es la herramienta que mejor se adapte a nuestras necesidades, o a la exigencia de la prueba a ejecutar" [1].

Nessus: Es una de las principales herramientas para realizar escaneo de vulnerabilidades y auditoría, se usa principalmente por expertos informáticos para saber qué tan segura está su red y sus equipos de cómputo, tiene sus versiones para Windows, Linux y Mac Os X, permite escanear un máximo de 16 máquinas en modo de uso libre, para grandes empresas es necesario que sea con licenciamiento, ya que por lo general son más de 16 máquinas a las que se le realiza el escaneo

Nexpose: Es una herramienta bastante completa para realizar un análisis de vulnerabilidades que permite el análisis, el descubrimiento y verificación de los riesgos que se tienen en toda la red. El software se complementa como Metasploit de rapid7 para la explotación de vulnerabilidades. Nexpose es una herramienta que se tiene algunas versiones gratuitas, pero su licencia para uso completo este alrededor de 2,000 dólares por año, tiene instaladores para sistema operativo Windows, Linux.

Nipper: Nipper studio es una herramienta la cual procesa sus configuraciones nativas para auditoría en una red de datos, es decir basado en agentes de red con prueba de penetración manual, puede experimentar varios campos de acción, que no afectan el software de auditoría de seguridad de Nipper Studio. Trae su versión trial, pero limitado, lo más apropiado sería comprar su licenciamiento para su uso full y está disponible para sistemas operativos Windows, Linux, Mac os x.

Openvas: Es un escáner de vulnerabilidades totalmente gratuito se extrajo de la última versión de un escáner que ya dejó de funcionar (Nessus), Openvas corrigió errores y complementos para su correcto funcionamiento, está disponible para Windows y Linux en todas sus versiones Free.

QualysGuard: Un software que ayuda por lo general alas grandes compañías a simplificar sus infraestructuras y operaciones para reducir el costo del cumplimiento de seguridad, auditoria y protección de un sistema TI. Tiene su versión comercial y una gratuita pero limitada a diferencia de los anteriores está disponible para Linux, Windows y Mac OS X.

Retina: Es uno del software de escaneo de vulnerabilidades más respetado por su estabilidad y seguridad, sirve como motor para las soluciones de gestión de vulnerabilidades, según expertos es una excelente opción, tiene un pago aproximado de Us $ 1,700.00 anuales y está diseñado para soportar su instalación en sistemas operativos Windows.

Saint: Es un programa pago, pero muy completo ya que se especializa en el análisis de protocolos, en este caso SCAP el protocolo de contenido de seguridad y automatización como vulnerabilidad autenticada, de igual manera examina los protocolos básicos de un tráfico de red como lo son los UDP Y TCP, busca las vulnerabilidades y sus resultados los clasifica según su criticidad, funciona para Linux Windows y Mac OS X.

Cada una de estas herramientas contiene una metodología y métrica de escaneos con propuestas de solución para mejorar los sistemas informáticos, la idea es optar por la herramienta más completa y funcional para el proyecto que permita ofrecer información actualizada en cuanto a las vulnerabilidades existentes en los sistemas para gestionarlas y así la empresa pueda tomar decisiones frente a las soluciones propuestas.

4.2.2 Seguridad de las telecomunicaciones

En la actualidad tenemos que estar a la vanguardia de como tener nuestros sistemas de información seguros, como lograr no estar expuestos a un ataque cibernético y para esto existen normas técnicas las cuales no dan pautas para llegar a lograrlo; en la ISO27002 nos permite analizar el objetivo que es “asegurar la protección de la información que se comunica por redes telemáticas y la protección de la infraestructura de soporte.

La gestión segura de las redes, la cual puede abarcar los límites organizacionales, requiere de la cuidadosa consideración del flujo de datos, implicaciones legales, monitoreo y protección.

La información confidencial que pasa a través de redes públicas suele requerir de controles adicionales de protección. Los intercambios de información por parte de las organizaciones se deberían basar en una política formal de intercambio y en línea con los acuerdos de intercambio, y debiera cumplir con cualquier legislación relevante" [3].

5. Glosario de términos

Activo: Los activos son los recursos del Sistema de Seguridad de la Información ISO 27001, necesarios para que la empresa funciones y consiga los objetivos que se ha propuesto la alta dirección.

Riesgo: Es la probabilidad latente de que ocurra un hecho que produzca ciertos efectos, la combinación de la probabilidad de la ocurrencia de un evento y la magnitud del impacto que puede causar, así mismo es la incertidumbre frente a la ocurrencia de eventos y situaciones que afecten los beneficios de una actividad

Amenaza: Potencial ocurrencia de un hecho que pueda manifestarse en un lugar específico, con una duración e intensidad determinadas. Cuando el Agente de riesgo selecciona una víctima contra la cual pretende cometer un acto delictivo, automáticamente se convierte en una amenaza para ella. Se puede considerar que es la materialización del riesgo.

Vulnerabilidad: Está íntimamente relacionado con el riesgo y la amenaza y se puede definir como la debilidad o grado de exposición de un sujeto, objeto o sistema. También son aquellas fallas, omisiones o deficiencias de seguridad que puedan ser aprovechadas por los delincuentes.

Ataque: método por el cual un individuo, mediante un sistema informático intenta tomar el control, desestabilizar o dañar otro sistema informático (ordenador personal, red privada, etcétera).

ISO 27001: es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización.

Internet: es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, lo cual garantiza que las redes físicas heterogéneas que la componen formen una red lógica única de alcance mundial.

Análisis de vulnerabilidades: En un análisis de este tipo se tienen en cuenta todos y cada uno de los aspectos que puedan representar un riesgo que comprometa la información de la empresa. Desde la seguridad perimetral y la programación hasta la sensibilización de los trabajadores y los Backup. Tras su estudio se cuantifica el nivel de amenaza de cada elemento, normalmente de forma numérica, y se procede a mejorar los que se consideran una vulnerabilidad.

Seguridad de la información: Proteger la información de una organización, independientemente del lugar en el que se localice: impresos en papel, discos duros de las computadoras, etc. Tiene 3 principios fundamentales: Confidencialidad, Integridad, Disponibilidad. Su radio de acción cubre análisis de riesgos, seguridad personal/física, gestión de comunicaciones, control acceso, gestión de incidentes, gestión continuidad del negocio, entre otros.

Seguridad informática: Proteger las infraestructuras tecnológicas y de comunicación que soportan la operación de una organización (hardware, software) y que estas sean utilizadas de la manera indicada por la organización. Su radio de acción cubre pruebas de evaluación de vulnerabilidades, test de penetración, hacking ético, entre otros.

Nmap: Es una herramienta de código abierto para exploración de red y auditoría de seguridad. Se diseñó para analizar rápidamente grandes redes, aunque funciona muy bien contra equipos individuales. Nmap utiliza paquetes IP "crudos" en formas originales para determinar qué

equipos se encuentran disponibles en una red, qué servicios (nombre y versión de la aplicación) ofrecen, qué sistemas operativos (y sus versiones) ejecutan, qué tipo de filtros de paquetes o cortafuegos se están utilizando.

Nessus: es un programa de escaneo de vulnerabilidades en diversos sistemas operativos. Consiste en un demonio, nessusd, que realiza el escaneo en el sistema objetivo, y nessus, el cliente (basado en consola o gráfico) que muestra el avance e informa sobre el estado de los escaneos. En operación normal, nessus comienza escaneando los puertos con nmap o con su propio escaneador de puertos para buscar puertos abiertos y después intentar varios exploits para atacarlo. Las pruebas de vulnerabilidad, disponibles como una larga lista de plugins, son escritos en NASL (Nessus Attack Scripting Language, Lenguaje de Scripting de Ataque Nessus por sus siglas en inglés), un lenguaje scripting optimizado para interacciones personalizadas en redes.

Seguridad de la información: es el conjunto de medidas preventivas y reactivas de1 las organizaciones y sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos.

Seguridad informática: también conocida como ciberseguridad o seguridad de tecnología de la información,1 es el área relacionada con la informática y la telemática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida en una computadora o circulante a través de las redes de computadoras. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información.

Integridad: Hace referencia a la cualidad de la información para ser correcta y no haber sido modificada, manteniendo sus datos exactamente tal cual fueron generados, sin manipulaciones ni alteraciones por parte de terceros. Esta integridad se pierde cuando la información se modifica o cuando parte de ella se elimina, y una gran garantía para mantenerla intacta es, como hemos mencionado en anteriores ocasiones, la firma digital.

Confidencialidad: Es la cualidad de la información para no ser divulgada a personas o sistemas no autorizados. Se trata básicamente de la propiedad por la que esa información solo resultará accesible con la debida y comprobada autorización.

Disponibilidad: El tercer y último pilar de la Seguridad de la Información es la disponibilidad, y es posiblemente el término que menos apreciaciones requiere. Por disponible entendemos aquella información a la que podemos acceder cuando la necesitamos a través de los canales adecuados siguiendo los procesos correctos.

No repudio: En origen: garantiza que la persona que envía el mensaje no puede negar que es el emisor de este, ya que el receptor tendrá pruebas del envío. En destino: El receptor no puede negar que recibió el mensaje, porque el emisor tiene pruebas de la recepción de este.

Gusanos: Software malicioso que puede replicarse a sí mismo en ordenadores o a través de redes de ordenadores. [4]

Malware: El malware (abreviatura de "software malicioso") se considera un tipo molesto dañino de software destinado a acceder a un dispositivo de forma inadvertida, sin el conocimiento del usuario. [2]

Protocolo RDP: Protocolo de escritorio remoto se basa en la comunicación de varios canales virtuales con el fin de transportar datos y recibir datos. [3]

Ransomware: El Ransomware (también conocido como rogueware o scareware) restringe el acceso a su sistema y exige el pago de un rescate para eliminar la restricción. [1]

Troyanos: Programas maliciosos que realizan acciones no autorizadas por el usuario. [5]

VPN: Virtual Private Network es una tecnología de red que se utiliza para conectar una o más computadoras a una red privada utilizando Internet [6]

Hackers: Es un experto tecnológico con conocimientos y habilidades en seguridad, sistemas operativos y/o programación, con la capacidad de detectar errores o fallos en sistemas informáticos para luego informar los fallos y las técnicas de mejora a los desarrolladores del software encontrado vulnerable o a todo el público.

Crackers: "Criminal Hacker", es alguien que rompe la seguridad de un sistema informático con intenciones maliciosas, como robo de datos dañar el sistema o para obtener beneficio económico. no obstante, algunos lo hacen solo por diversión.

Phreakers: Es una persona que investiga y comprende el funcionamiento de los sistemas telefónicas y de las tecnologías de las telecomunicaciones, y su objetivo específico es romper, manipular la seguridad de las redes telefónicas fijas y móviles, y en ocasiones también poder obtener algún beneficio como llamadas gratuitas y realizar espionaje. estas personas marcan como su afición el conocimiento y el reto que conlleva conocer más a los sistemas telefónicos.

Lammers: Persona que se cree Hacker y no tiene los conocimientos necesarios ni la lógica para comprender que es lo que realmente está sucediendo cuando utiliza algún programa ya hecho para hackear y romper alguna seguridad.

Ciberterrorista: Persona o grupo de personas que utilizan los medios tecnológicos de información, comunicación, informática, electrónica o similar con el propósito de generar terror o miedo generalizado en una población, clase dirigente o gobierno, causando con ello una violación a la libre voluntad de las personas. Los fines pueden ser económicos, políticos o religiosos principalmente.

Interrupción: Éste es un ataque contra la disponibilidad. Un recurso del sistema es destruido o se vuelve no disponible.

Interceptación: Una entidad no autorizada consigue acceso a un recurso. Éste es un ataque contra la confidencialidad.

Modificación: Éste es un ataque contra la integridad. Una entidad no autorizada no sólo consigue acceder a un recurso, sino que es capaz de manipularlo.

Fabricación: Un ente no autorizado inserta objetos adulterados en el sistema. Éste es un ataque contra la autenticidad, un ejemplo claro la suplantación de una página web de un banco con el objetivo de robar datos del usuario.

Conexión no Autorizada: Se buscan riesgos o debilidades de la seguridad de un equipo o un servidor de la red, y cuando se descubren, se realiza una conexión no autorizada a los servicios.

Denegación de servicios: Su objetivo es la interrupción de un servicio bien sea web, o de una red, también son llamados Dos (denial of service).

Ingeniería social: Su objetivo es obtener datos e información confidencial de una persona u organización para utilizarla con fines maliciosos. Los ejemplos más llamativos son el phishing.

Keyloggers: Es un software o hardware que puede interceptar y guardar las pulsaciones realizadas en el teclado de un equipo que haya sido infectado.

Phishing: Es un método que los ciberdelincuentes utilizan para engañarle y conseguir que revele información personal, como contraseñas o datos de tarjetas de crédito y de la seguridad social y números de cuentas bancarias. Lo hacen mediante el envío de correos electrónicos fraudulentos o dirigiéndole a un sitio web falso.

Spoofing: "Suplantación" hace referencia al uso de técnicas a través de las cuales un atacante, generalmente con usos maliciosos o de investigación, se hace pasar por una entidad distinta a través de la falsificación de los datos en una comunicación (IP, ARP, DNS, WEB).

Sniffing: Es una técnica que consiste en "escuchar" o capturar toda la información que circula por una red. Esta información se almacena y se interpreta para poder descubrir datos

sensibles como contraseñas, información bancaria, etc. Este ataque es uno de los principales que se realizan cuando se intenta robar información.

6. Justificación

Hoy en día toda organización o empresa requiere de una infraestructura de red acorde con los objetivos de la misma. La cual debe estar optimizada correctamente con el fin prevenir y controlar gran cantidad de riesgos a los cuales se estaría expuesta.

Mediante un análisis de seguridad se pretende conocer las vulnerabilidades con las que se encuentra la empresa de esta forma ALIMENTOS PHD podrá ejecutar correctivos que le permitan asegurar y administrar su información de forma segura, lo que le permitirá lograr tener un máximo beneficio y funcionamiento con el mínimo coste de inversión.

Mediante este proyecto se tomará como modelo los requerimientos de la empresa y se planteará una posible solución a los mismos garantizando así los tres pilares de la información los cuales son la integridad, confidencialidad y disponibilidad.

7. Objetivos

7.1. General

Determinar mediante un análisis de vulnerabilidades los riesgos actuales y posibles a los que la empresa ALIMENTOS PHD está sujeta con el fin de informar y generar las recomendaciones adecuadas que permitan aportar al buen funcionamiento y continuidad del negocio asegurando la integridad, confidencialidad y disponibilidad de la información de la empresa.

7.2. Específicos

Identificar y clasificar los activos de la red computacional de la empresa ALIMENTOS

PHD.

Analizar las vulnerabilidades, amenazas y riesgos encontrados, identificando los que pueden afectar los pilares de la seguridad de la información y la continuidad del negocio.

Proponer recomendaciones de hardening que permita mitigar y controlar los riesgos, amenazas y vulnerabilidades encontrados en la red.

8. Requerimientos

Para dar alcance a los requerimientos específicos de este proyecto, se hizo necesario realizar un diagnóstico inicial con nuestra empresa aliada para la investigación de este proyecto, a continuación se describe el desarrollo de esta análisis donde se utilizaran herramientas tecnológicas que permitirán encontrar las vulnerabilidades relevantes del sistema de información y la red local de la organización, esto con el fin de saber la mejor manera de generar unas recomendaciones generales de prevención y hardening de los sistemas de información y de sus activos

Realizar diagnóstico de los activos de red de la organización.

Realizar análisis de la Red con herramientas tales como Nessus y Nmap.

Fabricar un documento con las recomendaciones de los riesgos encontrados en el análisis realizado.

Generar unas recomendaciones de capacitación a personal de la organización.

Analizar y documentar los objetivos planteados con la metodología MAGERID (metodología de análisis y gestión de los riesgos de la información)

Se van a realizar un análisis de riesgos con los activos de información de la red, el cual permitirá evaluar la criticidad del mismo.

Basados en las ISO 27000 y 31000 se generar recomendaciones según la norma.

Con el conocimiento adquirido, se realizará el análisis de vulnerabilidades a toda la red de la organización.

9. Metodología

Como se sabe existen múltiples metodologías para el análisis gestión de riesgo de la información en este caso se trabajará sobre la metodología de **MAGERID (METODOLOGIA DE ANALISIS Y GESTION DE RIESGOS DE SISTEMAS DE LA INFORMACION)** la cual trata de conocer el riesgo al que la información se encuentra sometido y saber el estado de exposición y determinar si la información se encuentra segura o es vulnerable.

Magerid es el método que expone los riesgos que soportan los sistemas de información y permite recomendar las medidas apropiadas que se deben adoptar en un control de riesgos e implementar esquemas de seguridad para la protección de la información, esta metodología va tras unos objetivos como concientizar a los responsables de los sistemas de información y la necesitad de atajar o detener a tiempo los riesgos, ofrecer un sistema o modelo sistemático para analizar los riesgos que se presentan, ayudar a descubrir y planificar las medidas oportunas para mantener dichos riesgos bajo control, preparar a las organizaciones para realizar procesos tales como evaluación, certificación, acreditación, auditoria o certificación de la organización bajo un estándar internacional como por ejemplo la ISO 27000, ISO 31000.

Dicho lo anterior **MAGERIT** es uno de los procesos con el que se puede llegar a una certificación bajo los lineamientos del marco de la ISO 31000 el cual relaciona o implementa la gestión de riesgos con el fin de que cualquier empresa constituida tome las decisiones más adecuadas que permitan mitigar los riesgos asociados al uso de las herramientas y tecnologías de la información, para ello también trata mediante informes que recopilan y extraen información de una base “lecciones aprendidas” que se pueden categorizar o generar un modelo de valor, mapa de

riesgos, declaración de aplicabilidad, evaluación de salvaguardas, estado del riesgo, informe de insuficiencias, cumplimiento de normativas y un plan de seguridad.

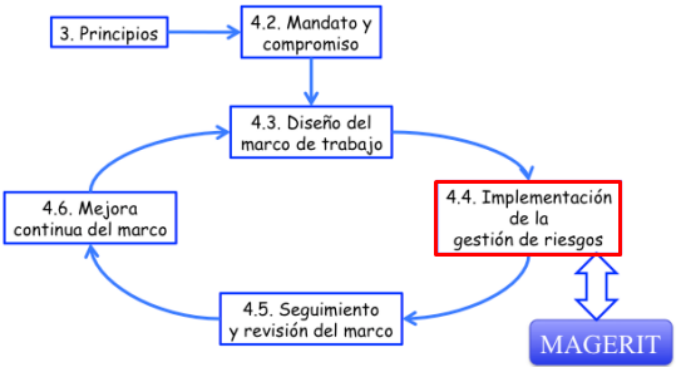


Ilustración 1. ISO 31000 - Marco de trabajo para la gestión de riesgos

Bajo el modelo descrito anteriormente se pretende realizar el levantamiento de inventario y la clasificación de los activos de información que maneja la empresa ALIMENTOS PHD con el objetivo de identificar y clasificar que activos manejan y cuales son críticos para el negocio. Según la valoración y clasificación otorgada por la empresa se determinarán los riesgos a los que se pueden ver expuestos o que un incidente pueda llegar a materializarse exponiendo los pilares de la información los cuales son su confidencialidad, integridad y disponibilidad.

Dicha clasificación de activos y según un mapa de calor que se genera según la valoración se determinara la criticidad y el impacto que tendría dicho activo y sobre el cual se tomarían las acciones de mejora y robustecimiento con el fin de poder garantizar la continuidad del negocio ante eventos que puedan llegar a impactar la empresa, tomando como referencia la normativa ISO 31000 de 2018**.**

Para ello se ejecutarán las siguientes fases:

- Identificar y clasificar activos
- Valoración del riesgo según activo

- Identificar Riesgo
- Tratamiento del riesgo

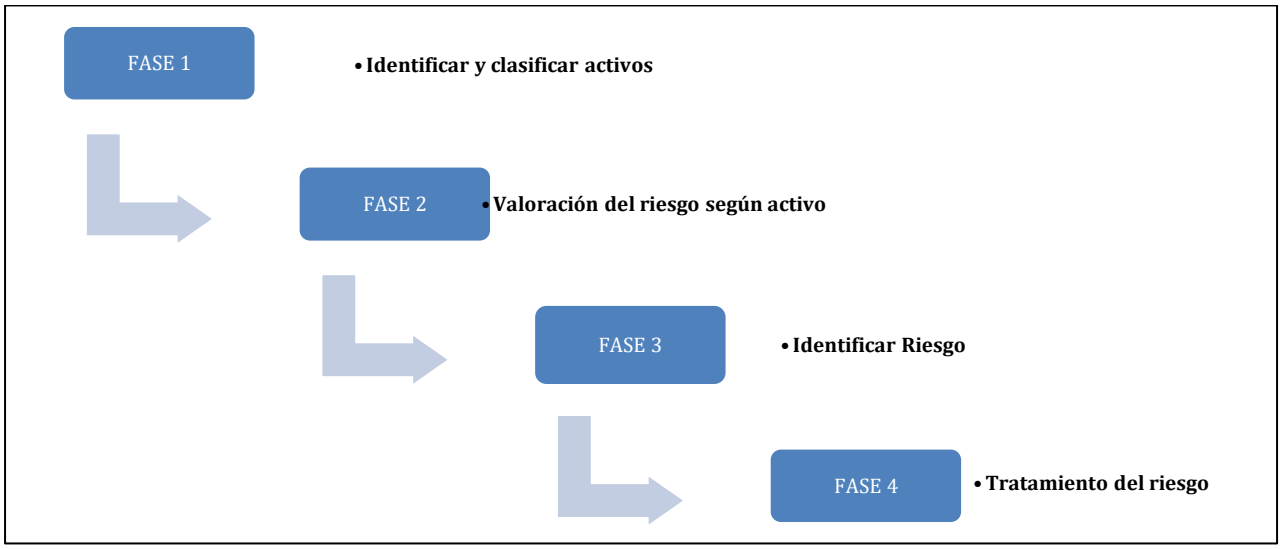


Ilustración 2. Fases del Análisis de Riesgos

Una vez realizadas las fases se procede a realizar las recomendaciones de hardening que permita solventar las vulnerabilidades, amenazas o riesgos encontrados en la red.

10. Identificar y clasificar los activos

Para la identificación y clasificación de activos Magerit determina y conceptualiza que en cualquier tipo y sistema de información se describen o se encuentran dos cosas fundamentales como lo son la información que se maneja en la empresa y los servicios que presta entre estos dos se encuentran clasificados los siguientes:

Datos: son todos los activos involucrados en los procesos que se generan dentro de una organización.

Servicios: Hace referencia a los activos que puede prestar y que son necesarios para el procesamiento de información.

Aplicaciones informáticas: Activos que relacionan o permiten almacenar y generar información en pocas palabras es el Software utilizado.

Equipos informáticos: Activos que relacionan o permiten almacenar y generar información en pocas palabras es el Hardware o equipos que permiten ejecutar la aplicación informática.

Redes de comunicación: Hace referencia a equipos que permiten la conexión hacia recursos que facilitan el intercambio o conexión de red.

Instalaciones: son aquellas donde se resguardan lo equipos de interconexión o comunicación puede ser una o varias sedes, centros de cableado o interconexión.

Personas: Se involucran o se cuentan como activo las personas " trabajadores" dado que están son las que interactúan manipulas y administran las herramientas y equipos que permiten desempeñar las tareas cotidianas de cualquier organización y que pueden llegar a ser un activo crítico para las organizaciones ya que son consideradas como el eslabón más débil de cualquiera por lo que pueden ser víctimas o victimarios que generen un alto riesgo para la continuidad del negocio y de información de las empresas

Dentro de esta tarea también define la dependencia, como las áreas o dependencias a las que pertenecen estos activos de información y que dependiendo de la seguridad que se le otorgue al área o dependencia así mismo será la seguridad que se verá reflejada en los activos pertenecientes a estas.

Expuesto lo anterior se describe brevemente a continuación:

Tabla 1. Dependencia organizacional

ÁREA/DEPENDENCIA	IDENTIFIICACION DE ACTIVO	ACTIVO
Gerencia	Instalaciones	Sedes
Comercial	Servicios	Productos
Sistemas	Redes de comunicación	Equipos de red Aplicaciones informáticas Redes de comunicación
Recursos humanos	Personas	Trabajadores

Para ello se realiza un esquema Organizacional en el que se puede identificar actualmente como se distribuyen los activos de la empresa con el fin de identificar quien tiene acceso a los mismos. El organigrama y acceso se encontrará dentro de los anexos para visualizarse detalladamente.

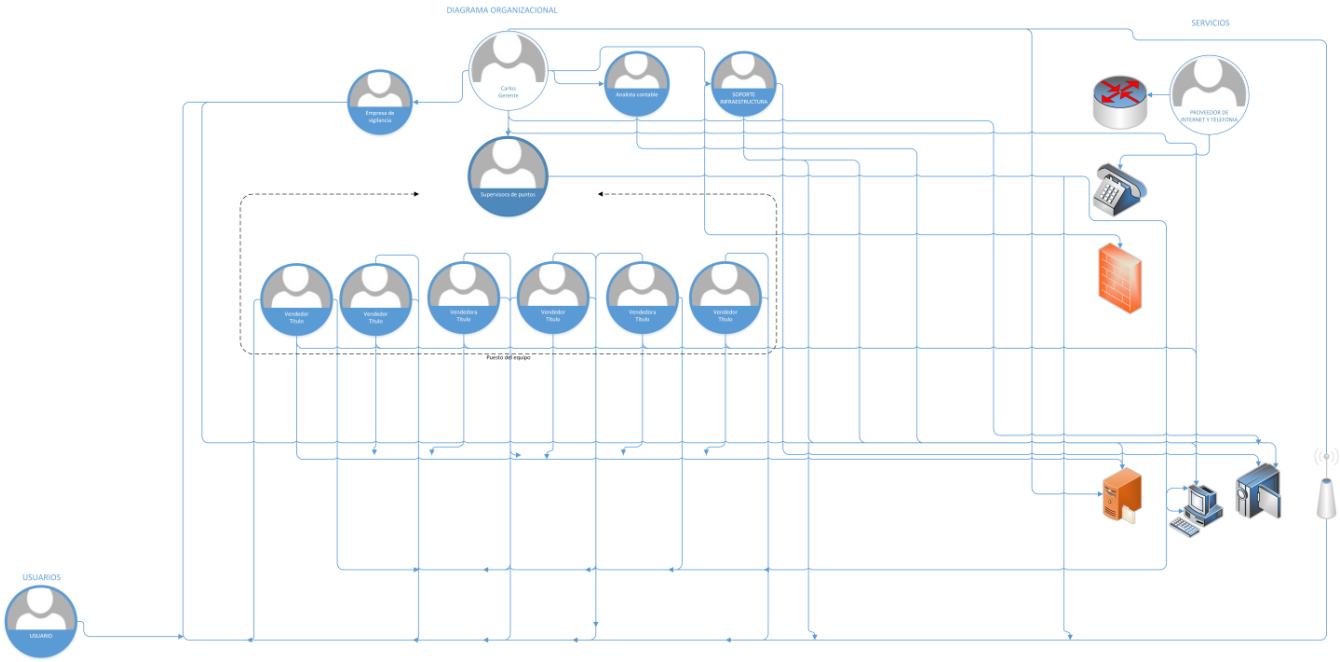


Ilustración 3. Diagrama organizacional

Adicional a la identificación esta tarea involucra una valoración y una dimensión, para ello este modelo describe una apreciación denotando que no es a lo que cuesta económicamente si no al valor que tiene este activo de información y que tiene la necesidad de que sea resguardado o que

tenga que asegurar o proteger dándole una dimensión tal como confidencialidad, integridad, disponibilidad los cuales se mencionaran en el capítulo de valoración del riesgo.

Para ellos se puede determinar o definir de la siguiente manera:

Confidencialidad: Daño que causaría que lo conociera quien no debe

Integridad: Perjuicio que causaría que se dañe.

Disponibilidad: Perjuicio que causaría el no poder utilizarlo.

10.1 10.1. Valoración del Riesgo

Dentro de la valoración Magerit determina dos tipos de valoración las cuales son: una valoración cualitativa, cuantitativa y el valor que tendría la interrupción del servicio que se esté prestando. Ya una vez determinadas las dimensiones de los activos que existen es necesario darle un valor al activo el cual puede determinar o suponer cuanto le costaría a la organización recuperarse o restablecer el activo ante cualquier eventualidad, ante esto se podrían considerar factores tales como el valor de reposición valor de mano de obra y pérdida de ingresos, las sanciones que le repercutirían a la organización en caso de que llegara a materializarse un riesgo, daños que podrían repercutir en pérdidas o limitantes de operación de otros activos.

La metodología implementada “MAGERIT” proporciona una escala de valoración de tal forma que permita calcular o definir el daño que se representaría sobre el activo en ausencia de que no se tenga un proceso, control o política definida para mitigar el riesgo.

La escala definía por Magerit equivale o se ve reflejada entre los valores de 0-5 donde se podrá valorar el riesgo que generaría por dicha ausencia. Para ello se define o clasifica la valoración de los activos de la siguiente manera:

Tabla 2. Valoración de activos

VALORACIÓN		
Cualitativa /Cuantitativa		**CRITERIO**
5	MUY ALTO	DAÑO MUY GRAVE
4	ALTO	DAÑO GRAVE
3	MEDIO	DAÑO IMPORTANTE
1-2	BAJO	DAÑO BAJO
0	N/A	DAÑO IRRELEVANTE-NULO

Una vez se realiza la respectiva valoración de los activos se procede a realizar la sumatoria de los valores otorgados a la confidencialidad integridad y disponibilidad de estos, generando así el valor total representativo de los activos dicho esto el valor máximo que se tendría en un activo el cual seria 30 como critico suponiendo que la C, I y D tengan valor de 10 cada uno.

10.2 10.2. Identificación Amenazas y riesgos

Es el proceso actividad o tarea que permite determinar la acción causa o circunstancia que puede llegar a afectar un activo de información o a una organización. Las amenazas se pueden catalogar como: Origen natural, industrial, defecto de aplicaciones causadas por personas de forma accidental o deliberada.

Dentro de estas amenazas se logran identificar factores que se ven involucrados tales como terremotos inundaciones incendios, fallas eléctricas, vulnerabilidades, accesos no autorizados, ataques deliberados, espionaje industrial, entre otros. Para cada uno de estos actos o factores se debe dar una valoración con una probabilidad de ocurrencia y de impacto a que esto llegue a materializarse y genere pérdida parcial o total de una actividad o tarea relacionada a la operación y pueda generar pérdidas reputaciones, legales o económicas sobre la empresa.

Para ellos se realiza la clasificación o valoración de probabilidad de que llegue a materializarse y de impacto que pueda llegar a ocasionar un evento sobre el activo definiéndolo en una escala de 1-5 las cuales se describen a continuación:

Clasificación de Probabilidad

- Improbable
- Remoto
- Ocasional
- Moderado
- Frecuencia

Tabla 3.Clasificación o valoración de probabilidad

Probabilidad	
5	Frecuente
4	Moderado
3	Ocasional
2	Remoto
1	Improbable

Clasificación de Impacto

Insignificante: Si llegara a presentarse su impacto sería mínimo sobre la organización o entidad.

Menor: Si llegara a presentarse habría un bajo impacto sobre la organización o entidad.

Moderado: Si llegara a presentarse tendría medianas consecuencias sobre la organización o entidad.

Mayor: Si llegara a presentarse tendría altas consecuencias sobre la organización o entidad.

Catastrófico: Si llegara a presentarse consecuencias sería catastrófica.

Tabla 4. Clasificación o valoración de impacto

Impacto	
5	Catastrofico
4	Mayor
3	Moderado
2	Menor
1	Insignificante

La recopilación de información de este capítulo se puede plasmar mediante la siguiente tabla:

Tabla 5. Evaluación de riesgo sobre activo

EVALUACIÓN DEL RIESGO						
ACTIVO	*ID ACTIVO*	*AMENAZA/RIESGO*	*ID RIESGO*	*VULNERABILIDAD*	*PROBABILIDAD*	*IMPACTO*

Con el fin de plasmar la información recopilada en los capítulos anteriores en un mapa de calor en el que se logra identificar que al aumentar el riesgo y la probabilidad el riesgo crece logrando así distinguir cada uno en cuatros (4) zonas las cuales están definidas según Magerit como:

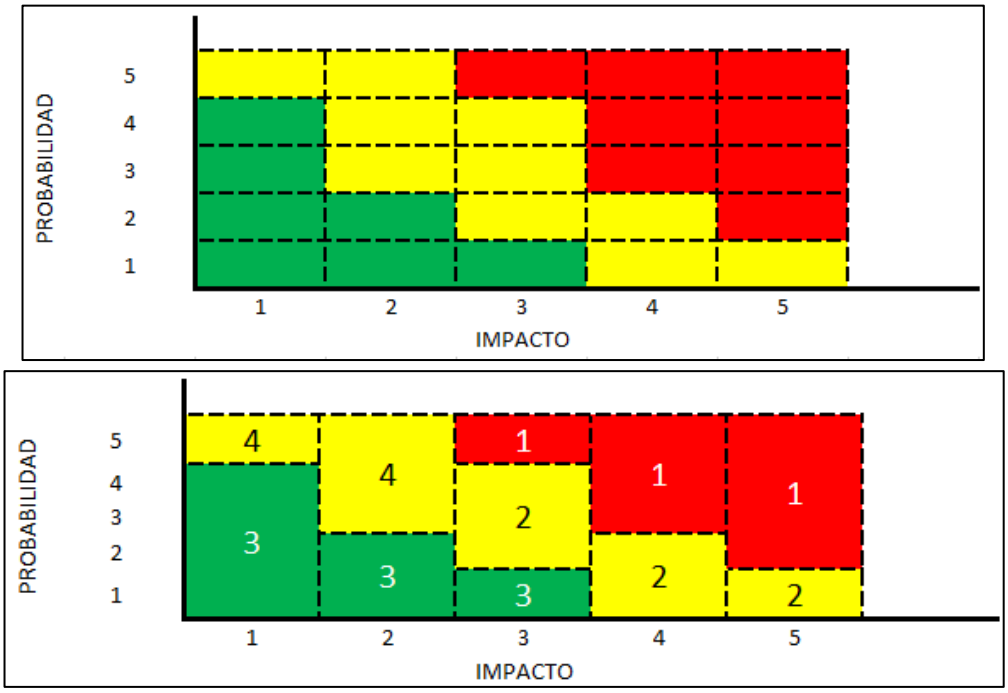
Zona 1: son los riesgos probables pero que se caracterizan por tener un alto impacto.

Zona 2: cubre un rango de situaciones que pueden ser improbables y que conllevan a un impacto medio, pero también aquellas que son muy probables, pero de impacto bajo y muy bajo

Zona 3: Son los riesgos improbables que tiene un impacto bajo.

Zona 4: Son los riesgos improbables que tiene un impacto alto

Tabla 6. Matriz de riesgos



10.3. Tratamiento del riesgo

El tratamiento de riesgo es el conjunto de procedimientos y elementos tecnológicos que permiten reducir de manera preventiva las amenazas buscando como objetivo limitar prevenir disuadir corregir y eliminar la posible amenaza que puede materializarse sobre el activo. Dicho lo anterior dentro de la metodología de Magerit se exponen tres opciones para tratar el riesgo los cuales esta metodología los define como ELIMINACIÓN la cual es considerada como una opción hacia un riesgo que no es aceptable siempre y cuando este no afecte a la organización en este caso al llegar a tomar esta opción se tendría prácticamente que reevaluar la misión de dicha organización. Sin embargo, puede esta eliminar algún activo y poder reemplazarlo para erradicar el riesgo presente o pueda realizar un hardening o más conocido como robustecimiento de la infraestructura de red que se tiene actualmente el cual implica reordenar realizar un esquema de segmentación y aislamiento de las redes.

Otra de las opciones de tratamiento del riesgo es la MITIGACIÓN del riesgo el cual se asocia a deducir la degradación que se genera por la amenaza o que pueda llegar a reducir o

minimizar la probabilidad de que la amenaza se pueda llegar a materializar esto implicaría generar medidas cautelarías o de seguridad sobre los activos más relevantes conteniéndolos con ayuda de nuevos equipos esta opción implicaría generar un nuevo análisis involucrando estos equipos que ayudarían a mitigar el riesgo.

Magerit involucra otra opción de tratamiento del riesgo el cual lo llama como COMPARTICIÓN o TRANSFERENCIA DEL RIESGO el cual describe que se puede transferir el riesgo de forma parcial o total de los activos a un tercero que los administre correctamente y que a su vez estas dos empresas asuman en un porcentaje los riesgos. Como se mencionó anteriormente esta transferencia o compartimiento de riesgos se pueden ejecutar de dos formas como lo son el riesgo cualitativo y el riesgo cuantitativo los cuales se describen a continuación:

RIESGO CUALITATIVO: Este método pretende que tanto la empresa como quien opera y administra los activos los administre adecuadamente y por parte de la organización se tendrán en cuenta las acciones legales que implicarían en sanciones al no operarlas y administrarlas adecuadamente.

RIESGO CUANTITATIVO: Este método opta por compartir por medio de la contratación de seguros asegurando cada uno de los activos ante una eventualidad esta le dé un porcentaje del valor total o parcial del o los activos más relevantes del negocio.

Por último, se habla de la opción de aceptación del riesgo en la cual la organización no ejecuta ninguna medida, pero en caso de que llegase a materializarse una amenaza la organización tendría que disponer de algún fondo o reserva para invertir nuevamente sobre el o los activos afectados y reponerlos.

Descrito lo anterior y recopilando la información de los capítulos anteriores se pude concluir que el valor del riesgo al conocer el impacto de las amenazas que se presentan sobre los activos de involucrados se determina el riesgo teniendo en cuenta la probabilidad de que este ocurra dado que el riesgo incrementa o disminuye con el impacto por tanto para saber el valor del riesgo que acción tomar de las que se mencionaron anteriormente se genera una formula la cual consiste

en tomar el valor total de activo (C, I y D) * la probabilidad de que ocurra * por el impacto que este generaría al materializarse y esto nos daría el valor del riesgo el cual asociado a una escala se procedería aceptar, reducir, compartir o transferir.

$$C \times D \times I \times P \times I = \text{Valor total del riesgo}$$

No obstante, para realizar una valoración dentro del análisis de riesgos y según lo mencionado anteriormente se da una valoración de escala de la siguiente manera en el que la empresa dependiendo el valor que arroje el valor de riesgo sobre el activo determinaría la importancia y criticidad del mismo para así tomar las medidas necesarias en las que constaría asumir el riesgo, compartirlo, transferirlo o eliminarlo.

Tabla 7. Escala de tratamiento de riesgo

ANALISIS DE RIESGOS	
V.T.RIESGO	**VALORACIÓN**
0-32	**ACEPTACION DEL RIESGO**
32-108	**SE COMPARTE O TRANSFIERE**
108-350	**SE TRANSFIERE O ELIMINA**

10.4. Salvaguardas

Son aquellas medidas, procedimientos o mecanismos de avance tecnológico los cuales permiten reducir el riesgo de un activo para ello se requiere realizar una valoración de los mismos con el propósito de verificar que dichas medidas procesos o mecanismos de protección estén funcionando de manera correcta o para ser ajustados con el fin de que estos solventes mitiguen o reduzcan la amenaza.

Dentro de las salvaguardas se pueden emplear procedimientos, políticas, soluciones

técnicas, capacitación a personal, robustecimiento de equipos que realmente cumplan con el objetivo de asegurar proteger y analizar tráfico indebido o malicioso, este varía según el avance tecnología.

11. Análisis de vulnerabilidades

Un análisis de vulnerabilidades informáticas tiene como finalidad principal buscar y analizar un sistema informático, con unas características definidas y asociadas al tipo de la organización, es decir cada sistema informático está ajustado a la necesidad de una organización. En el caso de la compañía está ajustada a la necesidad de los usuarios y sus trabajadores según lo expresa el cliente.

Se va realizar un análisis profundo de todos los dispositivos de red de la compañía, los cuales nos van arrojar algunas vulnerabilidades las cuales se tendrán en cuenta al realizar una serie de recomendaciones de lo encontrado.

11.1 ¿Qué es un análisis de vulnerabilidades?

El objetivo principal de un análisis de vulnerabilidades consiste en el descubrimiento, identificación y clasificación de las debilidades o las vulnerabilidades presentes en distintos dispositivos de la red; (Servidores, router, Access Point, DVR, etc.) de una compañía. Al realizar dicho análisis se logra obtener provecho ya que recolecta adicionalmente los activos de infraestructura con los que cuenta la compañía.

Castro I (2016-26-06) “Hoy en día todas las organizaciones y personas utilizan dispositivos inteligentes, computadoras, redes inalámbricas, etc. Y están expuestas a diferentes amenazas cibernéticas derivadas de la utilización de páginas web, apps, documentos, correos electrónicos, servicios de chat, redes sociales, etc.

La mayoría de estas amenazas están siendo creadas para extraer información personal o corporativa y con esto realizar ataques dañinos que vulneran nuestra capacidad para realizar transacciones, acceso a documentos, sistemas internos, etc.

Mientras que por un lado hoy tenemos a la disposición cientos de servicios de interconexión entre personas y organizaciones, por el otro estamos teniendo mucha mayor exposición de nuestra información personal y corporativa hacia personas no autorizadas que utilizan diferentes métodos para atacar y estos están siendo cada vez más complejos, más difíciles de prevenir y sobre todo más dañinos. Esto ha llevado a las organizaciones a poner mucho más énfasis en la ciberseguridad y los aspectos preventivos y correctivos ante un ataque.

Dentro de una correcta planeación de protección preventiva y correctiva se debe de considerar el análisis de vulnerabilidades como una actividad clave para asegurar que estamos al día ante la creciente ola de amenazas que día a día va creciendo de manera exponencial."

11.2 ¿Por qué hacer un análisis de vulnerabilidades?

Como bien se sabe en esta investigación es necesario conocer cómo esta nuestra infraestructura y toda la información relevante; cual es la mejor manera de protegerla y qué medidas tomar en caso de un ataque.

11 .3 Herramientas para realizar análisis de vulnerabilidades

Se van a utilizar ciertas herramientas para hacer un análisis avanzado de la red local de la oficina para a si mismo poder realizar una serie de recomendaciones

Nessus es una herramienta de análisis de vulnerabilidades en la red la cual permite encontrar ciertos problemas de configuración, para conocer un poco más de su definición y sus características según el sitio Web define "Nessus es el estándar mundial para la prevención de ataques de red, identificación de vulnerabilidades y detección de problemas de configuración que utilizan los hackers para entrar en la red. Nessus se ha utilizado por más de 1 millón los usuarios en todo el mundo, por lo que es el líder mundial de evaluación de la vulnerabilidad, configuración de seguridad y cumplimiento de las normas de seguridad." (Gb advisor, 2000, p.18).

Nmap es un software de análisis de vulnerabilidades en la red totalmente gratuito y disponible para los 3 principales sistemas operativos (Windows, Linux Mac os), es una herramienta de código abierto para exploración de red y auditoría de seguridad. Se diseñó para analizar rápidamente grandes redes, aunque funciona muy bien contra equipos individuales. Nmap utiliza paquetes IP "crudos" («raw», N. del T.) en formas originales para determinar qué equipos se encuentran disponibles en una red, qué servicios (nombre y versión de la aplicación) ofrecen, qué sistemas operativos (y sus versiones) ejecutan, qué tipo de filtros de paquetes o cortafuegos se están utilizando, así como docenas de otras características. Aunque generalmente se utiliza Nmap en auditorías de seguridad, muchos administradores de redes y sistemas lo encuentran útil para realizar tareas rutinarias, como puede ser el inventariado de la red, la planificación de actualización de servicios y la monitorización del tiempo que los equipos o servicios se mantiene activos." https://nmap.org/man/es/index.html#man-description.

Para este análisis se realizó la instalación de un S.O Kali-linux el cual ya trae la herramienta por defecto install.

12. Hardening

El Hardening consiste en el proceso de fortalecer sistema mediante la reducción o mitigación de las vulnerabilidades y riesgos. Las actividades dentro del proceso de hardening en gran parte son realizadas por el administrador del sistema quien elimina software, servicios, usuarios, etc.; innecesarios en el sistema.

Paul Castro en su blog Smartekh (2019) ¿QUÉ ES HARDENING? Establece unas actividades para el desarrollar el proceso de Hardening, Son las siguientes:

Configuraciones necesarias para protegerse de posibles ataques físicos o de hardware de la máquina, Por ejemplo: actualizaciones de firmware, establecer contraseñas fuertes para el inicio del sistema y acceso a la BIOS, deshabilitar el inicio del sistema operativo desde otra unidad que no sea el disco duro principal, deshabilitar las unidades ópticas, puertos usb para evitar que malware malicioso pueda ser inyectado desde un flash driver.

Instalación segura del sistema operativo, Esto implica, entre otras cosas, el considerar al menos dos particiones primarias (para el sistema operativo en sí y otra para carpetas y archivos de importancia), el uso de un sistema de archivos que tenga prestaciones de seguridad, y el concepto de instalación mínima, es decir, evitando la instalación de cualquier componente de sistema que no sea necesario para el funcionamiento del sistema. (Castro, 2019, p. 10).

Activación y/o configuración adecuada de servicios de actualizaciones automáticas, para asegurar que el equipo tendrá todos los parches de seguridad que entrega el proveedor al día. En caso de que se encuentre dentro de una corporación, es adecuado instalar un servidor de actualizaciones, que deberá probar en un entorno de laboratorio el impacto de la instalación de actualizaciones antes de instalarlas en producción.

Instalación, configuración y mantención de programas de seguridad tales como Antivirus, Antispyware, Antispam según las necesidades del sistema.

Configuración de la política local del sistema, considerando varios puntos relevantes: Política de contraseñas robusta, con claves caducables, almacenamiento histórico de contraseñas (para no usar contraseñas cíclicas), bloqueos de cuentas por intentos erróneos y requisitos de complejidad de contraseñas. Renombramiento y posterior des habilitación de cuentas estándar del sistema, como administrador e invitado. Asignación correcta de derechos de usuario, de tal manera de reducir las posibilidades de elevación de privilegios, y tratando siempre de limitar al mínimo los privilegios y/o derechos de los usuarios activos. (Castro, 2019).

Configuración de opciones de seguridad generales, como aquellas relacionadas con rutas de acceso compartido, apagado de sistema, inicio y cierre de sesión y opciones de seguridad de red.

Restricciones de software, basado en lo posible en el uso de listas blancas de software permitido más que en listas negras del mismo.

Activación de auditorías de sistema, claves para tener un registro de algunos intentos de ataque característicos como la adivinación de contraseñas.

Configuración de servicios de sistema. En este punto es necesario tratar siempre de deshabilitar todos aquellos servicios que no vayan a prestar una funcionalidad necesaria para el funcionamiento del sistema. Por ejemplo, si su equipo no posee tarjetas de red inalámbrica, el servicio de redes inalámbricas debería estar deshabilitado.

Configuración de los protocolos de Red. En la medida de lo posible, es recomendable usar sistemas de traducción de direcciones (NAT) para direccionar los equipos internos de una organización. Deshabilitar todos aquellos protocolos de red innecesarios en el sistema y limitar el uso de los mismos al mínimo. TCP/IP es un protocolo que no nació pensando en seguridad, por lo que limitar su uso al estrictamente necesario es imperativo.

Configuración adecuada de permisos de seguridad en archivos y carpetas del sistema. En la medida de lo posible, denegar explícitamente cualquier permiso de archivo a las cuentas de acceso anónimos o que no tengan contraseña. Un correcto set de permisos a nivel de carpetas y archivos es clave para evitar acceso no deseado al contenido de los mismos.

Configuración de opciones de seguridad de los distintos programas, como clientes de correo electrónico, navegadores de internet y en general de cualquier tipo de programa que tenga interacción con la red.

Configuración de acceso remoto. En caso de no ser estrictamente necesario, es bueno deshabilitar el acceso remoto. Sin embargo, cuando es necesario tener control remoto de la máquina, es preciso configurarlo de manera adecuada, restringiendo el acceso a un número muy limitado de usuario, restringiendo al mínimo las conexiones concurrentes, tomando cuidado en la desconexión y cierre de sesión y estableciendo un canal cifrado de comunicaciones para tales propósitos, como SSH.

Configuración adecuada de cuentas de usuario, tratando de trabajar la mayor parte del tiempo con cuentas de acceso limitado y deshabilitando las cuentas de administrador. Es absolutamente recomendable usar la personificación de usuarios para realizar labores administrativas en vez de

iniciar sesión como administradores.

Cifrado de archivos o unidades según las necesidades del sistema, considerando un almacenamiento externo para las llaves de descifrado. Considerar además la opción de trabajar con sistemas de cifrado de mensajería instantánea y correo electrónico.

Realizar y programar un sistema de respaldos frecuente a los archivos y al estado de sistema. En la medida de lo posible, administrar los respaldos vía red o llevar los respaldos a unidades físicas que estén alejadas del equipo que las origina.

Todas las actividades anteriormente mencionadas deben ser evaluadas y equilibradas con el objetivo de negocio de la empresa, en tanto a que no vayan a ser restrictivas con el negocio, si no por el contrario deben estar alineadas.

Entre las ventajas del proceso de hardening está la disminución de incidentes de seguridad, quitar carga inútil al sistema y con ello mejorar el rendimiento, administración más simple, rapidez en la identificación de problemas y hacer seguimiento a los incidentes.

13. Resultados

En este capítulo se exponen los resultados que se realizaron analizaron y ejecutaron durante los capítulos descritos anteriormente no obstante se socializó con la empresa los resultados y esta acogerá las recomendaciones con el fin de mitigar las vulnerabilidades y los riesgos a los que se está expuesta.

13.1 Resultados de identificación y clasificación de activos

Se realiza dicha identificación y clasificación de activos con visitas y entrevistas con los directos implicados o responsables del manejo los mismos. Se procede a crear una plantilla en Excel donde se pueda llenar la información de forma clara y concisa, dicha plantilla de inventarios y clasificación nos permite de forma general identificar y describir cada uno de los activos

encontrados en las tres sedes de la empresa ALIMENTOS PHD. Se genera una forma de identificación en el que se evidencia ID de activo, Activo (nombre del equipo), Descripción del equipo o especificaciones técnicas, Tipo (hardware o dato) dueño del activo (área o dependencia) y Ubicación (donde se encuentra el activo).

Tabla 8. Formato de inventario de activos de información

Proceso:	Clasificación de Activos						**Fecha :**					
ID	**Activo**	**Descripción**	**Tipo**	**Dueño del Activo**	**Dependencia**	**Ubicación**	**Clasificación**				**Reglas**	
							C	**I**	**D**	**Valor Activo**	**Nivel de acceso**	**T. Conservación**

.

Sin embargo la identificación y clasificación de activos se divide en tres partes donde se identifican en primera instancia activos de información seguido de los activos de red y por ultimo un inventario relacionado con el factor humano el cual no deja de ser significativo para el análisis dado que las personas en algunos aspectos de evaluación y análisis no son tomados en cuenta pero es necesario ya que las personas en este caso trabajadores y externos son un eslabón muy débil por el que se puede filtrar o generar una afectación o perdida de información y que pueda incurrir en la continuidad del negocio.

Se individualiza o separan los activos mencionados anteriormente para identificar y generar el respectivo análisis de riesgo que se establece, identifican; Esta identificación se plasma en la plantilla mencionada anteriormente para cada activo.

Este nos permite conocer los diferentes riesgos a los que la empresa puede estar expuesta generando afectación en la confidencialidad integridad y disponibilidad de la información en los activos de información que se identifican en las diferentes sucursales y la sede principal para ellos se debe en primera instancia identificar y clasificar los activos de información, posteriormente se debe identificar el riesgo asociado al activo de información.

Como se menciona se da inicio con el inventario de información el cual se expone a continuación:

13.1.1. Inventario de activos de información

Tabla 9. Inventario de activos de información

ID	Activo	Descripción	Tipo
1	ARCHIVO BACKUPS BASE DE DATOS	ALMACENAMIENTO INFORMACION CLIENTES Y PROVEEDORES/SQL	Datos
2	CARPETAS DE INFORMACION PROVEEDORES	INFORMACION DE PROVEEDORES	Documento
3	OFIMATICA (OFFICE 365)	LICENCIAS SOFTWARE OFIMATICO	Software
4	SERVIDOR	ALMACENAMIENTO INFORMACION CLIENTES Y PROVEEDORES/SQL	Hardware

13.1.2. Inventario de activos de red

Tabla 9. Inventario de activos de red

ID	Activo	Descripción	Tipo
1	ROUTER ADSL	SERVICIO DE INTERNET SEDE PRINCIPAL Y SUSCURSALES (4)	Hardware
2	FIREWALL	SEGURIDAD PERIMETRAL	Hardware
3	SERVIDOR	ALMACENAMIENTO INFORMACION CLIENTES Y PROVEEDORES/SQL	Hardware/Datos
4	DVR	Repositorio de videos de seguridad	Hardware/Datos
5	UBIQUITI	Pc de escritorio	Hardware/Datos
6	EQUIPO DE ESCRITORIO	Pc de escritorio (4)	Hardware/Datos

13.1.3. Inventario factor humano

Tabla 10. Inventario de activo factor humano

ID	ACTIVO	DESCRIPCION	TIPO
1	GERENTE	DUEÑO DE LA EMPRESA	DATOS
2	SUPERVISOR	ADMINISTRADOR DE LAS SEDES	DATOS
3	ANALISTA CONTABLE	ADMINISTRADOR CONTABLE	DATOS
4	TECNICO	SOPORTE TECNICO DE SEDES (OUTSOURCING)	DATOS
5	VENDEDORES	SUPERNUMERARIOS DE TIENDAS	DATOS
6	VIGILLANTES	GUARDAS DE SEGURIDAD	DATOS
7	CLIENTES	COMPRADORES	DATOS

14. Identificación de amenazas y riesgos en la empresa alimentos PHD

Dentro de esta fase de resultados se identifica la amenaza o vulnerabilidad presente en los diferentes activos de información, de red más significativos para la empresa tales como el firewall y el servidor, y factor humano los cuales identifican sobre la empresa ALIMENTOS PHD. Estas amenazas o riesgos identificados en los activos corresponden al suministro de información de la metodología Magerit en su catálogo de elementos adicional a esto se realiza un escaneo de vulnerabilidades mediante los aplicativos tales como Nessus con el que fue posible realizar el análisis de vulnerabilidades a la red de datos de la compañía no obstante se utiliza **Nmap** en un Kali-Linux para hacer el barrido de puertos con el propósito de ajustar y correlacionar las vulnerabilidades encontradas en los equipos específicos mencionados anteriormente con referencia al suministro referido por la metodología aplicada. Cable aclarar a solicitud de la empresa ningún direccionamiento de red y nombres del personal que labora en ella se puede exponer; Los resultados obtenidos del análisis realizado se discutirán en el siguiente capítulo con mayor amplitud.

Adicional a esto Se reitera que el proceso de identificación y valoración de activos que comprenden la información, red y factor humano se trabajaron y valoraron de manera separada teniendo así tres matrices de riesgos por cada clasificación de activos.

14.1 Evaluación de riesgos

A continuación, se describen dichos inventarios con las amenazas o riesgos respectivos con la probabilidad he impacto que se generan por cada activo identificado. Cabe resaltar que dentro de los objetivos específicos del proyecto no se incluye la ejecución o implementación de los controles que conlleven a la mejora y mitigación de las falencias encontradas en los diferentes activos; este proyecto brinda única y exclusivamente la identificación y las recomendaciones establecidas en la industria para mitigarlas y asegurar la continuidad de negocio.

14.1.1 Evaluación del riesgo de información (EDRI)

Tabla 11. EDRI

EVALUACIÓN DEL RIESGO DE INFORMACIÓN						
ACTIVO	ID ACTIVO	AMENAZA/RIESGO	ID RIESGO	VULNERABILIDAD	PROBABILIDAD	IMPACTO
ARCHIVO BASE DE DATOS	1	FALLA TECNICA	R1	ENERGIA ELECTRICA	3	5
			R2	ERROR DE USUARIO	4	4
		ERRORES DE CÓDIGO	R3	PERSONAL NO CALIFICADO	1	3
CARPETAS DE INFORMACION PROVEEDORES	2	ROBO DE INFORMACIÓN	R4	LA INFORMACION DE PROVEEDORES SE ENCUENTRA VISIBLE PARA TODOS LOS TRABAJADORES	4	5
		INCENDIO	R5	PERDIDA DE INFORMACION POR DESASTRE	1	4
OFIMATICA (OFFICE 365)	3	ERRORES DE CÓDIGO	R6	ERRORES POR NATENIMIENTO /ACTUALIZACIONES DE LA HERRAMIENTA	2	4
		ROBO DE INFORMACIÓN	R7	ACCESO NO CONTROLADO	3	5
SERVIDOR	4	FALLA DE RED	R8	CAIDA DE SERVICIO	2	2
		ROBO DE INFORMACIÓN	R9	ACCESO NO CONTROLADO	4	5
		FALLA ELECTRICA	R10	PERDIDA DE FLUIDO ELECTRICO	4	4

14.1.2. Evaluación de riesgos de red (EDRR)

Como se mencionó Anteriormente se realiza la evaluación sobre todos los activos de red sin embargo se realiza el análisis de vulnerabilidad sobre los activos más relevantes de la empresa como los son firewall y el servidor ya que son administrados por un técnico (outsourcing) y la gerencia solicito realizarlo específicamente sobre estos dos activos.

A continuación, se describe el análisis y resultados generados mediante el mismo, sobre estos dos activos y posteriormente se realizará la evaluación de riesgos involucrando los demás activos de red de la empresa. Para ellos se inicia el análisis del estado en que se encuentra el firewall mediante NESUS.

14.1.3. Análisis de vulnerabilidad del firewall

En este subtema, como se ha venido mencionado, se realiza el análisis de vulnerabilidades a la red de datos de la compañía, esto con el fin de encontrar las falencias y lo que necesitamos reforzar. Esta herramienta Nessus nos permite realizar un barrido inicial de la red local de la siguiente manera.

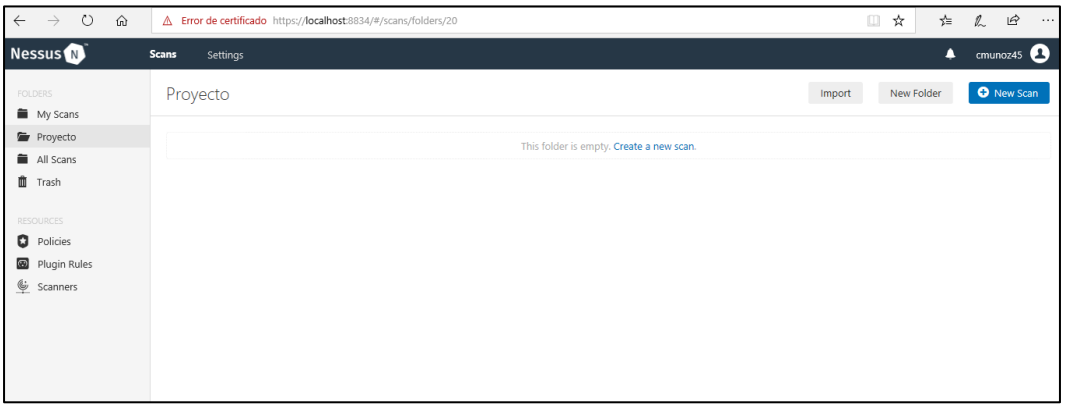


Ilustración 4. Proyecto Inicial para realizar el análisis

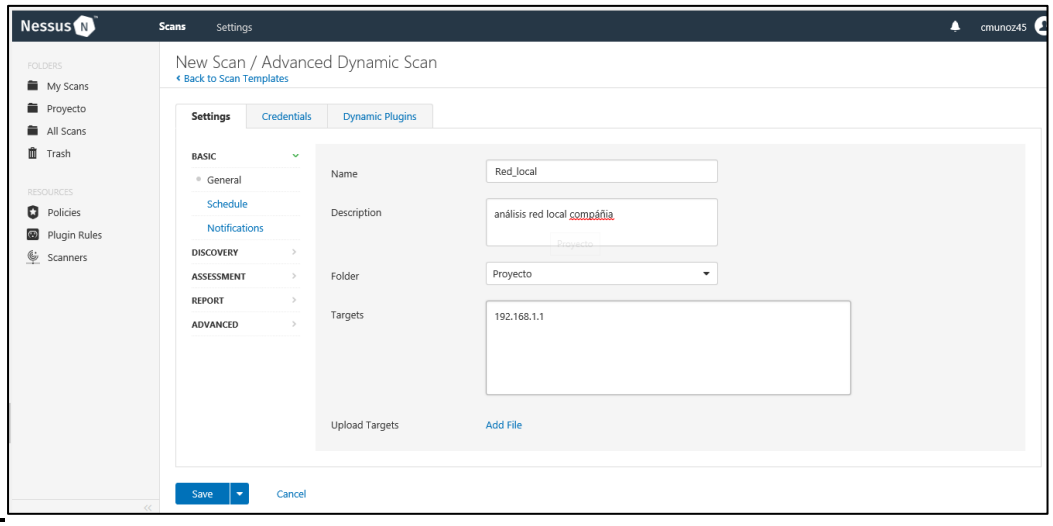


Ilustración 5 .Configuración direccionamiento red local IP firewall

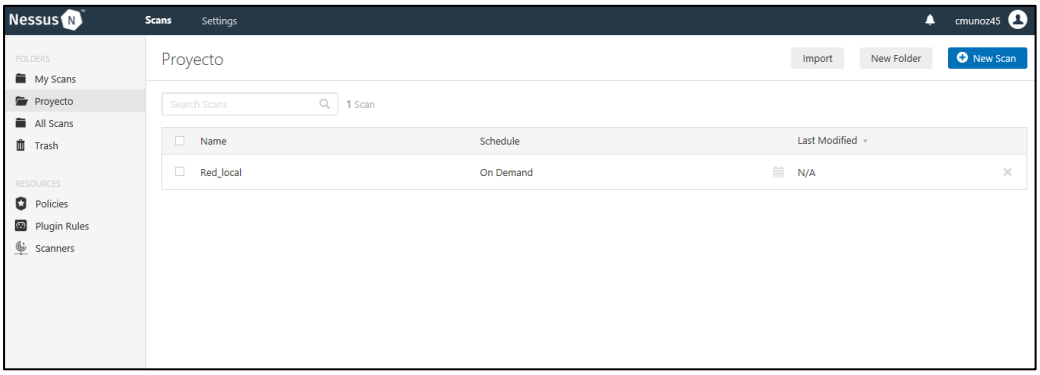


Ilustración 6 Análisis Inicial Firewall

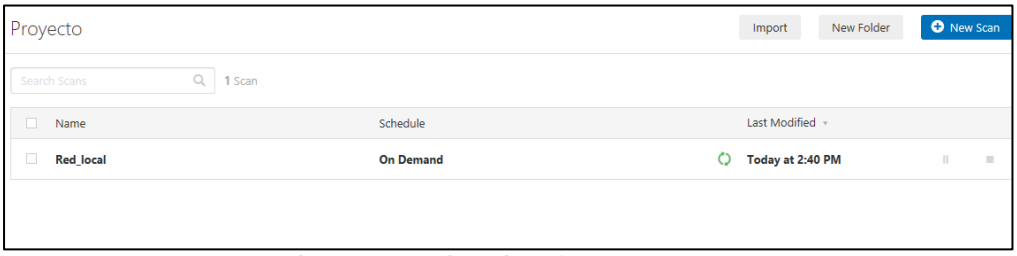


Ilustración 7 Finalización análisis firewall

Una vez termina el escaneo este nos arroja unas estadísticas que indican las vulnerabilidades presentes sobre el equipo.

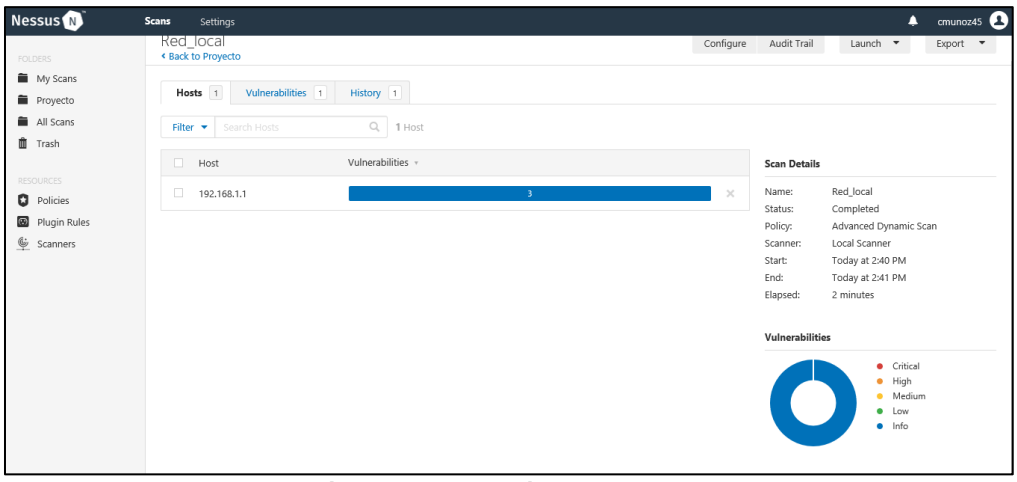


Ilustración 8 Resultados Análisis de vulnerabilidades

Como se puede observar encontró 3 vulnerabilidades en el firewall debemos realizar la validación de dichas vulnerabilidades.

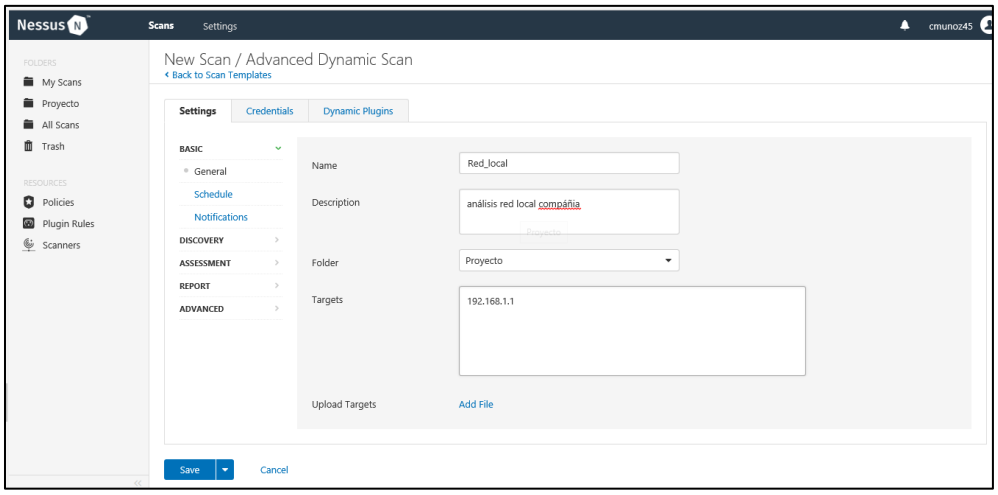


Ilustración 9 Análisis 2 firewall

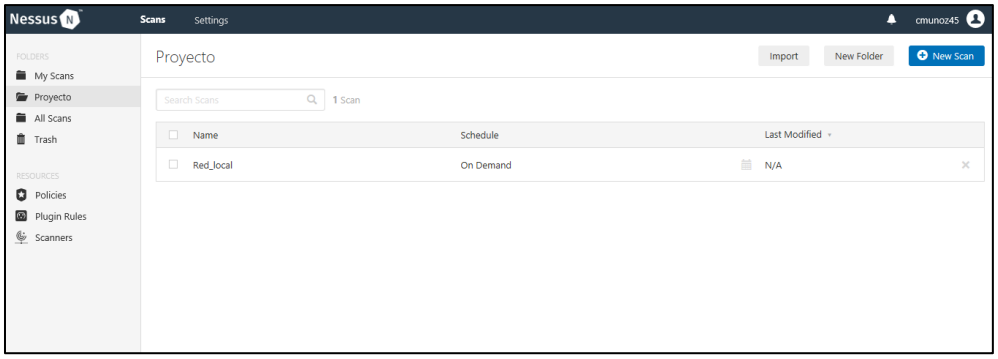


Ilustración 10 Finalización Análisis 2 avanzado

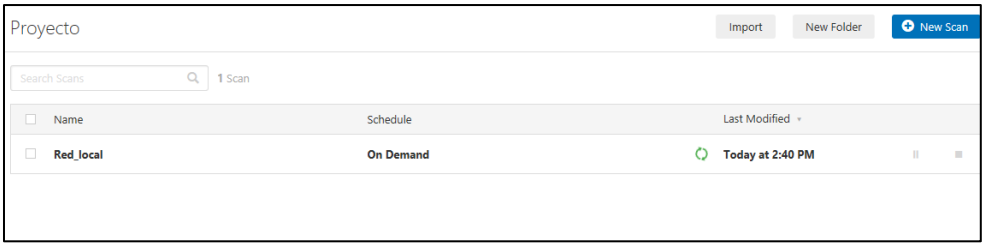


Ilustración 11. Proyecto Nessus finalizado

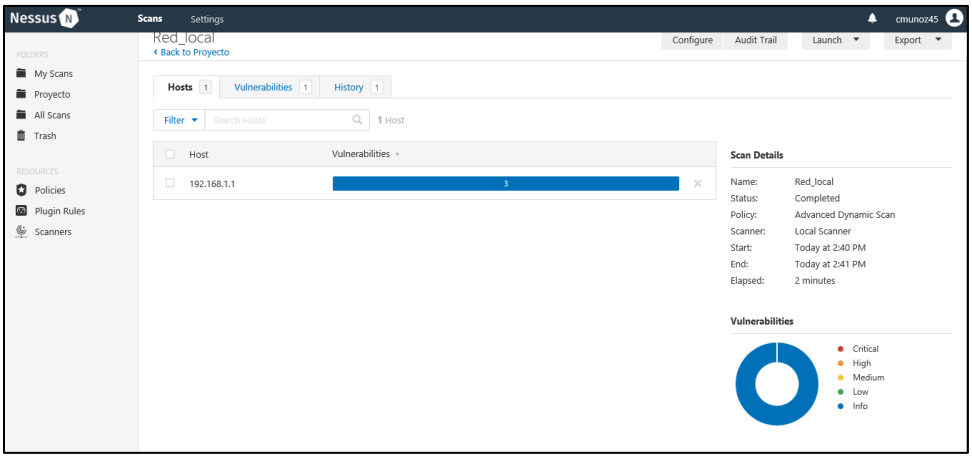


Ilustración 12 .Validación resultados análisis 2

Como se puede observar se encontraron 3 vulnerabilidades en el firewall debemos realizar la validación de dichas vulnerabilidades.

14.1.4 Vulnerabilidades a nivel del firewall

Vulnerabilidad # 1. Esta vulnerabilidad hace referencia a los

Ataques a los cuales está expuesto el puerto SSH 22 y su recomendación es hacer el cierre de dicho puerto, este puerto se encuentra actualmente en este estado ya que se realizan configuraciones del firewall por este medio, Las recomendaciones con respecto a este puerto se muestran en el capítulo de hardening y en el anexo de recomendaciones.

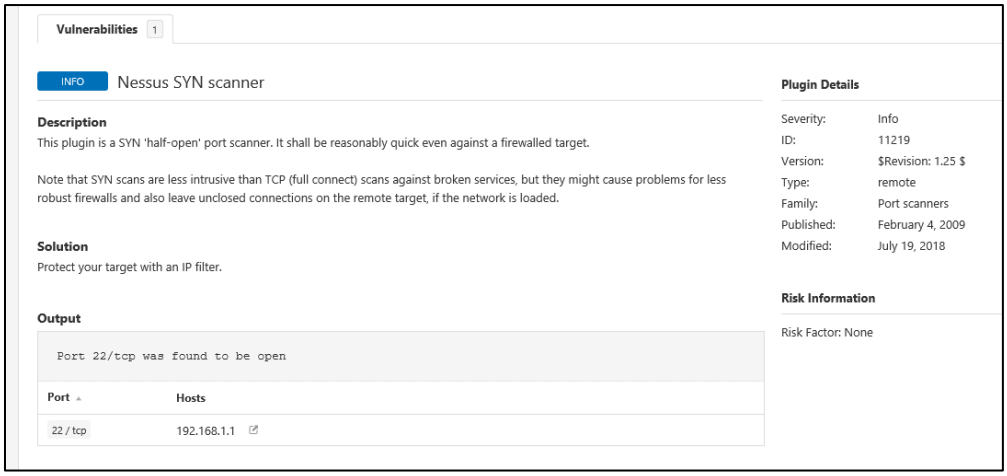


Ilustración 13. Vulnerabilidad puerto SSH

Vulnerabilidad # 2. Para esta vulnerabilidad que se encontró se debe validar el tipo de firewall que se tenga en este caso un fortigate y el utiliza este puerto para el forti manager y en este caso es un ambiente controlado y seguro.

Ilustración 14. Vulnerabilidad puerto 541

Vulnerabilidad # 3. Como se puede observar el puerto 80 sale como una vulnerabilidad, pero como lo sabemos todo sitio no seguro que sale a internet o expone sus servicios por dicho puerto; Las recomendaciones con respecto a este puerto se muestran en el capítulo de hardening.

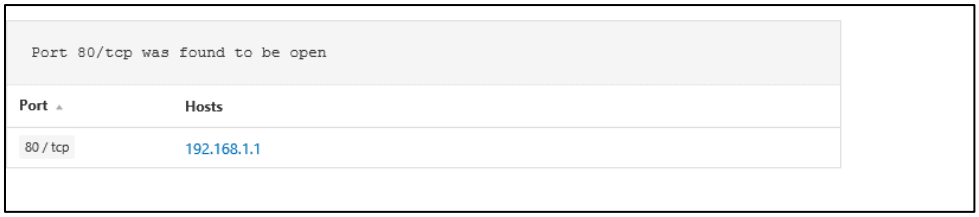


Ilustración 15 .Vulnerabilidad puerto 80

14.1.5 Análisis puertos Firewall con Nmap

Se realiza la instalación de la herramienta Nmap en un Kali-Linux para hacer el barrido de puertos desde la misma red local y el resultado es el siguiente:

```
Nmap done: 1 IP address (1 host up) scanned in 4.72 seconds
[root@jlvazquez docker]# nmap 192.168.1.1

Starting Nmap 6.40 ( http://nmap.org ) at 2019-03-11 15:46 -05
Nmap scan report for fwsoaint.soain.lcl (192.168.1.1)
Host is up (0.00041s latency).
Not shown: 996 filtered ports
PORT    STATE  SERVICE
22/tcp  open   ssh
80/tcp  open   http
113/tcp closed ident
541/tcp open   uucp-rlogin
MAC Address: 90:6C:AC:B8:2A:CC (Unknown)
```

Ilustración 16. Análisis firewall Nmap

A diferencia de la herramienta Nessus se pueden observar los puertos que no se encuentran abiertos como lo es el caso del puerto 113 que es de autenticación identificación local.host

Como recomendaciones generales, para tener una red segura y poco vulnerable es necesario cambiar los puertos SSH y HTTP por que como se sabe todos los ataques van dirigido hacia estos puertos ya que son los más conocidos y como altas fallas.

14.1.6 Vulnerabilidades servidor principal

El servidor principal es el encargado de realizar la conexión externa con todas las demás sedes; como se había mencionado anteriormente por medio del protocolo RDP, el objetivo es realizar un análisis general del equipo para poder validar las vulnerabilidades a las cuales puede estar expuesto y así mismo recomendar como es la mejor manera de evitarlo.

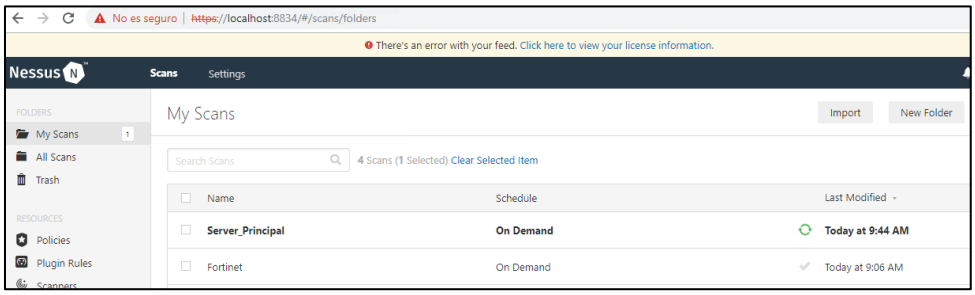


Ilustración 17. Análisis Servidor Principal

Se deben validar las vulnerabilidades a fondo para poder realizar recomendaciones pertinentes.

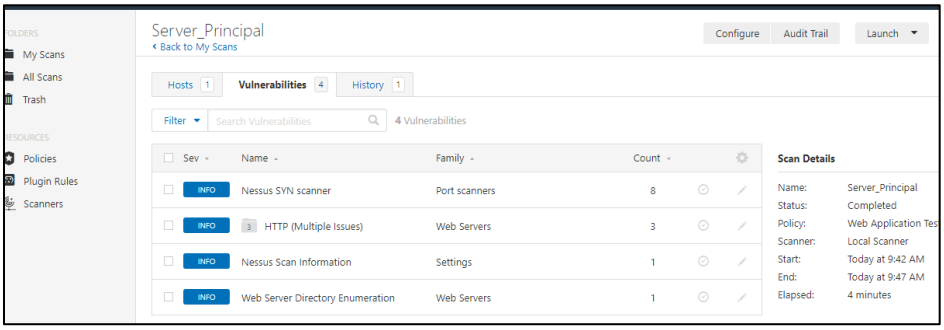


Ilustración 18. Análisis finalizado

14.1.7 Validación Puertos

Puerto 135; Su funciona es realizar la conectividad de máquinas en la red Cliente-Servidor, según recomendaciones Microsoft no es necesario realizar el cambio de dicho puerto ya que podría generar conflictos con las distintas distribuciones de sistemas operativos.

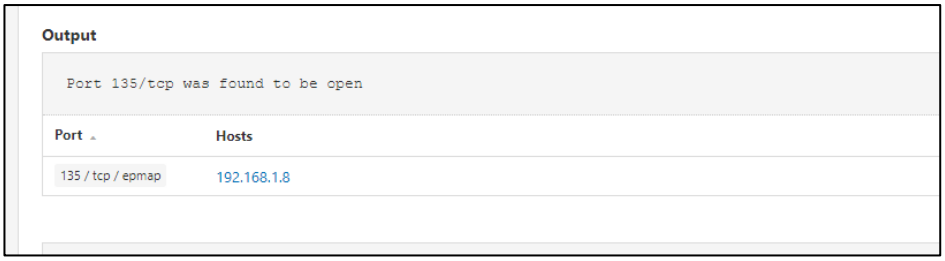


Ilustración 19 Vulnerabilidad puerto 135

Puerto 139; Como se sabe este puerto está atado a protocolo de seguridad del Netbios y se han hecho bastantes análisis de vulnerabilidad y se puede decir que es seguro.

Ilustración 20 Vulnerabilidad puerto 139

Ilustración 21 .Vulnerabilidad puerto 443

Puerto 443; este puerto este asignado a la navegación segura, por lo tanto, se le recomienda al cliente deshabilitar el servicio y cerrar el puerto y que desde el servidor no es necesario tener navegación.

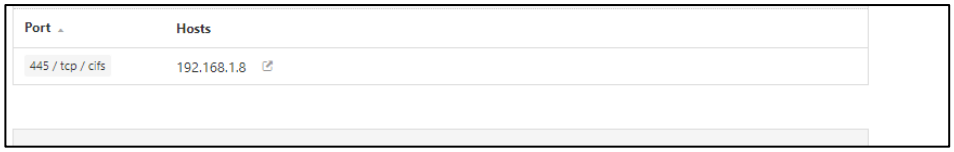


Ilustración 22 .Vulnerabilidad puerto 445

Puerto 445 comparte sus recursos de red a través del puerto 445 como se implementó en Windows 7 es más eficiente que la ejecución de SMB en este caso para los archivos compartidos es más eficiente.

Ilustración 23. Vulnerabilidad puerto 1688

Puerto 1688 al igual que los anteriores, su función es la transmisión de datos por medio del protocolo TCP/UDP, pero para este caso en especial normalmente hacen la apertura de dicho puerto para la activación de productos en la red, un ejemplo bastante claro o común es la activación simultanea de los antivirus con un Cliente-Servidor.

Ilustración 24 .Vulnerabilidad puerto 3389

Puerto 3389 Como se sabe este es el puerto del protocolo RDP el cual está utilizando la compañía para su conexión, como recomendaciones directas de Microsoft no se debería cambiar, para poner más seguro dicho protocolo sería bueno tener un Firewall el cual proteja como tal toda la red local. En el anexo de hardening del firewall se especifica la regla a configurar para este servicio.

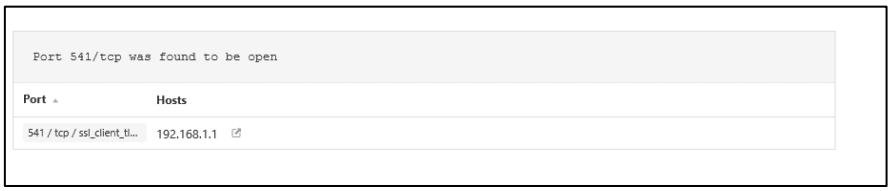


Ilustración 25 .Vulnerabilidad puerto 541

Puerto 541 este puerto es el que utiliza fortigate para la autenticación de la aplicación web como tal.

14.1.8 Validación Puertos desde el PowerShell de Windows

Se pueden realizar validaciones de acceso o test de los puertos abiertos de igual manera desde el PowerShell de Windows de la siguiente manera.

Prueba desde el servidor principal al firewall (fortigate) con napeo al puerto 80

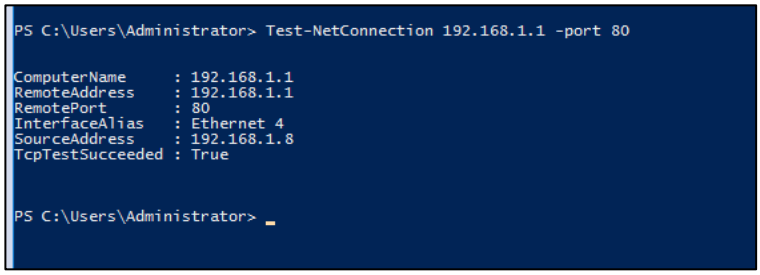


Ilustración 26 .Validación Acceso puerto 80

Prueba desde el servidor principal al firewall (fortigate) con napeo al puerto 22 SSH.

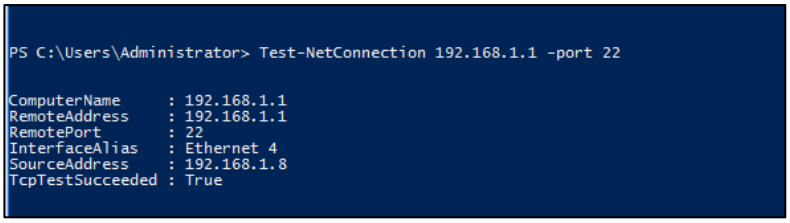


Ilustración 27 Validación Acceso puerto 22

Validación puertos abiertos Firewall y Servidor RDP mediante NMAP

14.1.9 Servidor RDP

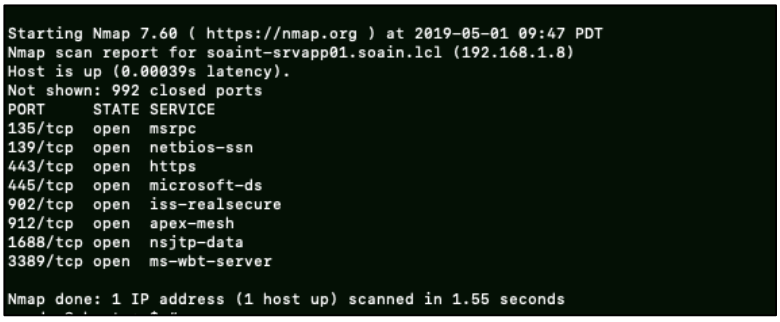


Ilustración 28. Análisis Servidor con Nmap

Se realiza el análisis del servidor RDP que es al que se conectan las demás sedes y se puede ratificar el análisis del Nessus, de igual manera se podrán tomar ciertas recomendaciones para su seguridad perimetral.

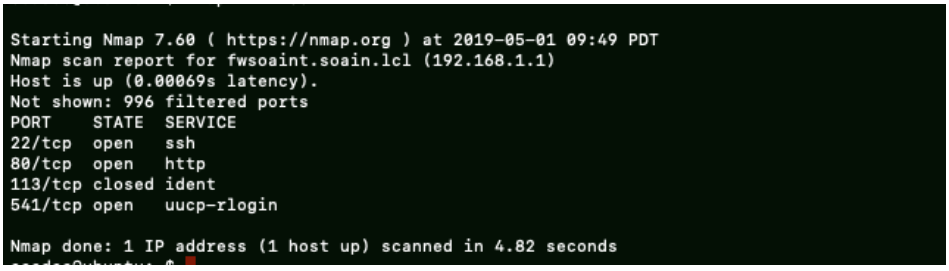


Ilustración 29 .Análisis Firewall con Nmap

A nivel del firewall actualmente solo se tienen abiertos los puertos identificados como seguros adicionalmente el puerto 541 para la autenticación, para realizar la implementación de una

VPN esto haría la red local y expuesta a internet más segura.

Para este análisis de riesgos de red una vez obtenidos los resultados de escaneo de vulnerabilidades y de haber identificado los riesgos bajo la metodología implementada se procede a generar la tabla de evaluación de riesgo.

.

Tabla 12. EDRR

EVALUACION DEL RIESGO DE RED						
ACTIVO	ID ACTIVO	AMENAZA /RIESGO	ID RIESGO	DESCRIPCION DE A-R-V	PROBABILIDAD	IMPACTO
ROUTER ADSL	1	FALLA DE RED	R1	INTERMITENCIA	2	2
		FALLA DE RED	R2	CAÍDA DE SERVICIO	4	4
		FALLA DE RED	R3	DAÑO DEL EQUIPO	5	5
		FALLA ELECTRICA	R4	PERDIDA PARCIAL O TOTAL DE ENERGIA ELECTRICA	2	3
		DOS	R5	ACCESO NO AUTORIZADO	3	5
FIREWALL	2	POLITICAS	R6	NO SE CUENTA SE EVIDENCIA UNA GUIA DE HARDENING ADECUADA PARA LA CONFIGURACION DE ESTE ELEMENTO **MALA CONFIGURACION DE POLITICAS DE ACCESO (RDP)**	5	5
		PUERTOS	R7	NO SE CUENTA NI SE EVIDENCIA UNA GUIA DE HARDENING ADECUADA PARA LA CONFIGURACION DE ESTE ELEMENTO **SE ENCUENTRAN HABILITADOS EN SU MAYORIA TALES COMO: 22,PING,443**	3	4
SERVIDOR	3	PUERTOS	R8	NO SE CUENTA NI SE EVIDENCIA UNA GUIA DE HARDENING ADECUADA PARA LA CONFIGURACION DE ESTE ELEMENTO **SE ENCUENTRAN HABILITADOS EN SU MAYORIA TALES COMO:22,80,541,135,3389**	5	5
		ACCESO NO AUTORIZADO	R9	NO SE CUENTA CON UN PROCEDIMIENTO FORMAL Y DOCUMENTADO Y DIVULGADO AL PERSONAL REFERENTE A **AUTENTITCACION Y CREACION DE USUARIOS**	3	5

		ERRORES DE CÓDIGO	R10	NO SE CUENTA CON UN PROCESO DOCUMENTAL NI SE CUENTA CON UNA TAREA QUE EJECUTE BACKUPS	4	4
DVR	4	ACCESO NO AUTORIZADO	R11	NO SE CUENTA NI SE EVIDENCIA UNA GUIA DE HARDENING ADECUADA PARA LA CONFIGURACION DE ESTE ELEMENTO **EL EQUIPO SE ENCUENTRA CON CLAVES POR DEFECTO**	3	4
		FALLA TECNICA	R12	DAÑO DEL EQUIPO	3	3
		FALLA DE RED	R13	NO SE CUENTA NI SE EVIDENCIA UNA GUIA DE HARDENING ADECUADA PARA LA CONFIGURACION DE ESTE ELEMENTO **NO PODRIA REALIZAR MONITOREO DE CÁMARAS DADO QUE NO SE ENCUENTRA AISLADA O SEGMENTADA LA RED PARA ESTE ELEMENTO**	5	5
		FALLA ELECTRICA	R14	IMPIDE ACCESO Y CONTROL DE CÁMARAS	3	3
UBIQUITI	5	ACCESO NO AUTORIZADO	R15	EL EQUIPO SE ENCUENTRA CON CLAVES POR DEFECTO UN USUARIO MAL INTENCIONADO CON ACCESO **PODRIA CAPTURAR MONITOREAR EL TRAFICO Y PODER TOMAR CONTROL DEL SERVIDOR.**	4	5
		POLITICAS	R16	NO SE TIENE UNA RESTRICCIÓN QUE IMPIDA QUE DESDE LA CONEXIÓN DE Wi-Fi **ALCANCE EL SERVIDOR**	5	5
		FALLA DE RED	R17	NO PODRIA PRESTAR SERVICIO DE WI-FI GRATIS	2	4
EQUIPO DE ESCRITORIO	6	DESACTUALIZACION SISTEMA OPERATIVO	R18	LOS EQUIPOS SE ENCUENTRAN DESACTUALIZADOS ACTUALMENTE NO CUENTAN CON LICENCIA DE ANTIVIRUS	4	4
		ACCESO NO AUTORIZADO	R19	NO SE CUENTA CON UN INICIO DE SESION O AUTENTITCACION DE USUARIOS	4	4
		ROBO DE INFORMACIÓN	R20	CUALQUIER PERSONA ACCEDE FACILMENTE A LOS EQUIPOS	3	5

14.1.10 Evaluación de riesgos factor humano (EDRH)

Para este caso se relaciona **p**or separado la identificación y evaluación de riesgos encontrados dentro de la clasificación de este inventario para facilitar la lectura del mismo.

Tabla 13. RH

IDENTIFICACIÓN	
Nº	**DESCRIPCION DE A-R-V**
R1	EL FACTOR HUMANO NO SES EXCENTO DE COMETER ERROR DE DIGITACION EN LAS ACTIVIDADES PERTENECIENTES A SU CARGO
R2	DEBIDO A QUE LA RED DE LA EMPRESA NO SE ENCUENTRA SEGMENTADA Y CON SEGURIDAD PRESENTA UN RIESGO CRITICO AUNQUE CON UNA PROBABILIDAD MEDIA NINGUNA EMPRESA ES EXCENTA DE ROBO DE INFORMACION. SE PUEDE GENERAR UN DAÑO REPUTACIONAL Y LEGAL DADA LA DEBILIDAD DE SEGURIDAD EN RED PUEDA QUE LOS TRABAJADORES Y PERSONAS MAL INTENCIONADAS QUE SE HAGAN PASAR POR CLIENTES PUEDAN MONITOREAR EL TRAFICO DE RED Y PUEDAN TOMAR CONTROL SOBRE EL SERVIDOR Y PUEDAN ROBAR INFORMACION IMPORTANTE PARA EL NEGOCIO.
R3	NO SE CUENTA CON POLITICAS DE SEGURIDAD PERIMETRAL QUE IMPIDAN UN ATAQUE DE DENEGACION DE SERVICIO
R4	NO SE CUENTA CON UN PROCEDIMIENTO FORMAL Y DOCUMENTADO Y DIVULGADO AL PERSONAL REFERENTE A AUTENTITCACION Y CREACION DE USUARIOS
R5	SE PUEDE GENERAR PERDIDA PARCIAL O TOTAL DE ENERGIA ELECTRICA A CASUSA UN EXTERNO
R6	PERSONAL INSATISFECHO RENCOROSO O PERSONAL EXTERNO CON ALEVOCIA
R7	NO SE CUENTA CON POLITICAS DE SEGURIDAD PERIMETRAL QUE IMPIDAN UN ATAQUE DE DENEGACION DE SERVICIO

Tabla 14. EDRH

EVALUACIÓN DEL RIESGO DE RED						
ACTIVO	ID ACTIVO	ID RIESGO	AMENAZA/RIESGO	PROBABILIDAD	IMPACTO	VALOR TOTAL ACTIVO
GERENTE	1	R1	ERROR DE USUARIO	2	2	10
		R2	ROBO DE INFORMACIÓN	4	4	
SUPERVISOR	2	R4	ACCESO NO AUTORIZADO	2	3	10
		R2	ROBO DE INFORMACIÓN	4	4	
ANALISTA CONTABLE	3	R1	ERROR DE USUARIO	2	2	11
		R2	ROBO DE INFORMACIÓN	4	4	
VENDEDORES	4	R4	ACCESO NO AUTORIZADO	2	3	9
		R2	ROBO DE INFORMACIÓN	4	4	
		R3	DOS	5	5	
TECNICO	5	R5	FALLA TECNICA	3	5	11
		R7	POLITICAS MAL CONFIGURADAS	3	4	
		R4	ACCESO NO AUTORIZADO	2	3	
		R2	ROBO DE INFORMACIÓN	4	4	
VIGILLANTES	6	R2	ROBO DE INFORMACIÓN	4	4	7
CLIENTES	7	R2	ROBO DE INFORMACIÓN	4	4	15
		R6	INCENDIO	1	5	
		R4	ACCESO NO AUTORIZADO	2	4	
		R3	DOS	5	5	

Una vez realizada la evaluación se procede a valorar el riesgo total sobre los activos relacionados anteriormente en una escala de 0-32 donde el cliente acepta el riesgo de 32-108 donde el riesgo es compartido con un tercero o se delega totalmente la gestión administración y seguridad del activo al tercero y el ultimo de 108-350 es en el que nos enfocaremos para dar las respectivas recomendaciones y hardening los cuales serán tratados detalladamente en el siguiente capítulo de recomendaciones.

Tabla 15.Valoración de aceptación transferencia compartición y eliminación del riesgo

ANALISIS DE RIESGOS	
V.T.RIESGO	**VALORACIÓN**
0-32	**ACEPTADO**
32-108	**COMPARTIDO O TRANSFERIDO**
108-350	**SE TRANSFIERE O ELIMINA**

A continuación, se detalla la valoración del riesgo en la tabla la cual se diligencio de acuerdo a la evaluación realizada en los diferentes activos con el propósito de generar la respectiva matriz de riesgos dicha tabla se diligencio con la siguiente información:

N°: equivale al ID representativo del riesgo expuesto en la evaluación e identificación de riesgos:

Amenaza: identificación según catálogo de elementos del libro II de la metodología Magerit.

Análisis: Define la valoración de la probabilidad y el impago que generaría es sobre el activo.

Evaluación: es valor generado del riesgo total identificado por el producto de probabilidad, integridad y el valor de los activos el cual se ve reflejado en la evaluación de riesgos y que se considera como el producto de confidencialidad integridad y disponibilidad mencionadas en los capítulos anteriores.

Tabla 16. Mapa de calor activo de red (MDCAI)

IDENTIFICACIÓN		ANÁLISIS		EVALUACIÓN	VALOR ACTIVO
Nº	**AMENAZA**	**P**	**I**		
R1	PERDIDA DE FLUIDO ELECTRICO	2	4	96	12
R2	ERROR DE USUARIO	4	4	192	
R3	PERSONAL NO CALIFICADO	1	3	36	
R4	LA INFORMACION DE PROVEEDORES SE ENCUENTRA VISIBLE PARA TODOS LOS TRABAJADORES	4	5	160	8
R5	PERDIDA DE INFORMACION POR DESASTRE	1	4	32	
R6	ERRORES POR NATENIMIENTO /ACTUALIZACIONES DE LA HERRAMIENTA	2	4	120	15
R7	ACCESO NO CONTROLADO	3	5	225	
R8	CAIDA DE SERVICIO	2	2	60	15
R9	ACCESO NO CONTROLADO	4	5	300	
R10	PERDIDA DE FLUIDO ELECTRICO	2	4	120	

Tabla 17.Mapa de calor activo de información

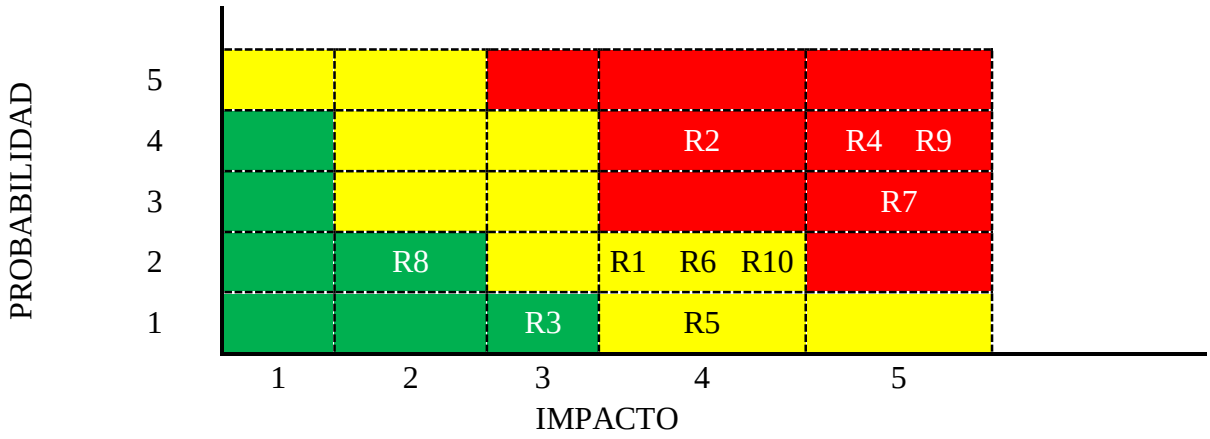


Tabla 18. Mapa de calor activo de red (MDCAR)

IDENTIFICACIÓN		ANÁLISIS		EVALUACIÓN	TIPO DE IMPACTO
Nº	**DESCRIPCION DE A-R-V**	**P**	**I**		
R1	INTERMITENCIA	2	2	56	14
R2	CAÍDA DE SERVICIO	4	4	224	
R3	DAÑO DEL EQUIPO	5	5	350	
R4	PERDIDA PARCIAL O TOTAL DE ENERGIA ELECTRICA	2	3	84	
R5	ACCESO NO AUTORIZADO	3	5	210	
R6	NO SE CUENTA SE EVIDENCIA UNA GUIA DE HARDENING ADECUADA PARA LA CONFIGURACION DE ESTE ELEMENTO MALA CONFIGURACION DE POLITICAS DE ACCESO (RDP)	5	5	300	12
R7	NO SE CUENTA SE EVIDENCIA UNA GUIA DE HARDENING ADECUADA PARA LA CONFIGURACION DE ESTE ELEMENTO SE ENCUENTRAN HABILITADOS EN SU MAYORIA TALES COMO: 22,PING,443	3	4	144	
R8	NO SE CUENTA SE EVIDENCIA UNA GUIA DE HARDENING ADECUADA PARA LA CONFIGURACION DE ESTE ELEMENTO SE ENCUENTRAN HABILITADOS EN SU MAYORIA TALES COMO:22,80,541,135,3389	5	5	325	13
R9	NO SE CUENTA CON UN PROCEDIMIENTO FORMAL Y DOCUMENTADO Y DIVULGADO AL PERSONAL REFERENTE A AUTENTITCACION Y CREACION DE USUARIOS	3	5	195	
R10	NO SE CUENTA CON UN PROCESO DOCUMENTAL NI SE CUENTA CON UNA TAREA QUE EJECUTE BACKUPS	4	4	208	
R11	NO SE CUENTA SE EVIDENCIA UNA GUIA DE HARDENING ADECUADA PARA LA CONFIGURACION DE ESTE ELEMENTO EL EQUIPO SE ENCUENTRA CON CLAVES POR DEFECTO	3	4	108	9
R12	DAÑO DEL EQUIPO	3	3	81	

R13	NO SE CUENTA SE EVIDENCIA UNA GUIA DE HARDENING ADECUADA PARA LA CONFIGURACION DE ESTE ELEMENTO NO PODRIA REALIZAR MONITOREO DE CÁMARAS DADO QUE NO SE ENCUENTRA AISLADA O SEGMENTADA LA RED PARA ESTE ELEMENTO	5	5	225	
R14	IMPIDE ACCESO Y CONTROL DE CÁMARAS	3	3	81	
R15	EL EQUIPO SE ENCUENTRA CON CLAVES POR DEFECTO UN USUARIO MAL INTENCIONADO CON ACCESO PODRIA CAPTURAR MONITOREAR EL TRAFICO Y PODER TOMAR CONTROL DEL SERVIDOR.	4	5	200	10
R16	NO SE TIENE UNA RESTRICCIÓN QUE IMPIDA QUE DESDE LA CONEXIÓN DE Wi-Fi ALCANCE EL SERVIDOR	5	5	250	
R17	NO PODRIA PRESTAR SERVICIO DE WI-FI GRATIS	2	4	80	
R18	LOS EQUIPOS SE ENCUENTRAN DESACTUALIZADOS ACTUALMENTE NO CUENTAN CON LICENCIA DE ANTIVIRUS	4	4	224	14
R19	NO SE CUENTA CON UN INICIO DE SESION O AUTENTITCACION DE USUARIOS	4	4	224	
R20	CUALQUIER PERSONA ACCEDE FACILMENTE A LOS EQUIPOS	3	5	210	

Tabla 19. Mapa de calor activo de red

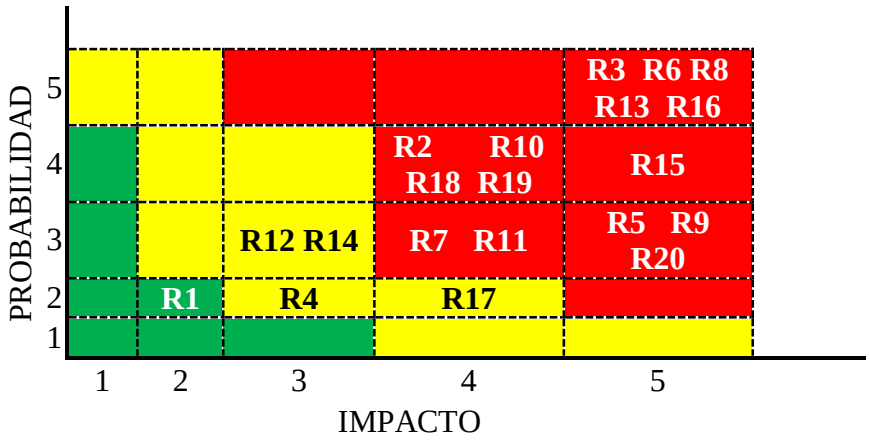
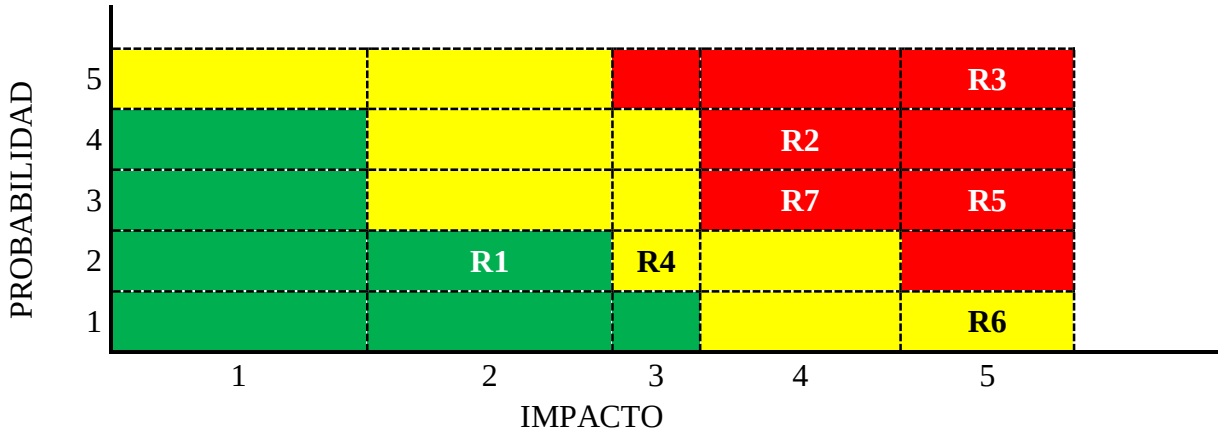


Tabla 20. Mapa de calor activo factor humano (MDCFH)

IDENTIFICACIÓN		ANÁLISIS		EVALUACIÓN	TIPO DE IMPACTO
Nº	**DESCRIPCION DE A-R-V**	**P**	**I**		
R1	EL FACTOR HUMANO NO SES EXCENTO DE COMETER ERROR DE DIGITACION EN LAS ACTIVIDADES PERTENECIENTES A SU CARGO	2	2	40	10
R2	DEBIDO A QUE LA RED DE LA EMPRESA NO SE ENCUENTRA SEGMENTADA Y CON SEGURIDAD PRESENTA UN RIESGO CRITICO AUNQUE CON UNA PROBABILIDAD MEDIA NINGUNA EMPRESA ES EXCENTA DE ROBO DE INFORMACION. SE PUEDE GENERAR UN DAÑO REPUTACIONAL Y LEGAL DADA LA DEBILIDAD DE SEGURIDAD EN RED PUEDA QUE LOS TRABAJADORES Y PERSONAS MAL INTENCIONADAS QUE SE HAGAN PASAR POR CLIENTES PUEDAN MONITOREAR EL TRAFICO DE RED Y PUEDAN TOMAR CONTROL SOBRE EL SERVIDOR Y PUEDAN ROBAR INFORMACION IMPORTANTE PARA EL NEGOCIO.	4	4	160	10
R3	NO SE CUENTA CON POLITICAS DE SEGURIDAD PERIMETRAL QUE IMPIDAN UN ATAQUE DE DENEGACION DE SERVICIO	5	5	250	11
R4	NO SE CUENTA CON UN PROCEDIMIENTO FORMAL Y DOCUMENTADO Y DIVULGADO AL PERSONAL REFERENTE A AUTENTITCACION Y CREACION DE USUARIOS	2	3	60	9
R5	SE PUEDE GENERAR PERDIDA PARCIAL O TOTAL DE ENERGIA ELECTRICA A CASUSA UN EXTERNO	3	5	150	11
R6	PERSONAL INSATISFECHO RENCOROSO O PERSONAL EXTERNO CON ALEVOCIA	1	5	35	7
R7	NO SE CUENTA CON POLITICAS DE SEGURIDAD PERIMETRAL QUE IMPIDAN UN ATAQUE DE DENEGACION DE SERVICIO	3	4	180	15

Tabla 21. Mapa de calor activo factor humano



15. Recomendaciones de Hardening

15.1 Protocolo SSH

SSH (Secure Shell), es una de las herramientas más utilizadas para conectarse remotamente a un servidor, con una conexión SSH podremos administrar un servidor de manera remota utilizando línea de comandos.

Por defecto el puerto utilizado por el protocolo SSH es el 22, este es uno de los puertos más utilizados por scripts maliciosos para realizar ataques por fuerza bruta o denegación de servicio por lo cual es recomendable cambiarlo, por ejemplo, por el puerto 2445.

Otras consideraciones que debemos tener en cuenta el permitir conexiones por SSH son:

- Permitir y denegar usuarios específicos para que puedan o no utilizar la conexión por SSH.

- Tiempo de gracia, limitar el tiempo que puede tardar un usuario en ingresar sus credenciales, si realmente es quien dice ser no debería tardar mucho, se estipula que este tiempo debe ser 20 segundos.

- Definir usuarios, maquinas, cuentas y direcciones IPs que se pueden conectar por SSH, aunque pueda estar conectándose con una cuenta conocida, pero con otra dirección IP, no se le permitirá el acceso.

- Limitar el número de intentos de autenticación, con ello reducimos el riesgo y éxito de ataque por fuerza bruta.

- No permitir credenciales con passwords vacíos.

- Definir un número máximo de usuarios conectados a la máquina, con ello evitaremos saturar el servidor, para nuestro caso se fija en 3.

- No permitir la creación de túneles SSH, ya que por medio de estos podremos acceder a maquinas que inicialmente son inaccesibles desde la red exterior; adicionalmente es posible saltarse medidas de seguridad como FIREWALLS e IDS.

- Utilizar claves publica/privada para la autenticación, en los puntos anteriores se ha mencionado la autenticación con cuentas de usuarios, con la utilización de claves publica/privada, la maquina tendrá deberá contener la clave pública, mientras que el usuario debe tener la clave privada para poder autenticarse.

- Utilizar la versión más actualizada de SSH.

15.2 Auditoria de servicios

Tras la instalación estándar de un sistema operativo pueden llegar a tener puertos abiertos, algunos pueden ser necesarios para el funcionamiento de servicios, mientras que otros no. Los puertos abiertos representan un riesgo para la seguridad, ya que pueden ser utilizados por un usuario malicioso para entrar a nuestras maquinas.

El no asegurar estos puertos o dejarlos abiertos puede llevarnos a tener vulnerabilidades como por ejemplo Ataque CGI, Buffer Oveflow, Denegación de Servicio (DoS), Back Door y

Posibilidad de sniffer.

Haciendo una mención especial a los puertos descritos en la tabla podemos ver:

15.2.1. El puerto de seguridad 445

SMB es un protocolo de red que permite a una aplicación o al usuario de una aplicación compartir archivos, discos, directorios, impresoras, puertos seriales y mail slots, a través de una red que usa el sistema operativo Microsoft Windows. SMB se define como la estructura cliente-servidor, donde el cliente formula una solicitud y el servidor envía su respuesta. En otras palabras, permite a un cliente leer, crear y modificar archivos de un servidor remoto.

15.2.2. Riesgo asociado al puerto 139

Los puertos NetBIOS son utilizados por el intercambio de archivos y aplicaciones de uso compartido de impresoras. Los usuarios de la red con sede fuera de la red acceden a estos servicios a través del puerto 139. Los virus Chode, el Gusano Mensaje de Dios, Msinit, Netlog, Red, Qaz sadmind y SMB Relay utilizan este puerto. Los administradores de red y los proveedores de servicios de Internet tienden a bloquearlo.

Los servicios SMB y NetBios/NetBT están diseñados para ser consultados por clientes de confianza dentro de ambientes seguros. Esto significa que usualmente no es buena idea exponer estos servicios directamente en Internet o en general, en un ambiente donde clientes no confiables puedan acceder a dichos servicios.

Debido a que la organización hace uso de compartir y almacenar información en el servidor,

Lo mejor es actualizar el sistema operativo con los últimos parches de seguridad y configurar el firewall para que nunca permita el tráfico de red saliente del puerto 445-139-137-138, Y el tráfico entrante solo de orígenes conocidos. En el anexo de plantilla de hardening del firewall se especifica la regla a configurar para este servicio.

15.2.3. El puerto 3389

Es normalmente utilizado por el RDP (Protocolo de Escritorio Remoto), y dentro de ALIMENTOS PHD le dan la misma utilización para que las sedes remotas se puedan conectar al servidor principal donde se encuentra la aplicación de ventas y contabilidad.

Pero esta conexión es realizada a través de internet sin una capa de cifrado o de privacidad que proteja la información que se envía y se recibe.

RDP también es utilizado cibercriminales para instalar herramientas de cryptomining, keyloggers, backdoors y malware.

Para mitigar los ataques basados en RDP deberíamos realizar las siguientes acciones. (CSO, Edición Digital, N° 37).

Contraseña Seguras: Utilizar usuarios y contraseñas fuertes, las contraseñas deben ser robustas, largas y seguras.

Restringir los accesos basados en roles: Limitar la cantidad de usuarios con privilegios de acceso de administrador la consola RDP. También limitar los privilegios de los usuarios que se conectan.

Habilitar autenticación por NLA (Network Level Authentication): NLA ofrece una capa adicional de protección, un usuario primero debe autenticar su identidad para si después conectarse por RDP.

Cambiar el puerto de RDP: Con esto podemos evitar que los programas que escanean puertos en busca de RDP abierto, no lo encuentren.

Mantenga registro de los servidores RDP: Tener documentado y en pleno conocimiento que sistemas tienen habilitado RDP dentro de nuestra red, asegurar que no hay servidores con el servicio RDP habilitado y menos cuando tienen conexión directa a internet.

Utilice una puerta de enlace RDP: Con la función de esta característica es que permite pasar de forma segura el tráfico hacia y desde la sede remota a la sede principal.

15.3. Funcionamiento de la red de conectividad

La red de conectividad de la empresa ALIMENTOS PHD se basa en servicios de internet banda ancha contratados con diferentes operadores prestadores del servicio en la ciudad de Bogotá D.C. Y conectados directamente al equipo de cómputo en la sede, proporcionando acceso a correo electrónico y gestión remota con el servidor principal mediante RDP (Remote Desktop Protocol) donde se encuentra la aplicación contable para registrar todas las ventas y guardar la facturación.

En la siguiente topología se muestra la red de conectividad.

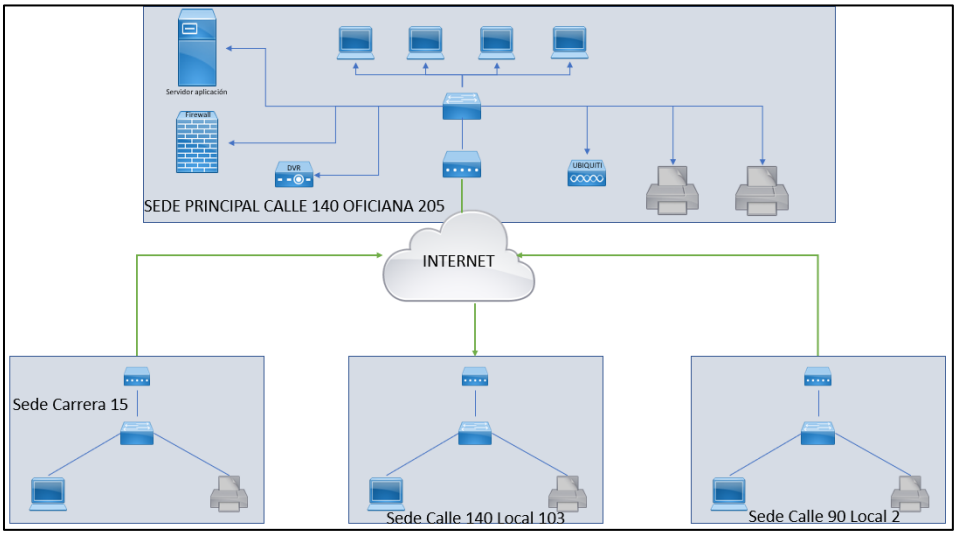


Ilustración 30.Topologia de red Empresa PHD

Como ha sido demostrado el protocolo RDP tiene fallas de seguridad desde el año 1996 cuando empezó a incluirse dentro del sistema operativo de Microsoft, los ciberdelincuentes han intentado muchas veces con éxito hackear los dispositivos a través de este protocolo y también se han presentado ataques de RDP hechos por diferentes tipos de malware.

Realizando una búsqueda en la página del CVE (Common Vulnerabilities and Exposures cve.mitre.org) encontramos 64 CVEs relacionados con RDP, el ultimo es de este año con el nombre CVE-2019-0708.

CVE (2019), 0708 afirma: “A remote code execution vulnerability exists in Remote Desktop Services formerly known as Terminal Services when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests, aka 'Remote Desktop Services Remote Code Execution Vulnerability'.”

Esta vulnerabilidad permite la ejecución de código remoto y está catalogada como critica; es de pre-autenticación y no requiere interacción del usuario, por lo cual un atacante podría escribir un exploit para la misma e incorporarlo en un malware, lo permitiría un ataque en que el malware

se pueda propagar de forma similar a un gusano, como lo fue el caso de WannaCry hace 2 años.

Aunque a la fecha de realización de este documento Microsoft ya lanzo parche para las versiones 2003 de Windows, XP, Windows 7, Windows Server 2008 y Windows Server 2008 R2 que se ven afectados por este fallo.

Haciendo una búsqueda en el Shodan (www.shodan.io) por el puerto 3389 que corresponde a RDP y por país Colombia encontramos 9,336 servicios expuestos e indexados en shodan. Como ha sido demostrado el protocolo RDP tiene fallas de seguridad desde el año 1996 cuando empezó a incluirse dentro del sistema operativo de Microsoft, los ciberdelincuentes han intentado muchas veces con éxito hackear los dispositivos a través de este protocolo y también se han presentado ataques de RDP hechos por diferentes tipos de malware.

Para el estado actual de la empresa ALIMENTOS PHD el RDP es una herramienta de trabajo diario muy importante, por lo cual se debe mantener, pero no se publicará directamente a internet. Por lo cual se propone utilizar una conexión VPN entre las sedes remotas y la sede principal.

15.4 Implementación de VPN

Una VPN por sus siglas en inglés (Virtual Private Network) es una tecnología de red creada a través de internet o dentro de otra red, que comunica a los dispositivos conectados de forma aislada; permite interconectar a la empresa y al trabajador a través de internet de forma privada y sin que terceros tengan acceso a dicha conexión.

Las conexiones VPN encapsulan la información, creando un túnel VPN. Este funciona como si los dispositivos estuvieran conectados físicamente a pesar de la distancia. Una implementación correcta de esta tecnología permite asegurar la confidencialidad e integridad de la información.

Dentro de los principales protocolos de comunicación VPN tenemos a IPSec (Internet Protocol Security), L2TP (Layer 2 Tunneling Protocol), PPTP (Point-to-Point Tunneling Protocol), L2F (Layer 2 Forwarding), VPN SSL VPN SSL (Secure Sockets Layer).

Para la empresa ALIMENTOS PHD proponemos la implementación de una VPN basada en cliente-servidor con el protocolo SSL, esta funciona a través de una aplicación que se encarga de entablar la comunicación firewall de la sede principal y levantar la VPN. El usuario debe ejecutar la aplicación y autenticarse con el usuario y contraseña. De esta manera se crea el canal cifrado entre el equipo y la red remota, para el intercambio seguro de datos.

Es verdad que este tipo de VPN ya se encuentra en sistemas operativos como Windows, Mac y Linux y nos ofrecen la posibilidad de configurar un canal cifrado de comunicación basado en diversos estándares como L2TP (Layer 2 Tunneling Protocol), PPTP o SSTP. Pero para ALIMENTOS PHD no es una opción implementarla ya que ellos no cuentan con personal de soporte técnico.

Debido a esto se propone implementar una solución contratada a un proveedor de servicios y que adicionalmente entregue más servicios necesarios para los puestos de trabajo como lo son antivirus y firewall.

15.5. Control de Riesgos

Conociendo todos los riesgos a los que estos expuestos la información y continuidad del negocio para ALIMENTOS PHD se deben sugerir una serie de recomendaciones teniendo en cuenta la clasificación de los riesgos estipulados en este proyecto, que es la siguiente:

Tabla 22. Valoración de Riesgos

ANALISIS DE RIESGOS	
V.T.RIESGO	**VALORACIÓN**
0-32	**LEVE**
32-108	**MODERADO**
108-350	**CRITICO**

Después de evaluar y conocer los resultados de los diferentes riesgos se proponen recomendaciones y controles de seguridad para mitigar, prevenir y controlar en especial aquellos

con nivel crítico, en acuerdo con la empresa.

15.6 Control de riesgos de la información

A continuación, se especifican los controles para para mitigar, prevenir y controlar los riesgos asociados con la INFORMACION, así como también los activos que en conjunto con el cliente se clasificaron críticos.

Tabla 23. Pilares de la Información

PILAR	DESCRRIPCION
C	CONFIDENCIALIDAD
D	DISPONIBILIDAD
I	INTEGRIDAD

Tabla 24. Control de riesgos de la información (computadores de escritorio)

ACTIVO	RIESGO / AMENAZA	SEGURIDAD			CONTROLES
		C	D	I	
COMPUTADOR DE ESCRITORIO	ACCESO NO CONTROLADO A LOS EQUIPOS DE COMPUTO	X	X	X	Emisión de guía de uso de PC
					Copia de respaldo de documentos
					Cifrar información sensible del equipo
					Educación en medidas de seguridad e informática
					Configuración de acceso limitado a redes
					Creación de contraseñas robustas
					Bloqueo de acceso a páginas de internet no seguras
					Firewall Activado
					Políticas de acceso a internet
					Adquirir antivirus con licenciamiento

					empresarial
					Mantener antivirus actualizado en los equipos
					Bloquear panel de configuración de antivirus para usuarios finales
					Implementar contraseña de arranque en la BIOS de los equipos
					Restringir el uso de puerto USB
					Hacer renovación tecnología con un mínimo de 3 años
					Realizar mantenimiento preventivo en los equipos al menos 2 veces al año
					Copia de seguridad de la configuración
					Actualización del sistema operativo y parches de seguridad
					Control de temperatura y humedad

Tabla 25. Control de riesgos de la información (Servidor)

ACTIVO	RIESGO / AMENAZA	SEGURIDAD			CONTROLES
		C	D	I	
SERVIDOR	ACCESO NO CONTROLADO AL SERVIDOR	X	X	X	Determinación de niveles de responsabilidad y acceso
					Mejorar los niveles de seguridad en las instalaciones
					Inventario de aplicaciones
					Control de temperatura y humedad
					Implementar contraseña de arranque en la BIOS de los equipos
					Copias de seguridad de la información

					Copia de seguridad de la configuración
					Firewall Activado
					Políticas de acceso a internet
					Restringir la salida de equipos de las instalaciones
					Tener hoja de vida de servidor
					Hacer renovación tecnología con un mínimo de 5 años
					Realizar mantenimiento preventivo en los equipos al menos 2 veces al año
					Actualización del sistema operativo y parches de seguridad

Tabla 26. Control de riesgos de la información (Carpetas de información proveedores)

ACTIVO	RIESGO / AMENAZA	SEGURIDAD			CONTROLES
		C	D	I	
CARPETAS DE INFORMACION PROVEEDORES	LA INFORMACION DE PROVEEDORES SE ENCUENTRA VISIBLE PARA TODOS LOS TRABAJADORES	X	X	X	Almacenar los archivos físicos bajo llave
					Definir política de administración de documentos
					Definir política para el manejo de información compartida
					Definir política para el manejo de información sensible
					Acuerdos de confidencialidad
					Plan de formación y concientización en seguridad de la información
					Cada usuario es responsable de asegurar todo documento que contenga información restringida o confidencial.

					Los informes o documentación impresos deben ser retirados inmediatamente de las impresoras
					Los documentos restringidos o confidenciales deben ser destruidos en equipos de destrucción de papel.
					Hacer una clasificación de la información que se maneja en PHD

Tabla *27*. Control de riesgos de la información (Archivo BD)

ACTIVO	RIESGO / AMENAZA	SEGURIDAD			CONTROLES
		C	D	I	
ARCHIVO BASE DE DATOS	ERROR DE USUARIO	X	X	X	Copias de seguridad
					Políticas de gestión de la base de datos
					Medidas de acceso robustas con id usuario y contraseña
					Gestión de claves y/o perfiles para la generación, distribución, almacenamiento y borrado
					Política de retención de datos
					Actualización frecuente de respaldos
					Almacenamiento interno de respaldos con protección de acceso
					Almacenamiento externo de respaldos en ubicaciones diferentes a la organización
					Capacitación a usuarios respectivos en el proceso de restauración de los datos
					Políticas de respaldos de la base de datos
					Mantener la base de datos actualizada a la última versión

15.7 Gestión de riesgos de red

A continuación, se especifican los controles para para mitigar, prevenir y controlar los riesgos asociados con la RED, así como también los activos que en conjunto con el cliente se clasificaron críticos.

Tabla 28. Pilares de Información

PILAR	DESCRRIPCION
C	CONFIDENCIALIDAD
D	DISPONIBILIDAD
I	INTEGRIDAD

Tabla 29. Gestión de riesgos de red (Router)

ACTIVO	RIESGO / AMENAZA	SEGURIDAD			CONTROLES
		C	D	I	
ROUTER ADSL	CAÍDA DE SERVICIO DAÑO DEL EQUIPO		X		Mantener contacto con el proveedor de servicios
					Mantener contacto con los operadores de telecomunicaciones
					Inventario de equipos y servicios
					Aseguramiento de la disponibilidad del servicio
					Monitorización de fallas e incidencias
					Mantenimiento solo por personal autorizado
					Monitorización del trafico
					Registro de navegación web
					Control de descargas
					Control de direcciones ips
					Control de temperatura y humedad

Tabla 30. Gestión de riesgos de red (Servidor)

ACTIVO	RIESGO / AMENAZA	SEGURIDAD			CONTROLES
		C	D	I	
SERVIDOR	ACCESO NO AUTORIZADO	X	X	X	Política de identificación y autenticación de usuarios
					Procedimientos para identificación y autenticación de usuarios
					Llevar registro de la activación, modificación y borrado de usuarios
					Política de compromiso de mantener la confidencialidad
					Política de acceso a la información.
					Planificación y seguimiento de las tareas de soporte técnico externo
					Restringir la salida de equipos de las instalaciones
					Mejorar los niveles de seguridad en las instalaciones
					Adquirir antivirus con licenciamiento empresarial
					Firewall Activado
					Tener hoja de vida de servidor
					Actualización del sistema operativo y parches de seguridad
					Evitar el trabajo no autorizado

Tabla 31. Gestión de riesgos de red (Servidor)

ACTIVO	RIESGO / AMENAZA	SEGURIDAD			CONTROLES
		C	D	I	
SERVIDOR	ERRORES DE CÓDIGO	X	X	X	Planificación y seguimiento de las tareas de soporte técnico externo
					Llevar registro de la activación, modificación y borrado de usuarios
					Tener hoja de vida de servidor
					Política de compromiso de mantener la confidencialidad
					Copia de respaldo de documentos
					Copia de seguridad de la configuración
					Capacitación al personal

Tabla 32. Gestión de riesgos de red (Servidor)

ACTIVO	RIESGO / AMENAZA	SEGURIDAD			CONTROLES
		C	D	I	
SERVIDOR	PUERTOS	X	X	X	Monitoreo de puertos
					Pruebas periódicas de la recuperación del sistema
					Firewall Activado
					Configuración de acceso limitado a redes
					Monitoreo de conexiones activas
					Adquirir antivirus con licenciamiento empresarial
					Actualización del sistema operativo y parches de seguridad

15.8 Control de riesgos de factor humano

A continuación, se especifican los controles para para mitigar, prevenir y controlar los riesgos asociados con la FACTOR HUMANO, así como también los activos que en conjunto con el cliente se clasificaron críticos.

Tabla 33. Pilares de Información

PILAR	DESCRRIPCION
C	CONFIDENCIALIDAD
D	DISPONIBILIDAD
I	INTEGRIDAD

Tabla 34. Control de riesgos de factor humano

ACTIVO	RIESGO / AMENAZA	SEGURIDAD			CONTROLES
		C	D	I	
PERSONAS	ROBO DE INFORMACIÓN	X	X	X	Política de gestión del personal en materia de seguridad
					Relación del personal propio y subcontratado
					Acuerdos de confidencialidad
					Plan de formación y concientización
					Comprobaciones previas para la contratación de personal
					Normativa de obligado cumplimiento en el desempeño del puesto
					Llevar registro de la activación, modificación y borrado de usuarios
					Definir política de administración de documentos
					Autorización previa a la publicación de datos

					Protección del correo electrónico
					Normativa de uso del correo electrónico
					Implementar medidas anti-spam
					Protección del intercambio electrónico de documentos

16. Discusión

Dentro de los resultados obtenidos en la ejecución del proyecto se identificó el estado crítico en el que se encuentra la organización, por lo cual se sugiere que los controles y recomendaciones consignados en el documento sean implementados de carácter urgente sin embargo una vez la organización aplique o implemente estas recomendaciones es necesario dar continuidad con una segunda etapa que permita la consolidación de un sistema de gestión de la información (SGSI) el cual debe estar alineado con los objetivos y continuidad del negocio. con el fin de asegurar la información es necesario que la organización cuente con los procesos, controles y lineamientos que rige la ISO 27001, ISO 27002, los documentos anexos que se entregaran generaran un valor agregado para que esta implemente las salvaguardas y controles necesarios para mitigar las amenazas a las que se encuentra hoy día expuesta.

17. Conclusiones

Sin la colaboración de la organización hubiera sido imposible definir los activos objetivos de este proyecto, causando el aplazamiento según cronograma de actividades y en el peor de los casos la inviabilidad del proyecto.

Se logró realizar el análisis de vulnerabilidades a los equipos de red activos, y exponer los puertos abiertos para realizar su respectiva recomendación.

El manejo inadecuado de todos los recursos con los que cuenta la organización se debe a que los funcionarios no cuentan con capacitación y conocimiento adecuado en seguridad de la información por consiguiente se recomienda que la organización defina políticas de seguridad a los activos y usuarios que hacen uso de ellos.

Los resultados generados del análisis de riesgos y junto con los controles entregados a la organización permiten tener un mayor control sobre todos los activos de información.

Se realiza la recomendación de la implementación de una VPN, con el fin de proteger la información de la compañía y tener una manera más segura a la conexión de la red local.

Con la ejecución y finalización del proyecto se logró cumplir con los objetivos propuestos entregando a la organización una propuesta dirigida a minimizar los riesgos de su infraestructura de información.

18. Documentación de Referencia

Gómez, A. .Ministerio de Hacienda y Administraciones Públicas

Ávila, F.., (Mayo, 2018). Blogs de seguridad en redes. Recuperado de «https://securityhacklabs.net/,

Ávila, F. (Mayo -octubre, 2018). Escáner de vulnerabilidades (Herramientas # 2). https://securityhacklabs.net/articulo/escaner-de-vulnerabilidades-herramientas-2

Candau, J.Centro Criptológico Nacional, Ministerio de la Presidencia

Castro. P. (Junio, 2019). Blog Grupo Smar5tekh. Publicacion por Marketing. Recuperado de http://blog.smartekh.com/que-es-hardening

Condra Serans. (2017). Menage Engine Desktop Central. Recuperado de https://www.avast.com/es-es/c-ransomware,» [En línea].,» [En línea].

CSO Compterworld. (2019). Edicion digital N 37. Recuperado de: https://cso.computerworld.es/defensa-perimetral/consejos-para-mitigar-ataques-que-se-

aprovechan-de-los-accesos-remotos-rdp

Dalia, V. gb. Advisor (2000). Recuperado de https://www.gb-advisors.com/es/gestion-de-vulnerabilidades/nessus-escaner-vulnerabilidad/

Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica

Documento de Metodología de Análisis de vulnerabilidad. Fase 5 -6. Recuperado de https://javeriana.edu.co/biblos/tesis/ingenieria/tesis181.pdf

Estudio de vulnerabilidad y riesgo de las redes infraestructura de telecomunicaciones en zonas vulnerables. (Diciembre, 2010). Recuperado de http://colombiatic.mintic.gov.co/679/w3-article-73949.html

Goujan, Andre. (septiembre 2012). Que es y como funciona una VPN para la privacidad de la informacion. Recuperdo de https://www.welivesecurity.com/la-es/2012/09/10/vpn-funcionamiento-privacidad-informacion/,» [En línea].

ISO 27002. Controles de Seguridad. Recuperado de http://iso27000.es/iso27002.html

Kaspersky, (2017). Lucha contra el malwuare y el delito cibernetico. Recuperado de https://www.kaspersky.es/resource-center/threats/trojans,» [En línea].

Margerit – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Método

Rodríguez y Peralta .I. . Gestión de Riesgos Magerit Editado por tiThink

Tincorp. (2012. Kaspersky. Soluciones Colombia. Seguridad empresas. Recuperado de «https://www.kaspersky.es/resource-center/threats/viruses-worms,» [En línea].

The successor of WannaCry that exploited the same vulnerability as WannaCry and caused chaos for businesses. Though Petya was originally launched as ransomware, it was later upgraded to be a wiper, and would delete encrypted information. (2017). Recuperado de https://support.microsoft.com/es-co/help/186607/understanding-the-remote-desktop-protocol-rdp,» [En línea].

Mañas, Catedrático de la Universidad Politécnica de Madrid. Consultor Externo

Responsable edición digital: Subdirección General de Información, Documentación y Publicaciones Adobe Acrobat 5.0

González Barroso, J. (octubre 2012). Disponible esta publicación en el Portal de Administración Electrónica (PAE). Recuperado de http://administracionelectronica.gob.es/

Ministerio de Hacienda y Administraciones Públicas. Secretaría General Técnica

Subdirección General de Información, Documentación y Publicaciones Centro de Publicaciones

Colección: administración electrónica. NIPO: 630-12-171-8

Norma técnica Colombiana NTC-ISO31000. (2011-02-16)

Video Link: https://www.youtube.com/watch?v=hsGzYVVxyTE

El Ransomware (también conocido como rogueware o scareware) restringe el acceso a su sistema y exige el pago de un rescate para eliminar la restricción. Recuperado de https://www.avast.com/es-es/c-ransomware

Troyanos: Programas maliciosos que realizan acciones no autorizadas por el usuario.

Recuperado de https://www.avast.com/es-es/c-ransomware

VPN: Virtual Private Network es una tecnología de red que se utiliza para conectar una o más computadoras a una red privada utilizando Internet https://www.xataka.com/seguridad/que-es-una-conexion-vpn-para-que-sirve-y-que-ventajas-tiene

https://blog.cerounosoftware.com.mx/que-es-un-analisis-de-vulnerabilidades-inform%C3%A1ticas

https://nmap.org/man/es/index.html#man-description

Nmap es una herramienta de código abierto para exploración de red y auditoría de seguridad. Se diseñó para analizar rápidamente grandes redes, aunque funciona muy bien contra equipos individuales https://nmap.org/man/es/index.html#man-description.

19. Anexos

- Anexo 1 - Acta de Calificación y Aprobación de Trabajo de Grado
- Anexo 2 - Carta presentación estudiantes - PGC-F1
- Anexo 3 - Carta aceptación propuesta de proyecto de grado - PGC-F2
- Anexo 4 - Carta aprobación del trabajo de grado - PGC-F3
- Anexo 5 - Carta aceptación empresa PGC-F6
- Anexo 5 - Recomendaciones y controles de seguridad de la información
- Anexo 5 - Fortigate-hardening-your-fortigate-56
- Anexo 5 - HARDENING_DVR
- Anexo 5 - HARDENING_FIREWALL
- Anexo 5 - HARDENING_PC
- Anexo 5 - HARDENING_SERVIDOR1
- Anexo 5 - FortiOS-6.0.0-Cookbook
- Anexo 5 - RECOMENDACIONES Y CONTROLES DE SEGURIDAD DE LA INFORMACION