MEJORAMIENTO DE LA SEGURIDAD EN LAS REDES LAN Y WAN DE LAS EMPRESAS QUE CONFORMAN EL GRUPO MAYOREO

Autor: Pérez Luis

C.I: 21.454.443

Urbanización Yuma II, Calle Nº 3. Municipio San Diego.

Teléfonos: 0241-8714240 (Master) – Fax: 0241-8712394

REPÚBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD JOSÉ ANTONIO PÁEZ
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA DE TELECOMUNICACIONES

MEJORAMIENTO DE LA SEGURIDAD EN LAS REDES LAN Y WAN DE LAS EMPRESAS QUE CONFORMAN EL GRUPO MAYOREO

Informe de pasantías presentado para optar al título de
INGENIERIO EN TELECOMUNICACIONES

EMPRESA: FEBECA C.A.

Autor: Pérez Luis
C.I: 21.454.443

San Diego, Junio de 2017

REPÚBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD JOSÉ ANTONIO PÁEZ
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA DE TELECOMUNICACIONES

MEJORAMIENTO DE LA SEGURIDAD EN LAS REDES LAN Y WAN DE LAS EMPRESAS QUE CONFORMAN EL GRUPO MAYOREO

CONSTANCIA DE ACEPTACIÓN

Karen Ramírez 14571040

Nombre, firma y cédula de identidad del tutor académico

FEBECA, C.A.
RIF. J-000033927

Hubert Ramírez 16791579

Nombre, firma y cédula de identidad del tutor empresarial

AUTOR: **Pérez Luis**

C.I. **21.454.443**

San Diego, Junio de 2017

AGRADECIMIENTOS

Le agradezco primeramente a Dios por haberme guiado a lo largo de mi carrera, por ser mi fortaleza en los momentos de debilidad y por brindarme una vida llena de aprendizajes, experiencias y sobre todo felicidad.

A mi Madre Tibisay López por apoyarme en todo momento, gracias a sus consejos, los valores inculcados, por haberme dado la oportunidad de tener una excelente educación y por sobre todo haber confiado siempre en mí.

A mi Padre Luis Pérez por querer siempre lo mejor para mí, aconsejarme, apoyarme, ser un ejemplo a seguir, gracias papa por guiarme por buen camino, todo lo que he logrado te lo debo a ti.

A mi tutor académico la profesora Karen Ramírez y mi tutor empresarial Hebert Ramírez, por su gran ayuda y colaboración en cada momento de consulta en este proyecto.

A mis compañeros por todos los momentos que compartimos, todo lo que aprendí de ustedes y por haber echo de mi etapa universitaria un trayecto que nunca olvidare.

Por último y no menos importante quiero dar gracias a todas las personas que han formado parte de este largo trayecto en el cual siempre me dieron ánimos de seguir adelante, la comprensión y el apoyo tanto de familiares y amigos.

Luis Fernando Pérez López

DEDICATORIA

Primeramente, debo dedicarle y ante todo agradecer a DIOS, por darme la oportunidad de vivir, por estar conmigo en cada paso que doy, por fortalecer mi corazón e iluminar mi mente durante esta etapa tan importante de mi formación profesional.

A mis padres Tibisay López y Luis Pérez, por ser los pilares fundamentales en mi vida y en mi carrera profesional, por ayudarme con los recursos necesarios para estudiar, por su gran apoyo, comprensión y sobre todas las cosas siempre confiaron en mí, por todo eso y mucho más este logro es de ustedes los Amo.

A mi hermana Nikool Pérez por estar conmigo siempre, apoyarme y por traer al mundo a mi sobrino Luciano Gabriel quien ha sido una motivación más en este último tramo de mi carrera.

A todos mis familiares que siempre estuvieron apoyándome y que contribuyeron de alguna forma durante esta etapa de mi vida, especialmente mi primo Carlos López quien en vida siempre estuvo para mí cuando más lo necesite.

ÍNDICE GENERAL

CONTENIDO Pp

ACEPTACION DEL TUTOR ……. III
AGRADECIMIENTOS ……... IV
DEDICATORIA ……... V
ÍNDICE DE FIGURAS ……...……. IX
INTRODUCCIÓN …… 1

CAPÍTULO I

LA EMPRESA

1.1 Reseña Histórica …… 3
1.2 Misión ……... 5
1.3 Visión ……..... 6
1.4 Valores …….. 6
1.5 Organigrama General de la empresa ……. 6

CAPITULO II

EL PROBLEMA

2.1 Planteamiento del Problema ……..… 8
2.2 Formulación del Problema ……. 10
2.3 Objetivos de la Investigación …… 10

2.3.1 Objetivo General …… 10
2.3.2 Objetivo Especifico …… 10
2.4 Justificación …… 11
2.5 Alcance …….. 12
2.6 Limitaciones …….. 12

CAPITULO III

MARCO REFERENCIAL CONCEPTUAL

3.1 Antecedentes …….. 14
3.2 Bases Teóricas …… 16
3.2.1 Seguridad WLAN …….. 16
Protocolos de Encriptación ……. 16
Protocolos de Confidencialidad …….. 18
EAP ……. 19
3.2.2 Seguridad LAN …….. 19
3.2.3 Servidor NTP ……. 20
3.2.4 Servidor LOG ……. 20
3.2.5 Monitor SNMP ……... 21
3.3 Definición de Términos Básicos …… 21

CAPITULO IV

FASES METODOLOGICAS

4.1 Fases Metodológicas …….. 24

Fase I: Identificación de la estructura de red y diseño de las topologías en cada una de las empresas del grupo Mayoreo ……. 24

Fase II: Diseño e implementación de herramientas para fortalecer la seguridad en las redes LAN y WAN del grupo Mayoreo …… 24

Fase III: Identificación de los equipos de comunicación que conforman la red y sus Características ……... 25

Fase IV: Diseño de normas y estrategias para mejorar la seguridad en las redes LAN y WAN del grupo Mayoreo ……..... 25

CAPITULO V

RESULTADOS

Resultados ……...…….……... 26

Fase I ……...…….……... 26

Fase II ……...……. 29

Fase III ……..……. 31

Fase IV …….…….. 33

CONCLUSIONES …….……. 35

RECOMENDACIONES …….…… 37

REFERENCIAS BIBLIOGRAFICAS …… 38

ANEXOS ……. 40

ÍNDICE DE FIGURAS

Pp.

Figura Nº1. Organigrama General de la Empresa …….. 6

Figura Nº2. Organigrama del dpto de Sistema …….…….. 7

Figura Nº3. Proceso de Autenticación WPA …….. 17

Figura Nº4. Seguridad en la red …….. 19

Figura Nº5. Dispositivos Inalámbricos ……... 22

Figura Nº6. WLC Cisco …….. 22

Figura Nº7. Modelo jerárquico 3 capas de cisco …… 26

Figura Nº8. Diagrama de topología de Red Febeca …… 28

Figura Nº9. Banner de Seguridad Beval- Sillaca ……..... 29

Figura Nº10. Creación de Usuario …….……. 30

Figura Nº11. Configuración equipos .....……...……..... 31

Figura Nº12. Datos del dispositivo ……. 32

Figura Nº13. Inventario de dispositivos ……. 32

Figura Nº14. Servidor Proxy …….. 34

INTRODUCCION

Actualmente el avance de las nuevas tecnologías está consistiendo una serie de cambios estructurales, la evolución de las redes nos ha obligado a conocer y mejorar su seguridad ya que las amenazas a ellas han evolucionado de forma paralela a las redes y en el ámbito empresarial es muy importante mantener un alto nivel de seguridad en las redes de comunicación para disminuir los ataques de hacker, cracker entre otros, ya que el acceso externo a las redes ha aumentado con el auge de internet y cada vez existen más sistemas dependientes de administración remota.

El objeto a estudio, es la vulnerabilidad de la seguridad en las redes LAN y WAN de las empresas que conforman el grupo Mayoreo, la cual se ve en la necesidad de implementar herramientas que disminuyan los ataques y aumente su nivel de seguridad en las redes.

Existen una gran cantidad de amenazas en las redes de comunicación, uno de los riesgos más comunes es la seguridad de la infraestructura física de nuestros sistemas entre las cuales pueden ser amenazas ambientales, amenazas eléctricas, amenazas al mantenimiento con rotulado inadecuado, también existen ataques de reconocimientos, como escaneo de puertos, programas detectores de paquetes y también existen las amenazas de virus y caballos de troya, estos pueden ofrecer acceso al atacante e infectar otros equipos de la organización para conseguir información o dañar el equipo.

Estos ataques se pueden mitigar aplicando medidas según cada tipo de amenaza, entre las cuales podríamos mencionar algunas: limitar el acceso al recinto físico donde están situados los dispositivos y la conexión al puerto de consola; crear un entorno controlado de temperatura, humedad, flujo de aire y vigilancia; evitar problemas de alimentación eléctrica con sistemas UPS, generadores y fuentes redundantes; utilización de redes conmutadas en lugar de hubs para evitar la difusión de mensajes;

uso de encriptación; utilización de túneles VPN; creación de banner de seguridad; generar contraseñas con alto nivel de seguridad y cambiarlas periódicamente.

Es importante considerar todas las medidas necesarias a implementar para garantizar la efectividad de la mejora en las redes, quedando la investigación organizada de la siguiente manera:

Capítulo I, aborda la reseña histórica de la empresa, misión, visión, valores y el organigrama general de la misma.

Capitulo II, está conformado por el planteamiento y la formulación del problema, objetivo general y objetivos específicos, justificación, alcance y limitaciones del proyecto.

Capitulo III, describe el marco conceptual, en cuanto a los antecedentes de la investigación, bases teóricas y la definición de términos básicos.

Capitulo IV, describe las fases metodológicas de la implementación del proyecto de investigación.

Capítulo V, detalla los resultados obtenidos en la implementación del proyecto, refleja las conclusiones, recomendaciones, finalmente se elaboran las referencias bibliográficas y los anexos.

CAPITULO I
LA EMPRESA

En este capítulo se describirá a la Empresa, partiendo de una reseña histórica, posteriormente se hará mención a la visión, misión, valores y por último se presentará la estructura organizativa.

1.1 Reseña Histórica

En 1829 oriundo de Alemania llego a Venezuela Georg Blohm, en 1835 estableció la firma Overmann, Blohm & CO en la Guaira. De estos comienzos se desarrolló la organización comercial conocida principalmente con el nombre Blohm & Co, que posteriormente inicia operaciones en Maracaibo (1854), Caracas (1857), Valencia (1880) y Barquisimeto (1896). En 1944 la compañía se dedicaba a negocios bancarios, a la comercialización de víveres, textiles, licores, café, cacao, azúcar, cigarrillos, ferretería, quincalla, materiales de construcción, negocios de automóviles, gasolina, lubricantes, velería, entre otros. Con motivo de la segunda guerra mundial, por exigencias de los Estados Unidos y por un decreto venezolano se excluyó a los empleados alemanes, lo que trajo como consecuencia el debilitamiento de la formación gerencial, además se prohibió importar y exigió el cambio de nombre de Blohm & Co en Compañía Anónima prohibiendo el uso invariable del viejo nombre y logotipo.

Desde 1958 hasta 1960, respuesta a las nuevas realidades laborales, así como a la necesidad de especializar a los colaboradores en el trabajo, se reestructuraron en casas especializadas, constituyéndose así: Becoblohm C.A en Caracas, Becoblohm Valencia C.A, Becoblohm Puerto Cabello C.A, Becoblohm Lara C.A, Becoblohm Maracaibo C.A. En 1984 la empresa Distribuidora Sillas Californias C.A. nace en la ciudad de Caracas y luego es trasladada a la ciudad de Valencia. En 1999 la responsabilidad de operar el negocio pasa a Becoblohm Valencia, dicha empresa se ha ido desarrollando hacia el área de la quincallería y hogar.

En 2004 con el crecimiento observado del ramo repuestero, surge la necesidad de darle nombre propio a las actividades y se decide registrar una nueva firma con el nombre de Mayor Beval C. A.

En 2008 a partir del 1ro de abril, la razón social de la empresa, Becoblohm Valencia C.A., pasa a Denominarse: FEBECA C.A por las siglas de Ferretería Becoblohm C.A. Este cambio de nombre forma parte de las estrategias de modernización que estamos implementando a los diferentes niveles de nuestra empresa orientados a seguir aumentando nuestra eficiencia y productividad. El mayor Ferretero toma el nombre de FEBECA C.A, Completándose entonces la total diferenciación de las empresas, cada una con su denominación comercial propia, según el ramo.

Somos una organización que por más de 173 años ha operado de forma ininterrumpida en el área comercial en Venezuela. Hemos sobrevivido a guerras civiles, caudillismos, dictaduras y democracias. Nos caracterizamos por ser COMERCIANTES sin involucrarnos en la política. La razón de la continuidad de la organización se debe en gran parte a las recomendaciones del fundador de la firma que ha sido seguida por los socios y gerentes: vivir en forma simple y austera, sin ambiciones sociales, dedicarse al trabajo constante y abnegado y aceptar únicamente lo que el propio trabajo produzca, evitando situaciones que puedan llegar a la vanidad.

El comerciante debe al igual que el soldado o navegante, enfrentarse valientemente a los peligros, no debe paralizar sus energías y su ánimo lamentándose. Sería imposible definir la Razón de Ser de FEBECA C.A, sin prever las contribuciones que la empresa realizará en los ámbitos educativo, familiar, social y económico, que impactarán en el beneficio de los distintos grupos que la integran:

Para Los Colaboradores: Desarrollar mejores ciudadanos. Significa otorgar estabilidad y crecimiento personal, para que sean mejores seres humanos y mejores profesionales; brindando, además, sustento a sus familias y creando la oportunidad de servir con orgullo de pertenencia.

Para Los Clientes: Confianza Significa crecer de la mano, ofertando asistencia, comodidad y recursos para el crecimiento, con relaciones sanas y saludables que

perduren en el tiempo.

Para Los Accionistas: Permanencia. Significa retorno seguro de la inversión. Implica perdurabilidad y crecimiento, que impulsan el desarrollo del país, mediante la inversión nacional y la responsabilidad social.

Para Los Proveedores: Socios Estratégicos. Significa incentivo a la producción nacional y seguridad de inversión. Expandir el mercado. Ser un aliado para cumplir su misión, favorecer la generación de empleos y ser un canal eficiente de distribución; proporcionando permanencia, crecimiento y rentabilidad.

Para Las Comunidades: Bienestar Social. Significa fomentar el servicio al prójimo, realizar obras sociales de apoyo a la comunidad, creando bienestar y progreso. Además de fortalecer nuestra economía nacional, al pagar impuestos y generar empleos. Se entiende como bienestar social, al conjunto de factores que participan en la calidad de vida de la persona y que hacen que su existencia posea todos aquellos elementos que den lugar a la tranquilidad y la satisfacción humana.

1.2 Misión

Ofrecer la mejor opción en servicios, surtidos y precio en el mercado ferretero. En FEBECA distribuimos más de 300 marcas nacionales e importadas a pequeños y medianos comerciantes del sector ferretero, a través de nuestra fuerza de ventas con una cobertura de más de 10.000 clientes en todo el territorio nacional. Dentro de nuestras categorías de productos ofrecemos: herramientas manuales y eléctricas, herramientas agrícolas y de jardinería, seguridad industrial y automotriz, alambres, clavos y tornillos, artículos para baños y cocinas, cerrajería, electricidad, iluminación y conductores, plomería y grifería, impermeabilizantes y misceláneos. Nuestra cultura se basa de solidez, calidad, permanencia, confianza y crecimiento.

1.3 Visión

Ser el mayorista, líder en satisfacción de nuestros clientes, colaboradores,

accionista, proveedores y comunidad en donde operamos. Teniendo como soporte nuestros valores de compromiso con el desarrollo del país mediante el apoyo a nuestra comunidad y la responsabilidad social. Buscamos favorecer la generación de empleos y ser un canal eficiente de distribución, proporcionando crecimiento y rentabilidad.

1.4 Valores

• Honradez “Ser sinceros con nosotros mismos y los demás es la regla fundamental”.
• Igualdad “Reconoce a los individuos los mismos deberes y derechos en una justa medida”.
• Constancia “Es la perseverancia en la que nos afianzamos para lograr nuestros propósitos”.

1.5 Organigrama General de la Empresa

La estructura organizativa de la empresa Febeca está constituida de la siguiente manera (Ver en la Figura N°1).

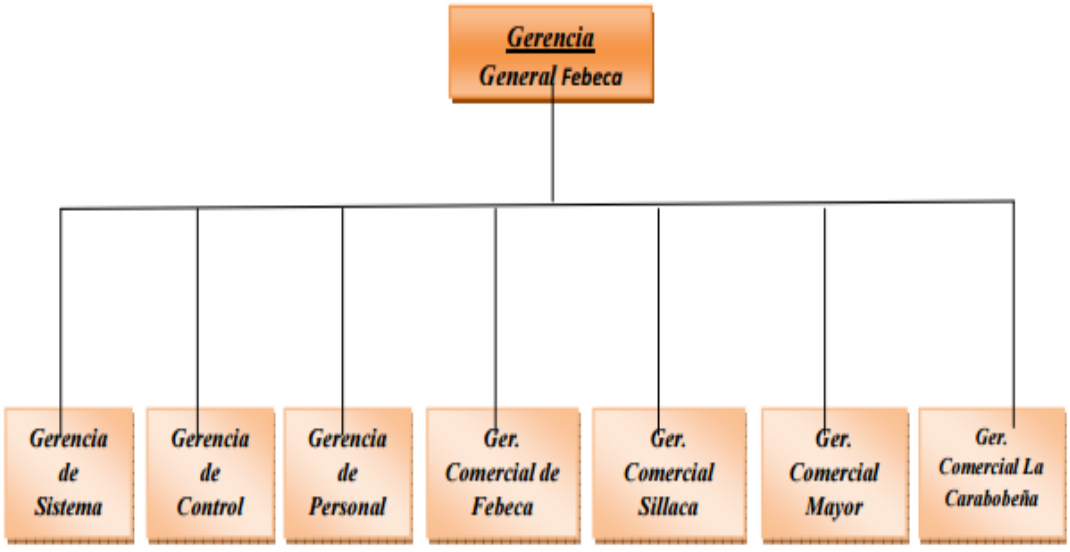


Figura N°1 Organigrama de la empresa.
Fuente: Febeca C.A.

Por otra parte, el área de sistema de la empresa Prisma está conformada de la siguiente manera. (Ver en la Figura N°2).

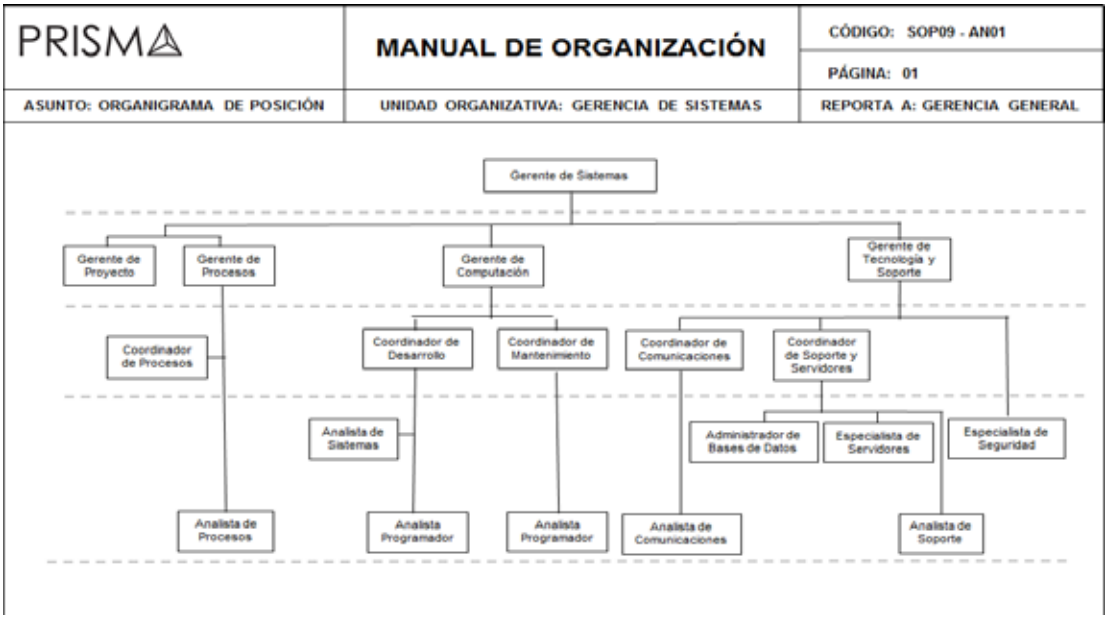


Figura N°2 Organigrama del departamento de Sistema.
Fuente: Prisma C.A. Sistemas de Información

CAPITULO II
EL PROBLEMA

En el presente capitulo se pretende proveer una visión global sobre el fenómeno de estudio, a través de un enfoque metodológico, y dar a conocer los parámetros como es la definición del planteamiento y formulación del problema, los objetivos de estudio, la justificación, alcance y limitación del proyecto.

2.1 Planteamiento del Problema

En la actualidad predomina la propiedad y gestión privadas de las redes. Los servicios de comunicación están abiertos a la competencia y la seguridad forma parte de la oferta de mercado. No obstante, muchos clientes ignoran la amplitud de los riesgos en materia de seguridad a la hora de conectarse a la red y toman su decisión sin estar perfectamente informados.

Las redes y los sistemas de información están en un proceso de convergencia. Cada vez están más interconectados, ofrecen el mismo tipo de servicio sin discontinuidad y personalizado y comparten en cierta medida infraestructura.

Las redes son internacionales, una parte significativa de la comunicación actual es transfronteriza y transita por terceros países (a veces sin que el usuario final sea consciente de ello), por lo que cualquier solución a los problemas de seguridad habrá de tener en cuenta este factor. La mayoría de las redes están formadas por productos comerciales procedentes de proveedores internacionales. Los productos de seguridad deberían ser compatibles con las normas internacionales.

La seguridad de las redes y de la información puede entenderse como la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, todos los accidentes o acciones malintencionadas que pongan en peligro la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o

transmitidos y de los correspondientes servicios que dichas redes y sistemas ofrecen o hacen accesibles.

A la hora de implantar una política de seguridad en la empresa hay que partir de la base de que el sistema o la red 100% segura no existen. Se ha de hacer una valoración de los recursos a proteger, de tal manera que el esfuerzo y coste de la implementación del sistema de seguridad sea proporcional a su valor. Incluso se pueden definir áreas de la red interna de la empresa con información más valiosa o confidencial que deberán ser protegidas con mayor cuidado que otros.

Cualquier sistema, sobre todo si está conectado a cualquier tipo de red informática, debe tener asignado un administrador. Se ha de tener especial cuidado si además el sistema es un servidor dentro de la red. Son obligaciones del administrador del sistema las siguientes tareas:

- Instalar el S.O y el software de aplicaciones del servidor manteniéndolos convenientemente actualizados e instalando los parches que los fabricantes elaboren para corregir los eventuales problemas que tanto de seguridad como de funcionamiento pueden surgir.
- Modificar las contraseñas de acceso tanto del usuario administrador del sistema como de los demás usuarios, según sea necesario para mantener la seguridad de la red.
- Definir y borrar cuentas de usuarios.
- Designar usuarios con privilegios especiales.
- Asegurarse de que los datos están convenientemente salvaguardados con políticas de copia de seguridad adecuada y otros sistemas.

La seguridad de acceso contempla básicamente la identificación del usuario o entidad que desea acceder, la autorización del acceso y la auditoria de las tareas realizadas en el sistema por la entidad que ha accedido. La identificación de usuarios o entidades que acceden se realiza generalmente mediante palabras clave, sistemas de firma digital de los mensajes u otros medios. Esta identificación incluye a las maquinas

involucradas en la comunicación en casos como el comercio electrónico.

Los ataques a la seguridad pueden realizarse desde el interior de la red de la empresa, bien por parte de usuarios de esa red, por intrusos que accedan físicamente a alguno de los sistemas de la red o por intrusos que desde el exterior de la red han ganado el acceso a alguno de los sistemas internos de la red. En estos dos últimos casos el intruso generalmente suplanta a uno de los usuarios legítimos de la red o acceden a través de algún agujero de seguridad en el sistema.

Las empresas que conforman el grupo Mayoreo, no escapan a la problemática ya descrita, debido a que carece de políticas de seguridad en las redes LAN y WAN y esto genera una alta vulnerabilidad en dichas redes.

2.2 Formulación del Problema

¿De qué forma se pueden mitigar las vulnerabilidades de la seguridad en las redes LAN y WAN de las empresas que conforman el grupo Mayoreo?

2.3. Objetivos de la investigación

2.3.1 Objetivo General

Implementar mejoramiento de la seguridad en las redes LAN y WAN de las empresas que conforman el grupo Mayoreo.

2.3.2 Objetivos Específicos

- Establecer la topología de red de cada una de las empresas del grupo Mayoreo.
- Diseñar herramientas para fortalecer la seguridad en las redes LAN y WAN de las empresas del grupo Mayoreo.
- Determinar los equipos disponibles en cada una de las empresas e identificar sus características y ubicación.
- Diseñar normas y estrategias para mejorar la seguridad de las redes LAN y

WAN del grupo Mayoreo.

2.4 Justificación

La implementación de una mejora en la seguridad en las redes LAN y WAN de cada una de las empresas que conforman el grupo Mayoreo, es notable, ya que se implementaran herramientas y configuraciones las cuales permitirán que la información que se maneja dentro de la organización este protegida y se disminuya en un alto porcentaje el acceso de cualquier usuario externo a obtener algún tipo de información confidencial que pueda perjudicar a cualquiera de las empresas que conforman el grupo de Mayores.

De igual manera, desde el aspecto institucional, es importante dado que la empresa mitigara sus vulnerabilidades en las redes, ya que son un grupo de empresas mayoristas y utilizan la red para vender sus productos y organizar la entrega de los mismos y podrían verse paralizadas por algún ataque a la red. La información personal y financiera puede ser interceptada y utilizada con fines fraudulentos.

La protección de la red contra la intercepción es una tarea compleja y costosa. El método clásico utilizado por los operadores de servicios de telecomunicaciones para garantizar la seguridad de las redes ha sido controles del acceso físico de las redes en las instalaciones y directrices para el personal.

El acceso no autorizado a equipos o redes de ordenadores se realiza habitualmente de forma malintencionada para copiar, modificar o destruir datos. Técnicamente, se conoce como intrusión y adopta varias modalidades: explotación de información interna, ataques de diccionario, ataques de fuerza bruta (aprovechando la tendencia de la gente a utilizar contraseñas previsibles), ingeniería social (aprovechar la tendencia de la gente a desvelar información a personas en apariencia fiables) e intercepción de contraseñas. Esta intrusión a menudo se produce dentro de la organización (ataques internos).

Los métodos más ampliamente utilizados para protegerse contra el acceso no

autorizado son los controles de contraseña, la instalación de cortafuegos y los banners de seguridad en los equipos. Estas soluciones ofrecen una protección limitada y deben completarse con otros controles de seguridad, por ejemplo, el reconocimiento de ataques, la detección de intrusiones y el control a nivel de aplicaciones. Es preciso establecer un equilibrio entre la protección de la red y las ventajas del libre acceso. Debido a la rápida evolución de la tecnología y de las correspondientes nuevas amenazas para las redes, los controles independientes de la seguridad de las redes deberán ser revisados permanentemente. Mientras los usuarios y los proveedores no sean plenamente conscientes de la vulnerabilidad de sus redes, no se recurrirá plenamente a las posibles soluciones.

2.5 Alcance

La mejora de la seguridad en las redes de la empresa contempla la implementación de herramientas y configuraciones para lograr mitigar los diferentes tipos de ataques que se pueden presentar en la red que componen los equipos de comunicación de la empresa.

Las fallas de seguridad pueden ocasionar graves consecuencias como la perdida de privacidad, robo de información confidencial, responsabilidades legales derivadas de algunas de estas causas. Se necesitará implementar características específicas según el tipo de red, para infraestructura cableada y para infraestructura inalámbrica.

2.6 Limitaciones

Entre las posibles limitaciones se pueden encontrar que la empresa no cuente con equipos capacitados para la optimización de la seguridad en la red, el alto costo de algunas licencias para proteger los sistemas, también existen equipos los cuales se encuentran ubicados en áreas en donde cualquier persona puede tener acceso y ocasionar fallas en la red. Las posibles amenazas físicas como terremotos o inundaciones también son fallas las cuales no podrían ser evitadas en su totalidad.

Falta de estándares de seguridad: problemas ocasionados por la falta de estándares de seguridad para las transmisiones, frente a una audiencia más sofisticada, siempre existe la posibilidad de violaciones de privacidad y otros actos anti-sociales.

CAPITULO III
MARCO REFERENCIAL CONCEPTUAL

El marco teórico de una tesis conforma el aspecto de los antecedentes, fundamentación legal y referentes teóricos sobre los cuales se cimienta la investigación. De acuerdo a la Universidad Pedagógica Experimental Libertador, (2006), el contenido del marco teórico se basa en situar el problema en estudio dentro de un conjunto de conocimientos sólidos y confiables que permiten orientar la búsqueda y ofrezcan una conceptualización adecuada de los términos que se van a utilizar. El marco teórico permite integrar la teoría con la investigación y establecer sus interrelaciones. Según Escalona R. (2013), representa un sistema coordinado coherente, de conceptos y propósitos para abordar el problema.

3.1. Antecedentes

Barajas, B (2016), informe titulado **Seguridad de redes de telecomunicaciones en el PREP del IEEM,** México, trabajo realizado en la Universidad Autónoma del Estado de México. El objetivo de este reporte de aplicación de conocimientos es documentar la seguridad en las telecomunicaciones del Programa de Resultados Electorales Preliminares (PREP) del instituto Electoral del Estado de México (IEEM) en las elecciones de Diputados Locales y Ayuntamientos del 7 de junio de 2015. El PREP es el sistema de información en el que cualquier persona puede consultar avances el día de la jornada electoral, donde podrá conocer momento a momento los resultados preliminares que van obteniendo los partidos y los candidatos a diversos puestos de elección popular a nivel local. La labor que desempeña el área de Telecomunicaciones de la Unidad de Informática y Estadística (UIE) del IEEM, se enfoca en la interconexión de 125 juntas municipales y 45 juntas distritales, dando un total de 170 sitios hacia el edificio central, realizando la instalación de equipos de red, verificando los enlaces de internet y supervisando los requerimientos de seguridad.

Este informe nos sirve de guía para saber que protocolos de seguridad se pueden implementar en la red de manera que aun cuando tengan acceso muchos usuarios exista un sistema de seguridad robusto y solo puedan monitorear el área que les corresponde sin vulnerar la confidencialidad, integridad y la autenticidad.

Suarez (2012), trabajo titulado **Mecanismos de seguridad en redes inalámbricas,** se describe los principales mecanismos usados en las WLAN para garantizar su seguridad, para ellos se implementa el algoritmo de seguridad WEP (Wired Equivalent Privacy), el cual tiene como propósito incrementar el nivel de seguridad para aquellos dispositivos habilitados con WEP, con la finalidad de obtener el mismo nivel de seguridad que los dispositivos en redes cableadas. Es por ello que la información protegida por WEP, es cifrada con la finalidad de dar confidencialidad y un contador previniendo que los paquetes sean modificados por atacantes activos, así como verificar que solo los usuarios autentificados son los que reciben el servicio de la WLAN. El algoritmo WEP tiene sus debilidades y para ello también se implementa WPA (Wi-Fi Protected Access) el cual soluciona una gran parte de esas debilidades de WEP y se considera suficientemente seguro, este se distingue por tener una distribución dinámica de claves, utilización más robusta del vector de inicialización y nuevas técnicas de integridad y autentificación.

El informe especifica bajo que estándares se trabajara en las redes inalámbricas para garantizar un alto nivel se seguridad e impedir el acceso de personas no autorizadas.

Lazo (2012), trabajo titulado **Diseño e implementación de una red LAN y WAN con sistema de control de acceso mediante servidores AAA**, esta investigación fue de campo, en la cual en se describe que en las redes WAN se implementaron estándares y protocolos de seguridad entre los cuales se podrían mencionar IEEE 802.11i también conocido RNS (Robust Security Network) el cual permite implementar una WLAN más segura a través de la encriptación y autenticación; RADIUS es un software instalado como servicio en el sistema operativo de una computadora, es el encargado de administrar las cuentas de acceso; en la red LAN se utilizaron los protocolos

TACACS+ el cual se encuentra en la capa de aplicación este cifra todo el cuerpo del paquete y separa autenticación, autorización y contabilidad; ACS (Access Control Server) es una solución de Cisco para proveer un servidor AAA altamente escalable, óptimo para el control de acceso y opera como servidor centralizado TACACS+ o RADIUS.

El protocolo RADIUS maneja ambos servicios de manera combinada, mientras que el protocolo TACACS+ los ofrece como servidores independientes. A pesar de ello fueron implementados en una misma red, coexisten para brindar una red con sistema de control de acceso robusto.

Este trabajo de investigación especifica los parámetros a tomar en cuenta en la implementación de los sistemas de autenticación y los protocolos de seguridad para cada infraestructura de red.

3.2 Bases Teóricas

3.2.1 Seguridad WLAN

Las redes inalámbricas son vulnerables a diferentes tipos de ataques debido a que el aire es un medio de acceso para cualquier persona que se encuentre en la cobertura de un punto de acceso a la red, dejando la posibilidad de interceptar la transmisión de datos. Para garantizar la seguridad en este tipo de redes es necesario el cifrado de la información antes de ser enviada y la autenticación de los usuarios antes de acceder a la red.

3.2.1.1 Protocolos de encriptación

- WEP (Wired Equivalent Privacy) es el protocolo de encriptación incluido originalmente en el estándar IEEE 802.11, emplea CRC (Cyclic Redundancy Check) como algoritmo de verificación de integridad, y como algoritmo de encriptación utiliza RC4, el cual viene acompañado de una clave secreta de 40 o 104 bits que es combinada con el vector de inicialización (IV) de 24 bits. El

envió de la clave es en texto plano, lo que lo hace vulnerable a ataques basados en el uso de analizadores de tramas (sniffers) y decodificadores de código WEP (WEP crackers).

- WPA (Wi-Fi Protected Access) fortalece el algoritmo de encriptación utilizado por el WEP con el incremento de la clave secreta de 104 a 128 bits, el incremento del vector de inicialización de 24 a 48 bits y la implementación del protocolo de claves dinámicas TKIP (Temporal Key Integrity Protocol). De esta forma se soluciona el problema del tamaño y reutilización del vector, con esto se evita los ataques estadísticos que permiten recuperar la clave WEP. WPA también implementa el código MIC (Message Integryti Code) para el control de integridad, debido a que el control CRC (cyclic Redundancy Check usado por el WEP) es inseguro al permitir alterar la información sin conocer la clave WEP para luego actualizar el CRC haciendo que el cambio no sea perceptible. (Ver Figura N°3).

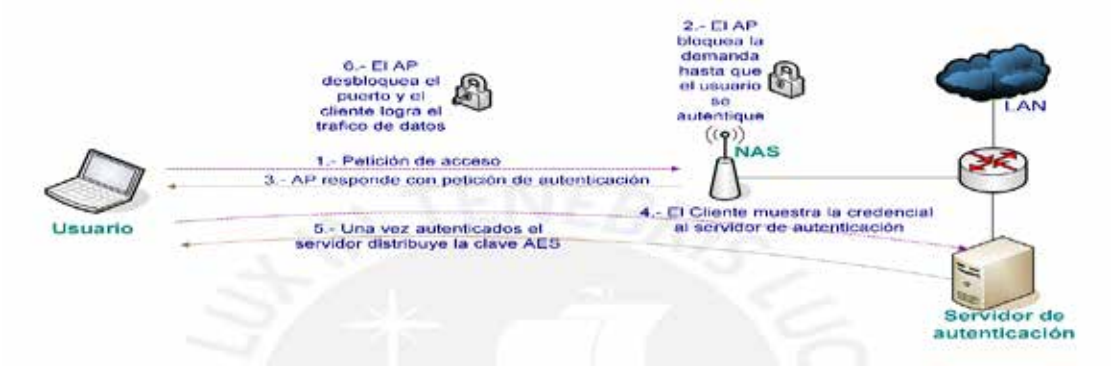


Figura N°3. Proceso de Autenticación WPA
Fuente: https://1289619.netacad.com/courses/447952

- WPA2 (Wi-Fi Protected Access 2) es compatible con WPA y WEP. Las principales diferencias respecto a WPA son: el empleo de otro algoritmo de cifrado, mientras WPA usa TKIP basado en RC4, WPA2 emplea CCMP (Counter Mode with Clipher Block Chaining Message Autentication Code Protocol) basado en AES; además usa la siguiente versión del código MIC para el algoritmo de control de integridad.

3.2.1.2 Protocolos de confidencialidad e integridad de datos

Los protocolos de confidencialidad e integridad de datos han pasado por un proceso evolutivo desde TKIP incorporado en el protocolo de encriptación WAP hasta el protocolo CCMP incorporado en el protocolo de encriptación WAP2.

- **TKIP (Temporal Key Integrity Protocol):** Protocolo de integridad de clave temporal, surgió como una actualización (Wi-Fi CERTIFIED nombra esta actualización como WAP) para reforzar los sistemas WEP, sin tener que cambiar el antiguo hardware de red. Por ello, al igual que WEP, se basa en el algoritmo de encriptación RC4, lo que acarrea limitaciones de seguridad que son remediadas con la desconexión de 60 segundos y establecimiento de nuevas claves cuando se produzcan más de 2 fallas de MIC por minuto.

  Corrige las siguientes vulnerabilidades de WEP:

  - Integridad de mensaje: lo logra usando un nuevo control de integridad del mensaje MIC basado en el algoritmo Michael de Niels Ferguson con 20 bits de seguridad, que impide la modificación de los datos dentro de un paquete mientras es transmitido.
  - Reutilización de claves de inicialización: incluye nuevas reglas de selección y va incrementando su valor, evitando su reutilización, genera una nueva clave cada 10000 paquetes o 10 Kbytes de información transmitida.
  - Gestión de claves: aplica el algoritmo “hash” el vector de inicialización es encriptado y repartido por distintas ubicaciones del paquete.
- **WRAP (Wireless Robust Authenticated Protocol):** Basado en el algoritmo de encriptación AES, fue el primer protocolo elegido por el estándar IEEE 802.11i, pero se abandonó por motivos de propiedad intelectual y posibles licencias.

3.2.1.3 EAP

EAP (Extensible Authentication Protocol) es una extensión del protocolo PPP (Point-to-point Protocol), proporciona un mecanismo estándar para aceptar métodos de autenticación, al usar EAP se puede agregar varios esquemas de autenticación como: RADIUS, Kerberos, tarjetas de identificación, certificados entre otros.

3.2.2 Seguridad LAN

Para controlar las conexiones dentro de la misma LAN, se va contar con un sistema centralizado de administración de cuentas de los usuarios para el acceso a los recursos de la red y administración de todos los dispositivos de la red. Lo cual va proveer un mayor grado de escalabilidad a nivel de línea y una administración rápida y precisa para el control de acceso de usuarios y administración de los dispositivos. (Ver Figura N°4).

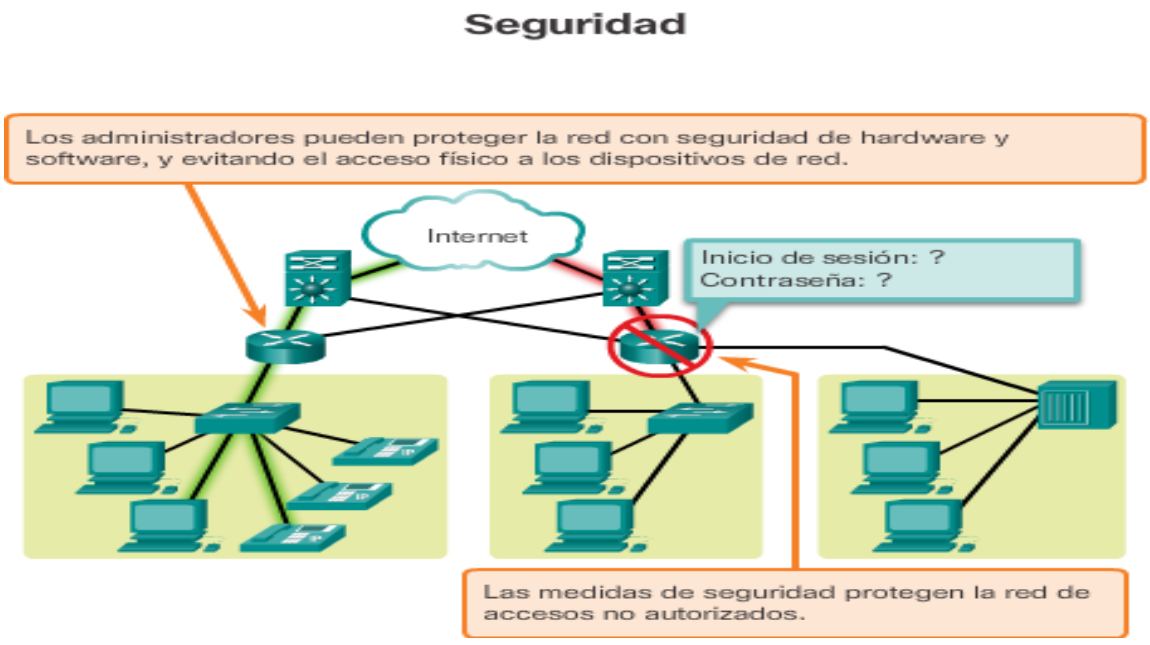


Figura N°4. Seguridad en la red.
Fuente: https://1289619.netacad.com/courses/447952

3.2.3 Servidor NTP

Network Time Protocol (NTP) es un protocolo de internet para sincronizar los relojes de los sistemas informáticos a través del enrutamiento de paquetes en redes con latencia variable. NTP utiliza UDP como su capa de transporte. El protocolo trabaja a través del puerto 123.

NTP utiliza el sistema jerárquico de estratos de reloj. Los cuales se clasifican de la siguiente manera:

Estrato 0: Son dispositivos, como relojes GPS o radio relojes, que carecen de conectividad hacia redes. Solo están conectados a computadoras que son las encargadas de distribuir los datos.

Estrato 1: Los sistemas se sincronizan con dispositivos del estrato 0. Los sistemas de este estrato son referidos como servidores de tiempo.

Estrato 2: Los sistemas envían sus peticiones NTP hacia servidores del estrato 1, utilizando el algoritmo de Marzullo para recabar las mejores muestras de datos, descartando que parezcan proveer datos erróneos y compartiendo datos con sistemas del mismo estrato 2.

Estrato 3: Los sistemas utilizan funciones similares a las del estrato 2, sirviendo como servidores para el estrato 4.

Estrato 4: Los sistemas utilizan funciones similares a las del estrato 3.

3.2.4 Servidor LOG

Parte de una buena estrategia de seguridad informática es saber administrar el log de los dispositivos de la red de forma segura y efectiva. El log o como diríamos en español “la bitácora”, es un conjunto de mensajes generados por el sistema operativo (Cisco IOS) y/o los servicios con el objetivo de establecer un registro de las actividades del sistema.

Esta información almacenada en el log sirve para que el SysAdmin pueda realizar labores de Troubleshooting y detección de actividades maliciosas en nuestra red. Por

lo tanto, es vital la administración adecuada de esta información para mantener corriendo de manera estable una red y principalmente para poder mitigar las amenazas de seguridad a las que nos podamos ver expuestos.

Es importantísimo que antes de implementar el almacenamiento de log en un Syslog Server todos los dispositivos de la red estén sincronizados con la misma hora, día y fecha. Para esto debemos de configurar el protocolo Network Time Protocol (NTP) en los switches y routers.

3.2.5 Monitor SNMP

Las redes de gran tamaño son difíciles de manejar. Utilizar un monitor SNMP como el PRTG Network Monitor le ayuda a vigilar el uso de ancho de banda y parámetros importantes del sistema. Y le permite reaccionar ante posibles complicaciones antes de que causen periodos de inactividad.

El protocolo de gestión de red básica (SNMP por sus siglas en inglés) es un conocido protocolo para la gestión de redes. Se utiliza para recopilar información de los dispositivos de redes, como servidores, impresoras, hubs, switches y routers, y configurarlos en una red de protocolo de internet (IP).

Utilizando un monitor SNMP, puede monitorizar el rendimiento de red, auditar el uso de la red, detectar errores en la red o accesos inadecuados. El monitor SNMP de PRTG puede comunicar e interactuar con cualquier dispositivo compatible con SNMP. La sencilla e intuitiva interfaz del monitor SNMP permite a los usuarios llevar a cabo varias funciones con pocos clics del mouse.

3.3 Definición de términos básicos

WLAN: (Wireless Local Área Network) es un sistema de comunicación de datos inalámbrico flexible muy utilizado como alternativa a la LAN cableada o como una extensión de esta. Utiliza tecnología de radiofrecuencia que permite mayor movilidad a los usuarios al minimizarse las conexiones cableadas. (Ver Figura N°5).

Figura N°5. Dispositivos Inalámbricos.
Fuente: https://1289619.netacad.com/courses/447952

VLAN: es un método para crear redes lógicas independientes dentro de una misma red física. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el tamaño del dominio de difusión y ayudan en la administración de la red, separando segmentos lógicos de una red de área local (los departamentos de una empresa, por ejemplo) que no deberían intercambiar datos usando la red local.

MPLS: (Multiprotocol Label Switching) es un mecanismo de datos estándar creado por la IETF y definido en el RFC 3031. Opera entre la capa de enlace de datos y la capa de red del modelo OSI.

WLC: (Wireless LAN Controller) es un dispositivo que asume una función central en el CUWN (Red Inalámbrica Unificada de Cisco). Las funciones tradicionales de los puntos de acceso, tales como asociación o autenticación de los clientes de red inalámbrica, son realizadas por el WLC. (Ver Figura N°6).

Figura N°6. WLC Cisco.
Fuente: Pérez, 2017

STP: (Spanning-Tree Protocol), es un protocolo de red de nivel 2 del modelo OSI (enlace de datos) cuya función es gestionar la presencia de bucles en topologías de red debido a la existencia de enlaces redundantes. El protocolo permite a los dispositivos de interconexión activar o desactivar automáticamente los enlaces de conexión, de forma que se garantice la eliminación de bucles.

SSID: (Service Set Identifier) es un nombre incluido en todos los paquetes de una red inalámbrica para identificarlos como parte de esa red.

DHCP: (Dynamic Host Configuration Protocol, en español Protocolo de configuración dinámica de host), es un servidor que usa protocolo de red de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme estas van quedando libres, sabiendo en todo momento quien ha estado en posesión de esa IP, cuanto tiempo la ha tenido y a quien se la ha asignado después. Así los clientes de una red IP pueden conseguir sus parámetros de configuración automáticamente.

Telnet: (Telecommunication Network) es un método no seguro para establecer de forma remota una sesión de CLI a través de una interfaz virtual, en una red. A diferencia de SSH, telnet no proporciona una conexión cifrada segura. La autenticación de usuario, las contraseñas y los comandos se envían por la red en texto no cifrado.

SSH: (Shell Seguro) es un método para establecer de forma remota una conexión segura a través de una interfaz virtual, en una red. A diferencia de la conexión de consola, las sesiones de SSH requieren servicios de red activos en el dispositivo, que incluye una interfaz activa configurada con una dirección.

CAPÍTULO IV
MARCO METODOLÓGICO

El marco metodológico constituye el eje del trabajo de investigación donde se describen el conjunto de métodos, procedimientos, técnicas y estrategias para llevar a cabo una investigación según Caricote (2008) y Hurtado de Barrera (2007).

4.1 Fases Metodológicas

Fase I: Identificación de la estructura de red y diseño de las topologías en cada una de las empresas que conforman el grupo Mayoreo.

En esta fase se estableció el diseño de las topologías de red identificando en ella los puertos entre las cuales se establece la comunicación entre cada uno de los equipos (Routers, Switches).

De allí se puede ofrecer una documentación de cómo está elaborado la infraestructura física en la cual se identifican tanto la ubicación física de los dispositivos intermedios, la instalación de los cables, como la infraestructura lógica en la que se detallan los dispositivos, puertos y esquema de direccionamiento, con esto se ha logrado identificar las fallas que se presenten de manera más fácil y rápida para poder mantener la operatividad de las redes de la empresa.

Fase II: Diseño e implementación de herramientas para fortalecer la seguridad en las redes LAN y WAN del grupo Mayoreo.

En esta segunda fase se implementó un banner de seguridad, se realizó un cambio en las contraseñas de todos los usuarios y se restringió el acceso a la red, también se creó un respaldo en las configuraciones existentes en los equipos de comunicación que integran la red y con esto prevenimos que algún usuario intente hacer algún cambio en las configuraciones y no tener respaldo para poder reversarlo.

Se creó un usuario general con privilegio máximo para todos los equipos de comunicación que conforman la red del grupo Mayoreo el cual fue guardado en una bóveda y solo será utilizado si alguno de los operadores encargados del área presenta algún inconveniente para ingresar a los equipos o en caso de alguna emergencia que amerite utilizarlo.

Fase III: Identificación de los equipos de comunicación que conforman la red y sus características.

En esta fase se generó una documentación acerca de los dispositivos que conforman las redes, su direccionamiento ip, modelo, serial de tarjeta madre y la versión del sistema operativa, con esto se mantiene un control de la cantidad de dispositivos para lograr establecer un estándar y manejar una sola versión al momento de aplicar alguna configuración nueva para mejorar la seguridad de las redes LAN y WAN del grupo Mayoreo.

Así mismo, todo esto se logró implementar ingresando de manera remota a través de un emulador de terminales llamado Putty el cual nos permite ingresar a cada dispositivo que conforme la red y de allí obtener la información requerida.

Fase IV: Diseño de normas y estrategias para mejorar la seguridad en las redes LAN y WAN del grupo Mayoreo.

Desde el punto de vista teórico y práctico, esta implementación de mejora en la seguridad de las redes se fundamenta en el diseño de estrategias y normas, entre las cuales se implementó un servidor LOG, el cual se encarga de guardar un registro de cada uno de los eventos que ocurran en los dispositivos que conforman la red, ya sea por alguna falla o por algún intento de sabotaje, esto queda registrado con fecha y hora, también quedan registros de los usuarios cuando ingresen y realicen algún cambio, todo esto con el fin de mantener monitoreada la red y así mejorar la seguridad.

CAPÍTULO V
RESULTADOS

En este apartado se exponen de manera clara y objetiva los resultados de cada uno de los pasos que se llevaron a cabo, mediante el cumplimiento de las fases metodológicas que fueron definidas brevemente en el capítulo anterior. A continuación, se presentan los resultados obtenidos a lo largo del periodo de las pasantías:

Fase I: Identificación de la estructura de red y diseño de las topologías en cada una de las empresas que conforman el grupo Mayoreo.

Es notable considerar que en esta fase se estableció el diseño de las topologías de red en cada una de las empresas que conforman el grupo de los mayores, el tipo de topología empleado fue el modelo jerárquico de 3 capas de cisco. En sí, definimos funciones dentro de cada capa, ya que las redes grandes pueden ser extremadamente complejas e incluir múltiples protocolos y tecnologías; así, el modelo nos ayuda a tener uno fácilmente entendible de una red y por tanto a decidir una manera apropiada de aplicar una configuración.

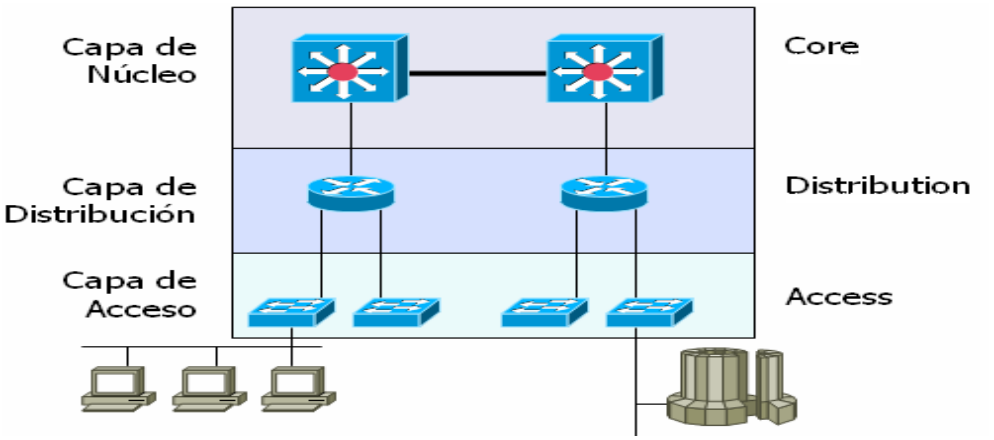


Figura N°7. Modelo jerárquico 3 capas de cisco
Fuente: Pérez, 2017

Entre las ventajas que nos ofrece separar las redes en 3 niveles tenemos que es fácil diseñar, implementar, mantener y escalar la red, además de que la hace más confiable, con una mejor relación costo/beneficio. Cada capa tiene funciones específicas asignadas y no se refiere necesariamente a una separación física, sino lógica; así que podemos tener distintos dispositivos en una sola capa o un dispositivo haciendo las funciones de más de una de las capas.

La capa de Acceso es por donde los dispositivos controlados por el usuario, dispositivos accesibles al usuario y otros dispositivos terminales se conectan a la red. La capa de acceso ofrece conectividad tanto inalámbrica como alámbrica, contiene características y servicios para garantizar seguridad y recuperabilidad para toda la red.

La capa de Distribución admite muchos servicios importantes. En una red donde la conectividad debe atravesar la LAN completa, ya sea entre distintos dispositivos de la capa de acceso o desde un dispositivo de la capa de acceso a la WAN, la capa de distribución hace posibles esta conectividad.

En un entorno de LAN grande con frecuencia surge la necesidad de contar con varios switches de capa de distribución. Uno de los motivos es que cuando los switches de la capa de acceso se ubican en varios edificios geográficamente dispersos, puede ahorrarse la instalación de fibra óptica (potencialmente costosa) entre los edificios mediante la colocación de un switch de capa de distribución en cada uno de esos edificios. Dado que las redes crecen más allá de las tres capas de distribución en una sola ubicación, las organizaciones deberían usar una capa de núcleo central para optimizar el diseño.

En cada una de las topologías podemos identificar los equipos de comunicación (Routers, Switches,) que conforman la red en dicha empresa, las interfaces en las que están conectados, su direccionamiento ip, la capa a la que pertenecen con la finalidad de poder identificar y dar soluciones a posibles fallas sin tener que trasladarnos hasta donde están los equipos. (Ver Figura Nº8).

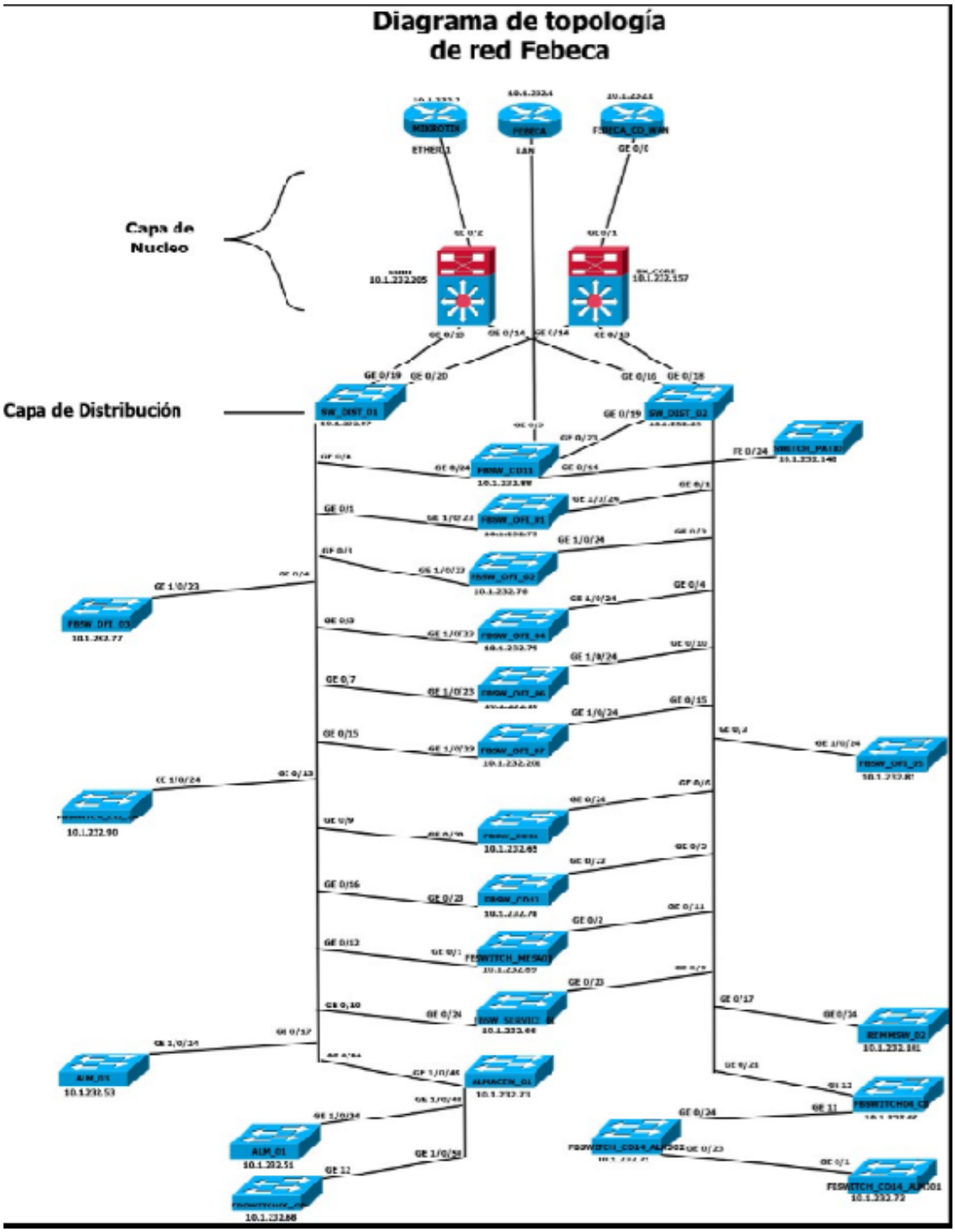


Figura N°8. Diagrama de Topología de Red FEBECA
Fuente: Pérez, 2017

Fase II: Diseño e implementación de herramientas para fortalecer la seguridad en las redes LAN y WAN del grupo Mayoreo.

En esta fase se implementaron herramientas para mitigar la vulnerabilidad en la seguridad de las redes LAN y WAN de cada una de las empresas que conforman el grupo mayoreo.

En primer lugar, se generó un banner de seguridad y se le asignó a la configuración de cada uno de los equipos que conforman la red, con esto quedan advertidos los usuarios que no pueden ingresar de manera desautorizada a los equipos ni poder realizar ningún cambio en las configuraciones existentes ya que de incumplir esto incurrirán en una violación de la normativa corporativa, que supondrá la comisión de un delito y serán sancionados.

Los banners son mensajes de advertencia que se muestran cuando alguien quiera establecer una sesión de telnet, ssh o por puerto de consola. Para configurar este banner, escribimos en consola los siguientes comandos. (Ver Figura Nº9)

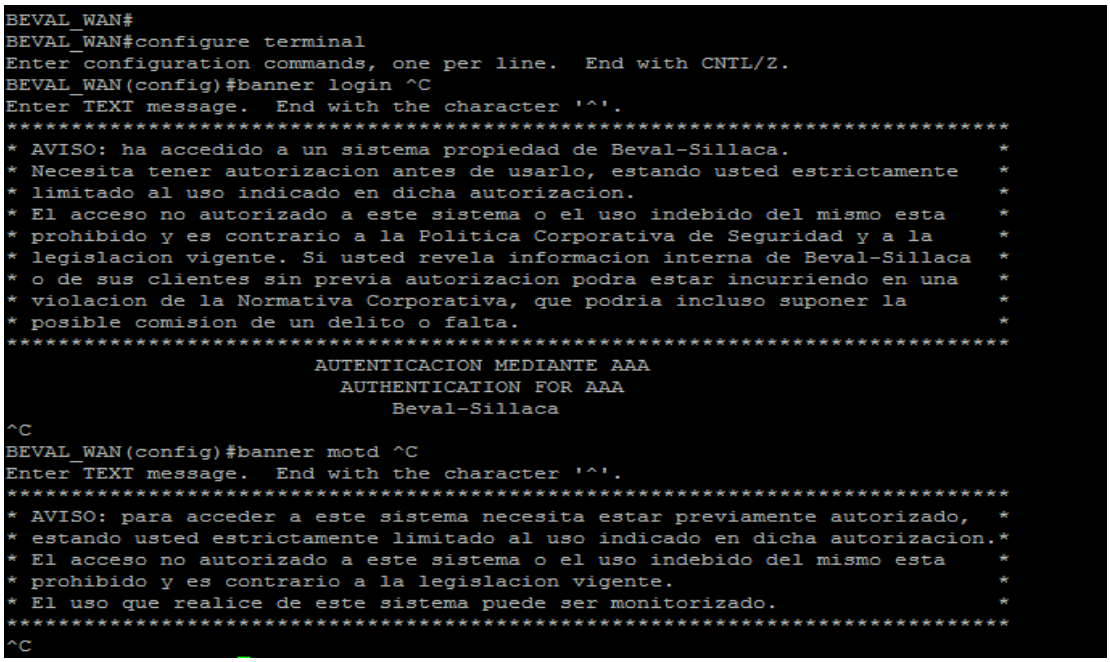


Figura N°9. Banner de Seguridad Beval-Sillaca
Fuente: Pérez, 2017

Cabe destacar, que los routers y switches CISCO trabajan con el sistema operativo IOS el cual cuenta con 3 modos:

1) Modo usuario, (**Router>**): en este modo no se puede modificar ni leer la configuración del equipo, solo se utilizan los comandos, (show), (ping), (telnet), (tracerouter).

2) Modo privilegiado o EXEC, (**Router#**): modo de visualización con privilegios, es decir, podemos consultar o borrar configuración del router.

3) Modo global, {**Router (config)**}: en este modo podemos configurar el nombre del equipo, acceder a las interfaces, configurar Access list, establecer contraseñas para los distintos accesos (vía telnet, consola, aux o para entrar a los modos) además de muchísimas otras cosas más.

Además, existen distintos niveles de usuario, podemos configurar 16 niveles de usuario diferente (0 a 15), nivel 0 solo accede al modo usuario, del nivel 1 al 14 se pueden asignar diferentes comandos para cada nivel y el nivel 15 tiene acceso a modo privilegiado completo.

Se creó un usuario general con el máximo nivel de privilegio, con acceso a todos los equipos que conforman la red del grupo mayoreo, cuyas credenciales fueron entregadas al gerente del departamento de Sistemas en un sobre sellado y solo se utilizara en caso de presentarse algún inconveniente en la red que amerite ingresar a la administración de los equipos y que no se encuentre en la localidad ninguno de los operadores encargados del área.

Este usuario se generó con los siguientes comandos mostrados en la imagen siguiente. (Ver Figura Nº10)

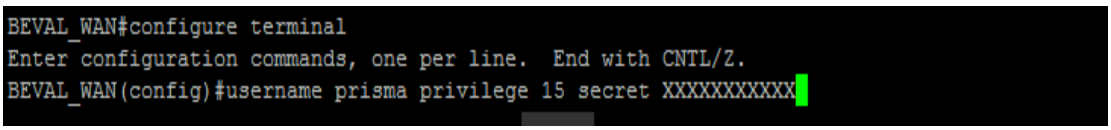


Figura N°10. Creación de Usuario
Fuente: Pérez, 2017

Por otra parte, se realizó un respaldo general de la configuración de cada uno de los equipos que conforman la red del grupo mayoreo, esto con el fin de que si se daña

algún equipo, este se tiene que reemplazar en el cual se aplicara la configuración respaldada al equipo nuevo para reestablecer sus funciones de manera rápida y no afectar las operaciones comerciales del negocio.

El comando que se utiliza para ver la configuración que está corriendo en el dispositivo se muestra en la imagen. (Ver Figura Nº11)

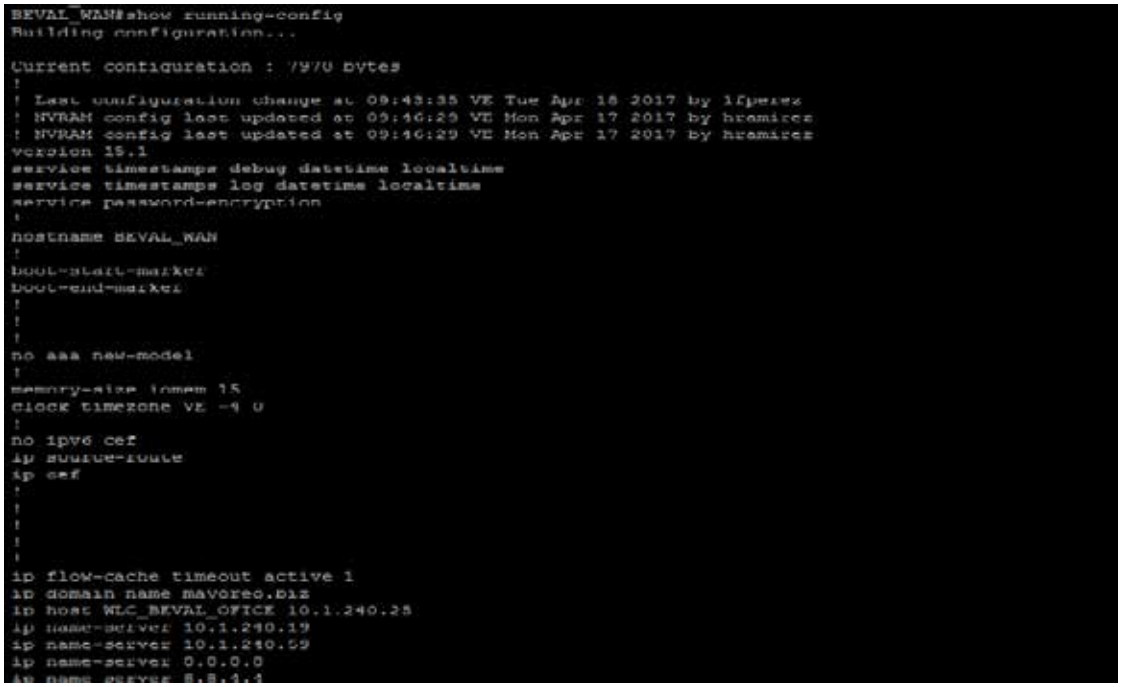


Figura N°11. Configuración Equipos
Fuente: Pérez, 2017

Fase III: Identificación de los equipos de comunicación que conforman la red y sus características.

En esta fase se logró realizar un inventario de todos los dispositivos que conforman las redes del grupo mayoreo, se estableció una base de datos en la cual se tienen todos los datos requeridos de cada equipo como: su direccionamiento ip, nombre, serial de tarjeta madre , modelo y versión del sistema operativo, esto con el fin de mantener un control de activos de dichos equipos de comunicación, facilitar cualquier información que se requiera en auditorias, reemplazar aquellos equipos que ya se encuentren en

obsolescencia y lograr establecer un estándar para mejorar el performance de las redes LAN y WAN del grupo.

Dicho inventario se realizó de forma manual ingresando a la configuración de cada uno de los equipos por conexión ssh a través de un emulador de terminales llamado Putty, escribimos en consola el siguiente comando. (Ver Figura Nº12).

```
BEVAL_WAN#show version
Cisco IOS Software, C2900 Software (C2900-UNIVERSALK9-M), Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Tue 20-Mar-12 18:57 by prod_rel_team
```

Figura N°12. Datos del dispositivo
Fuente: Pérez, 2017

Luego de obtener los datos de cada dispositivo se genero una base de datos utilizando la herramienta excel, en la cual especificamos los equipos de cada una de las empresas que conforman el grupo mayoreo, . (Ver Figura Nº13).

EQUIPOS DE COMUNICACIÓN DE COFERSA				
Direccion IP	Nombre	Modelo	Serial Tarjeta Madre	Version Sistema Operativo
190.0.1.250	COFERSA_WAN	CISCO2911/K9	FTX1544AMGJ	15.1(4)M2
190.0.1.16	rack_dell	WS-C2960G-24TC-L	FOC104731JQ	12.2(25)SEE2
190.0.1.10	CORE	WS-C3560G-48PS	FOC101941NT	12.2(25)SEB4
190.0.1.14	Oficinas_B	WS-C3560G-24PS	FOC10164PN8	12.2(25)SEB4
190.0.1.13	Bodega_A	WS-C3560G-48PS	FOC101942SA	12.2(25)SEB4
190.0.1.8	rack_ibm	WS-C3750X-48P	FDO16190UK9	12.2(55)SE3
190.0.1.3	COFERSA_VPN	CISCO2911/K9	FTX1704AJFG	15.1(4)M4

Figura N°13. Inventario de dispositivos
Fuente: Pérez, 2017

Fase IV: Diseño de normas y estrategias para mejorar la seguridad en las redes LAN y WAN del grupo Mayoreo.

Durante esta fase se implementó el servidor LOG el cual genera un registro de todos los eventos que ocurren en los dispositivos que integran la infraestructura de red en el grupo mayoreo, con esto hemos podido validar todos los cambios que se han generado con fecha hora nombre usuario y el cambio realizado; también se instaló el servidor de WSUS (Windows Server Update Services) el cual centraliza la distribución de parches a través de actualizaciones automáticas a todas las computadoras de la red corporativa, con esto se disminuirá el colapso de la red que se generaba cuando el sistema operativo de Windows descargaba las actualizaciones en todos los equipos al mismo tiempo, lo cual generaba lentitud en la red, con esto únicamente las descargas estarán centralizadas y luego son difundidas a los equipos clientes luego.

Se estableció configuración de todas las contraseñas de los equipos de comunicación, la tecnología CISCO cuenta con cinco contraseñas que se utilizan para asegurar el acceso: consola, auxiliar, telnet, enable password, enable secret, la conexión remota a los equipos de comunicación se hace mediante el protocolo ssh debido a la encriptación de la información para la seguridad a la hora de transferir datos, cabe destacar que existen colaboradores a los que se les asigna una cuenta VPN, para que desde cualquier otro lugar externo a las instalaciones de la empresa puedan acceder a los recursos de la organización, a través de una VPN pasa información privada y confidencial que en manos equivocadas podría resultar perjudicial para la empresa, y mucho más si el usuario se conecta utilizando un Wi-Fi público sin protección, esto se mitigo utilizando la tecnología PPTP (Point to Point Tunneling Protocol) que soporta varios protocolos VPN con cifrado de 128bits.

El diagrama de red cuenta con un servidor proxy como dispositivo intermedio, en el cual se diseñaron nuevas reglas para fortalecer la seguridad dentro de la red que nos permita disminuir al máximo cualquier posibilidad de ataques de personas ajenas a la

organización, de esta manera se aplica una capa de seguridad a nivel de cortafuego, políticas de control de acceso, cache de las páginas web visitadas, permite el análisis del consumo de ancho de banda y sitios visitados por los usuarios. (Ver Figura Nº13)

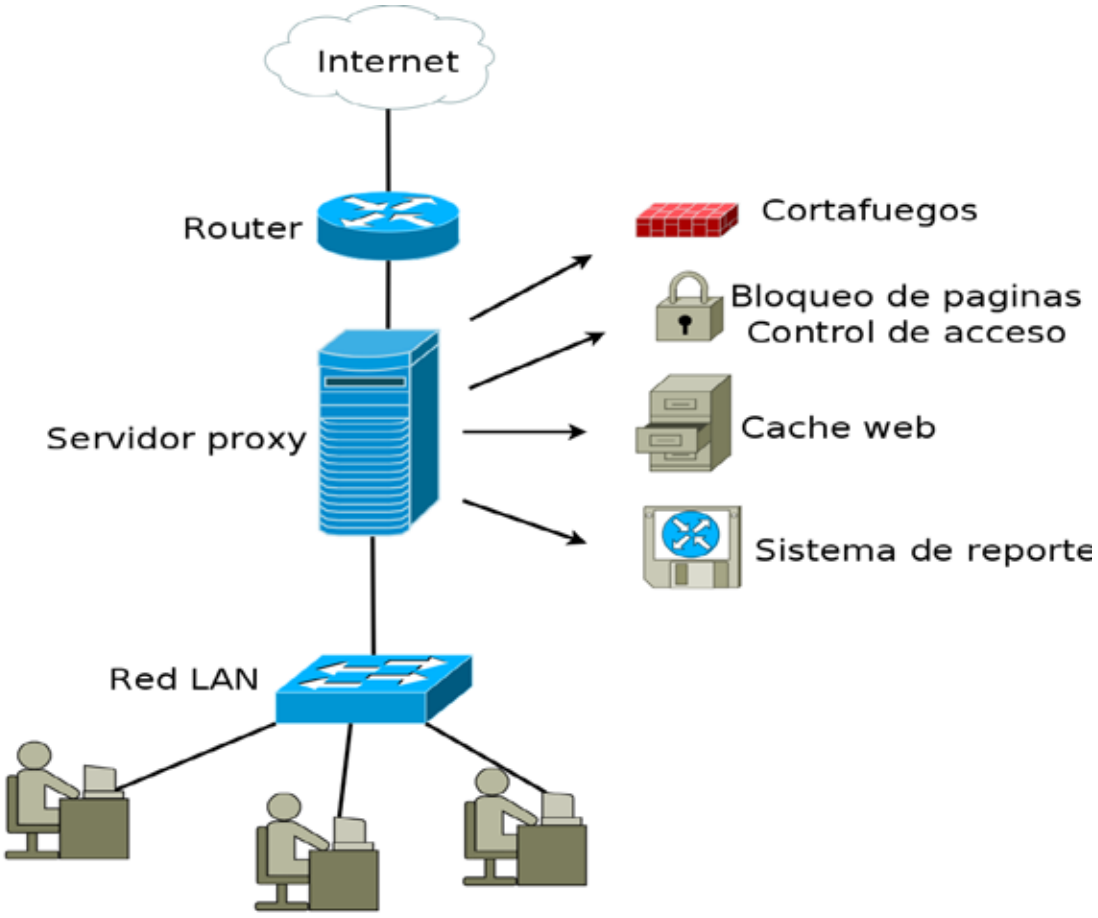


Figura N°13. Servidor Proxy
Fuente: Pérez, 2017

CONCLUSIONES

Como resultado de este proyecto es posible concluir que durante el proceso de mejora de la seguridad en las redes LAN y WAN de las empresas que conforman el grupo mayoreo se obtuvieron conocimientos de cómo identificar las brechas de seguridad existentes en la red para poder ir atacándolas de acuerdo a sus niveles de riesgo, se diseñaron herramientas para fortalecer la seguridad en las redes, en primer lugar se establecieron las topologías de red en cada una de las empresas en las que se detalla nombre de los dispositivos, direccionamiento ip para su administración remota, se identifican las interfaces entre las cuales se establece la conexión entre los dispositivos dentro de la red.

Por otra parte, se estableció un banner de seguridad para informar a los usuarios de no ingresar a los dispositivos sin previa autorización, se generó un respaldo de las configuraciones existentes en cada uno de los dispositivos que conforman la red (Routers, Switches) para mantener un estándar al momento de que se deba incluir algún dispositivo adicional o en su defecto reemplazar alguno que se dañe y mejorar el tiempo al momento de poner en funcionamiento el equipo.

Seguidamente se realizó un inventario de todos los equipos que conforman las redes dentro de cada una de las empresas, a través de la conexión remota al equipo principal dentro de la red mediante un comando nos refleja los dispositivos que están conectados a él y las interfaces utilizadas, también a través de otro comando utilizado se pudo conocer las características principales de cada dispositivo como su modelo, serial de tarjeta madre, versión , dirección ip, obteniendo todos estos datos de cada dispositivo para luego ser llevados a una base de datos y manejar dicha información con el fin de conocer cuales equipos se encuentran en obsolescencia y poder reemplazarlos a tiempo para no generar alguna brecha de seguridad nueva.

Por último, se diseñaron un conjunto de normas y estrategias, entre las cuales fue la implementación de un servidor LOG, el cual guarda registros de todos los eventos que ocurran en cualquiera de los dispositivos pertenecientes a la red, en dichos registros quedara el nombre de usuario, la fecha y hora en la cual se realizó el cambio, con esto se mantiene un control y monitoreo de la red.

La ejecución de mejora de la seguridad en las redes LAN y WAN fue de vital importancia en las empresas que conforman el grupo, ya que las comunicaciones son la base fundamental para la operatividad del negocio y con una seguridad robusta en su red se garantiza la confidencialidad de todos sus datos y la información para que no sea utilizada por personas externas a la empresa por medio de ataques a la red.

RECOMENDACIONES

Cabe destacar que se recomienda realizar periódicamente las actualizaciones en las herramientas, normas y estrategias basadas en los protocolos utilizados para mantener la confidencialidad y encriptación de los datos que se envían y reciben a través de la red, para mantener la seguridad de las redes en óptimas condiciones y evitar el acceso de personas ajenas a información confidencial.

Otra recomendación es mantener actualizados las topologías de red en cada una de las empresas que conforman el grupo para garantizar que se mantenga una resolución rápida a las averías que se presenten.

Al igual que se recomienda validar que los respaldos de las configuraciones de los equipos de la infraestructura de red en cada una de las empresas que conforman el grupo mayoreo tengan una vigencia no mayor a tres meses; también se debe monitorear el servidor LOG y revisar los eventos semanalmente para validar si existen registros de algún ingreso de usuarios no autorizados o que se haya realizado algún cambio sin previa notificación. Monitoreo y actualización de las reglas aplicadas al servidor proxy.

Por último, se recomienda reemplazar aquellos equipos que se encuentren en obsolescencia y mantener un estándar en los equipos para garantizar que se puedan implementar futuras configuraciones para proteger la red de ataques.

REFERENCIAS BIBLIOGRÁFICAS

Impresas

Arias, F. (2010). **Proyecto de Investigación: Introducción a la metodología científica**. Caracas: Episteme.

Balestrini, M. (2002). **Como se Elabora el Proyecto de Investigación**. 6ta Edición. Editorial Consultores Asociados. Caracas, Venezuela.

Barajas, Belmonte (2016). **Seguridad de redes de telecomunicaciones en el PREP del IEEM.** Trabajo de investigación. México. Universidad Autónoma del estado de México.

Caricote, N (2008). **Como investigar sin complicaciones**. Colombia: Stilo Impresores.

Hernández, R. (2009). **Metodología de la Investigación**. México: McGraw – Hill.

Hurtado de Barrera, J. (2010). **Metodología de la investigación** Caracas.

Lazo, García. (2012). **Diseño e implementación de una red LAN y WLAN con sistemas de control de acceso mediante servidores AAA.** Trabajo de Grado. Perú. Universidad Católica del Perú.

Mijares, H. & García, L (2007). **Normas para elaboración y presentación de los anteproyectos, proyectos y trabajos de grado**. Valencia Carabobo, Venezuela.

Nuñes, J (2008). Corporación Universitaria Minuto de Dios. **Seguridad en las redes LAN y WLAN.**

Peña Rojas, H (2006). Universidad Libre-Seccional Cali **Seguridad en Redes WLAN.** Cali Colombia.

Suarez, Gutiérrez. (2012). **Mecanismos de seguridad en redes inalámbricas.** Trabajo de investigación.

Universidad Pedagógica Experimental Libertador (2006). **Manual de Trabajo de Grado de Especialización, Maestría y Tesis Doctorales**. Caracas UPEL.

Electrónicas

Enguita Gonzales, J (2012). **Redes de Computadoras**. http://www.isa.uniovi.es/redes

Escalona, R (2013) **aprenderLyX**. Recuperado el 2 de mayo de 2013, de aprenderlyx; http://aprenderlyx.com/marco-teorico-de-una-tesis-ejemplo/

Fernández, J (2015). **Optimización e Implementación de Seguridad en Redes**. https://prezi.com/p5flywxdymf4/optimizacion-e-implementacion-de-seguridad-en-redes-audito/

Guía de la Academia de Networking de Cisco Systems. (2010).

Morales, J. **Seguridad en redes Inalámbricas IEEE 802.11**, Criptografía y seguridad de redes. http://docencia.ac.upc.es/FIB/CASO/seminaris/2q0304/T10.pdf

Anexos

ANEXO A
Diagrama de Topología de red Sillaca-Mayor Beval
Fuente: Pérez, 2017

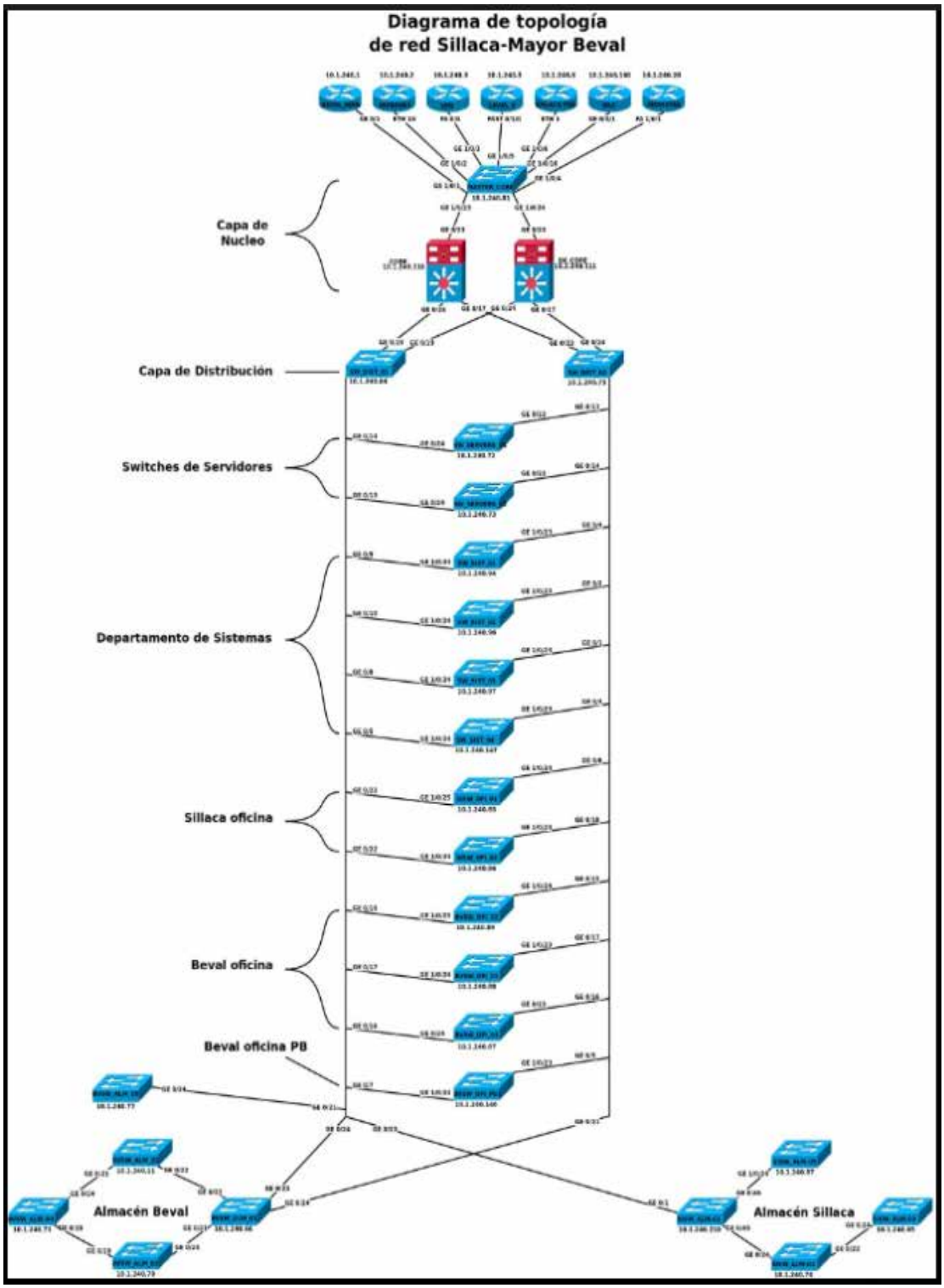
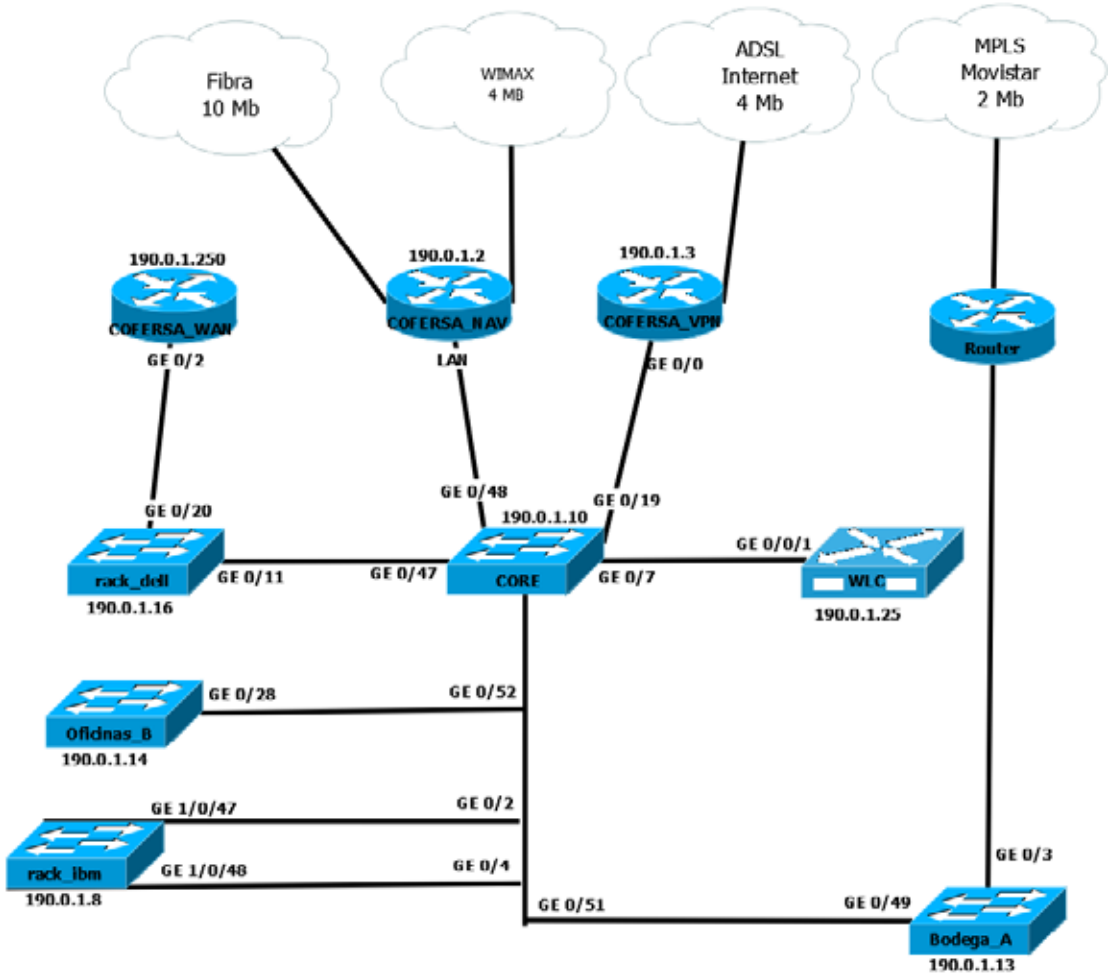


Diagrama de topología
de red Sillaca-Mayor Beval
Capa de
Nucleo
Capa de Distribución
Switches de Servidores
Departamento de Sistemas
Sillaca oficina
Beval oficina
Beval oficina PB
Almacén Beval
Almacén Sillaca

ANEXO B
Diagrama de Topología de red Cofersa
Fuente: Pérez, 2017

DIAGRAMA DE TOPOLOGIA
DE RED COFERSA



ANEXO C
Cuarto de Datos Febeca
Fuente: Pérez, 2017