UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA.

PROCESO DE TITULACIÓN

JUNIO –SEPTIEMBRE 2020

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

INGENIERÍA EN SISTEMAS

PREVIO A LA OBTENCION DEL TITULO DE INGENIERO EN SISTEMAS

TEMA:

ÁNALISIS DE VULNERABILIDADES EN LA RED DE CONECTIVIDAD DE LA EMPRESA ALTEC S. A, UBICADA EN LA CIUDAD DE BABAHOYO.

EGRESADO:

CAVERO AMAIQUEMA RONMEL MAURICIO

TUTOR:

ING. FREDY MAXIMILIANO JORDÁN CORDONEZ, MSC

AÑO 2020

INTRODUCCIÓN

Altec s.a. es una empresa ubicada en la ciudad de Babahoyo provincia de Los Ríos, dedicada a la elaboración e instalación de objetos de aluminio y vidrio para uso residencial y comercial, que abarcaba el mercado local. La entidad está conformada por los departamentos finanzas, taller, bodega, departamento de ventas entrelazados a través de una infraestructura basada en una red LAN la cual realiza los procesos tales como facturación, pedios, reclamos, devoluciones, que permiten llevar un control adecuado de los bienes y actividades internas que se realizan en la institución.

La problemática existente en Altec S.A se basa en el bajo cumplimiento de las medidas o protocolos de seguridad informática que garantizan la seguridad física y lógica de la red. Para el intercambio de información con la página web es importante usar un protocolo encriptado del tipo SSL, que no garantiza un cifrado de extremo a extremo, es decir, desde el servidor hasta el equipo cliente y viceversa. (ayudaleyprotecciondatos, 2017)

La seguridad de la información tiene que ver con proteger la información del acceso no autorizado. Es parte de la gestión de riesgos de la información e implica prevenir o reducir la probabilidad de acceso, uso, divulgación, interrupción, eliminación, modificación, inspección o registro no autorizados. (instituciones.sld.cu, 2013)

El presente trabajo tiene como objetivo analizar las Vulnerabilidades en la red de conectividad de la Empresa Altec S. A, ubicada en la ciudad de Babahoyo y todo lo relacionado con transmisión y seguridad de la información utilizando la metodología descriptiva, tiene como objetivo la descripción de las cualidades de la red LAN, se basa por un tipo de enfoque cualitativo el cual nos permite realizar las observaciones de los hechos, sucesos y recolección, el análisis de datos durante el proceso a desarrollar.

El caso de estudio se realizó de acuerdo a lo determinado en la línea de investigación de sistemas de información y comunicación, emprendimiento e innovación, donde la sub línea de

investigación es la de redes y tecnologías inteligentes de software y hardware, en donde se utilizó como técnica a la entrevista que permitirá la recolección de la información y trabaja con el instrumento guía de la entrevista que estará dirigido al gerente de la empresa, el propósito de esta entrevista es saber los síntomas que está presentando la red de Altec s.a.

Esta entrevista fue dirigida al gerente de la empresa porque no existe un personal asignado en el área de red dentro de la empresa, según este admite que se asignaron usuarios a la red rigiéndose a las políticas que posee esta empresa.

Se utilizó el método inductivo, donde Estela (2020) afirma que "El razonamiento inductivo consiste, así, en una forma de hipótesis que, a partir de una evidencia singular, sugiere la posibilidad de una conclusión universal." Con este método logramos observar anomalías que presenta la red de conectividad, con el propósito de brindar una propuesta referencial como guía hacia los usuarios de la red para tratar de mantener la seguridad de la información.

Una vez realizado el análisis de vulnerabilidades en la red de conectividad de la empresa Altec s.a., podemos determinar cuáles son las debilidades que presenta dicha red y sugerir acciones necesarias para la correcta seguridad de la información que se manipula en dicha entidad.

DESARROLLO

Altec S.A se encuentra ubicada en la ciudad de Babahoyo, provincia de Los Ríos, inició sus operaciones en 1984, el talento humano se encuentra formado por 15 personas distribuidos de la forma como muestra el anexo 5 correspondiente al organigrama de la empresa.

Se pudo observar que no existe algún tipo de departamento orientado a la administración y seguridad de la red, por ende, la empresa tampoco consta de personal especializado en el área, esto puede aumentar la probabilidad que la red sea aún más vulnerable. Además de que existen fallas en el servidor de esta empresa puestas en evidencia el anexo 1.1 correspondiente a la guía de la entrevista donde el entrevistado menciona que cuando existen fuertes lluvias se producen estas fallas, esto puede dar facilidades a las personas que quieran infiltrarse en la red.

Una vez realizado el testeo de la red de conectividad de la empresa Altec s.a., podemos determinar cuáles son las vulnerabilidades que presenta dicha red y sugerir acciones necesarias para la correcta seguridad de la información que se manipula en dicha entidad.

La técnica que se implementó fue la de entrevista, que nos permitió la recopilación de la información, donde se logró obtener los datos mostrados en el anexo 1 correspondiente a la entrevista.

Cuando existe alguna falla en la red de cualquier tipo, menciona que la más común es por la condición climática de fuertes lluvias produce que los equipos se desconecten del equipo servidor, acuden a un técnico en particular o también acuden a un técnico de la empresa que les provee internet que es CNT (corporación nacional de telecomunicaciones), se muestra en el anexo #5 el tiempo en que se tardan en solucionar los problemas es alrededor de una hora cuando los técnicos no están disponibles, pero también existe acceso remoto mediante TeamViewer y se dice que es un poco más rápido la solución de problemas, el gerente considera que es una prioridad ubicar una persona especializada encargada de la red, con el objetivo de tener un técnico de disponibilidad inmediata ya que optimiza el tiempo de operaciones de la

misma. Para conocer un poco más la situación de la empresa se desarrolló el siguiente análisis FODA.

FORTALEZAS	OPORTUNIDADES
✓ El departamento cuenta con un servidor de red. ✓ Disposición del personal. ✓ Expansión económica de una base de pc. ✓ Compartición de programas y archivos.	✓ Buenas relaciones con el proveedor. ✓ Compartición de recursos en la red. ✓ Accesos a otros sistemas operativos. ✓ Mejora en la organización de la empresa.
DEBILIDADES	**AMENAZAS**
✓ Deficiencias de infraestructura de red. ✓ No tener información en tiempo real de lo que pasa. ✓ La empresa no cuenta con las seguridades de data center, es decir que no cuenta con estándares de certificación (piso térmico, puerta de escape, seguridad techo falso, etc. ✓ No existe personal técnico.	✓ El mantenimiento de la red (muchas veces es costoso). ✓ Ataques informáticos. ✓ Informaciones vulnerables. ✓ Perdidas de datos. ✓ No contar con una persona que se encargue de la red.

Tabla 1: análisis de FODA.

Elaborado por: Ronmel Cavero Amaiquema.

La implementación de los procesos de gestión de servicios permite a la organización obtener un control permanente de sus actividades, un aumento de la eficiencia e incorporar a la cultura de la empresa la mejora continua en todos los ámbitos, la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos. La aplicación de ISO-27001 significa una diferenciación respecto al resto, que mejora la competitividad y la imagen de una empresa. (isotools.org, 2020).

La ISO 27001 debe fundamentarse en tres aspectos que son los siguientes:

- Confidencialidad. Que la información sea únicamente accesible por las personas que estén autorizadas para ello. (ISOTools, 2016)
- Disponibilidad. El acceso a la información debe estar siempre accesible en el momento que se necesite. (ISOTools, 2016)
- Integridad. La información debe mantenerse completa e inalterada y en ningún caso puede ser manipulada sin autorización. (ISOTools, 2016)

Se ha convertido en la principal norma a nivel mundial para la seguridad de la información y muchas empresas han certificado su cumplimiento (Segovia, 2020)

¿Dónde interviene la gestión de seguridad de la información en una empresa?

Básicamente, la seguridad de la información es parte de la gestión global del riesgo en una empresa, hay aspectos que se superponen con la ciberseguridad, con la gestión de la continuidad del negocio y con la tecnología de la información. (Rivera, 2019)

Una vulnerabilidad es cualquier debilidad en el sistema informático que puede permitir a las amenazas causarle daños y producir pérdidas en la organización. Se corresponden con fallos en los sistemas físicos y lógicos, aunque también pueden tener su origen en los defectos de ubicación, instalación, configuración y mantenimiento de los equipos. (Tensor, 2015)

Se considera amenaza a cualquier evento accidental o intencionado que pueda ocasionar algún daño en el sistema informático, provocando pérdidas materiales, financieras o de otro tipo a la organización. (Tensor, 2015)

AMENAZAS EN UNA RED DE DATOS		
Personas	**Físicas**	**Lógicas**
Ex trabajadores Piratas informáticos Curiosos remunerados	Sustracciones de información Abastecimientos eléctricos Catástrofes naturales	Perdidas de datos Ataques en la red Virus

Tabla 2: Amenazas en una Red.

Elaborado por: Ronmel Cavero Amaiquema.

A la hora de estudiar los distintos tipos de ataques informáticos, podríamos diferenciar en primer lugar entre los ataques activos, que producen cambios en la información y en la situación de los recursos del sistema, y los ataques pasivos, que se limitan a registrar el uso de los recursos y/o a acceder a la información guardada o transmitida por el sistema. (Vieites, 2019)

Un ataque a las redes de datos, consiste en aprovechar una vulnerabilidad de un sistema informático (sistema operativo, programa de software o sistema del usuario) con propósitos desconocidos por el operador del sistema y que, por lo general, causan un daño. (ecured, 2014)

✓ Los ataques pueden ejecutarse por diversos motivos:
✓ obtener acceso al sistema
✓ robar información, como secretos industriales o propiedad intelectual
✓ recopilar información personal acerca de un usuario
✓ obtener información de cuentas bancarias
✓ Para obtener información acerca de una organización (la empresa del usuario, etc.).

Tabla 3: Motivos Por El Cual Se Realizan Ataques.

Elaborado *por: Ronmel Cavero Amaiquema.*

Los sistemas informáticos utilizan múltiples componentes, desde electricidad para proveer alimentación a los equipos hasta el programa de software ejecutado mediante el sistema operativo que emplea la red.

La manera que se podría reducir los riesgos de que la información sea extraída mediante la red es implementando normas que resguarden la información. La norma ISO27001 tiene como propósito gestionar la seguridad de la información que permite garantizar que los riegos de seguridad sean conocidos por las organizaciones de manera eficiente, documentada y adaptada a cambios tecnológicos. (Vásquez, 2017)

El escaneo de puertos es una de las técnicas de reconocimiento más populares que utilizan los atacantes para descubrir los servicios expuestos a posibles ataques. Todas las máquinas conectadas a una red de área local (LAN) o Internet ejecutan muchos servicios que escuchan en puertos conocidos y no tan conocidos. (ciberseguridad.blog, 2018)

Un escaneo de puertos ayuda al atacante a localizar qué puertos están disponibles, básicamente, un escaneo de puertos consiste en remitir un mensaje a cada puerto, uno a uno. El tipo de respuesta recibida indica si el puerto está a la escucha y, por lo tanto, puede probarse más detalladamente para detectar debilidad.

Los ataques se pueden producir en cada eslabón de esta cadena, siempre y cuando exista una vulnerabilidad que pueda aprovecharse.

Acceso físico	Denegación de servicios
En este caso, el atacante tiene acceso a las instalaciones e incluso a los equipos: • Interrupción del suministro eléctrico. • Apagado manual del equipo. • Vandalismo. • Apertura de la carcasa del equipo y robo del disco duro. • Monitoreo del tráfico de red.	El objetivo de estos ataques reside en interrumpir el funcionamiento normal de un servicio. Por lo general, las denegaciones de servicio se dividen de la siguiente manera: • Explotación de las debilidades del protocolo TCP/IP. • Explotación de las vulnerabilidades del software del servidor.
Ingeniería social • En la mayoría de los casos, el eslabón más débil es el mismo usuario. Muchas veces es él quien, por ignorancia o a causa de un engaño, genera una vulnerabilidad en el sistema al brindar información (la contraseña, por ejemplo) al pirata informático o al abrir un archivo adjunto. Cuando ello sucede, ningún dispositivo puede proteger al usuario contra la falsificación: Sólo el sentido común, la razón y el conocimiento básico acerca de las prácticas utilizadas pueden ayudar a evitar este tipo de errores.	**Intrusiones** • Análisis de puertos. • Elevación de privilegios: este tipo de ataque consiste en aprovechar una vulnerabilidad en una aplicación al enviar una solicitud específica (no planeada por su diseñador). • Los ataques de desbordamiento de la memoria intermedia (búffer) usan este principio. • Ataques malintencionados (virus, gusanos, troyanos).

Tabla 4: Algunos riesgos para los cuales hay que estar preparados.

Elaborado por: Ronmel Cavero Amaiquema.

Formas frecuentes en que ocurren los Ataque en una red	
Intento de ingreso. - En esta etapa, el atacante investiga a la organización blanco. Él puede obtener toda la información pública sobre una organización y sus empleados y realizar exploraciones completas en todas las computadoras y dispositivos que son accesibles desde Internet.	**Penetración en la red. -** Después de que el atacante haya localizado vulnerabilidades potenciales, intenta aprovecharse de una de ellas. Por ejemplo, el atacante explota las vulnerabilidades en un Servidor Web que carece de la última actualización de seguridad.
Elevación de privilegios. - Luego que el atacante ha penetrado con éxito la red, procura obtener los derechos de Administrador a nivel de sistema. Por ejemplo, mientras que explota el servidor Web, gana control de un proceso funcionando bajo el contexto LocalSystem. Este proceso será utilizado para crear una cuenta de administrador. En general, la pobre seguridad como resultado de usar configuraciones por defecto, permite que un atacante obtenga el acceso a la red sin mucho esfuerzo.	**Explotar vulnerabilidades.-** Después de que el atacante haya obtenido los derechos necesarios, realiza el intento de romper la seguridad de la red. Por ejemplo, el atacante elige desfigurar el sitio Web público de la organización. **Borrado de huellas.-** La etapa final de un ataque es aquella donde un atacante procura ocultar sus acciones para escapar a la detección o el procesamiento. Por ejemplo, un atacante borra entradas relevantes de la intervención en archivos log**.**

Tabla 5: Formas frecuentes de como ocurren los ataques.

Elaborado por: Ronmel Cavero Amaiquema

Para la realización del escaneo de los puertos se utilizó Nessus y Nmap, son dos herramientas que se utilizan para identificar vulnerabilidades en una red, estas herramientas se detallan a continuación.

Se encontró un rango alto de vulnerabilidad en los siguientes host: 192.168.1.40, 192.168.1.1, 192.168.1.46, 192.168.1.25, los cuales fueron identificados mediante los escaneos de nessus y nmap en la red de la empresa altec sa. se muestra desde el anexo #2 hasta el anexo#3.4.

Nessus es la solución más usada para las evaluaciones de vulnerabilidad, configuración y compatibilidad. Previene ataques a la red mediante la identificación de vulnerabilidades y problemas de configuración que los piratas informáticos utilizan para penetrar su red**.** (Ara, 2016)

¿Cómo funciona? En una operación normal, comienza escaneando los puertos para buscar puertos abiertos y después intentar varios exploits para atacar. Algunas de estas pruebas pueden causar que los servicios o sistemas operativos se corrompan o caigan, esto se puede evitar desactivando "unsafe test". (Ara, 2016)

¿Para qué sirve? Sirve para detectar a través de la red vulnerabilidades en un sistema ya sea cliente, servidor, use Windows, Linux, MAC, etc… También detecta vulnerabilidades en el software, algunas de sus ventajas son las siguientes:

- Escanea el rango más amplio de dispositivos de red, sistemas operativos, bases de datos y aplicaciones
- Detecta amenazas como virus, malware, puertas traseras y servidores que se comunican con sistemas infectados con botnets;
- Informa y comunica problemas de seguridad en toda la organización mediante informes de solución.

Nessus nos permitió observar que, si hay existencia de vulnerabilidades dentro de la red, como se muestra en el anexo 2, Nessus nos muestra los hosts escaneados con sus respectivos niveles

de vulnerabilidad de los diferentes tipos encontrados, además de detallar los tipos de vulnerabilidades Nessus nos brinda una posible solución a estas vulnerabilidades como muestra en el anexo 2.4 mediante reportes que pueden ser generados en formatos pdf, html y csv.

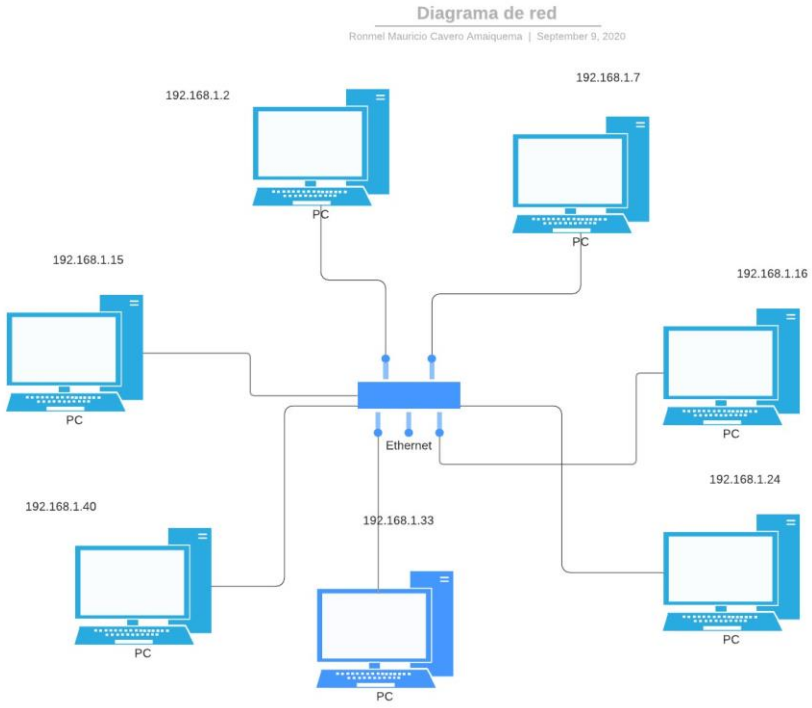

Ilustración 1: grafico de red

Elaborado por: Ronmel Cavero Amaiquema.

Centraremos como una de las vulnerabilidades de severidad alta encontrada en el host 192.168.1.40, donde Nessus nos informa que, el servicio remoto acepta conexiones cifradas mediante SSL 2.0 y / o SSL 3.0. Estas versiones de SSL se ven afectadas por varias fallas criptográficas, que incluyen: un esquema de relleno inseguro con cifrados CBC y esquemas inseguros de renegociación y reanudación de sesiones.

Un atacante puede aprovechar estas fallas para realizar ataques de intermediario o para descifrar las comunicaciones entre el servicio afectado y los clientes.

A la vez nos brinda como solución consultar la documentación de la aplicación para desactivar SSL 2.0 y 3.0 y utilizar TLS 1.2 (con conjuntos de cifrados aprobados) o superior.

Nmap es una aplicación multiplataforma usada para explorar redes y obtener información acerca de los servicios, sistemas operativos y vulnerabilidades derivadas de la conjunción de éstos. (seguinfo, 2007)

Es muy usado por todo aquél que se interesa por las tareas de seguridad y hacking en general, desde Administradores de Sistemas a interesados con fines menos respetables. Las técnicas de escaneo que usa Nmap han sido ya implementadas en sistemas de detección de intrusos y firewalls, ya que los desarrolladores de sistemas de seguridad también usan Nmap en su trabajo y toman medidas (seguinfo, 2007). A continuación, se muestran ventajas al utilizar Nmap:

- Este programa incluso en sus versiones graficas es muy poderoso, y tiene opciones para realizar escaneos muy difícilmente detectables por las "victimas" o supervisores de red. (Villalobos, 2010)
- Escanea cualquier rango de puertos que desees e incluso detecta el sistema operativo de la víctima, dando lugar a que el hacker identifique más claramente como puede acceder al equipo remoto. (Villalobos, 2010)

No obstante, pese a estar ampliamente documentado su funcionamiento, hay formas de escaneo que lo hacen difícil de detectar cuando se trata de obtener información. Bueno, descargamos Nmap del sitio oficial para nuestra plataforma y lo instalamos (seguinfo, 2007).

```
$ apt-get install nmap
```

Comenzemos a escanear…

```
$ nmap -sP 192.168.1.0/24
```

Esto escaneará las 255 direcciones de la red 192.168.1.0 El atributo -sP indica que será un escaneo mediante ping. Envia un ping (ICMP echo request) y un paquete TCP ACK al puerto 80. Si el destino contesta con otro ping o con un paquete TCP RST significa que está operativo. (seguinfo, 2007)

Para la realización del escaneo de puertos con Nmap se escogió la opción de escaneo intensivo, como objetivo escanear la siguiente ip 192.168.1.0-255 como se muestra en el anexo 3.1, además nos permite observar el estado de cada uno de los puertos en los host como podemos observar en el anexo 3.3 y también grafica el tipo de topología que usa esta red, en este caso usa una topología estrella como vemos en el anexo 3.2.

En la red se emplean políticas de seguridad informática pero no son suficientes para garantizar la misma al máximo, es por eso que se recomienda que la empresa debe acoger el uso de la norma ISO 27002 que corresponde a una guía de buenas prácticas para gestión de la seguridad de la información.

Tanto la norma ISO 27001 como la 27002 tienen un objetivo común: proporcionar un marco de referencia para la definición e implantación de un Sistema de Gestión de la Seguridad de la Información (SGSI). Sin embargo, existe una diferencia importante: la ISO 27001 es una norma certificable, mientras que la ISO 27002 es un compendio de recomendaciones y buenas prácticas. (ISOTools, 2016)

CONCLUSIONES.

En la red de conectividad se encontraron vulnerabilidades en la red, como lo que puede causar ataques informáticos de cualquier tipo, como perdidas de datos confidenciales de la empresa, con el propósito de robo de información o alteración de la misma.

Se demostraron debilidades en el diseño de protocolos utilizados en la red, errores en configuraciones inadecuadas en los equipos informáticos, desconocimientos de las herramientas que facilitan los ataques, existencias de puertas traseras, mediante las herramientas seleccionadas demostrando su rango de vulnerabilidad, además de que existen puertos abiertos innecesariamente, se sugiere aplicar las acciones que correspondan para mantener a la red segura de hipotéticos ataques que se realicen en un futuro mediante la infiltración por la red.

Se sugiere aplicar la norma ISO/ICE 27002 en la empresa Altec s.a. porque no constan con una política de seguridad eficiente, ya que esta norma nos permite confirma que, para obtener beneficios, tales como la oportunidad de descubrir y corregir puntos débiles, mejorar el conocimiento sobre la seguridad de la información a las personas que forman la empresa, así como también gestionar los servicios informáticos y a los usuarios logrando optimizar el tiempo.

La empresa debe de incorporar a su equipo de trabajo personal encargado de la red, además de que sea capacitado con frecuencia para estar en condiciones de resolver cualquier tipo de amenaza que se presente en la red.

BIBLIOGRAFÍA

ara, m. e. (28 de 09 de 2016). obtenido de fferia.wordpress.com: https://fferia.wordpress.com/nessus/

ayudaleyprotecciondatos. (20 de 06 de 2017). *ayudaleyprotecciondatos.es.* obtenido de https://ayudaleyprotecciondatos.es/2017/06/20/seguridad-informatica-empresas/#protocolo_ssl

ciberseguridad. (20 de enero de 2018). *ciberseguridad.blog.* obtenido de ciberseguridad.blog: https://ciberseguridad.blog/25-tipos-de-ataques-informaticos-y-como-prevenirlos/

ecured. (19 de marzo de 2014). *ecured.cu*. obtenido de ecured.cu: https://www.ecured.cu/ataque_a_las_redes_de_datos

estela, m. (20 de 08 de 2020). *concepto.de.* obtenido de https://concepto.de/metodo-inductivo/

gci. (20 de ene de 2020). *certificación iso: la clave de la excelencia*. obtenido de gci.mx: https://www.gci.mx/post-certificacion-iso--la-clave-de-la-excelencia-53.html

instituciones.sld.cu. (08 de 2013). *instituciones.sld.cu.* obtenido de https://instituciones.sld.cu/dnspminsap/files/2013/08/metodologia-psi-nuevaproyecto.pdf

isotools. (5 de enero de 2016). *isotools.* obtenido de https://www.isotools.org/2016/01/05/novedades-de-la-iso-27002-de-mejores-practicas-en-la-gestion-de-seguridad-de-la-informacion/

isotools.org. (2020). *isotools.org*. obtenido de isotools.org: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

rivera, j. f. (03 de 2019). obtenido de infosecurityvip.com: http://www.infosecurityvip.com/evt/wp-content/uploads/2019/03/informasi-pr-isec-infosecurity-san-juan-tour-2019.pdf

segovia, a. j. (2020). *player.vimeo.com*. obtenido de player.vimeo.com: https://player.vimeo.com/video/101239302

seguinfo. (27 de junio de 2007). *seguinfo.wordpress.com.* obtenido de https://seguinfo.wordpress.com/2007/06/27/%c2%bfque-es-nmap/

tensor. (20 de ago de 2015). *analisis de riesgos ii*. obtenido de es.slideshare.net: https://es.slideshare.net/tensor/analisis-de-riesgos-ii#:~:text=amenazas%20una%20amenaza%20es%20cualquier,otro%20tipo%20a%20la%20organizaci%c3%b3n.

vásquez, k. e. (2017). obtenido de pirhua.udep.edu.pe: https://pirhua.udep.edu.pe/bitstream/handle/11042/2787/mas_det_012.pdf?sequence=1&isallowed=y

vieites, á. g. (08 de 2019). *tipos de ataques e intrusos en las redes informáticas.* obtenido de edisa.com: https://www.edisa.com/wp-content/uploads/2019/08/ponencia_-_tipos_de_ataques_y_de_intrusos_en_las_redes_informaticas.pdf

villalobos, j. (10 de diciembre de 2010). *codigoprogramacion.* obtenido de http://codigoprogramacion.com/tag/nmap-hacking#.x0zvishkjiu

Anexos

UNIVERSIDAD TECNICA DE BABAHOYO
FACILTAD DE ADMINISTRACION, FINANZAS E INFORMATICA
ENTREVISTA DIRIGIDA AL GERENTE

Anexo 1: entrevista

Anexo 1.1: guía de la entrevista

1. ¿Cuál es su cargo y su tiempo de trabajo dentro de la empresa?

   Gerente, se encuentra laborando desde hace 10 años dentro de la empresa

2. ¿Se definieron usuarios de acuerdo a las políticas de la empresa?

Si porque existen usuarios que se encargan en la administración y procesos que se realizan en la institución.

3. ¿A quién acuden cuando existe alguna falla en la conectividad de la red?

Se acude a un técnico en particular o también a un técnico del proveedor del internet debido a que no existe una persona asignada para este tipo de problemas en la institución.

4. ¿Cuál es el proveedor de servicios de internet?

El proveedor de internet es Cnt.

5. ¿Existe algún software adicional para los procesos de la empresa?

Si, el software que se utiliza para la gestión de procesos se llama Dominio control que se encuentra conectada a la red.

6. ¿Cuáles cree usted que son las fallas en la red de conectividad y sus causas?

Las fallas más comunes es cuando los equipos se desconectan del servidor, pero este sigue estable, la causa de esto es proporcionada cuando se produce fuertes lluvias.

7. ¿Si existen fallas en la red cual es el tiempo que se tardan en detectar el problema?

El tiempo promedio es de 1 hora, cuando los técnicos no están disponibles, pero también por TeamViewer dan acceso remoto y es más rápido para dar solución al problema.

8. En caso de tener una persona encargada de la red LAN ¿Considera usted que mejoraría los procesos de control de la red?

Si porque optimiza el tiempo sistemático en la empresa, se considera que es una prioridad.

Anexo 1.2: evidencia de realización de la entrevista

Ilustración 2: evidencia de realización de la entrevista.

Elaborado por: Ronmel Cavero Amaiquema.

Anexo 2: capturas del testeo realizado con Nessus

Anexo 2.1: Ips encontradas al momento de ejecutar la acción del escaneo de Nessus

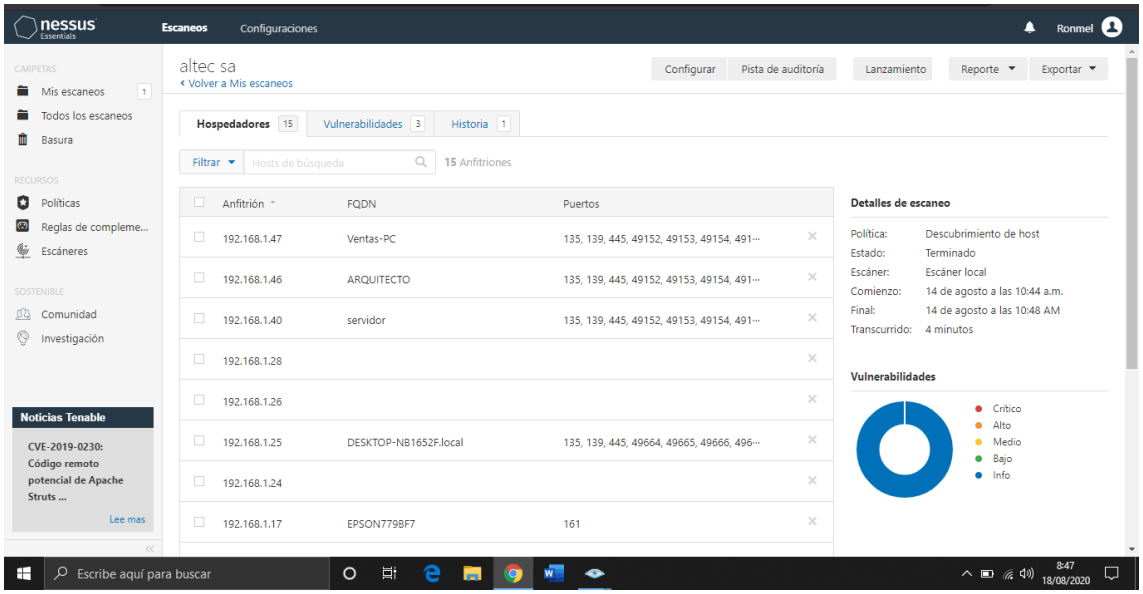

Ilustración 3: Ips encontradas al momento de ejecutar la acción del escaneo de Nessus

Elaborado por: Ronmel Cavero Amaiquema.

Anexo 2.2: Niveles de vulnerabilidad encontrados en cada uno de los hosts

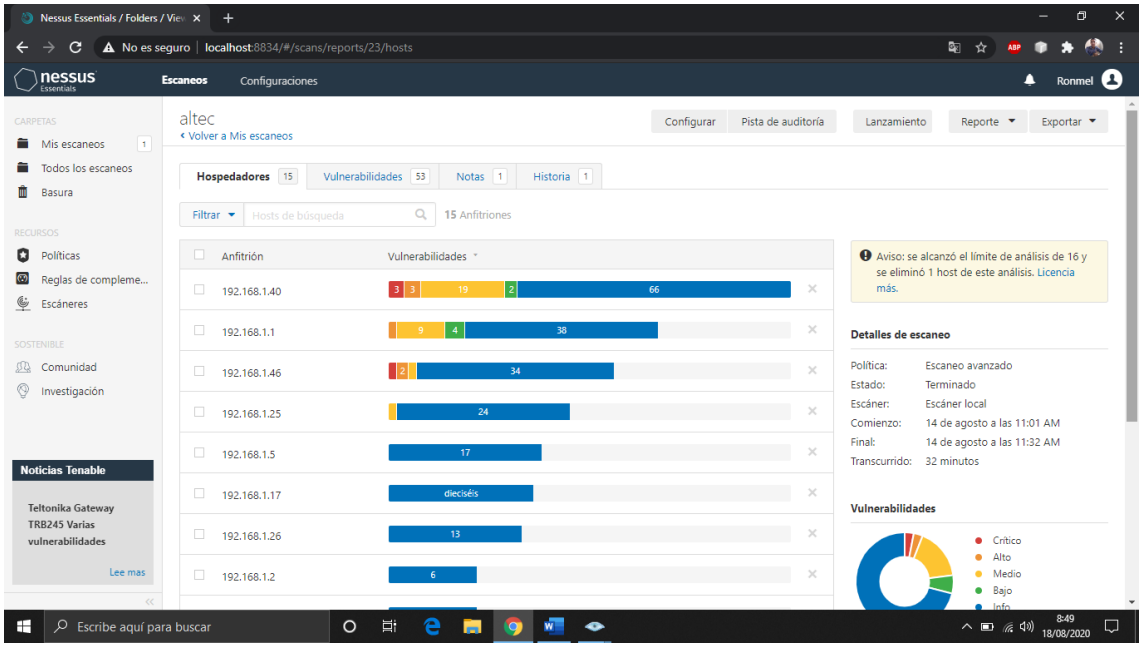

Ilustración 4: Niveles de vulnerabilidad encontrados en cada uno de los hosts.

Elaborado por: Ronmel Cavero Amaiquema.

Anexo 2.3: Detalles de vulnerabilidades encontradas en cada uno de los hosts

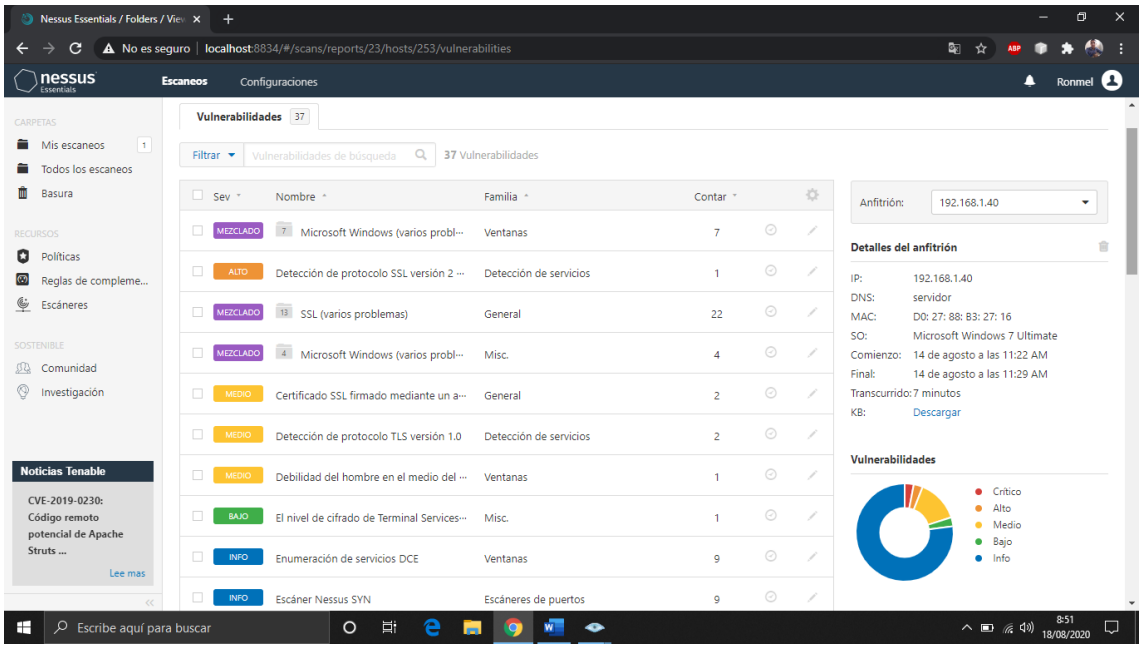

Ilustración 5: Detalles de vulnerabilidades encontradas en cada uno de los hosts.

Elaborado por: Ronmel Cavero Amaiquema.

Anexo 2.4: Como se muestra, Nessus además de identificar vulnerabilidades nos brinda una posible solución en cada una de ellas

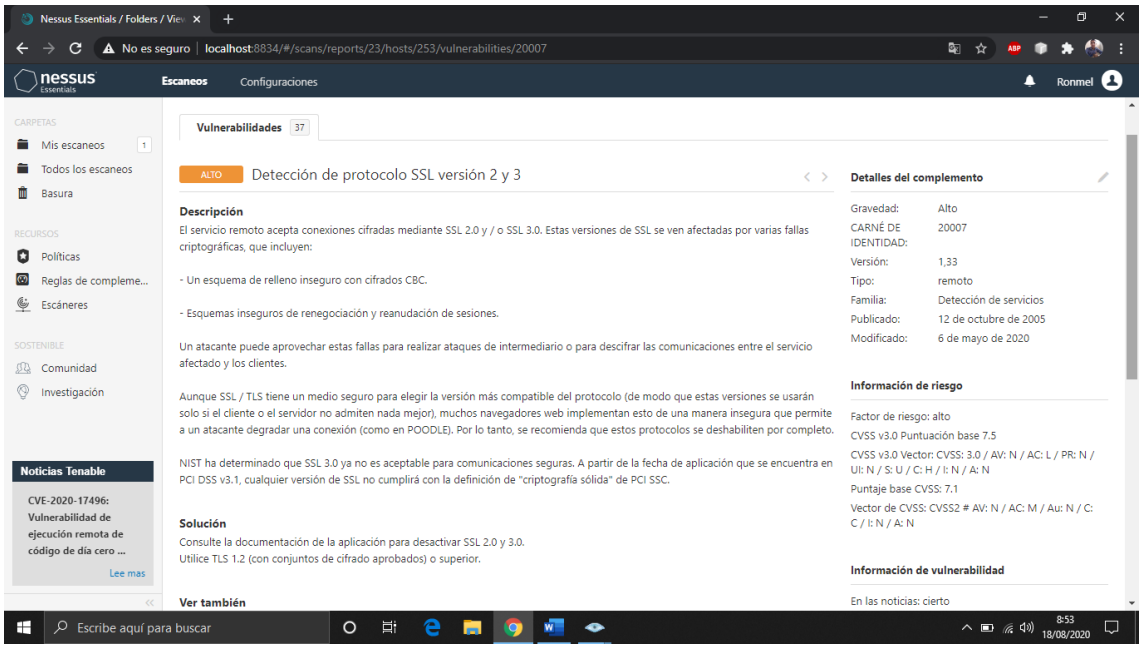

Ilustración 6: Como se muestra, Nessus además de identificar vulnerabilidades nos brinda una posible solución en cada una de ellas.

Elaborado por: Ronmel Cavero Amaiquema.

Anexo 3: capturas del testeo con nmap

Anexo 3.1: Finalización del escaneo con Nmap

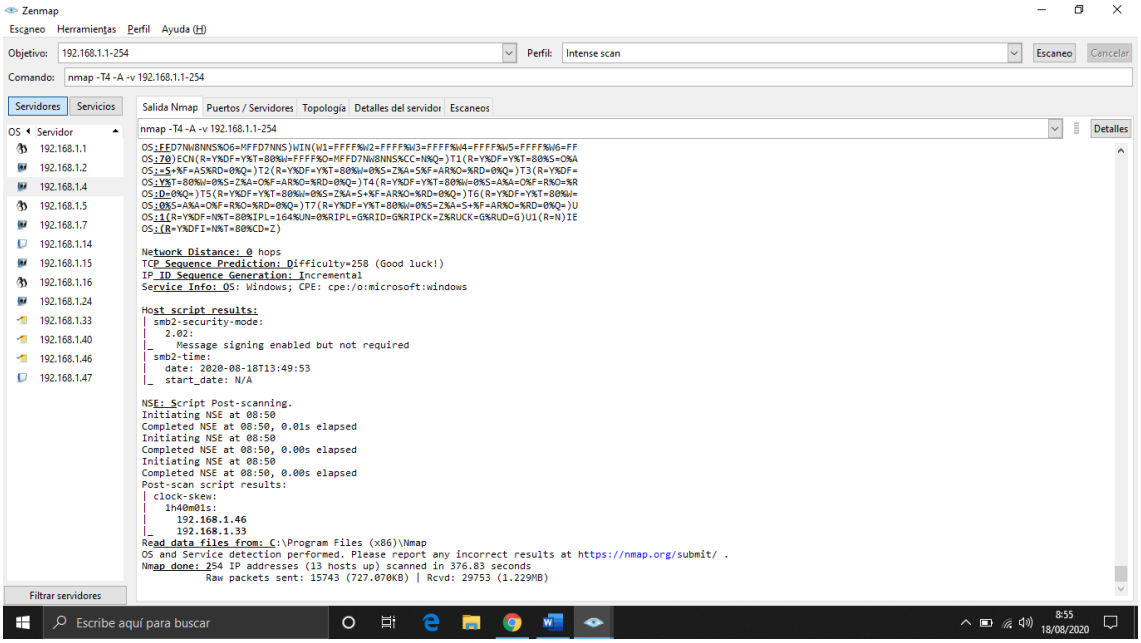

Ilustración 7: Finalización del escaneo con Nmap.

Elaborado por: Ronmel Cavero Amaiquema.

Anexo 3.2: Topología de red correspondiente a la empresa

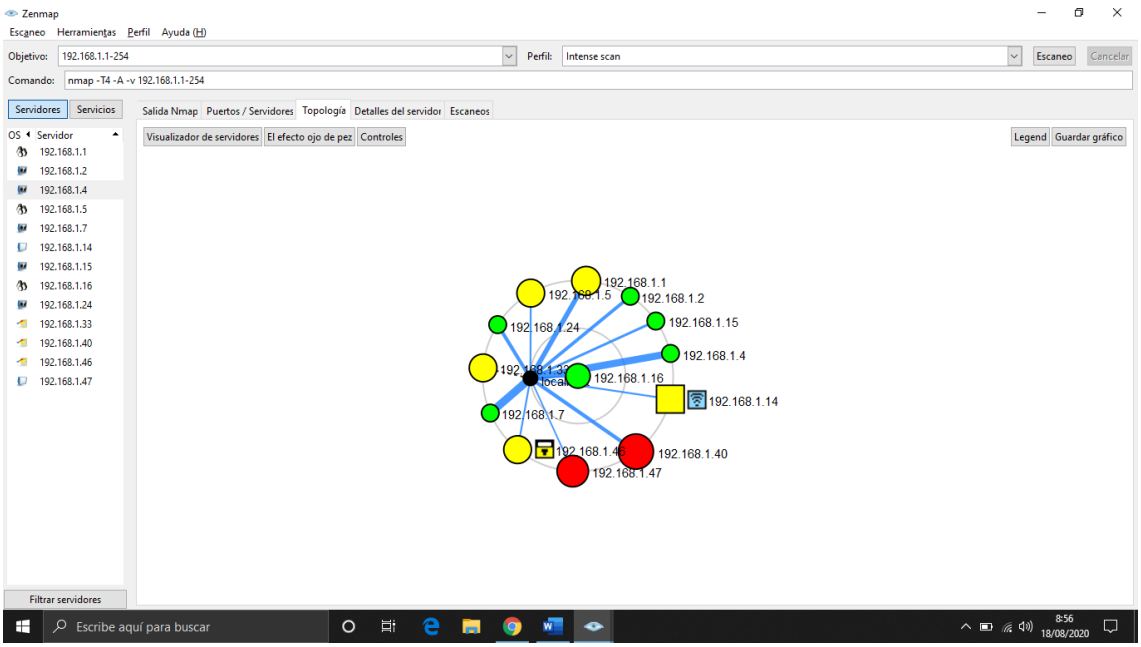

Ilustración 8: Topología de red correspondiente a la empresa.

Elaborado por: Ronmel Cavero Amaiquema.

Anexo 3.3: Estado de los puertos en uno de los hosts escaneados

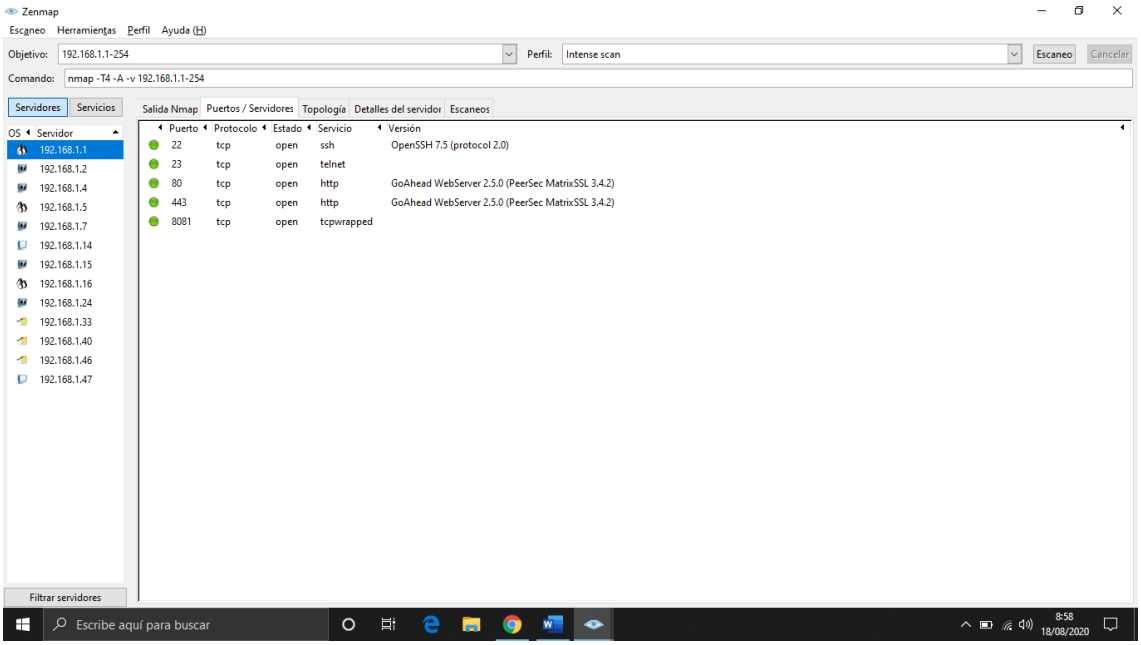

Ilustración 9: Estado de los puertos en uno de los hosts escaneados.

Elaborado por: Ronmel Cavero Amaiquema.

Anexo 3.4: Detalles del servidor

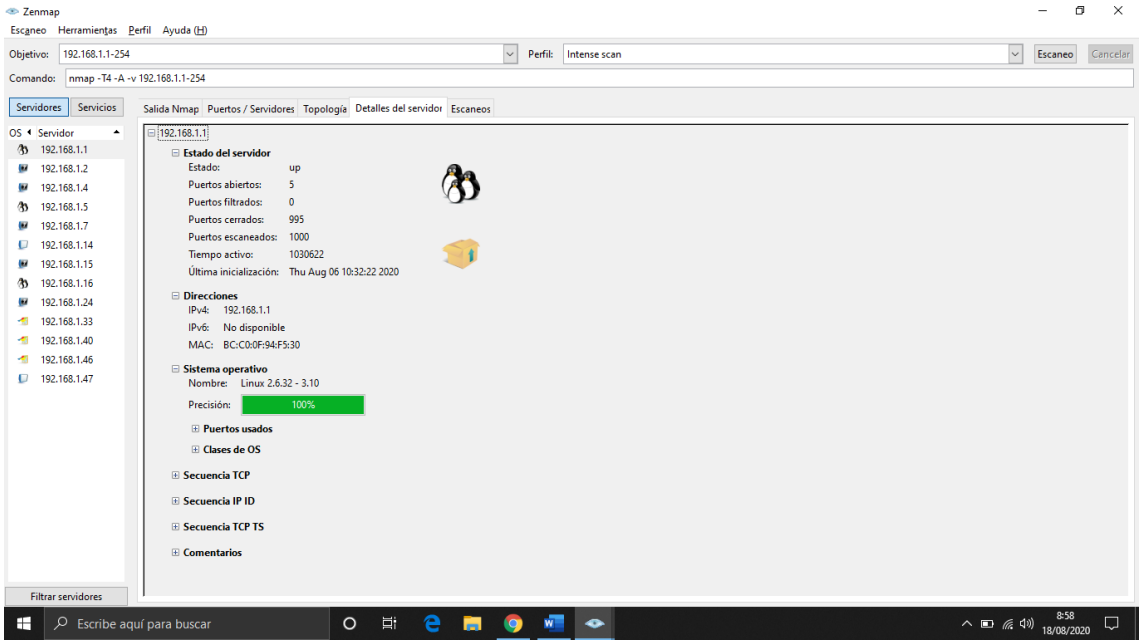

Ilustración 10: Detalles del servidor.

Elaborado por: Ronmel Cavero Amaiquema.

Anexo 4: árbol del problema

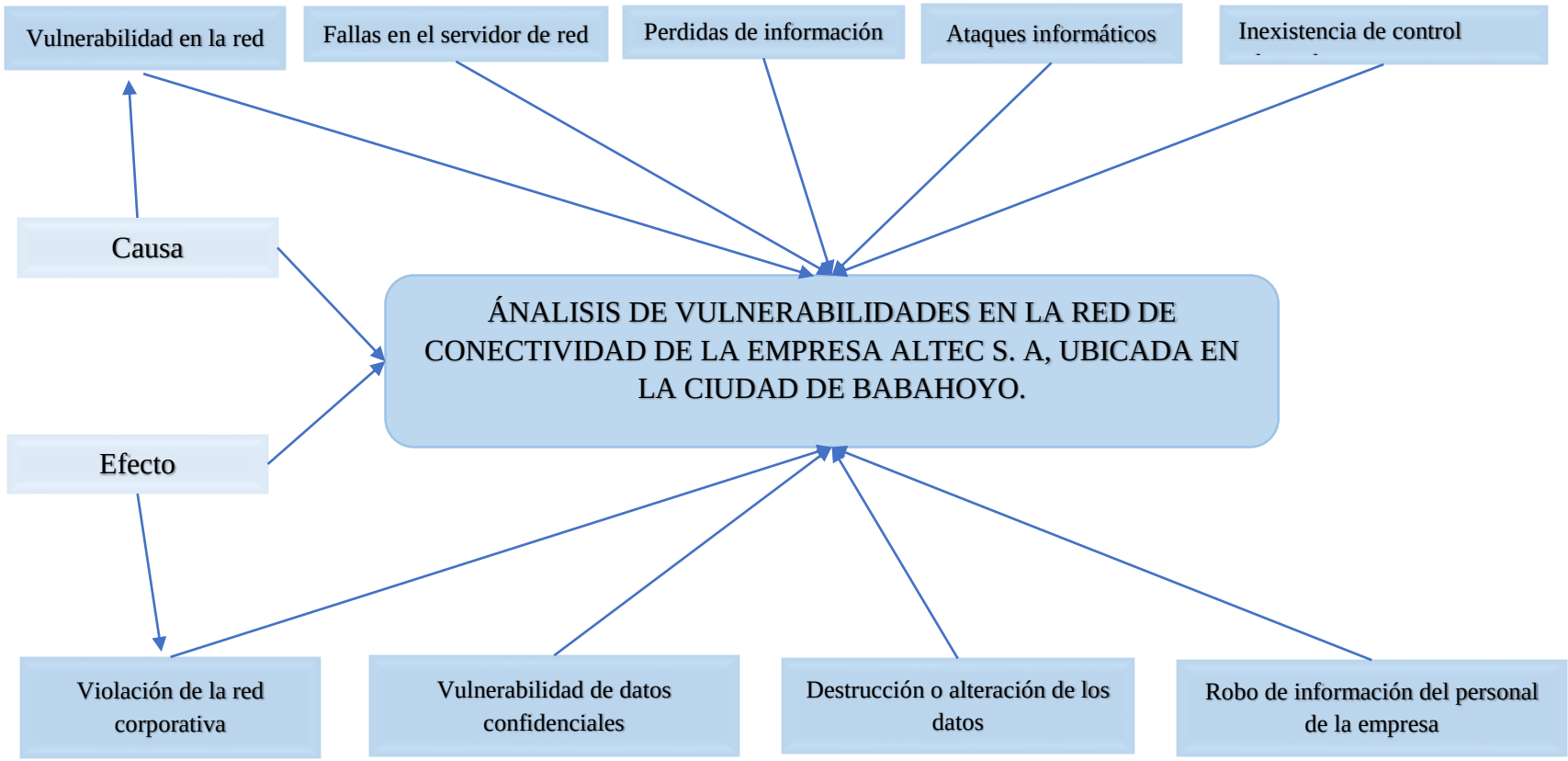

Ilustración 11: árbol del problema

Elaborado por: Ronmel Cavero Amaiquema.

Anexo 5: organigrama de la empresa

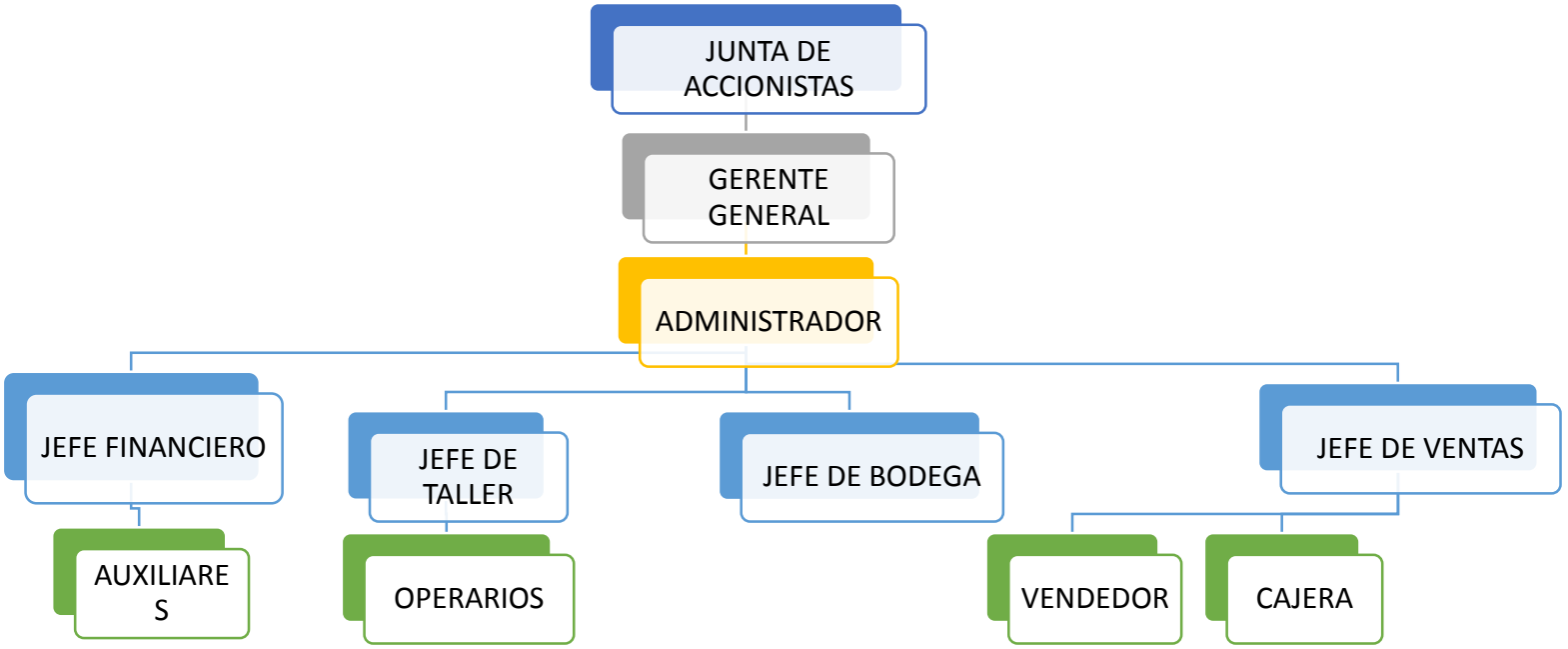

Ilustración 12:Organigrama de la empresa.

Elaborado por: Ronmel Cavero Amaiquema