ANÁLISIS A LA SEGURIDAD DE LOS ACTIVOS TECNOLÓGICOS DE RED DE LA EMPRESA SEGUROS COMERCIALES BOLÍVAR S.A.

DIEGO ANDRÉS GUTIERREZ RAMIREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2023

ANÁLISIS A LA SEGURIDAD DE LOS ACTIVOS TECNOLÓGICOS DE RED DE LA EMPRESA SEGUROS COMERCIALES BOLÍVAR S.A.

DIEGO ANDRES GUTIERREZ RAMIREZ

Proyecto de Grado – Proyecto Aplicado presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMATICA

Danny Fernando León Jaramillo
Director

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2023

NOTA DE ACEPTACIÒN

Firma del presidente de Jurado

Firma del Jurado

Firma del Jurado

Bogotá., Fecha sustentación

CONTENIDO

pág.

LISTA DE FIGURAS

Pág.

LISTA DE CUADROS

pág.

LISTA DE ANEXOS

pág.

GLOSARIO

CPE: (Customer Premises Equipment) es lo que comúnmente instala el operador de comunicaciones en las sedes de los clientes, también llamado equipo de última milla o último kilómetro.

CVE: (Common Vulnerabilities and Exposures): es un estándar que categoriza las vulnerabilidades conocidas según fabricante y versión de sistema operativo.

DATA PLANE: Es la parte del software de un equipo, por ejemplo de red, que procesa las peticiones que se le realizan.

DMVPN: Dynamic Multipoint VPN, protocolo de cisco para añadir una capa de seguridad adicional a las conexiones VPN.

EIGRP: Protocolo de enrutamiento dinámico disponible únicamente en dispositivos de la marca CISCO.

RED: Conjunto de dispositivos tecnológicos (computadores, impresoras, dispositivos móviles, entre otros) que se intercomunican entre sí.

HACKER: Individuo con conocimientos tecnológicos dedicado a encontrar fallos en los sistemas

HAKING ÉTICO: Practica que realiza un hacker, detectando brechas de seguridad para ayudar mitigarlas o erradicarlas.

INFRAESTRUCTURA TECNOLÓGICA: Conjunto de sistemas conformado por los equipos físicos como equipos de cómputo e infraestructura de red que soportan las plataformas o aplicaciones de la compañía.

IWAN: O WAN inteligente, da eficiencia en las comunicaciones intercedes, brindando seguridad y mejor comunicación con calidad de servicio entre los canales o medios conectados a esta solución.

NAC: (Network Access Control) es una tecnología que permite el control y la granularidad de decidir que equipos se les autoriza o no la conexión a la red.

PTES: (Penetration Testing Execution Standard), es una metodología que se utiliza para realizar pruebas de penetración tecnológica en la industria.

SD-WAN: WAN definida por software, esta tecnología está en auge reemplazando las conexiones normales entre oficinas con un simple Router y enrutamiento, ahora también se integra QoS, despliegues más rápidos, y sobre todo una administración con una visual total de lo que ocurre en la red.

SEGURIDAD DE LA INFORMACIÓN: Conjunto de medidas preventivas o reactivas de una compañía u organización que permiten mantener la privacidad, integridad y disponibilidad de la información.

SMOKE SCREENS: (Cortina de humo), es una técnica de ataque usada por hackers la cual tiene como finalidad distraer con un supuesto ataque y perpetrar uno de mayor impacto.

SPOOFING: Es la práctica del hacker usado para usurpar la identidad electrónica y así cometer actos delictivos.

TACACS+: (Terminal Access Controller Access Control System), es un protocolo usado para el registro, autenticación y autorización de dispositivos de comunicación y servidores.

TÚNELES GRE: (Generic Routing Encapsulation), es un protocolo para realizar comunicación segura a través de internet generando túneles encriptados.

VULNERABILIDAD: Debilidad de un sistema la cual puede ser aprovechada para acceder a dicho sistema o a información protegida por el mismo.

RESUMEN

La tecnología en los últimos años ha tenido un gran avance en todos los entornos que nos rodean, y con ello ha venido creciendo la explotación de vulnerabilidades de estos entornos digitales. Para ello se requiere estar a la vanguardia en cuanto a tecnologías que ayuden a repeler y proteger la infraestructura de forma ordenada, con el apoyo de metodologías diseñadas para este fin, y poder evitar que los recursos y activos tecnológicos estén en peligro, logrando así salvaguardarlos de ataques maliciosos.

Con la identificación en primera instancia los activos tecnológicos que se deben proteger se garantizan que la labores sean más eficientes a la hora de identificar posibles vectores de ataque en la infraestructura de red de la compañía de Seguros Comerciales Bolívar S.A. Al desarrollar la metodología PTES y obtener como resultado del proyecto un informe en el cual se detalle la información, clasificando los tipos de vulnerabilidades encontrados, entrega a la compañía una herramienta adicional para garantizar la seguridad de su infraestructura tecnológica.

ABSTRACT

Technology in recent years has had a breakthrough in all the environments that surround us, and with it has been growing the exploitation of vulnerabilities of these digital environments. This requires being at the 12outer1212f in terms of technologies that help to repel and protect the infrastructure in an orderly manner, with the support of methodologies designed for this purpose, and to prevent the resources and technological assets are at risk, thus safeguarding them from malicious attacks.

Having identified in the first instance the technological assets to be protected, makes the work more efficient when identifying 12outer12 attack vectors in the network infrastructure of the company Seguros Comerciales Bolivar S.A. by developing the PTES methodology and obtaining as a result a report detailing the information, classifying the types of vulnerabilities found, provides the company with an additional tool to ensure the security of its technological infrastructure.

INTRODUCCIÓN

Las entidades aseguradoras tienen en su poder información sensible de sus clientes, tanto financiera como personal, la cual debe estar muy bien resguardada por los riesgos que implica que caiga en manos equivocadas tanto para los clientes como para la propia compañía.

La compañía de Seguros Comerciales Bolívar S.A. no cuenta con una metodología con la que se pueda tener una radiografía actual de sus servicios y dispositivos de red iniciando desde el borde de su conexión, hasta su distribución en los dispositivos de usuario final. Por lo que se hace necesario aplicar una metodología como PTES para conocer las vulnerabilidades y el estado real de los quipos tecnológicos de RED.

1 DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

Los incidentes de seguridad informática afectan a miles de organizaciones alrededor del mundo, con miles de millones de dólares en pérdidas, esto según cifras de Kaspersky Lab[1], y de B2B International, donde se indica que tan solo en América Latina se incrementó en un 24 % los ciberataques en 2021[2].

La seguridad informática en cualquier compañía es un aspecto que se debe abordar con el mayor rigor posible, tanto por el cuerpo directivo como por las áreas específicas designadas para cumplir esta labor.

Defender una infraestructura tecnológica requiere que la organización este comprometida y tome la responsabilidad correspondiente, es un requisito indispensable contar con un inventario completo de dicha infraestructura tecnológica, para así realizar una estrategia de defensa adecuada, conocer los distintos vectores de ataque y los activos más sensibles para la compañía

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo realizar un assessment a la infraestructura tecnológica de red de la compañía de Seguros Comerciales Bolívar S.A., basado en la metodología abierta de testeo de seguridad – PTES, la cual permitirá encontrar vulnerabilidades y determinar el nivel de seguridad informática en dicha organización?

[1] KASPERSKY. (2020). Seguridad de la información a través de las cifras de pérdidas. [Sitio Web] Kaspersky Team [Consultado 24 de marzo 2022] Disponible en: https://latam.kaspersky.com/blog/security-economics-2019/17854/

[2] KASPERSKY. (2021). Ciberataques en América Latina crecen un 24% durante los primeros ocho meses de 2021. [Sitio Web] Kaspersky Team [Consultado 24 de marzo 2022] Disponible en: https://latam.kaspersky.com/blog/ciberataques-en-america-latina-crecen-un-24-durante-los-primeros-ocho-meses-de-2021/22718/

2 JUSTIFICACIÓN

La información y los servicios tecnológicos son un recurso muy importante para brindar un servicio adecuado y diligente a los clientes de la compañía de Seguros Comerciales Bolívar S.A., por lo que este proyecto pretende validar la seguridad de la infraestructura tecnológica de red de la compañía a fin de confirmar y garantizar la integridad, confidencialidad y disponibilidad de sus sistemas e información.

Aunque la compañía cuenta con mecanismos y planes de seguridad, nunca está de más realizar un testeo de la seguridad y las condiciones actuales de los equipos de red. Teniendo en cuenta que en su momento dichas herramientas de seguridad eran seguramente las más avanzadas y acordes a la necesidad, puede que hoy día debido a los también avanzados métodos de ataque de los hackers estas medidas de seguridad puedan tener falencias que se puedan corregir preventivamente.

Cualquier esfuerzo que se realice para encontrar brechas de seguridad es un impacto positivo para la compañía, ya que esto evitara a futuro contratiempos por servicios que no operen bien por un ataque o información que sea vulnerada y que a la final se traduce en una deficiencia de servicio a los clientes actuales o posibles nuevos clientes de la organización, la cual sin duda afectara económicamente a la compañía. Mostrar y poder hacer evidente que la compañía está expuesta a vulnerabilidades cibernéticas en su capa de conectividad no solo servirá para evitar daños futuros, sino que también permitirá al equipo humano involucrado obtener la experiencia necesaria para realizar acciones que aseguren la infraestructura tecnológica de red a futuro en la compañía de seguros comerciales bolívar y en otras compañías en las que puedan hacer parte más adelante.

Ahora bien, hacer uso de una buena metodología es esencial y clave para obtener buenos resultados en el proceso de validación de la seguridad, por lo que la metodología PTES es la escogida para llevar a cabo este análisis de vulnerabilidades en la compañía. La metodología PTES consta de 7 fases, con las cuales se pretende encontrar y asegurar en gran medida la infraestructura de red de la compañía, indicando al final del

proceso, cuáles son las debilidades y cómo es posible mitigarlas o mejor aún resolverlas de manera definitiva.

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Analizar la seguridad de los activos de información tecnológicos y de red de la empresa Seguros Comerciales Bolívar S.A., mediante la aplicación de la metodología PTES, generando las respectivas recomendaciones para el endurecimiento y aseguramiento de la red de datos de la compañía y seguridad de la información.

3.2 OBJETIVOS ESPECÍFICOS

Estructurar los principales elementos tecnológicos de red de la compañía mediante tabla descriptiva con el fin de planificar el alcance del análisis.

Desarrollar un assessment a la infraestructura de red de Seguros Comerciales Bolívar S.A., con el objetivo de evaluar y validar vulnerabilidades y riesgos a los que pueda estar expuesta la compañía.

Elaborar el informe resultado del assessment según el nivel de riesgo e impacto sobre la información de la compañía de acuerdo con la afectación en cuanto a disponibilidad, confidencialidad e integridad, indicando los hallazgos realizados sobre los activos de red basados en buenas prácticas.

4 MARCO REFERNCIAL

4.1 MARCO TEÓRICO

A través del tiempo la humanidad ha encontrado en el espionaje una herramienta para obtener la ventaja en casi cualquier aspecto de la vida cotidiana, a más información obtenida de un competidor o un rival mayores son las ganancias o control que se tiene en determinada situación. En la actualidad con el uso de la tecnología es cada vez más importante el papel que guarda la información, y lo es aún más la importancia que tiene salvaguardar ese activo que en algunas organizaciones a veces pasan por alto como lo es la información[3]

Ahora se debe tener claridad en dos conceptos que suelen ser confundidos con alguna regularidad como lo son la seguridad informática y seguridad de la información, el primero hace referencia al medio, las técnicas los procesos que buscan almacenar, procesar y trasmitir información. Ahora el concepto de seguridad de la información no se preocupa solo del medio y todo lo indicado anteriormente, abarca "todo" lo que tiene que ver con información sea física o digital, su almacenamiento transporte y demás, por lo anterior se puede apreciar que no solo el concepto es algo distinto sino que están diferenciados por el universo que manejan cada uno de estos conceptos[4]

Si bien el tema de la seguridad informática es algo que le merece atención a todo el mundo, en el lado de los países en vía de desarrollo es algo que aún no toma la suficiente fuerza como se quisiera. Según lo indicado por Kosévich en América Latina está muy rezagada respecto a otros países y regiones del mundo en la implementación de las tecnologías de información, protección de infraestructuras y tecnología en general. Esto

[3] MAROTO, J. P. (2018). El ciber espionaje y la ciberseguridad. In La violencia del siglo XXI. Nuevas dimensiones de la guerra (pp. 45-76). Instituto Español de Estudios Estratégicos. [En línea] Unirioja [Consultado 20 de abril 2022] disponible en: https://dialnet.unirioja.es/descarga/articulo/4549946.pdf

[4] Castro, M. I. R., Morán, *et al.* (2018). Introducción a la seguridad informática y el análisis de vulnerabilidades (Vol. 46). 3Ciencias [En línea] 3ciencias [Consultado 20 de abril 2022] disponible en: https://books.google.es/books?hl=es&lr=&id=5Z9yDwAAQBAJ&oi=fnd&pg=PA29&dq=Introducci%C3%B3n+a+la+seguridad+inform%C3%A1tica+y+el+an%C3%A1lisis+de+vulnerabilidades&ots=ymuVBZj7Nx&sig=ynVaFH7rLi37UoL9ZVtcqAsQJo0#v=onepage&q=Introducci%C3%B3n%20a%20la%20seguridad%20inform%C3%A1tica%20y%20el%20an%C3%A1lisis%20de%20vulnerabilidades&f=false

se ve en las estadísticas de los últimos cinco años donde la cantidad de ciberataques tomaron una gran ventaja, alrededor del 40%, lo que da un estimado y una cifra no muy alentadora de alrededor de 700 millones de ataques al año. Los ataques a infraestructuras tecnológicas vulnerando información de grandes compañías incluyendo algunas de las más importantes financieras en América Latina superan en un 50%. Anualmente, los ataques a la infraestructura tecnológica les causan daño a los países de América Latina por un monto de US$90 mil millones.

> Los tres países que acumulan el mayor número de los delitos cibernéticos son: Brasil (recibe el 55% de todos los ataques que se cometen en la región), México (es blanco del 17% de los ataques) y Colombia (el 9%). En una investigación conjunta, llevada a cabo en 2016 por la Organización de Estados Americanos (OEA) y el Banco Interamericano de Desarrollo (BID), se destaca que 16 de los 32 países de América Latina y el Caribe son totalmente incapaces de contrarrestar los ataques cibernéticos[5]

Los esfuerzos que realizo el gobierno Colombiano iniciando el siglo XXI, hicieron que lo convirtieran en pionero frente a los demás países locales, en hacerle frente al crimen cibernético que cada vez tomaba más y más ventaja contra las organizaciones y compañías tanto locales como extranjeras que desarrolla poniendo como uno de sus pilares fundamentales la seguridad digital, Colombia se convirtió en 2011 en el primer país de América Latina en iniciar el modelado y construcción de una Estrategia nacional de seguridad cibernética. Cinco años más tarde, en el segundo trimestre de 2016 Colombia ya había madurado su estrategia de seguridad e inicio la adopción de una nueva estrategia a la cual denomino "Política Nacional de Seguridad Digital". Actualmente se constituyó el Equipo de Seguridad Informática para la Reacción a Incidentes (ESIRI), el cual clasifica y neutraliza los ataques de seguridad cibernética presentados a lo largo y ancho del territorio, este equipo está conformado por un grupo de expertos en seguridad cibernética. Una de las tareas que cumple este equipo de expertos es realizar trabajos cooperativos con otros equipos tanto nacionales como internacionales, en donde Colombia se suma a los acuerdos internacionales sobre la seguridad informática garantizando su cumplimiento. Aquellas corporaciones sobre las cuales descansa la responsabilidad de gestión y velar por el cumplimiento en el ámbito nacional son: el departamento

[5] KOSÉVICH, Ekaterina Yu. Estrategias de seguridad cibernética en los países de América Latina. Iberoamérica. [En Línea] Federación Rusa, 18 de noviembre de 2019 [Consultado 20 de abril 2022] disponible en: https://www.researchgate.net/profile/Ekaterina-Kosevich/publication/340419950_Cyber_Security_Strategies_of_Latin_America_Countries/links/5eac0008a6fdcc70509e07c7/Cyber-Security-Strategies-of-Latin-America-Countries.pdf

Nacional de Planeación, Ministerio de Defensa Nacional y el Ministerio de Tecnologías de la Información y Comunicaciones. Esto según lo indica Arévalo[6]

En la industria, las empresas sin importar la cantidad de empleados, lo que coticen en bolsa de valores o el renombre que pueda tener, debería contar con sistemas de protección a su información y aplicaciones, sin embargo eso solo se aplica en la teoría ya que en la realidad no todas las empresas cuentan con los recursos y la disposición para atender su propia seguridad informática y tratar de minimizar los riesgos de ataques. No todas las empresas cuentan con los mismos recursos y no poseen las mismas necesidades, por lo que los planes y estrategias de protección y seguridad informática no puede ser la misma para todas las empresas.[7]

Entrando un poco en el detalle de lo que se puede identificar en una compañía, se puede iniciar con la forma en la que se "evalúa diferentes peligros de ciberseguridad a los que una organización puede estar expuesta como robos, intrusiones, denegación de servicios o cualquier otro ataque externo o interno.

Hoy en día la tecnología es fundamental para los procesos de cualquier organización, lo que conlleva a la implementación de varios sistemas informáticos, y quizás por desconocimiento o mala administración no somos conscientes de las vulnerabilidades que los sistemas pueden tener, ya sea a nivel humano, de programación, diseño, etc. En estos escenarios cobra importancia el análisis de riesgos, en el cual se integran varios factores como: Identificación de activos, vulnerabilidades, riesgos y amenazas[8]

---

[6] AREVALO Ochoa, Adrián P. Gobierno de Seguridad de la Información, un enfoque hacia el cumplimiento regulatorio. Revista Tecnológica-ESPOL, [En Línea] Cuenca, (Ecuador), 15 de noviembre de 2019 [Consultado 20 de abril 2022] disponible en: http://rte.espol.edu.ec/index.php/tecnologica/article/view/373/258

[7] RODRIGUEZ Gahona, G. Análisis comparativo de los modelos defensa en profundidad y mspi, para la implementación de la seguridad informática en el sector privado del país. [En Línea] Monografía especialización seguridad informática, Universidad Nacional Abierta y a Distancia, 2020 [Consultado 20 de abril 2022] disponible en: https://repository.unad.edu.co/bitstream/handle/10596/38717/grodriguezgah.pdf?sequence=1&isAllowed=y

[8] FUNCION PUBLICA, Ministerio TIC. [Sitio Web] Bogotá. Guía para la administración del riesgo y el diseño de controles en entidades públicas. [Consultado 30 de marzo de 2022] Disponible en: https://dapre.presidencia.gov.co/oci/normograma/Guia-administracion-riesgo-diseno-controles-entidades-publicas.pdf

Identificación de activos: al detectar los activos de información que posee una organización (software y hardware), permite tener un inventario de cada componente facilitando el despliegue de políticas o acciones de seguridad.

Riesgos y amenazas: al tener claridad sobre todos los activos y servicios de los cuales una compañía depende, se hace preocupante no solo el robo o perdida de la información, también se considera la continuidad del negocio ya sea por desastres naturales o situaciones poco típicas como la que afronta el mundo hoy día como lo es el caso de la pandemia debido al covid-19.

Vulnerabilidades: los activos y servicios siempre están en riesgo, ya sea por errores humanos o en la programación de los mismos sistemas, el análisis de riesgos involucra las detecciones de vulnerabilidades permitiendo tomar acciones sobre las brechas y mitigar estos riegos, también es importante fomentar campañas para la capacitación del personal, con el fin que adquiera la capacidad de manipular los sistemas de forma adecuada y comprendan las diferentes amenazas como phishing, los malware, entre otras, para que no sean víctimas de engaños[9].

4.2 MARCO CONCEPTUAL.

4.2.1 Seguridad en el Router.

Los Router por defecto traen una configuración inicial que no tiene protección en seguridad. Al igual que eso cuando a un equipo le es asignada una IP, esta es accesible desde el mundo exterior y puede ser fácilmente vulnerado el equipo.[10]

Algunos servicios habilitados por defecto deben ser deshabilitados para evitar consumo inadecuado de memoria y también para prevenir ataques o huecos de seguridad, a continuación algunos de esos servicios.

[9] OSPINA DÍAZ, Milton. R., y SANABRIA Rangel, Pedro. E. Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. Revista Criminalidad. [En línea]. Bogotá (Colombia). vol. 62, nro. 3 [Consultado 03 de abril 2022]. Disponible en: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1794-31082020000200199

[10] RAVELO ALFONSO, Rosmely. Material complementario basado en mecanismos de seguridad de routers. [En línea]. Tesis Doctoral. Universidad Central " Marta Abreu" de Las Villas. 2015 [Consultado 03 de abril 2022]. Disponible en: http://dspace.uclv.edu.cu:8089/handle/123456789/4476

- Finger: informa quien está conectado en el router, desde donde y por cuanto tiempo.
- PAD: Comando histórico, desde los días de X.25
- Small servers: puertos TCP y UDP menores de 20 para desarrollo de pilas IP y no necesario hoy en día.
- Bootp: usado por los sistemas para iniciar ellos mismos dentro de la red buscando un equipo central que tiene la información de carga inicial.
- Domain lookup: Comando para habilitar la traslación de nombres en el momento de ejecutar comandos en el CLI. Se debe deshabilitar en los CPEs.

4.2.2 Cisco Discovery Protocol

Permite a los administradores de red descubrir a sus vecinos, equipos Cisco, número de modelo y versiones de software.

Se usa este protocolo para saber cuáles son los equipos que puedan estar conectados en las interfaces de LAN y WAN de los CPEs.

En las interfaces WAN debe estar habilitado siempre el CDP, en algunos casos en las interfaces LAN podría deshabilitarse y solo usarse en labores operativas de gestión y mantenimiento. Para el caso de Seguros Bolívar no será necesaria su habilitación.

4.2.3 Control Plane

Este módulo menciona técnicas y guías de configuración para ayudar a proteger el plan de control de los equipos. Tales como protocolos de enrutamiento y/o sincronización usados para trasmitir información a cada uno de los equipos. Se da de manera informativa y se cubrirá en detalle en los productos que requieran protocolos de enrutamiento entre el CPE y el PE de Claro como proveedor de servicio. Las siguientes secciones son informativas sobre temas a ser tenidos en cuenta al momento de tener enrutamiento en los CPEs de la red de Seguros Bolívar.

4.2.4 Seguridad en protocolos de enrutamiento

Los protocolos de enrutamiento pueden ser atacados accidental o intencionalmente por Denegación de Servicio, Paquetes re enrutados, Información falsa, y "smoke screens".

Para EIGRP (protocolo usado para la red de IWAN) se debe tener en cuenta:

Filtrado: Existen dos formas de hacer filtrado: mediante una Lista distribuidas o un filtrado de prefijos. Se deben hacer filtrados en el cliente de entrada y salida para reforzar la seguridad y no permitir que lleguen o se publiquen redes adicionales que no deban ser recibidas ni enviadas. De esta forma se debe asegurar que el cliente reciba únicamente las redes que le interesan y que solo publique sus redes propias.

No se permitirá que en un CPE se publique dinámicamente hacia la nube del operador la ruta 0.0.0.0/0. El CPE deberá publicar únicamente las redes que están detrás y en su red LAN.

Convergencia: Una rápida convergencia significa que la red tiene alta velocidad ofreciendo mejores respuestas a incidentes de seguridad y consumo de tráfico. Para este caso se realizará un barrido de las troncales y consumo de estas, revisión de últimas millas y capacidad del tráfico en cada uno de los dispositivos.

4.2.5 Data Plane

Este módulo cubre técnicas y guías de configuración para ayudar a proteger el plan de datos de los equipos de Seguros Bolívar. Permite proteger paquetes que pasan a través del router del usuario o cliente en el cual el router envía tráfico de un puerto a otro.

Los clientes no deben enviar ningún paquete con una dirección IP fuente que no corresponda a las redes internas permitidas (Spoofing).

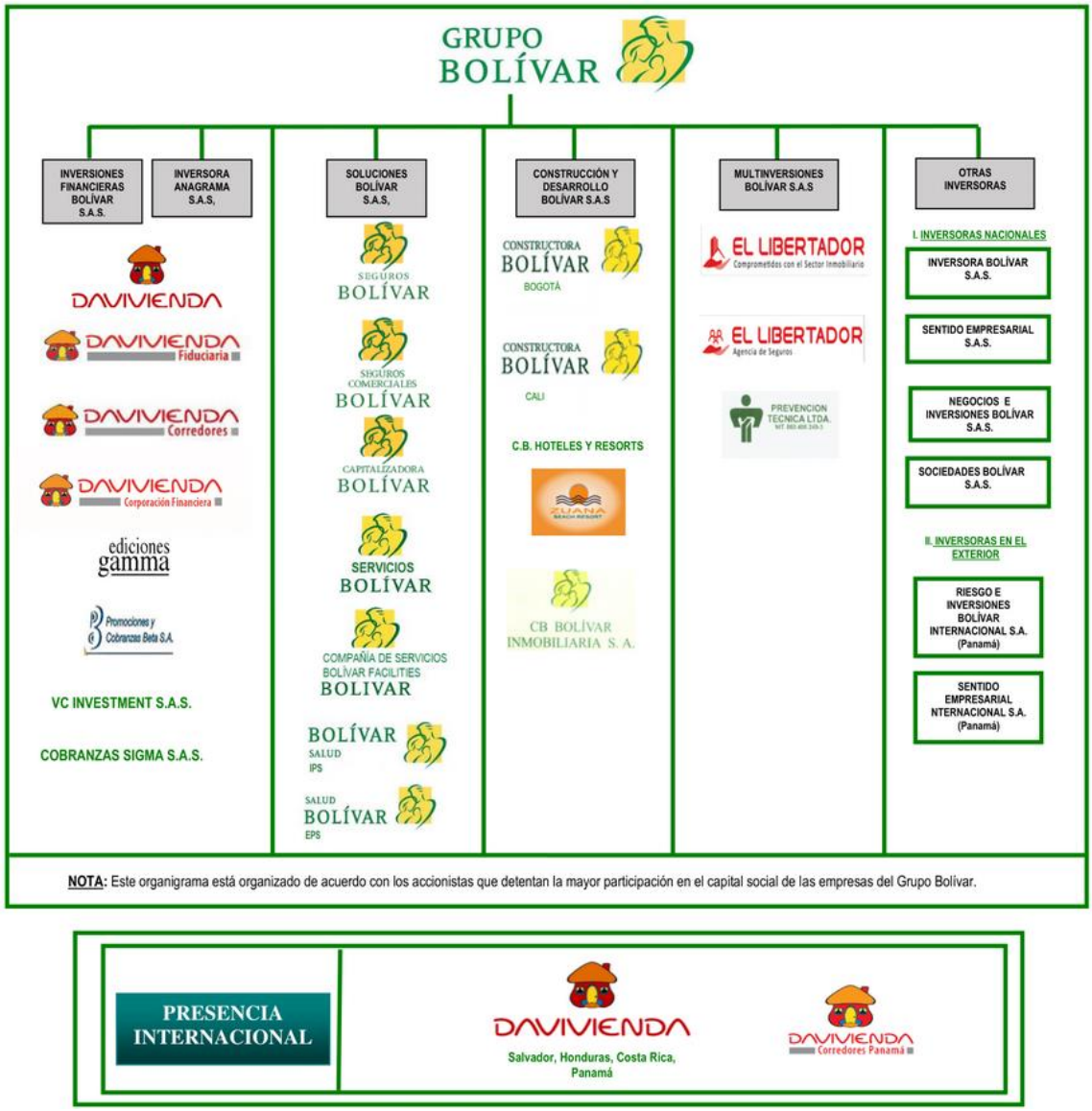
Este aseguramiento se puede hacer filtrando los paquetes, bajo los principios de:

- Filtrar tan cerca del borde como sea posible.
- Filtrar tan preciso como sea posible.
- Filtrar ambos: fuente y destino donde sea posible.

4.3 MARCO CONTEXTUAL

Seguros Comerciales Bolívar S.A. es una empresa de seguros que se fundó a finales de la década de 1930, con más exactitud en 1939, la cual tiene como servicio principal los seguros de vida. Hoy día hace parte de un conglomerado de empresas las cuales hacen parte del Grupo Bolívar, a las cuales pertenecen empresas como Davivienda, Constructora Bolívar, el Libertador, entre otras. A continuación un organigrama de cómo se distribuyen y cuales compañías hacen parte de este grupo:

Figura 1: Organigrama Grupo Bolívar



Fuente: Seguros Bolívar, Nuestras compañías [En línea] (Consultado en 10 de abril de 2022), disponible en: https://www.grupobolivar.com.co/wps/portal/web/

Con la constante evolución de la tecnología y los métodos en los que se realizan las ventas de los seguros en la compañía, se diversifico la forma en la que se concibieron las infraestructuras tecnológicas en su interior, además de su expansión en varias ciudades del territorio nacional, Seguros Bolívar cuenta con alrededor de 60 sedes, de las cuales su sede principal está ubicada en la Avenida el Dorado # 68b – 31.

En las diferentes sedes se cuenta con entornos de red tanto Wireless como ethernet, que brindan conectividad al usuario interno tanto a aplicaciones ubicadas en nube privada y servidores en datacenter de diferentes operadores, como conexión a internet.

Los usuarios finales, es decir quienes acceden a los distintos servicios de la compañía, hacen uso de distintos canales de comunicación como lo es la conexión tradicional por llamada telefónica, o el acceso por canales de internet, en este último se tiene un esfuerzo adicional para proteger las distintas bases de datos e información confidencial del mundo exterior, permitiendo solo el acceso a cierta parte de esta información a este usuario final.

La compañía cuenta de un área de redes la cual debe garantizar los protocolos y estrategias de seguridad en la red para interconectar los distintos dispositivos en ella, es a esta área a la que se le entregara el informe final y con quien se interactuara para todo lo relacionado con permisos y actividades propias de las pruebas de pentesting.

Seguros Bolívar cuenta con la cobertura tercerizada de sus entornos de red mediante empresas internacionales como lo son Claro (Telmex) e IBM, cada una maneja aspectos de configuración y políticas de seguridad de sus equipos capa 2 y capa 3 como los equipos Switch y los equipos de red inalámbrica o Access Point, con los que finalmente se les brinda acceso a los usuarios anteriormente mencionados.

Aplicando la metodología de PTES, la idea es validar si estos dispositivos de red tanto de la sede central como en las sedes remotas cuentan con el firmware adecuado, políticas de configuración y estándares mínimos para atender las necesidades de la compañía en cuanto a la seguridad de acceso de los componentes tecnológicos de los usuarios para que estos a su vez tengan acceso a la información que requieren para sus labores diarias.

4.4 MARCO LEGAL

El estado colombiano ha legislado para el cumplimiento en todo el territorio nacional, una serie de leyes que pretenden blindar la seguridad informática y dar castigo a los delitos considerados como cibercrimen o que son cometidos en aras de atentar con la integridad, disponibilidad y confidencialidad de la información en los ámbitos tecnológicos. A continuación se indicarán algunas de estas:

4.4.1 Ley Estatutaria 1581 De 2012:

Esta ley hace referencia específicamente a la protección de datos personales, pero específicamente a su recolección transferencia, actualización, eliminación, confirmación, uso y divulgación no autorizada.[11]

4.4.2 Ley 1273 del 5 de enero de 2009:

Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones[12]. Dentro de esta ley hace especial de valor resaltar los artículos que maneja.

Artículo 269ª. Acceso abusivo a un sistema informático.

Artículo 269B. Obstaculización ilegítima de sistema Informático o red de telecomunicación.

Artículo 269C. Interceptación de datos informáticos.

[11] COLOMBIA, CONGRESO DE LA REPUBLICA, Ley 1581 (17 de octubre de 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. En: Diario Oficial Alcaldía de Bogotá, [Sitio web] Disponible en: https://bibliotecadigital.ccb.org.co/bitstream/handle/11520/13629/Ley%201581%20de%202012.pdf?sequence=1

[12] COLOMBIA, CONGRESO DE LA REPUBLICA, Ley 1273 de 2009. (05 de enero de 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Senado de la Republica. [Sitio web] disponible en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

Artículo 269D. Daño Informático. En este ítem cabe aclarar que según la ley, este articulo aplica para quien realice algunas de las siguientes acciones sobre sistemas de tratamiento de información o sus componentes lógicos, las acciones son, borrar, suprimir, destruir, deteriorar, o alterar.

Artículo 269E. Uso de software malicioso.

Artículo 269F. Violación De Datos Personales. En este ítem cabe aclarar que según la ley, este articulo aplica para quien realice algunas de las siguientes acciones por beneficio propio o de un tercero sobre sistemas de tratamiento de información o sus componentes lógicos, obtener, compilar, sustraer, ofrecer, vender, intercambiar, enviar, comprar, interceptar, divulgar,
Modificar, emplear códigos personales, datos personales, contenidos en ficheros, archivos, bases de datos o medios semejantes.

Artículo 269G. Suplantación de sitios web para capturar datos personales.

Artículo 269I. Hurto Por Medios Informáticos Y Semejantes.

Artículo 269J: Transferencia No Consentida De Activos.

4.4.3 Decreto 1074 De 2015:

En este decreto se establece que cada organización debe contar con un gobierno o jerarquía de datos la cual debe estar bajo parámetros o normas formales. Este decreto lo que busca es regular y asignar la responsabilidad de los datos que se denominan como personales.[13]

4.4.4 CONPES 3701 DE 2011:

Lineamientos Ciberseguridad y Ciberdefensa.[14]

[13] COLOMBIA. MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO. Decreto 1074 (26, mayo, 2015). Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo. [Sitio web] Disponible en: http://wp.presidencia.gov.co/sitios/normativa/decretos/2015/Decretos2015/DECRETO%201523%20DEL%2016%20DE%20JULIO%20DE%202015.pdf

[14] COLOMBIA. CONSEJO NACIONAL DE POLITICA ECONÓMICA Y SOCIAL DE COLOMBIA. Conpes 3701de 2011: Lineamientos de política para la Ciberseguridad y Ciberdefensa. [Sitio Web]. Disponible en: https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

4.4.5 CONPES 3854 DE 2016:

"Política Nacional de seguridad digital."[15]

[15] COLOMBIA. CONSEJO NACIONAL DE POLITICA ECONÓMICA Y SOCIAL DE COLOMBIA. Op. Cit. p. 41. Conpes 3654 de 2016. [Sitio Web] Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos /3854.pdf

5 DISEÑO METODOLÓGICO

Para el desarrollo de este proyecto está dado bajo la modalidad de proyecto aplicado mediante el cual según los propios lineamientos de la Universidad Nacional Abierta y a Distancia (UNAD), permite al estudiante el diseño de proyectos para una transferencia social de conocimiento que contribuya de manera innovativa a la solución de problemas focalizados"[16]

La metodología para implementar en este proyecto está basada en PTES, la cual es una excelente herramienta para seguir y realizar pruebas de penetración en una empresa como en este caso Seguros Comerciales Bolívar.

5.1 METODOLOGIA DE INVESTIGACIÓN

PTES es una metodología muy completa la cual nos garantiza un excelente estándar y buenas prácticas para desarrollar el pentest en la compañía de Seguros Comerciales Bolívar S.A. garantizando una mejor protección y endurecimiento de los sistemas físicos y virtuales a los que se pondrán a prueba.[17]

El desarrollo de esta metodología consta de 7 fases las cuales al realizarlas garantizarían una buena práctica de pentest efectivo a los sistemas e infraestructura objetivo.[18]

Fase 1, Interacciones Previas: Se establecen los alcances y profundidad que se requiera o necesite evaluar en conjunto con los profesionales encargados del área o áreas afectadas en esta operación, también se indica el calendario o plan de trabajo, entre otros planes que se dictaminan de importancia, en esta fase debe quedar claro preguntas como que se va a evaluar y como se hará.

---

[16] UNAD. (s.f). Universidad Nacional Abierta y a Distancia. [Sitio web] Bogotá: ECBTI - Alternativas para grado. [Consulta 06 de abril 2022] Disponible en: https://academia.unad.edu.co/ecbti/oferta-academica/alternativas-para-grado

[17] BLOGSPOT. Metodología PTES (Penetration Testing Execution Standard). [Sitio web]. Colombia: [Consulta: 07 de abril 2022]. Disponible en http://blogdeauditoriadeseguridad.blogspot.com/2017/09/metodologia-ptes-penetration-testing.html

[18] RODRÍGUEZ-VÁSQUEZ, Elkin Germán, et al. Definición de una metodología personalizada de hacking ético para empresas públicas de Cundinamarca SAESP y ejecución de una prueba a la página web ya los servidores de la entidad, soportada sobre la metodología definida. [En línea]. Trabajo de Investigación. Universidad Católica, 2019. [Consultado 10 de abril 2022] Disponible en: https://repository.ucatolica.edu.co/handle/10983/23377

Fase 2, Recolección de la información: En esta fase como su nombre lo indica, la idea es recopilar a manera de inventario toda la información posible del objetivo, según Nickerson[19]

> esta recolección se divide en 3 tipos, el primero es la recolección de información simple por medio de herramientas. El segundo es la recolección de información con un análisis más profundo por medio del conocimiento de los procesos y estructura de la empresa. El tercero es la recolección de información avanzada por medio del conocimiento a profundidad de todo lo relacionado con la empresa. Esta fase es muy importante para determinar los posibles ataques y atacantes.

Fase 3, Modelado de amenaza: en esa fase no se cuenta con un estándar o norma a seguir, simplemente se realiza un recuento del equipo y herramientas a las cuales se tiene acceso y con lo que se realizaría la labor, se listarían amenazas principales, se indicarían los actores que intervendrían, principales vectores de ataque y posibles escenarios a los que se estaría expuesto de llegarse a materializar alguno ataque. El principal objeto de esta fase es categorizar los activos con lo que posteriormente se puede tener un mejor control.

Fase 4, Análisis de vulnerabilidades: Con toda la información recopilada y sobre todo con la que se brinda en la fase anterior re realiza el trabajo de validar y tratar de dictaminar las principales vías y como se pueden gestar los ataques a la infraestructura tecnológica incluyendo credenciales de usuarios, nombres y/o ubicaciones de equipos, por mencionar algunos, en este punto se realiza un listado definitivo de lo que se atacaría en la fase siguiente indicando con detalle hasta donde o que granularidad tendrá el ataque.[20]

Fase 5, Explotación: Es aquí donde toda la planeación anterior toma cuerpo, se utilizan las herramientas de pentesting escogidas para vulnerar el sistema, se debe tener presente la forma y la cantidad de elementos dispuestos por la empresa que pueden o no restringir los ataques.

---

[19] NICKERSON, Chris, *et al.* Penetration Testing Execution Standard. [Sitio web] [Consultado 16 de abril 2022]. Disponible en: http://www.pentest-standard.org/index.php/Main_Page

[20] GARCÍA PÉREZ, Kevin Alexis. Aplicación de hacking ético mediante test de intrusión Pentesting para la detección y análisis de vulnerabilidades en la red inalámbrica de una institución educativa de la provincia de Santa Elena. [En línea]. Trabajo de investigación. Universidad Peninsular Estatal de Santa Elena 2021 [Consultado 20 abril 2022] Disponible en: https://repositorio.upse.edu.ec/handle/46000/5855

Fase 6, Post-Explotación: En este punto de la metodología se llevan a cabo algunas configuraciones como el borrado de huellas digitales, validar que valor representa en general el elemento tecnológico comprometido. Se contempla el tema de hacer persistente y perdurable el ataque en el tiempo salvaguardando y manteniendo bajo parámetros la seguridad de la red.

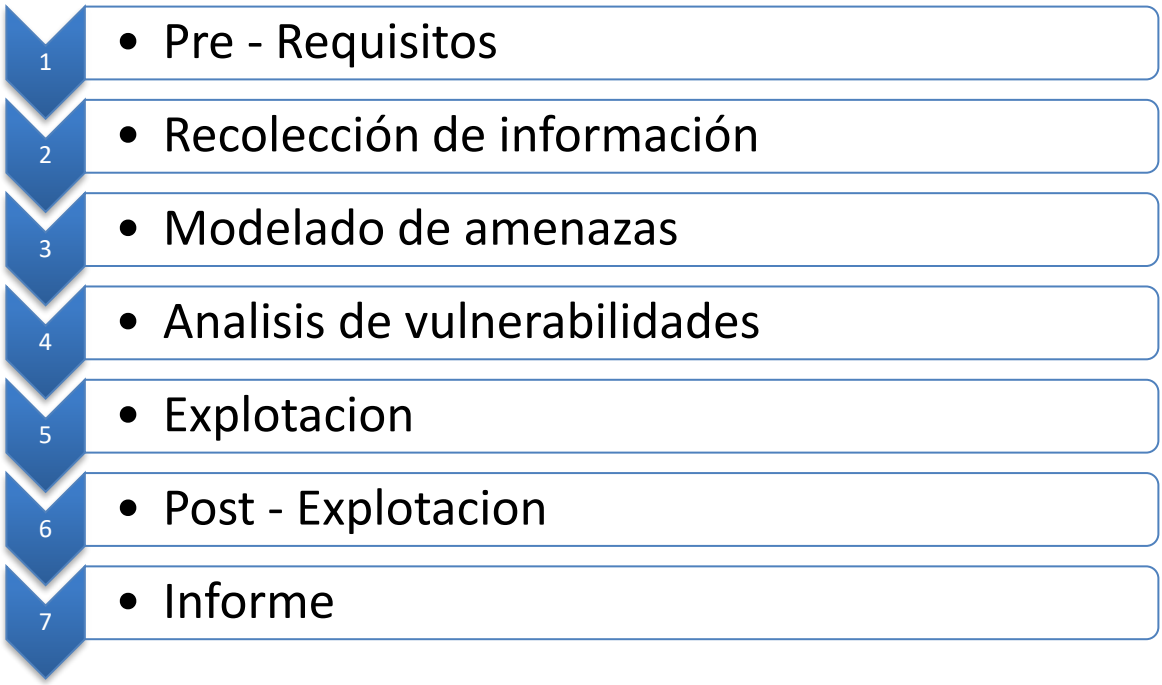
Fase 7, Informe Final: al llegar a esta fase ya se cuenta con información documentada la cual deberá ser organizada para presentarla de manera ejecutiva y técnica a quien corresponda en la compañía, aunque la metodología no cuente con los formatos específicos, si se requiere que se entreguen de manera detallada los hallazgos del pentesting, en estos informes se debe incluir las vulnerabilidades encontradas, en que contexto fueron halladas y bajo lineamientos, así como los objetivos alcanzados.

6 ANÁLISIS A LOS DISPOSITIVOS DE RED

6.1 ESTRUCTURAR LOS PRINCIPALES ELEMENTOS TECNOLÓGICOS DE RED DE LA COMPAÑÍA MEDIANTE TABLA DESCRIPTIVA CON EL FIN DE PLANIFICAR EL ALCANCE DEL ANÁLISIS.

La Figura a continuación indica las distintas fases de la metodología PTES, la cual servirá de guía del presente documento.

Figura 2. Fases de la metodología PTES.



"Elaboración Propia"

Para este caso y dando cumplimiento al objetivo propuesto, se desarrollarán las actividades correspondientes a las fases 1 y 2 de la metodología PTES.

6.1.1 Fase 1: Interacciones previas o pre – requisitos.

En esta fase se realiza un acuerdo entre los participantes, el jefe de are de redes, desarrollador del proyecto aplicado, residentes de proveedores (Claro) e IBM, para indicar que se iniciarán las actividades de validación y listado de equipos que serán objeto del testeo y validación de

vulnerabilidades. También se solicitan los permisos para el acceso a los equipos y poder validar detalles de versión y configuraciones estándar según buenas prácticas para garantizar la seguridad de la red.

Se acuerda que como primer paso se validaran los equipos de red ubicados en el borde de conectividad de cada sede o lo que comúnmente los operadores llaman CPE, posteriormente al listado se realizara una validación de vulnerabilidades según la versión de sistema operativo en el CVE.

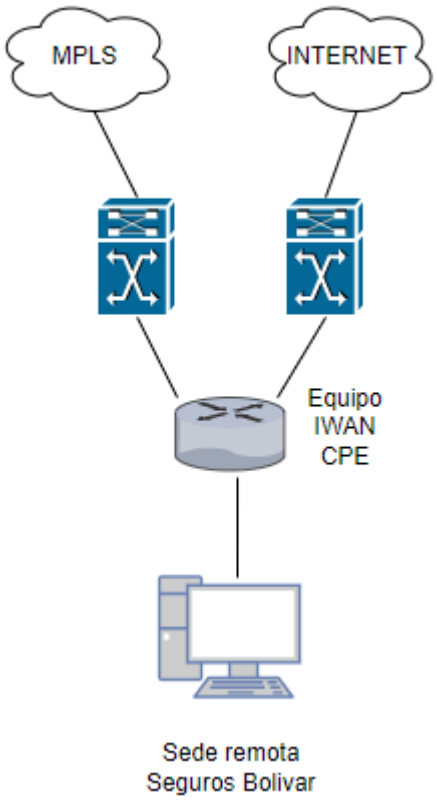
6.1.2 Fase 2: Recolección de la información.

Aquí se presenta la información recaudada sitio a sitio para conocer dos aspectos importantes, el modelo y la versión que actualmente corre en los equipos. También se valida como se interconectan las sedes con los demás servicios.

La conectividad para todas las sedes del grupo Bolívar a través de la red MPLS del operador Claro, se concentra en el punto central en el Datacenter principal de IBM en Celta Siberia. Cumpliendo con todos los requerimientos de conectada a nivel de intranet, internet y extranet, garantizando que los usuarios finales tengan una experiencia mejorada de todas las aplicaciones que maneja el Grupo de seguros Bolívar.
En la primera fase se implementarán temporalmente servicios normales de intranet. Las sedes están dentro de la plataforma de IWAN, proveída con equipos cisco, y donde en las siguientes topologías de conexión se indicará algunos detalles.

En las sedes remotas se encuentra un CPE ISR4431, ISR4321 que estarán conectadas a las dos nubes, donde terminarán los túneles GRE. Este esta es la única topología que se encontrara en las sedes remotas.
Este tipo de sedes tiene conexiones a dos links a través de dos dominios DMVPN, uno a cada link, PfR será configurado como un MC/BR

Figura 3. Topología de conexión WAN sede remota.



Fuente: "elaboración propia"

En la Figura 2 se puede apreciar como una sede remota hace conexión mediante dos canales, uno principal que esta denominado como MPLS y uno de respaldo que esta denominado como internet, la configuración se encuentra en modo activo – activo, es decir que cada enlace lleva tráfico, sin embargo se le da más prioridad al tráfico que cursa por el canal MPLS.

El segundo canal es un internet que se utiliza como red de transporte para los túneles GRE y también es un internet que se utiliza para navegación en cada sede, se configura un IP pública en una interface loopback y se hace NAT a la IP privada de cada sede de Seguros Bolívar, para que la sede tenga acceso a internet localmente sin que llegue a un sitio centralizado.
Este servicio no tiene contemplado umbrela router, pero si tiene Zona de FW centralizado, para la seguridad hacia internet, adicionalmente a eso los usuarios que salen a internet se validan en el directorio activo que está en el centro de datos de IBM, y este enruta el tráfico a un control de navegación que estará ubicado en el Datacenter de Triara el cual verifica

el perfil de navegación para que el usuario llegue a internet según su perfil.

A continuación se presenta en el cuadro 1 como está definida la prioridad respecto al tipo de tráfico.

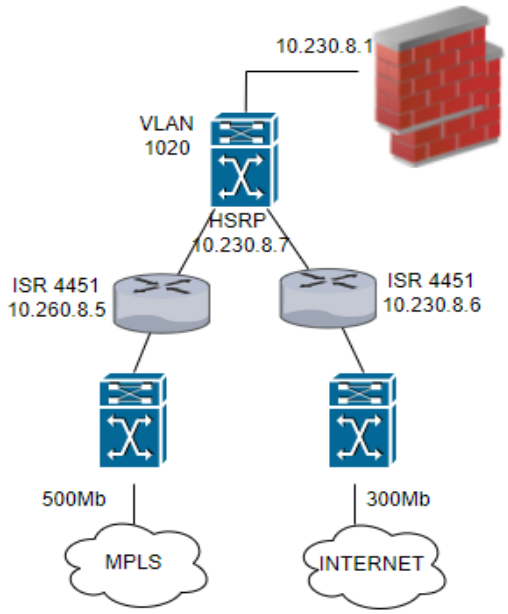
Cuadro 1. Definición de prioridades de tráfico.

Plantilla Predefinida	**Definición del Umbral**
Voice	Priority 1 one-way-delay threshold 150 threshold 150 (msec) Priority 1 one-way-delay threshold 150 threshold 150(msec) Priority 2 packet-loss-rate threshold 1 (%) Priority 2 byte-loss-rate threshold 1 (%) Priority 3 jitter 30 (msec)
Real-time-video	Priority 1 packet-loss-rate threshold 1 (%) Priority 1 byte-loss-rate threshold 1 (%) Priority 2 one-way-delay threshold 150 (msec) Priority 3 jitter 20 (msec)
Low-latency-data	Priority 1 one-way-delay threshold 100 (msec)) Priority 2 byte-loss-rate threshold 5 (%) Priority 2 packet-loss-rate threshold 5 (%)
Bulk-data	Priority 1 one-way-delay threshold 300 (msec) Priority 2 byte-loss-rate threshold 5 (%) Priority 2 packet-loss-rate threshold 5 (%)
Best-effort	Priority 1 one-way-delay threshold 500 (msec) Priority 2 byte-loss-rate threshold 10 (%) Priority 2 packet-loss-rate threshold 10 (%)
Scavenger	Priority 1 one-way-delay threshold 500 (msec) Priority 2 byte-loss-rate threshold 50 (%) Priority 2 packet-loss-rate threshold 50 (%)
Custom	Defines customized user-defined policy values

Fuente: CISCO. [Sitio web] [Consulta: 02 de mayo de 2022] disponible en: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/pfrv3/configuration/xe-3s/pfrv3-xe-3s-book/pfrv3.html

En la columna de la izquierda se presenta los tipos de paquetes que son reconocidos por los equipos de borde o IWAN, y en la columna derecha los parámetros de latencia y de pérdidas que están configurados para el tránsito de cada enlace, por ejemplo, si el tránsito del tráfico de voz configurado en el enlace MPLS supera un delay de 150 ms, este inmediatamente conmuta al enlace de internet si la latencia es inferior.
A continuación, en la Figura 3. Se puede observar cómo se hace la conexión del extremo contrario de una sede remota, en el punto de convergencia por donde todas las oficinas se conectan a internet. Esta misma topología se encuentra replicada para alta disponibilidad en un datacenter alterno del operador LUMEN, con el fin de garantizar alta disponibilidad

Figura 4. Topología de conexión WAN del punto central.



Fuente: "elaboración propia"

En el anexo A, se puede validar una topología integrada del núcleo de las redes para la conectividad de todas las sedes y la conectividad entre los equipos de seguridad perimetral con sus respectivas redundancias.

En el cuadro 2, siguiendo con parte de la fase 2 de la metodología PTES, se realizó un inventario de los equipos que forman parte de toda la red IWAN con su respectivo identificador de servicio interno, modelo

manejado por el equipo, y la versión de sistema operativo que se encuentra corriendo en él.

Cuadro 2: Características de equipos por sede.

#	CODIGO	SEDE	MODELO	VERSIÓN IOS
1	SCB0028	SUCURSAL POPAYAN	ISR4321/K9	16.6.2
2	SCB0074	SUCURSAL LIBERTADOR SUBA C.C CENTRO SUBA	ISR4321/K9	16.6.2
3	SCB0082	SUCURSAL EL LIBERTADOR AVES MARIA	ISR4321/K9	16.6.2
4	SCB0086	TORRE SEGUROS BOLIVAR TSB	ISR4431/K9	16.6.2
5	SCB0091	SUCURSAL AON	ISR4321/K9	16.6.2
6	SCB0092	SUCURSAL AREA ESP CALLE 69	ISR4321/K9	16.6.2
7	SCB0095	SUCURSAL BCM	ISR4331/K9	16.6.2
8	SCB0096	SUCURSAL CHAPINERO	ISR4321/K9	16.6.2
9	SCB0099	SUCURSAL SOCIO EMPRESARIO (FEA)	ISR4321/K9	16.6.2
10	SCB0101	LIBERTADOR INTERNACIONAL	ISR4331/K9	16.6.2
11	SCB0102	LIBERTADOR UNICENTRO	ISR4321/K9	16.6.2
12	SCB0103	SANTABARBARA	ISR4321/K9	16.6.2
13	SCB0113	SUCURSAL BARRANQUILLA MURILLO	ISR4331/K9	16.6.2
14	SCB0114	SUCURSAL BUCARAMANGA	ISR4331/K9	16.6.2
15	SCB0118	PRINCIPAL ARMENIA	ISR4321/K9	16.6.2
16	SCB0119	SUCURSAL PRADO	ISR4321/K9	16.6.2
17	SCB0120	LIBERTADOR BUCARAMANGA	ISR4321/K9	16.6.2
18	SCB0123	CONTROL DE NAVEGACIÓN	ISR4321/K9	16.6.2
19	SCB0124	SUCURSAL PRINCIPAL TUNJA	ISR4321/K9	16.6.2
20	SCB0128	LIBERTADOR PEREIRA	ISR4321/K9	16.6.2
21	SCB0129	SUCURSAL PEREIRA ACE	ISR4321/K9	16.6.2
22	SCB0133	SUCURSAL PRINCIPAL MONTERIA	ISR4321/K9	16.6.2
23	SCB0135	LIBERTADOR POBLADO	ISR4321/K9	16.6.2
24	SCB0136	SUCURSAL LAURELES	ISR4331/K9	16.6.2
25	SCB0137	SUCURSAL PRINCIPAL MANIZALES	ISR4321/K9	16.6.2
26	SCB0142	OFICINA PRINCIPAL OFP	ISR4431/K9	16.6.2
26	SCB0144	SUCURSAL FLORESTA	ISR4321/K9	16.6.2
28	SCB0145	CENTRO MEDICO LIFE	ISR4321/K9	16.6.2
29	SCB0148	SUCURSAL CHICO	ISR4321/K9	16.6.2
30	SCB0150	SUCURSAL CALLE 60	ISR4321/K9	16.6.2
31	SCB0153	AUDITORIA BOLIVAR CCI EDIFICIO DAVIVIENDA	ISR4321/K9	16.6.2
32	SCB0158	SUCURSAL PRINCIPAL CALI	ISR4331/K9	16.6.2
33	SCB0159	SUCURSAL ACE CALI	ISR4321/K9	16.6.2
34	SCB0164	SUCURSAL PRINCIPAL SINCELEJO	ISR4321/K9	16.6.2

35	SCB165	VALLEDUPAR	ISR4321/K9	16.6.2
36	SCB0166	CORREDORES CALI	ISR4321/K9	16.6.2
37	SCB0167	LIBERTADOR CALI	ISR4321/K9	16.6.2
38	SCB0169	PRINCIPAL CARTAGENA	ISR4331/K9	16.6.2
39	SCB0170	SUCURSAL PRINCIPAL CUCUTA	ISR4321/K9	16.6.2
40	SCB0171	SUCURSAL PRINCIPAL NEIVA	ISR4331/K9	16.6.2
41	SCB0173	SUCURSAL ACE MANIZALES	ISR4321/K9	16.6.2
42	SCB0178	PASADENA PARALELO 108	ISR4331/K9	16.6.2
43	SCB0180	PRINCIPAL IBAGUE	ISR4321/K9	16.6.2
44	SCB0181	SUCURSAL ACE MEDELLIN	ISR4321/K9	16.6.2
45	SCB0185	SUCURSAL PRINCIPAL PEREIRA	ISR4321/K9	16.6.2
46	SCB0188	SUCURSAL PRINCIPAL VILLAVICENCIO	ISR4321/K9	16.6.2
47	SCB0191	SUCURSAL PRINCIPAL SANTA MARTA	ISR4331/K9	16.6.2
48	SCB0193	SUCURSAL MEDELLIN CRA 71 (PROSEGUROS)	ISR4321/K9	16.6.2
49	SCB0194	ACE CARTAGENA	ISR4321/K9	16.6.2
50	SCB0196	SUCURSAL SOE MEDELLIN	ISR4321/K9	16.6.2
51	SCB0202	TORRE DAVIVIENDA CENTRO MEDICO SCB0215	ISR4321/K9	16.6.2
52	SCB0219	TORRE BAVARIA	ISR4451-X/K9	16.6.4
53	SCB0285	LIBERTADOR CENTRO COMERCIAL AVENIDA CHILE	ISR4331/K9	16.6.2
54	MC01	MASTER CONTROLLER 1	CSR1000V	16.3.3
55	MC02	MASTER CONTROLLER 2	CSR1000V	16.3.3
56	SCB0023	SUCURSAL PASTO PRINCIPAL	ISR4331/K9	16.6.2
57	SCB0197	HUB ROUTER 11	ISR4451-X/K9	15.5(3)S4b
58	SCB0206	HUB ROUTER 12	ISR4451-X/K9	15.5(3)S4b
59	SCB0209	HUB ROUTER 21	ISR4451-X/K9	15.5(3)S4b
60	SCB0224	HUB ROUTER 22	ISR4451-X/K9	15.5(3)S4b
61	SCB0081	SUCURSAL EL LIBERTADOR TINTAL	ISR4321/K9	16.6.2
62	SCB0025	BARRANCABERMEJA	ISR4321/K9	16.6.2
63	SCB0296	ELEMENTO MPLS	ISR4451-X/K9	16.6.2
64	SCB0298	ELEMENTO INTERNET	ISR4451-X/K9	16.6.2
65	SCB0306	VALLEDUPAR NUEVA	ISR4331/K9	16.6.2
66	SCB0308	SANTAMARTA	ISR4331/K9	16.6.2
67	SCB0325	TORRE CABRERA	ISR4321/K9	15.5(3)S4b

Fuente: "elaboración propia"

El código es un identificador que se utiliza para que el operador en este caso Claro pueda reconocer la ubicación física del servicio, El campo sede indica la forma en la que Seguros Bolívar reconoce la ubicación del servicio, el modelo y la versión con características propias de cada equipo.

6.2 DESARROLLAR UN ASSESSMENT A LA INFRAESTRUCTURA DE RED DE SEGUROS COMERCIALES BOLÍVAR S.A., CON EL OBJETIVO DE EVALUAR Y VALIDAR VULNERABILIDADES Y RIESGOS A LOS QUE PUEDA ESTAR EXPUESTA LA COMPAÑÍA.

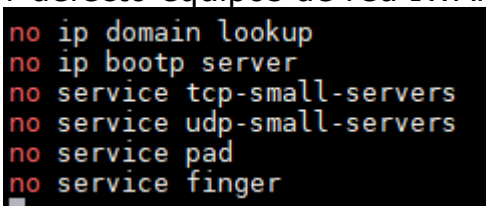
Para esta parte del desarrollo del proyecto se pretende llevar a cabo la fase 3, 4 y 5 de la metodología PTES. En donde se validarán diferentes aspectos de aseguramiento, vulnerabilidades y prácticas que conllevan a mantener lo más seguro posible el acceso a la red empresarial.

6.2.1 Fase 3: modelado de la amenaza.

En primera instancia se requiere verificar que todos los equipos instalados existentes tengan un estándar de aseguramiento y cumplan con ciertas normas y buenas prácticas mínimas para evitar riesgos de acceso no deseado.

No deben existir servicios por defecto habilitados por lo que se realizara la siguiente validación vía interface de comandos ya sea remota o por consola.

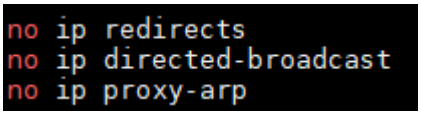
Figura 5. Servicios por defecto equipos de red IWAN.



Fuente: "elaboración propia"

En cuanto a la configuración de interfaces, todas deben cumplir con la siguiente configuración según lo indicado en la Figura 5.:

Figura 6. Servicios en las interfaces



Fuente: "elaboración propia"

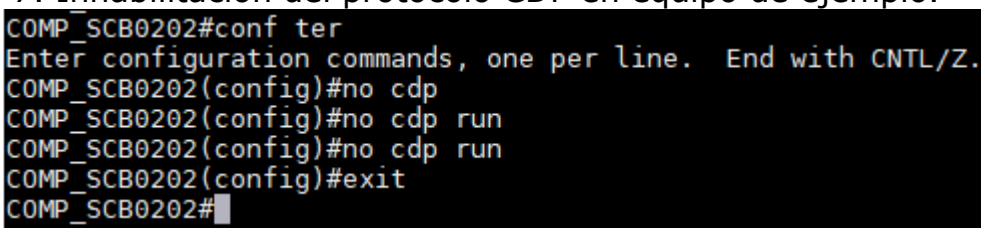
- **IP redirects:** el router enviará un mensaje de redirección si tiene que reenviar un paquete a través de la misma interface por donde lo recibió.

- **Direct Broadcast:** si el router recibe un mensaje de Broadcast, este hará un Broadcast sobre la red a la cual está conectado. Esta es la causa principal de ataques SMURF en Internet.

- **Proxy-ARP:** si el router sabe cómo llegar al destino, este instalara una entrada en la tabla ARP para este destino.

En las interfaces WAN de los equipos no debe estar habilitado el protocolo CDP el cual avisara a los equipos vecinos de esta interface características e incluso IP con la que se está configurando.

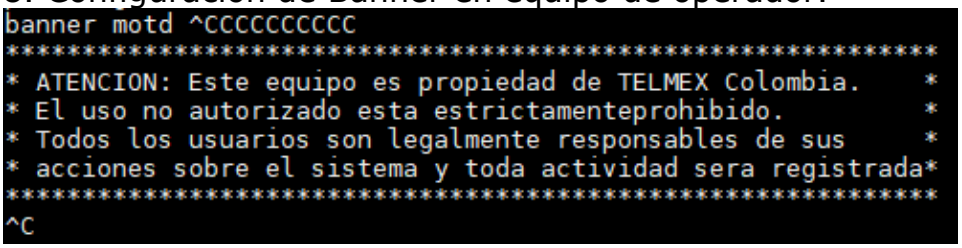
Figura 7. Inhabilitación del protocolo CDP en equipo de ejemplo.



Fuente: "elaboración propia"

Un tema que algunas veces no cobra relevancia y que es controversial en algunos casos es la habilitación de un banner de bienvenida o advertencia ya que si bien en él se puede especificar o advertir a un usuario a donde se está tratando de ingresar y las consecuencias legales que conllevaría hacerlo sin permiso, también se le está indicando indirectamente a un posible atacante que en efecto se está tratando de acceder a un equipo fundamental.

Figura 8. Configuración de Banner en equipo de operador.



Fuente: "elaboración propia"

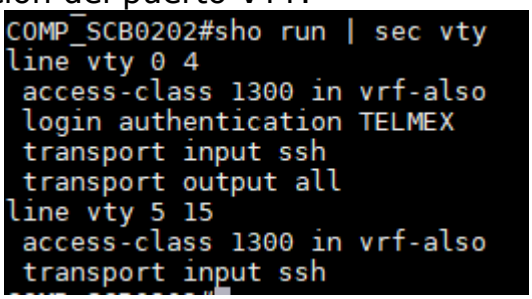
Otra buena práctica que se debe validar es el uso del comando "enable secret" para configurar el password de enable en el router y no el "enable password". El algoritmo de encripción del comando "enable secret" es mucho más seguro y en una sola vía. El "enable password" usa el método de encripción 7, el cual es reversible.

6.2.1.1 Asegurando el acceso al Router

En este apartado se mostrarán algunas herramientas que permiten asegurar el acceso a los routers, tales como el acceso por consola y telnet, la asociación con un AAA server usando TACACS+. La recomendación para el timeout y puerto de consola y VTY se define en un tiempo de 10 minutos 0 segundos.

El acceso por VTY debe ser controlado y no dejarlo abierto. Se permite únicamente desde la red de Gestión: 172.XX.XXX.0/24 y la red WAN que se asignó al CPE. Garantizar además, que se permita el acceso únicamente por SSH.

Figura 9. Configuración del puerto VTY.



Fuente: "elaboración propia"

6.2.1.2 AAA Usando TACACS+

El acceso a la infraestructura de red requiere de un sistema AAA (Authentication, Authorization, Accounting) para asegurar el acceso a los CPEs.

El protocolo TACACS+ está orientado a asegurar la red. A diferencia de RADIUS que encripta solo el password, TACACS+ encripta toda la trama, además de que está usando TCP y no UDP lo cual permite algunas ventajas de trasporte orientado a la conexión, reconocimiento de que los requerimientos han sido recibidos y TCP provee indicación inmediata de la caída de un servidor.

6.2.1.3 Autenticación en caso de caída del servidor AAA TACACS+

Es posible que el router no tenga conectividad con el AAA Server, y en este caso para poder ingresar al router se configura como backup un usuario y password local que solo será utilizado en caso de que el AAA Server este fuera del alcance del router.

De esta forma cuando el AAA no sea alcanzado desde el router, se usará el usuario local <localuser>. En condiciones ideales teniendo TACACS+, no se debería usar ni el usuario local ni el "enable secret", esto solo ocurriría en caso de falla total del TACACS+ o de la pérdida de conectividad hacia el Servidor.

6.2.1.4 Icmp Unreachable Overload

Originalmente los paquetes "ICMP unreachable" que responden los equipos Cisco, son apuntados de la LC / VIP (Line Card / Versatile Interface Processors) al GRP / RP (Gigabit Route Processor / Route Processor).

El resultado era que los recursos de la CPU de GRP / RP podrían ser saturados, únicamente respondiendo "ICMP unreachables". Luego este era un potencial hoyo de seguridad en los equipos para saturarlos fácilmente.

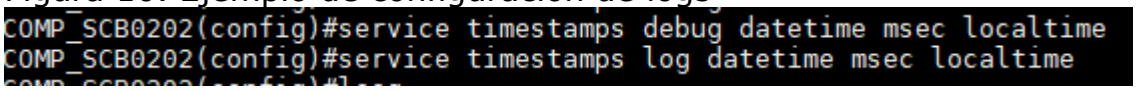
El problema fue resuelto a través de las plataformas basadas en LC / VIP. Ahora las LCs y VIPs manejan los "ICMP unreachables" y el comando "**no ip unreachables**".

Funciona en todas las interfaces. Para la solución de esta red no es tan necesario configurarlo debido al cifrado de tráfico manejado a través de los túneles DMVPN.

6.2.1.5 Prácticas Administrativas Y Operacionales

Los siguientes comandos deben estar configurados en los dispositivos para mejorar las labores de administración y a su vez ser más eficientes en labores operativas sobre los CPEs de Seguros Bolívar.
Se debe habilitar el servicio de log, en un formato claro y estándar para tener detalles de las actividades que suceden en el equipo.

Figura 10. Ejemplo de configuración de logs



Fuente: "elaboración propia"

Así los logs o eventos se presentarán como mensajes de esta forma:

"Apr 30 16:52:54.883: %SYS-5-CONFIG_I: Configured from console by ECF0395A on vty0 (172.31.239.198)
Apr 30 16:53:38.139: %SYS-5-CONFIG_I: Configured from console by ECF0395A on vty0 (172.31.239.198)"

6.2.1.6 Network Time Protocol (NTP)

Todos los equipos deben estar sincronizados con un reloj para de esta forma tener exactitud del momento en que ocurrió algún evento, para esto se usa el protocolo NTP.

Los CPEs se sincronizan con un servidor de gestión. Los CPEs al estar sincronizados en este esquema quedan en stratum 5.

La configuración en los CPEs es la siguiente según:

Figura 11. Configuración de protocolo NTP

```
COMP_SCB0202#sho run | sec ntp
no ntp allow mode control 0
ntp source Loopback47233
ntp server 1[redacted]
```

Fuente: "elaboración propia"

Seria recomendable aplicar el comando ntp update-calendar para que el calendario del CPE sea actualizado por medio del protocolo NTP. (Opcional).

Para verificar que el CPE este con el reloj sincronizado adecuadamente deben ejecutarse los comandos mencionados a continuación y la salida por pantalla es muy parecida a la que se presenta:

Figura 12. Validacion configuracion protocolo NTP.

```
COMP_SCB0202#show ntp associations

  address         ref clock       st   when   poll reach  delay  offset   disp
*~[redacted]       5    985   1024   377  4.910  57.486  1.045
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
```

Fuente: "elaboración propia"

Figura 13. Validacion estado NTP

```
COMP_SCB0202#show ntp status
Clock is synchronized, stratum 6, reference is 17[redacted]
nominal freq is 250.0000 Hz, actual freq is 250.0176 Hz, precision is 2**10
ntp uptime is 235974500 (1/100 of seconds), resolution is 4000
reference time is E1DD78E7.04189380 (10:46:47.016 BOGOTA Thu Apr 30 2022)
clock offset is 57.4866 msec, root delay is 227.99 msec
root dispersion is 672.16 msec, peer dispersion is 1.04 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is -0.000070692 s/s
system poll interval is 1024, last update was 22110 sec ago.
```

Fuente: "elaboración propia"

Todas las versiones de IOS sobre los dispositivos de Seguros Bolívar deberán soportar el comando NTP.

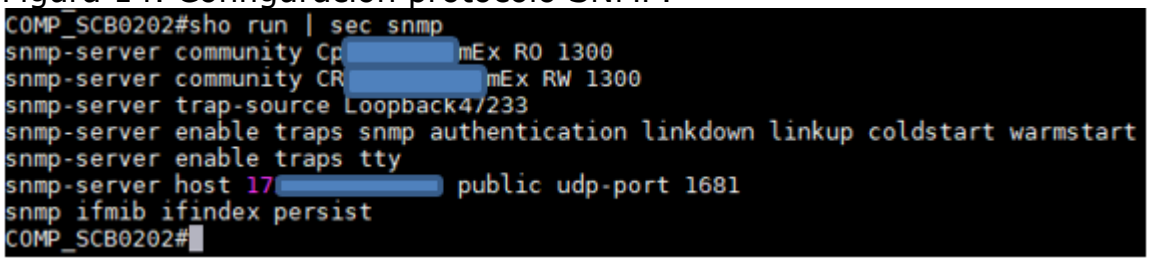
6.2.1.7 Simple Network Management Protocol (SNMP)

Se debe habilitar SNMP sobre los CPEs, creando una comunidad especial para los servidores de Gestión de Claro Colombia asociado a la ACL 1300.

De esta forma se necesita asegurar que cada uno de los dispositivos se encuentre haciendo Polling sobre la herramienta de monitoreo Solarwinds.

Las siguientes son las líneas que deben ser configuradas y garantizadas sobre los CPE´s:

Figura 14. Configuración protocolo SNMP.



Fuente: "elaboración propia"

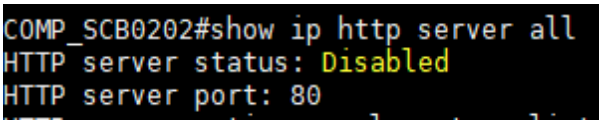
Las líneas de snmp y syslog siempre deben estar configuradas cuando el equipo lo permita.

La línea de config no debe ser configurada en ningún equipo. Este envía traps que no son interesantes para la gestión de un equipo. Además todos los cambios que se hagan sobre los equipos serán registrados en el servidor TACACS+.

6.2.1.8 Servicio HTTP

Los routers Cisco permiten hacer cambios de configuración vía Web. Por defecto no está configurado y así debe estar en los equipos. En caso de que se haya habilitado, este debe ser deshabilitado:

Figura 15. Validación de desconexión de servicio HTTP.



Fuente: "elaboración propia"

6.2.1.9 Técnicas de Filtrado Anti Spoofing

Existen 3 técnicas de filtrado Anti Spoofing en equipos Cisco que son:

A. Listas de acceso estáticas en el borde

Las ACL estáticas son el modo tradicional de asegurar que las direcciones IP fuente de los clientes correspondan con el bloque de Ips permitido. Esta lista permite todo el tráfico cuya IP fuente corresponde a las Ips permitida y bloquea cualquier otro paquete, que incluso podría registrarlo.

B. ACL dinámicas con perfiles AAA

Usadas para cuando los routers tienen autenticación AAA con TACACS+ en servidores donde se almacenan las ACLs sobre interfaces Dial-Up.
En los CPEs de Seguros Bolívar no se tienen generalmente este tipo de ingreso por dial por lo cual NO aplica para el objetivo de este documento y por ende no se entrará en detalles sobre este tipo de ACLs.

C. Modo Estricto usando Unicast Reverse Path Forwarding (URPF).

El método de uRPF es el mejor método para aplicar Anti Spoofing, no requiere de la aplicación de listas ni de tocar los protocolos de enrutamiento.

Se requiere de un solo comando sobre las interfaces donde se quiera aplicar Anti Spoofing. Requiere únicamente que este habilitado el protocolo CEF. Debido a que RPF usa la tabla CEF como ente certificador de cual paquete debe pasar y cuál debe ser bloqueado. Esto indica que la tabla de bloqueo se basa en la de enrutamiento.

El comando para usar en las interfaces es el siguiente:

Figura 16. Configuración comando Anti Spoofing.

```
COMP_SCB0202#conf ter
Enter configuration commands, one per line.  End with CN
COMP_SCB0202(config)#interface vlan 10
COMP_SCB0202(config-if)#ip verify unicast reverse-path
COMP_SCB0202(config-if)#exit
COMP_SCB0202(config)#exit
COMP_SCB0202#
```

Fuente: “elaboración propia”

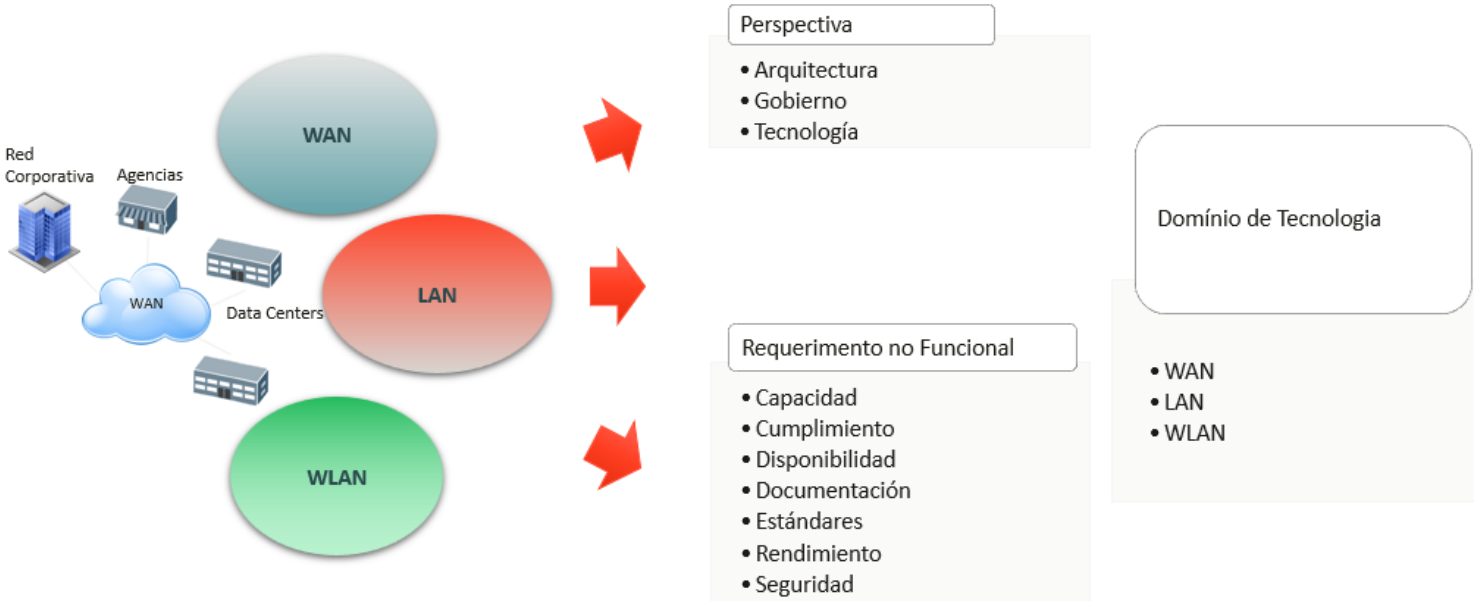
6.2.2 Fase 4. Análisis de vulnerabilidades.

En esta fase se realizará un análisis de las vulnerabilidades aplicando una entrevista a uno de los recursos encargados de la administración de la red en la compañía de Seguros Comerciales Bolívar S.A. el Ingeniero Rodolfo García Meneses, a quien básicamente se aplicaron una serie de preguntas (ver Anexo B) basadas en las buenas prácticas que se deberían tener en una red estándar las cuales al ser analizadas nos entregaran en gran medida las recomendaciones que se entregaran a la compañía, además se pretende

- Alinear el estado actual de la red y sus entornos.
- Identificar potenciales puntos de falla y mejora .
- Direccionar esfuerzos para correcciones críticas.
- Permitir una visión ejecutiva del estado actual.

Para definir el alcance se seleccionaron los ambientes más relevantes para el trabajo, analizados bajo las dimensiones de perspectiva, dominio de tecnología y requerimientos funcionales.

Figura 17. Alcance de la entrevista.

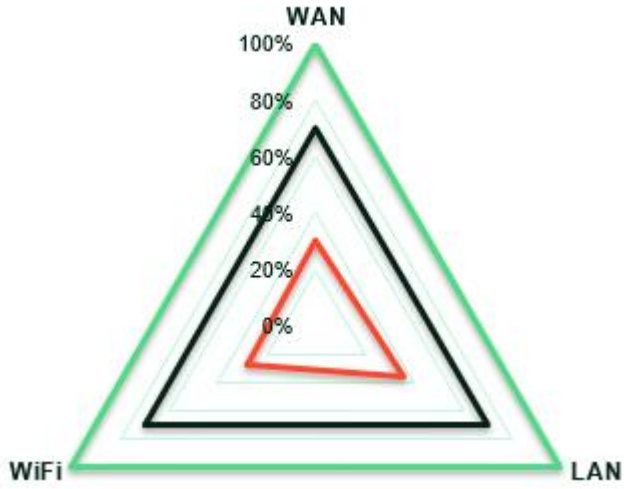


Fuente: "elaboración propia"

6.2.3 Fase 5. Explotación.

Después de aplicada la encuesta y tabular los respectivos puntos en común de cada ámbito de red se identifica un GAP considerable con respecto al promedio de la industria (70%). Existen oportunidades de mejora en los 3 dominios (WAN, LAN y WLAN) que permitirán reducir de manera significativa esta diferencia. A continuación se presenta en la figura 18 como es el estado actual (rojo), y donde está situado el promedio de la industria (negro)

Figura 18. Estado actual de la arquitectura WAN, WLAN y LAN en %.



Fuente: "elaboración propia"

Como parte del análisis se pueden destacar las siguientes oportunidades de mejora o falencias:

- WAN: Infraestructura tecnológica Cisco iWAN que limita el acceso a usuarios remotos y el despliegue ágil de recursos de red en premisas y cloud, deficiencia en el monitoreo y visibilidad a nivel de aplicación y enlaces de comunicaciones, deficiencia en analítica. Infraestructura, enlaces y operación en un modelo de servicios con el Carrier. Oportunidades de mejora con tecnologías SD-WAN y SASE.

- LAN y WLAN: Infraestructura tecnológica Cisco, cada uno de los dominios LAN y WLAN se gestionan por separado y manualmente, no se cuentan con herramientas de gestión para el monitoreo y

despliegue automatizado y centralizado de los servicios de red. Existen deficiencias en el control de acceso a la red (LAN y WLAN). Oportunidad de mejora con tecnologías SD-LAN.

A continuación se exponen los puntos a favor o fortalezas encontradas.

- Alta Disponibilidad: Configuraciones en HA a nivel de la red WAN (CPEs y enlaces redundantes en Sitios Principales), LAN (Core) y WLAN (WLC).

- Infraestructura de Red WAN/LAN/WLAN mono marca: Permite reducir al mínimo problemas de interoperabilidad y facilita la operación y resolución de fallas.

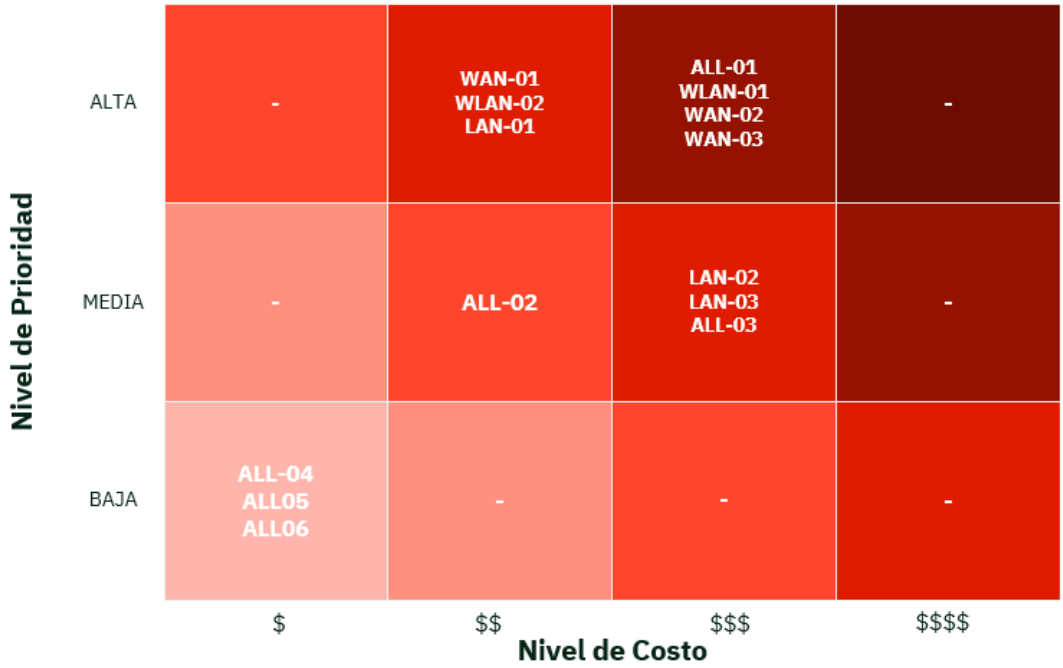
- Tercerización de la Operación LAN/WLAN: Permite disminuir los costos de O&M.

- Protocolos de Routing y Switching: Buenas prácticas y adopción de protocolos estándar, permitiendo la disminución de los problemas causados por los dominios de broadcast.

6.2.4 Fase 6. Post - Explotación.

Cada recomendación hecha como resultado del análisis se transporta a una matriz que puede ser utilizada por el Seguros Comerciales Bolívar S.A. para elegir su estrategia de implementación se puede apreciar en la imagen a continuación, Figura 19.

Figura 19. Matriz Prioridad Vs Costo



Fuente: "elaboración propia"

A continuación se indicará lo que se espera en los ítems de la matriz de la imagen 19, ALL-01, ALL-02, ALL-03, ALL-04, ALL-05, ALL-06, LAN-01, LAN-02, LAN-03, WAN-01, WAN-02, WAN-03, además se indicará la respectiva perspectiva donde tendrán mayor valor cada uno de ellos.

6.2.4.1 ALL- 01 Unificación de la Operación WAN/LAN/WLAN

Perspectivas: Disponibilidad / Performance / Seguridad.

Justificación: La unificación de la operación de las Redes WAN, LAN y WLAN permite tener una visibilidad de toda la red y detectar con mayor exactitud y rapidez el origen de las fallas.
La operación de las Redes WAN, LAN y WLAN, realizada por una empresa externa y experta en servicios administrados IT, garantiza la independencia de los Carriers/ISPs proveedores de los enlaces para un control transparente de los SLAs contratados.
El uso de una herramienta unificada para el control, gestión y monitoreo de las redes WAN, LAN y WLAN permite realizar configuraciones de equipos, políticas y tareas de monitoreo y control de SLAs desde una plataforma centralizada aumentando la eficacia de la O&M.

6.2.4.2 WAN – 01 Migración de canales MPLS a Internet en Sedes Remotas y de Baja Criticidad

Perspectiva: Disponibilidad / Performance.

Justificación: Con la implementación de nuevos modelos de trabajo (presencial, casa, remoto, hibrido, etc.) y el movimiento de cargas hacia AWS en los últimos años, la red de Seguros Comerciales Bolívar S.A. ha enfrentado un crecimiento considerable en el tráfico de Internet y de aplicaciones de video/conferencia, disminuyendo la utilización de los enlaces privados MPLS. La implementación de SD-WAN permitirá hacer uso de múltiples enlaces por sitio y tener control sobre el SLA de los mismos y subutilización de los enlaces MPLS existentes.
La implementación de enlaces de Internet banda ancha, permitirá disminuir los costos totales de adquisición de enlaces en más de un 40%.
Flexibilidad en la escogencia del Carrier / ISPs de preferencia.

6.2.4.3 WLAN – 01 Renovación y Transformación Infraestructura WLAN

Perspectiva: Performance.

Justificación: La movilidad de los usuarios es parte integral de la estrategia de transformación digital de una empresa, el despliegue de una red WLAN de alto rendimiento, aumenta el nivel de satisfacción de los usuarios y la calidad de la experiencia al permitir la conexión de múltiples dispositivos por usuario y permitir su libre movilidad dentro de la oficina.
La implementación de una red WLAN de alto rendimiento y capacidad, utilizando tecnologías de nueva generación WiFI6/6E, permite una reducción de costos, ya que se eliminan o se reducen al máximo las conexiones cableadas.
Una planeación adecuada y un diseño detallado de la red WLAN, teniendo en cuenta múltiples variables como áreas de cobertura, capacidades por dispositivos, cantidad de dispositivos, fuentes de interferencia, obstáculos y tipo de materiales de construcción, permite reducir al mínimo los ajustes o cambios requeridos durante la implementación.
Las redes WLAN de nueva generación, permiten el despliegue ágil de la infraestructura y configuración de equipos y políticas a través de herramientas SDN centralizadas y adicionalmente brindan capacidades de monitoreo y analítica inteligentes útiles para la O&M y el desarrollo del negocio.
Todos los equipos WLAN existentes ya se encuentran End of Sale y algunos modelos End of Support.

6.2.4.4 WAN – 02 Implementación Solución SD-WAN

Perspectiva: Disponibilidad / Performance / Seguridad.

Justificación: SD-WAN permite aprovechar al máximo los recursos de ancho de banda y aumentar el nivel de disponibilidad y performance de la red WAN, adicionalmente es agnóstico a cualquier tecnología de acceso (MPLS, dedicado, Banda Ancha, LTE, etc.) lo que permite flexibilidad y agilidad en el despliegue de nuevos sitios y/o cambios de tipos de enlaces o Carriers/ISPs.

SD-WAN permite aprovisionar y controlar de manera fácil y flexible los recursos de Red WAN y estar alineado con la estrategia de Transformación Digital y Journey to Cloud de Seguros Comerciales Bolívar, asegurando la conexión, disponibilidad, seguridad, monitoreo y visibilidad con diferentes tipos de Clouds. Este elemento es clave para la adopción de esquemas Multicloud, estratégico en la transformación digital. también permite aumentar la calidad de la experiencia del usuario al permitir implementar políticas de tráfico y prioridad a nivel de aplicación.

SD-WAN permite tener un monitoreo eficaz de los SLAs de los enlaces a través de métricas como jitter, packet loss y delay. A través de este monitoreo y medición se puede tener un control de calidad sobre los enlaces adquiridos al ISP/Carrier. También permite la optimización de enlaces para reducir la latencia utilizando tecnologías de aceleración de tráfico, para mejorar performance y aumentar la calidad de la experiencia del usuario a nivel de aplicación. Adicionalmente, este tipo de tecnologías son claves para la adopción de enlaces de Internet.
También permite el despliegue de funcionalidades de seguridad avanzada, como IPS/IDS, filtrado URL, detección de aplicaciones, bloqueo de aplicaciones, conexiones seguras (VPN y cifrado de datos) y antivirus.

6.2.4.5 LAN – 01 Actualización ISE e implementación de Políticas de Seguridad Avanzadas.

Perspectiva: Seguridad.

Justificación: Determinar si los usuarios acceden a la red en un dispositivo autorizado que cumple con las políticas de seguridad.
Establecer la identidad del usuario, la ubicación y el historial de acceso, que se pueden utilizar para el cumplimiento y la generación de informes.
Asignar servicios en función del rol de usuario, el grupo y la política asociada (función de trabajo, ubicación, tipo de dispositivo, etc.).
Otorgar a los usuarios autenticados acceso a segmentos específicos de la red, aplicaciones y servicios específicos, o ambos, según los resultados de la autenticación.
Controlar el acceso de invitados y los recursos de red a los cuales acceden.
Controlar el acceso y la administración de los equipos de red.

6.2.4.6 WLAN – 002 Integración de WLAN con ISE.

Perspectiva: Seguridad.

Justificación: Permitir tener un control de acceso de todos los dispositivos de la red, independientemente de la red o medio desde el que acceden.
Unificar la planeación, configuración y asignación de políticas de seguridad para las Redes LAN y WLAN.

Controlar el acceso de invitados a través del portal cautivo de Cisco ISE.
Controlar el acceso y asignar políticas de seguridad a dispositivos de usuario BYOD.

6.2.4.7 WAN – 03 Evolución a SASE

Perspectiva: Seguridad.

Justificación: SASE permite unificar los servicios de red y seguridad en una arquitectura basada en la nube para proteger a los usuarios, las aplicaciones y los datos en todas partes.
Teniendo en cuenta que muchos usuarios y aplicaciones ya no están en la red corporativa, las medidas de seguridad no pueden depender de los dispositivos físicos convencionales en el perímetro de la red.
SASE garantiza ofrecer la red y la seguridad necesarias como servicios basados en la nube.
SASE permite proporcionar un acceso seguro con independencia de la ubicación de los usuarios, los datos, las aplicaciones o los dispositivos.

6.2.4.8 ALL – 02 Considerar la solución de doble autenticación para todos usuarios MFA.

Perspectiva: Seguridad.

Justificación: Proporcionar seguridad Zero Trust (en español "Confianza cero") a los empleados de una organización.
Establecer la confianza del usuario y verificar la identidad de todos los usuarios antes de que estos accedan a las aplicaciones y recursos.
Proporcionar visibilidad de los dispositivos y permitir a los administradores obtener información detallada de cada tipo de dispositivo que accede a las aplicaciones en todas las plataformas.
Establecer confianza en los dispositivos y verificar que todos los dispositivos corporativos y personales que acceden a las aplicaciones de la empresa son legítimos.
Habilitar el acceso seguro a todas las aplicaciones y ofrecer a los empleados una experiencia de inicio de sesión segura y coherente, tanto para aquellas aplicaciones que se ejecutan en local, como aquellas que corren en la nube.

6.2.4.9 LAN – 02 Renovación Infraestructura de Switches de Acceso.

Perspectiva: Performance.

Justificación: Permitir la integración natural con soluciones WiFi 6/6E a través de interfaces Multigiga.
Soportar el crecimiento del tráfico inalámbrico al adoptar tecnologías WiFi 6/6E.
Los switches de acceso Catalyst 2960-L y Catalys 2960-X no soportan las funcionalidades de la solución Cisco SD-Access (SD-LAN).
Incrementar las capacidades de seguridad, visibilidad y detección de tráfico requeridas por SD-LAN.
Los switches de acceso Catalyst 2960-L y Catalys 2960-X se encuentran End of Sale.

6.2.4.10 LAN – 03 Implementación Solución SD-LAN.

Perspectiva: Performance.

La red de acceso es el punto más crítico de productividad de las organizaciones, las redes de acceso actual se aprovisionan manualmente, es muy complejo asegurarla, controlar el acceso a los usuarios y tener visibilidad del tráfico, todo esto hace muy difícil brindar la misma experiencia y calidad a los diferentes usuarios de la red cableada, inalámbrica y remotos.
Beneficios:

- Gestión consistente de políticas y el aprovisionamiento de redes LAN y WLAN que asegura la experiencia de usuarios.
- Capacidad de programación, automatización y la visibilidad unificada ofrece reducciones en OPEX y CAPEX.
- Defensa integrada contra amenazas al permitir que un usuario sospechoso esté "en cuarentena" en toda la red.
- Segmentación automatizada de la red y política basada en grupos. Tráfico separado con segmentación de extremo a extremo.
- Analítica para identificar y resolver proactivamente los problemas de seguridad, además de ayudar la planificación de capacidad.

6.2.4.11 ALL – 03 Convergencia WAN/LAN/WLAN (SD-Branch).

Perspectiva: Performance.

Justificación: Permitir el despliegue de soluciones de SD-WAN y SD-LAN a través de una solución convergente.
Permitir la definición y despliegue de políticas de seguridad a nivel de usuario y de manera unificada y global.
Disminuir la complejidad de la O&M y facilitar la detección y recuperación de fallas.

6.2.4.12 ALL – 04 Homologación y Estandarización de Soluciones

Perspectiva: Disponibilidad / Performance / Seguridad.

Justificación: Poner a prueba a través de un proceso de homologación las soluciones que se requieren implementar. Estandarizar las soluciones y definir las funcionalidades requeridas para cada solución. Tener un criterio de evaluación técnico acertado y permitir la comparación entre diferentes proveedores y/o fabricantes.

6.2.4.13 ALL – 05 Proceso de Documentación de la Red.

Perspectiva: Documentación.

Justificación: Mejorar la documentación con procesos formales, apoyados con herramientas, garantiza el acceso a la información detallada de toda la infraestructura de red. Esto ayuda a todos los equipos de trabajo a comprender el funcionamiento y ser mucho más ágiles en el momento de la detección de una falla por la caída de los servicios o la disminución del performance.

6.2.4.14 ALL – 06 Actualización y Estandarización de los OS y Firmwares de los equipos de Red.

Perspectiva: Documentación.

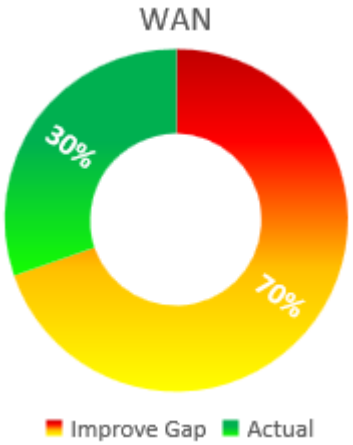
Justificación: El disponer de una plataforma de equipos de la misma familia (Modelo) con los OS y Firmware actualizados y con la versión estable disponible por el fabricante, garantiza una mínima exposición a bugs y vulnerabilidades de seguridad que se traducen en mayor disponibilidad.

El mantener homogénea las versiones de SW de los equipos de redes ofrece una mejor gestión y simplificación al momento de hacer troubleshooting y administración de la infraestructura de redes.

6.3 ELABORAR EL INFORME RESULTADO DEL ASSESSMENT SEGÚN EL NIVEL DE RIESGO E IMPACTO SOBRE LA INFORMACIÓN DE LA COMPAÑÍA DE ACUERDO CON LA AFECTACIÓN EN CUANTO A DISPONIBILIDAD, CONFIDENCIALIDAD E INTEGRIDAD, INDICANDO LOS HALLAZGOS REALIZADOS SOBRE LOS ACTIVOS DE RED BASADOS EN BUENAS PRÁCTICAS.

6.3.1 Fortalezas y Puntos Bien Ejecutados en la red WAN

Figura 20. Mapa de puntos de mejora VS estado actual de la red WAN.



Fuente: "elaboración propia"

- La red WAN cuenta con una infraestructura homogénea basada 100% en tecnología Cisco iWAN.

- Estandarización de protocolos de enrutamiento y operación tercerizada gestionada por el ISP.

- Actualmente no se cuenta con tecnología SDN pero esta puede ser parte de la estrategia de transformación digital y no se descarta la adopción de SD-WAN en la próxima renovación.

- Actualmente se están utilizando diferentes tipos y combinaciones de enlaces como MPLS, internet dedicado y Banda Ancha dependiendo de la importancia, los niveles de disponibilidad y criticidad de los sitios. Se está observando el comportamiento de los enlaces de Banda Ancha con respecto a los niveles de disponibilidad y latencia para aplicaciones críticas del negocio.

- Las cargas se encuentran distribuidas entre nube pública (AWS) y DC en premisas (Celta). El uso de enlaces de internet (DIA o Banda Ancha) es adecuado para este tipo de arquitectura de nube, permitiendo salir localmente hacia la nube pública.

- Se cuenta con un enlace MPLS y AWS Direct Connect de 1Gbps para la comunicación de DC en premisas (Celta) y AWS.

6.3.2 Puntos de mejora en la red WAN.

- No hay agilidad en el despliegue de nuevos sitios y/o cambios en las políticas de tráfico.

- No hay control ni monitoreo de los SLA’s de los enlaces.

- No hay monitoreo del tráfico y aplicaciones en la red WAN.

- Subutilización de enlaces WAN MPLS por aumento de la utilización de enlaces de Internet.

- Subutilización de los enlaces WAN de backup, solamente se utilizan en caso de contingencia.

- Subutilización del enlace de backup (Banda Ancha) hacia AWS, solamente se utiliza en caso de contingencia y la conmutación es manual.

- La interconexión con AWS se realiza a través de un enlace tradicional MPLS y Direct Connect, no hay una integración nativa ni visibilidad del enlace MPLS con Cisco iWAN.

- Se están presentando cuellos de botella en la red por el incremento de usuarios remotos y el uso de aplicaciones en la nube y de videoconferencia.

- La red WAN es una red tradicional, el provisionamiento y configuración de los equipos se realiza de forma manual y aún no se han implementado tecnologías SDN.

- El Carrier (Claro) es el proveedor de los enlaces de comunicaciones (MPLS, DIA, Banda Ancha) y a su vez tiene a cargo la operación red

WAN y el suministro como servicio de las plataformas y herramientas tecnológicas de infraestructura.

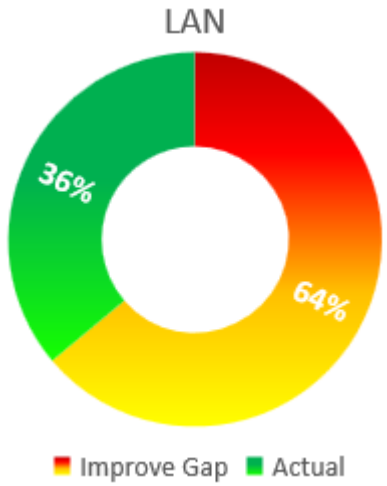
- Los enlaces WAN Principales y de Backup son proporcionados por un único proveedor (Claro).

- No se tiene acceso a herramientas para el control de los SLAs, monitoreo y visibilidad de los enlaces, tráfico y aplicaciones en la red WAN.

- Gestión de la documentación.

6.3.3 Fortalezas y Puntos Bien Ejecutados LAN.

Figura 21. Mapa de puntos de mejora VS estado actual de la red LAN.



Fuente: "elaboración propia"

- La red LAN cuenta con una infraestructura homogénea basada 100% en tecnología Cisco: Core: Catalyst C9500, Acceso: Catalyst 2960L y Catalyst 2960X, CISCO ISE.

- La capa de Core está implementada con 2 switches Cisco Catalyst 9500-16X) configurados en HA y tienen esquema de soporte y garantía extendida 7x24 garantizando la disponibilidad de la capa de Core.

- Integración con Cisco ISE e implementación de 802.1X.
- Los switches C9500 soportan características y permiten evolución a SD-LAN.

- Las capacidades de la RED LAN están bien dimensionadas y no se experimentan cuellos de botella en el tráfico en el escenario actual.

- Uso adecuado de protocolos estándar a nivel de capa 2 y capa 3 para la prevención y control de loops y tormentas de broadcast.

- Operación tercerizada permitiendo la reducción de los costos y aumentando la eficiencia y agilidad de la O&M (Organización y Métodos).

6.3.4 Puntos de mejora en la red LAN.

- La red LAN es una red de switches tradicional, la configuración o cambios sobre los equipos de red se realiza manualmente.

- No se tiene acceso a herramientas de gestión y monitoreo centralizadas.

- No hay una integración real a nivel de las redes LAN y WLAN, la operación, configuración y cambios sobre cada red se hace de manera manual e independiente.

- La integración con Cisco ISE solamente aplica para implementar políticas de 802.1x.

- No se tienen implementadas políticas de postura ni de identificación de endpoints.

- No es posible realizar un despliegue de políticas de seguridad y de tráfico de manera uniforme y centralizada para las redes LAN y WLAN.

- No es posible asignar políticas de tráfico y QoS a nivel de usuario y aplicación.

- No se tiene una segmentación de la Red para permitir o bloquear el acceso de los recursos de red a nivel de usuario/grupo.

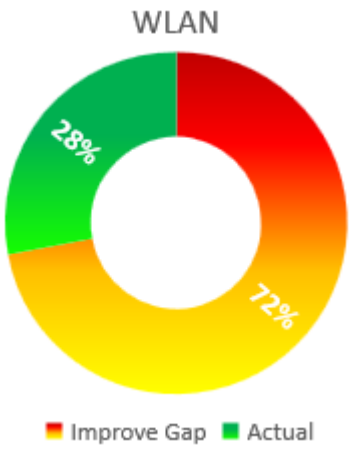
- No se tienen herramientas para el análisis del tráfico de la red LAN que permitan tener visibilidad a nivel de usuario, endpoint y aplicación.

- Se debe evaluar las capacidades de los switches de la red LAN antes de implementar una solución inalámbrica con tecnologías de nueva generación como WiFI6/6E y soportar el crecimiento exponencial del tráfico WLAN.

- Gestión de la documentación.

6.3.5 Fortalezas y Puntos Bien Ejecutados WLAN.

Figura 22. Mapa de puntos de mejora VS estado actual de la red WLAN.



Fuente: "elaboración propia"

- La red WLAN cuenta con una infraestructura homogénea basada 100% en tecnología Cisco: WLC: Cisco 5508, AP's de los modelos: AIR-CAP3502I, AIR-CAP3702I y AIR-AP2802I.

- Los controladores WLAN se encuentran implementados en una arquitectura centralizada y en configuración HA garantizando la disponibilidad de red WLAN.
- La red WLAN tiene configuradas 3 SSID para diferenciar y darle diferentes tipos de acceso a los usuarios: Red VIP, Red Corporativa, Red Invitados.

- Operación tercerizada permitiendo la reducción de los costos y aumentando la eficiencia y agilidad de la O&M (Organización y Métodos).

6.3.6 Puntos de mejora para la red WLAN

- No se tiene implementada una solución de NAC / 802.1X para la autenticación de los endpoints que acceden a la red WLAN.

- No se tiene implementada una solución de análisis de postura para el control de las políticas de seguridad de los endpoints que acceden a la red WLAN.

- No se tiene implementada una solución de identificación de los endpoints que se conectan a la red de WLAN.

- No se tienen implementadas políticas de seguridad robustas para permitir el acceso de los visitantes a la Red.

- La red de visitantes se accede a través de un SSID configurado con una contraseña.

- No existen políticas de hardening ni cambio de contraseñas.

- No se tienen herramientas para el análisis del tráfico de la red WLAN que permitan tener visibilidad a nivel de usuario, endpoint y aplicación.

- Las tareas de configuración de la Red WLAN se realizan de manera manual a través de la controladora centralizada.

- No hay una integración real a nivel de las redes LAN y WLAN, la operación, configuración y cambios sobre cada red se hace de manera manual e independiente.

- No existe una planeación adecuada para el despliegue de la red WLAN, no se realizan simulaciones, análisis de espectro ni capacidad.

- La Red WLAN no tiene la capacidad para reemplazar las conexiones de acceso cableado para tener un ambiente Full Wireless que permita la movilidad de los endpoints.

- Gestión de la documentación.

6.3.7 Proyectos recomendados a desarrollar.

Finalmente después de recopilar toda la información del assessment de red de la compañía y conocer el estado de su red LAN, WAN y WLAN, se pueden hacer algunas sugerencias de proyectos que mejorarían algunos aspectos de su infraestructura.

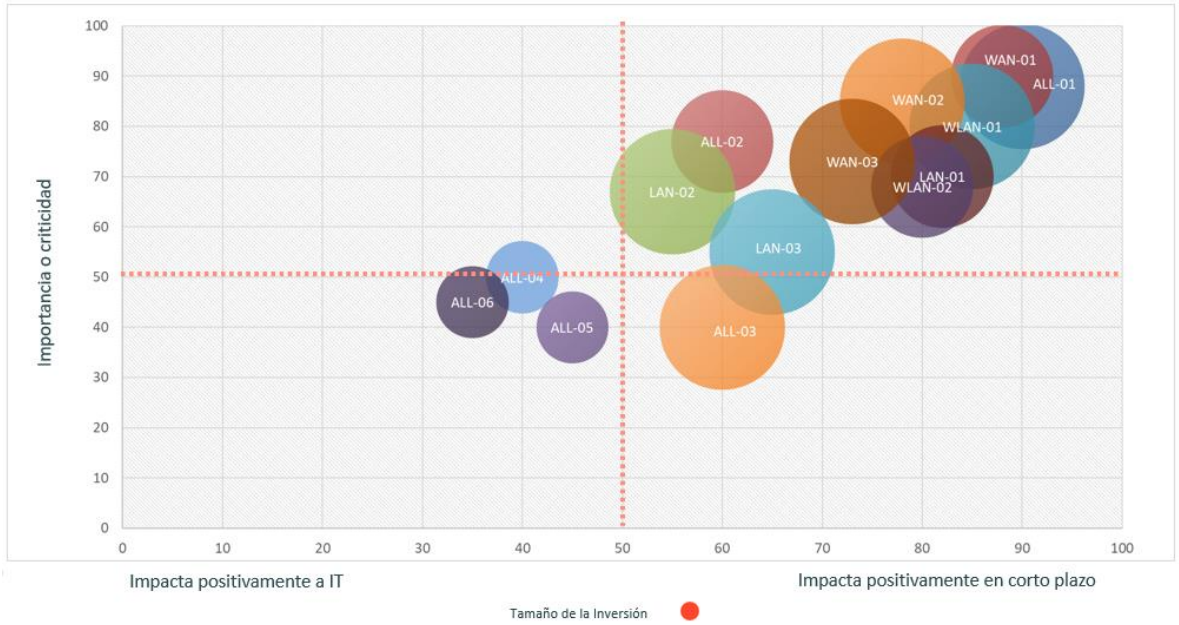
De estos proyectos algunos tendrán una mayor relevancia e impacto que otros y algunos estarán correlacionados con otros, es decir que en su ejecución se pueden dar fases y algunas deben estar alineadas y ejecutadas antes de iniciar el siguiente proyecto.

Cuadro 3. Lista de proyectos sugeridos

No.	ID	Ambiente	Perspectiva	Sugerencia	Prioridad	Servicios/HW-SW	$
1	ALL-01	ALL	Disponibilidad/Performance/Seguridad	Unificación de la Operación WAN/LAN/WLAN	Alta	Labor	$$$
2	WAN-01	WAN	Disponibilidad/Performance	Migración de canales MPLS a Internet en Sedes Remotas y de Baja Criticidad	Alta	Labor/Inversión	$$
3	WLAN-01	WLAN	Performance	Renovación Infraestructura WLAN	Alta	Labor/Inversión	$$$
4	WAN-02	WAN	Disponibilidad/Performance/Seguridad	Implementación Solución SD-WAN	Alta	Labor/Inversión	$$$
5	LAN-01	LAN	Seguridad	Actualización ISE e implementación de Políticas de Seguridad Avanzadas	Alta	Labor/Inversión	$$
6	WLAN-02	WLAN	Seguridad	Integración de WLAN con ISE	Alta	Labor/Inversión	$$
7	WAN-03	WAN	Seguridad	Evolución a SASE	Alta	Labor/Inversión	$$$
8	ALL-02	ALL	Seguridad	Implementación Solución de doble autenticación para todos usuarios MFA	Media	Labor/Inversión	$$
9	LAN-02	LAN	Performance	Renovación Infraestructura de Switches de Acceso	Media	Labor/Inversión	$$$
10	LAN-03	LAN	Disponibilidad/Performance/Seguridad	Implementación Solución SD-LAN	Media	Labor/Inversión	$$$
11	ALL-03	ALL	Performance	Convergencia WAN/LAN/WLAN (SD-Branch)	Media	Labor/Inversión	$$$
12	ALL-04	ALL	Disponibilidad/Performance/Seguridad	Homologación y Estandarización de Soluciones	Baja	Labor	$
13	ALL-05	ALL	Documentación	Proceso de Documentación de la Red	Baja	Labor	$
14	ALL-06	ALL	Disponibilidad/Performance/Seguridad	Actualización y Estandarización de los OS y Firmwares de los equipos de Red	Baja	Labor	$

Fuente: "elaboración propia"

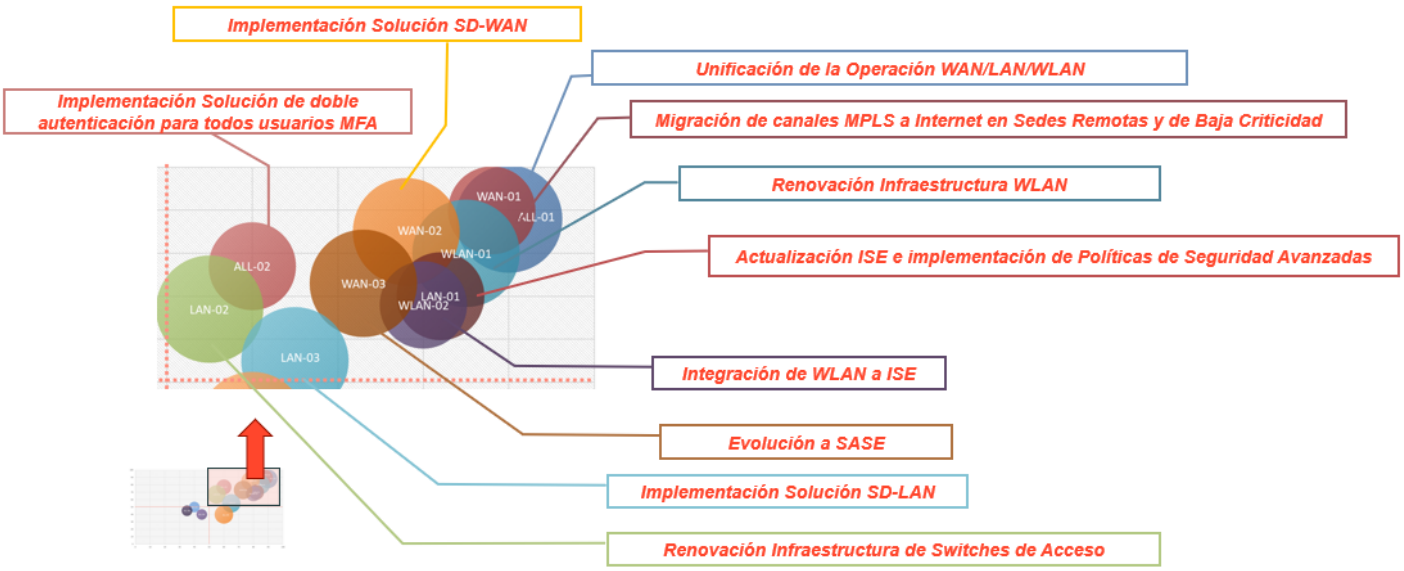
Figura 23. Análisis proporcional de recomendaciones de Impacto al negocio e IT



Fuente: "elaboración propia"

En la figura anterior Figura 23, se hace una distribución de los proyectos sugeridos en una escala entre 0 a 100 en el orden vertical argumentando la importancia o criticidad, y en el eje horizontal se les dio un valor estimado estimando el impacto positivo y de corto plazo al que dieran lugar.

Imagen 24. Vista detallada del cuadrante superior derecho de la imagen 23.



Fuente: "elaboración propia"

En la imagen anterior se da un mayor detalle del cuadrante del extremo derecho positivo de las recomendaciones del negocio, adicional se indican cuales son cada uno de los proyectos que están dentro de esta ubicación.

7 CONCLUSIONES

Gestión y documentación de activos de red:
Una deficiencia crucial en la red de Seguros Comerciales Bolívar S.A. es la falta de actualización y documentación de inventarios de equipos de red, como Access Points y Switches. No existe un registro preciso de las cantidades ni de las ubicaciones físicas de estos equipos, lo que dificulta el acceso y la validación del tráfico de la red tanto de manera física como remota. La ausencia de mapas topológicos y de conexiones, así como de información sobre propagación y cantidades de VLAN, dificultan aún más la visibilidad y el control de la red. Para abordar este problema, se debe implementar un sistema de gestión de activos de red actualizado y completo, que incluya:

a) Un inventario detallado de todos los dispositivos de red, incluyendo información sobre ubicaciones físicas y lógicas, así como datos de configuración y estado.

b) Mapas topológicos y de conexiones que reflejen la arquitectura actual de la red, facilitando la identificación de puntos críticos y la planificación de actualizaciones y mejoras.

c) Un registro de VLANs y segmentos de red, que permita una mejor comprensión de la propagación y el flujo de tráfico en la red.

Configuraciones por defecto y prácticas de seguridad:
Las configuraciones por defecto en los dispositivos activos de red presentan riesgos de seguridad significativos, ya que a menudo no se modifican ni desactivan. Estas configuraciones pueden incluir protocolos inseguros, contraseñas predeterminadas y puertos abiertos que pueden ser explotados por atacantes. Para mejorar la seguridad de la red, es necesario endurecer las configuraciones y reemplazar los protocolos inseguros. Algunas recomendaciones incluyen:

a) Reemplazar protocolos inseguros como Telnet y HTTP por sus contrapartes más seguras, como SSH y HTTPS, para garantizar la confidencialidad y la integridad de las comunicaciones en la red.

b) Cambiar las contraseñas predeterminadas en todos los dispositivos y aplicaciones, utilizando contraseñas únicas y robustas, y establecer

políticas de rotación de contraseñas para garantizar la seguridad a largo plazo.

c) Cerrar o restringir los puertos abiertos innecesarios en los dispositivos de red y utilizar listas de control de acceso (ACL) para limitar el tráfico a aquellos servicios y protocolos necesarios para el funcionamiento de la red.

d) Implementar una política de parches y actualizaciones de seguridad para garantizar que todos los dispositivos de red estén protegidos contra vulnerabilidades conocidas y que se apliquen rápidamente las actualizaciones de seguridad pertinentes.

Fortalezas en la diversificación de enlaces:
A pesar de los problemas mencionados, el análisis de la red de la compañía reveló ciertas fortalezas, como el uso de diferentes tipos y combinaciones de enlaces (MPLS, Internet dedicado e Internet de Banda Ancha) según la importancia y criticidad de las oficinas remotas. Esta diversificación permite a la empresa adaptar la conectividad y la disponibilidad de la red a las necesidades específicas de cada ubicación. Sin embargo, para aprovechar al máximo estos enlaces y garantizar una mayor seguridad, se recomienda:

a) Implementar políticas de seguridad y redundancia específicas para cada tipo de enlace, garantizando que cada conexión esté protegida de manera adecuada y que la información se transmita de forma segura.

b) Monitorear de manera activa el rendimiento y la disponibilidad de los enlaces, identificando posibles cuellos de botella y áreas de mejora en la infraestructura de la red.

c) Evaluar la necesidad de agregar enlaces redundantes en ubicaciones críticas para garantizar la continuidad del negocio en caso de fallos en la conectividad.

Limitaciones y obsolescencia de la tecnología Cisco iWAN:
La infraestructura tecnológica basada en Cisco iWAN presenta desafíos en términos de obsolescencia y limitaciones en la implementación de elementos de seguridad. Entre los problemas identificados se encuentran la falta de respaldo adecuado por parte del fabricante, limitaciones en el monitoreo y la visibilidad a nivel de aplicación y enlaces de comunicación, y dificultades en la operación con el Carrier. Estos problemas afectan el

acceso de usuarios remotos y la eficiencia en la gestión de recursos de red en premisas y en la nube. Para abordar estos desafíos, se sugiere:

a) Evaluar la posibilidad de migrar a tecnologías más recientes y eficientes, como SD-WAN y SASE, que ofrecen una mayor flexibilidad, seguridad y visibilidad en la red.

b) Implementar soluciones de monitoreo y análisis en tiempo real que permitan una visión más profunda del rendimiento y la salud de la red, facilitando la identificación de problemas y la toma de decisiones basadas en datos.

c) Establecer políticas y procedimientos claros para la actualización y el mantenimiento de la infraestructura de red, incluyendo la evaluación regular de nuevas tecnologías y soluciones que puedan mejorar la eficiencia y la seguridad.

d) Integrar soluciones de seguridad avanzadas, como sistemas de detección y prevención de intrusiones (IDS/IPS), control de tráfico, filtrado de contenido y prevención de pérdida de datos (DLP), para garantizar una protección completa de la red y los activos de la empresa.

Capacitación y concienciación en seguridad informática:
Uno de los aspectos clave para mejorar la seguridad de los activos tecnológicos de red es garantizar que los empleados y los responsables de la administración de la red estén debidamente capacitados y conscientes de las prácticas de seguridad adecuadas. Se recomienda implementar programas de capacitación y concienciación en seguridad informática que incluyan:

a) Capacitación regular para los administradores de red y otros empleados responsables de la gestión y el mantenimiento de la infraestructura de red, con énfasis en la identificación y mitigación de riesgos, la aplicación de políticas de seguridad y la respuesta a incidentes.

b) Campañas de concienciación en seguridad informática para todos los empleados, abordando temas como la importancia de utilizar contraseñas seguras, la identificación de correos electrónicos de phishing y la protección de la información confidencial.

c) Establecer canales de comunicación claros para la denuncia y la respuesta a incidentes de seguridad, asegurando que los empleados sepan a quién informar en caso de sospechas o problemas de seguridad.

Para mejorar la seguridad de los activos tecnológicos de red en Seguros Comerciales Bolívar S.A., es necesario abordar las áreas de mejora identificadas en este análisis, incluyendo la gestión de activos de red, la personalización de configuraciones, el fortalecimiento de las conexiones WAN y la migración hacia tecnologías más actuales. Además, es esencial capacitar y concienciar a los empleados sobre las prácticas de seguridad informática adecuadas. Al implementar estas medidas, la empresa podrá garantizar una infraestructura de red más segura y eficiente, protegiendo sus activos y manteniendo la continuidad del negocio.

8 RECOMENDACIONES

- Se recomienda hacer marcación física de los equipos de red activos dentro de los centros de datos, para poder así identificarlos de una mejor manera.
- Se recomienda tener un repositorio con el inventario accesible a los involucrados de la custodia para que puedan modificarlo y siempre este actualizado de acuerdo con las modificaciones realizadas.
- Se recomienda validar uno a uno los equipos inventariados para corroborar que se encuentren configurados de acuerdo con las buenas prácticas sugeridas.
- No hay una integración real a nivel de las redes LAN y WLAN, la operación, configuración y cambios sobre cada red se hace de manera manual e independiente.
- Se recomienda unificar la operación de las Redes WAN, LAN y WLAN, manteniendo un único punto de contacto y control, para aumentar el desempeño de la red y agilizar la resolución de fallas en todos los ámbitos.
- Se recomienda que la operación de las Redes WAN/LAN/WLAN sea realizada por una empresa externa y experta en servicios administrados de infraestructura IT, diferente de los Carriers/ISPs proveedores de los enlaces de comunicaciones, para poder garantizar el performance de la red, tiempos de respuesta, acceso a las herramientas de monitoreo y control de los SLAs.
- Se recomienda una migración progresiva de enlaces MPLS a enlaces de Internet banda ancha en sitios de baja criticidad de la Red y conforme a los resultados experimentados en los sitios que actualmente se han migrado y están bajo observación.
- Se recomienda siempre el despliegue de enlaces redundantes en todos los sitios.
- Se recomienda implementar una solución WLAN de alto rendimiento y capacidad, utilizando tecnologías de nueva generación como WiFi6/6E, para reducir al máximo las conexiones cableadas y permitir un escenario Full Wireless que permita garantizar la movilidad de los usuarios dentro de las oficinas.
- Se recomienda realizar una planeación adecuada y diseño detallado de la red WLAN, utilizando herramientas de simulación y medición RF profesionales.
- Basado en el análisis técnico realizado de la red WAN y considerando los nuevos modelos de trabajo implementados y la cantidad de oficinas/sucursales que actualmente tiene Seguros

Bolívar, se recomienda implementar tecnología SD-WAN, con enlaces redundantes en todas las sedes y utilizar diferentes tipos de tecnologías de acceso como MPLS, internet dedicado, Banda Ancha y/o LTE, de acuerdo con la criticidad de los sitios y provisionados por dos o más Carriers/ISPs. Esto permitirá la agregación del ancho de banda entre diferentes enlaces, mayor disponibilidad, visibilidad y performance. Adicionalmente, permite reducir las tareas y costos de O&M al tener una única plataforma de gestión para la configuración de las políticas de priorización de tráfico, seguridad, administración y monitoreo.

- Se recomienda actualizar la plataforma NAC Cisco ISE e implementar funcionalidades de seguridad adicionales al control de acceso a través de 802.1x.
- Se recomienda adquirir las licencias requeridas para implementar funcionalidades de authentication, authorization, accounting (AAA), postura, perfilamiento, control de acceso de invitados, descubrimiento y asignación de políticas basadas en tipo de terminal, asignación de políticas basadas en usuario y grupos de usuarios y TACACS para el control de la administración de equipos de red.
- Integrar y ampliar el alcance de la solución de "Network Access Control" con Cisco ISE a la red WLAN, para asegurar y controlar el acceso de todos los dispositivos inalámbricos a la red, para un control de acceso convergente y unificación de políticas de seguridad de LAN y WLAN.
- Se recomienda implementar y evolucionar a una solución SASE alineada con las políticas de ciberseguridad y la estrategia de transformación digital.
- Se recomienda implementar una solución de doble autenticación para todos usuarios, para el acceso a servicios y/o aplicaciones críticas, para mejorar y aumentar la seguridad interna.
- Se recomiendo renovar los switches de acceso por equipos con capacidades de puertos MultiGiga.
- Se recomienda implementar switches con capacidades SDN para evolución a SD-LAN.
- Se recomienda implementar una solución SD-LAN que permita despliegue automático de configuraciones y políticas, segmentación a nivel de usuario, monitoreo y visibilidad de tráfico avanzados y reducción de riesgos de seguridad originada por los usuarios internos.

- Se recomienda implementar una solución convergente WAN/LAN/WLAN tipo SD-Branch que permita el control, gestión, monitoreo y visibilidad unificados.
- Se recomienda implementar una política para estandarizar y homologar las soluciones como parte del proceso de selección de proveedores y previo a la implementación de cualquier solución.
- Mejorar y formalizar un proceso de documentación, que permita actualizar la documentación de conectividad e incluir diagramas lógicos.
- Implementar un proceso de proceso de actualización y homogenización de OS y Firmware de los equipos de redes, el cual se ejecute periódicamente validado con los fabricantes respectivos, para evitar la exposición a bugs y vulnerabilidades

9 BIBLIOGRAFÍA

ADVANCED IP SCANNER – Explorador de redes de descarga gratuita. (s. f.). advanced. [Sitio web], 2015 [Consultado 18 de abril 2022]. Disponible en: https://www.advanced-ip-scanner.com/es/

AREVALO Ochoa, Adrián P. Gobierno de Seguridad de la Información, un enfoque hacia el cumplimiento regulatorio. Revista Tecnológica-ESPOL, [En Línea] Cuenca, (Ecuador), 15 de noviembre de 2015 [Consultado 20 de abril 2022] disponible en: http://rte.espol.edu.ec/index.php/tecnologica/article/view/373/258

BLOGSPOT. Metodología PTES (Penetration Testing Execution Standard). [Sitio web]. Colombia: [Consulta: 07 de abril 2022]. Disponible en http://blogdeauditoriadeseguridad.blogspot.com/2017/09/metodologia-ptes-penetration-testing.html.

BOISSON MORALES, N. Aplicación de la metodología PTES en la clínica Medellín para la identificación de vulnerabilidades en historia clínica electrónica. [Sitio web] [Consultado 6 de abril 2022]. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/40837/nboissonm--.pdf?sequence=3&isAllowed=y

BERDUGO SIERRA, Helber Alirio. Importancia de definir la infraestructura critica en Colombia. [En línea]. Tesis de especialización. Universidad Militar Nueva Granada. [Consultado: 14 de abril de 2022]. Disponible en: https://repository.unimilitar.edu.co/bitstream/handle/10654/14342/BerdugoSierraHelber%20Alirio2016.pdf?sequence=1&isAllowed=y

CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES. Tendencias del Cibercrimen en Colombia 2019–2020. CCIT [Sitio web], 2019 [Consultado 9 de abril 2022]. Disponible en: https://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/

CASTRO, M. I. R., Morán, et al. (2018). Introducción a la seguridad informática y el análisis de vulnerabilidades (Vol. 46). 3Ciencias [En Linea] 3ciencias [Consultado 20 de abril 2022] disponible en: https://books.google.es/books?hl=es&lr=&id=5Z9yDwAAQBAJ&oi=fnd&pg=PA29&dq=Introducci%C3%B3n+a+la+seguridad+inform%C3%A1tica+y+el+an%C3%A1lisis+de+vulnerabilidades&ots=ymuVBZj7Nx&sig=

ynVaFH7rLi37UoL9ZVtcqAsQJo0#v=onepage&q=Introducci%C3%B3n%20a%20la%20seguridad%20inform%C3%A1tica%20y%20el%20an%C3%A1lisis%20de%20vulnerabilidades&f=false

COLOMBIA, CONGRESO DE LA REPUBLICA, Ley 1581 (17 de octubre de 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. En: Diario Oficial Alcaldía de Bogotá, [Sitio web] Disponible en: https://bibliotecadigital.ccb.org.co/bitstream/handle/11520/13629/Ley%201581%20de%202012.pdf?sequence=1

COLOMBIA, CONGRESO DE LA REPUBLICA, Ley 1273 de 2009. (05 de enero de 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Senado de la Republica. [Sitio web] disponible en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

COLOMBIA. MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO. Decreto 1074 (26, mayo, 2015). Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio,
Industria y Turismo. [Sitio web] Disponible en: http://wp.presidencia.gov.co/sitios/normativa/decretos/2015/Decretos2015/DECRETO%201523%20DEL%2016%20DE%20JULIO%20DE%202015.pdf

COLOMBIA. CONSEJO NACIONAL DE POLITICA ECONÓMICA Y SOCIAL DE COLOMBIA. Conpes 3701de 2011: Lineamientos de política para la Ciberseguridad y Ciberdefensa. [Sitio Web]. Disponible en: https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

COLOMBIA. CONSEJO NACIONAL DE POLITICA ECONÓMICA Y SOCIAL DE COLOMBIA. Op. Cit. P. 41. Conpes 3654 de 2016. [Sitio Web] Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

FREIRE LÓPEZ, K. B. Estudio y análisis de ciberataques en América Latina, su influencia en las empresas del Ecuador y propuesta de políticas de

ciberseguridad. [Sitio web], 2019 [Consultado 8 de abril 2022]. Disponible en: http://repositorio.ucsg.edu.ec/handle/3317/9203

FUNCION PUBLICA, Ministerio TIC. [Sitio Web] Bogotá. Guía para la administración del riesgo y el diseño de controles en entidades públicas. [Consultado 30 de marzo de 2022] Disponible en: https://dapre.presidencia.gov.co/oci/normograma/Guia-administracion-riesgo-diseno-controles-entidades-publicas.pdf

GAMBOA SUAREZ, J. L. Importancia de la seguridad informática y ciberseguridad en el mundo actual. [Sitio web], 2020 [Consultado 16 de abril 2022]. Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/8668/IMPORTANCIA%20DE%20LA%20SEGURIDAD%20INFORM%c3%81TICA%20Y%20CIBERSEGURIDAD%20EN%20EL%20MUNDO%20ACTUAL.pdf?sequence=1&isAllowed=y

GARCÍA PÉREZ, Kevin Alexis. Aplicación de hacking ético mediante test de intrusión Pentesting para la detección y análisis de vulnerabilidades en la red inalámbrica de una institución educativa de la provincia de Santa Elena. [En línea]. Trabajo de investigación. Universidad Peninsular Estatal de Santa Elena 2021 [Consultado 20 abril 2022] Disponible en: https://repositorio.upse.edu.ec/handle/46000/5855

KASPERSKY. (2020). Seguridad de la información a través de las cifras de pérdidas. [Sitio Web] Kaspersky Team [Consultado 24 de marzo 2022] Disponible en: https://latam.kaspersky.com/blog/security-economics-2019/17854/

KASPERSKY. (2021). Ciberataques en América Latina crecen un 24% durante los primeros ocho meses de 2021. [Sitio Web] Kaspersky Team [Consultado 24 de marzo 2022] Disponible en: https://latam.kaspersky.com/blog/ciberataques-en-america-latina-crecen-un-24-durante-los-primeros-ocho-meses-de-2021/22718/

KOSÉVICH, Ekaterina Yu. Estrategias de seguridad cibernética en los países de América Latina. Iberoamérica. [En Línea] Federación Rusa, 18 de noviembre de 2019 [Consultado 20 de abril 2022] disponible en: https://www.researchgate.net/profile/Ekaterina-Kosevich/publication/340419950_Cyber_Security_Strategies_of_Latin_America_Countries/links/5eac0008a6fdcc70509e07c7/Cyber-Security-Strategies-of-Latin-America-Countries.pdf

MAROTO, J. P. (2009). El ciber espionaje y la ciberseguridad. In La violencia del siglo XXI. Nuevas dimensiones de la guerra (pp. 45-76). Instituto Español de Estudios Estratégicos. [En Linea] Unirioja [Consultado 20 de abril 2022] disponible en: https://dialnet.unirioja.es/descarga/articulo/4549946.pdf

NICKERSON, Chris, et al. Penetration Testing Execution Standard. [Sitio web], 2014 [Consultado 16 de abril 2022]. Disponible en: http://www.pentest-standard.org/index.php/Main_Page

OSPINA DÍAZ, Milton. R., y SANABRIA Rangel, Pedro. E. Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. Revista Criminalidad. [En línea]. Bogotá (Colombia). Vol. 62, nro. 3 [Consultado 03 de abril 2022]. Disponible en: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1794-31082020000200199

RAVELO ALFONSO, Rosmely. Material complementario basado en mecanismos de seguridad de routers. [En línea]. Tesis Doctoral. Universidad Central "Marta Abreu" de Las Villas. 2015 [Consultado 03 de abril 2022]. Disponible en: http://dspace.uclv.edu.cu:8089/handle/123456789/4476

RODRIGUEZ GAHONA, G. Análisis comparativo de los modelos defensa en profundidad y mspi, para la implementación de la seguridad informática en el sector privado del país. [En Línea] Monografía especialización seguridad informática, Universidad Nacional Abierta y a Distancia, 2020 [Consultado 20 de abril 2022] disponible en: https://repository.unad.edu.co/bitstream/handle/10596/38717/grodriguezgah.pdf?sequence=1&isAllowed=y

RODRÍGUEZ VÁSQUEZ, Elkin Germán, et al. Definición de una metodología personalizada de hacking ético para empresas públicas de Cundinamarca SAESP y ejecución de una prueba a la página web ya los servidores de la entidad, soportada sobre la metodología definida. [En línea]. Trabajo de Investigación. Universidad Católica, 2019. [Consultado 10 de abril 2022] Disponible en: https://repository.ucatolica.edu.co/handle/10983/23377

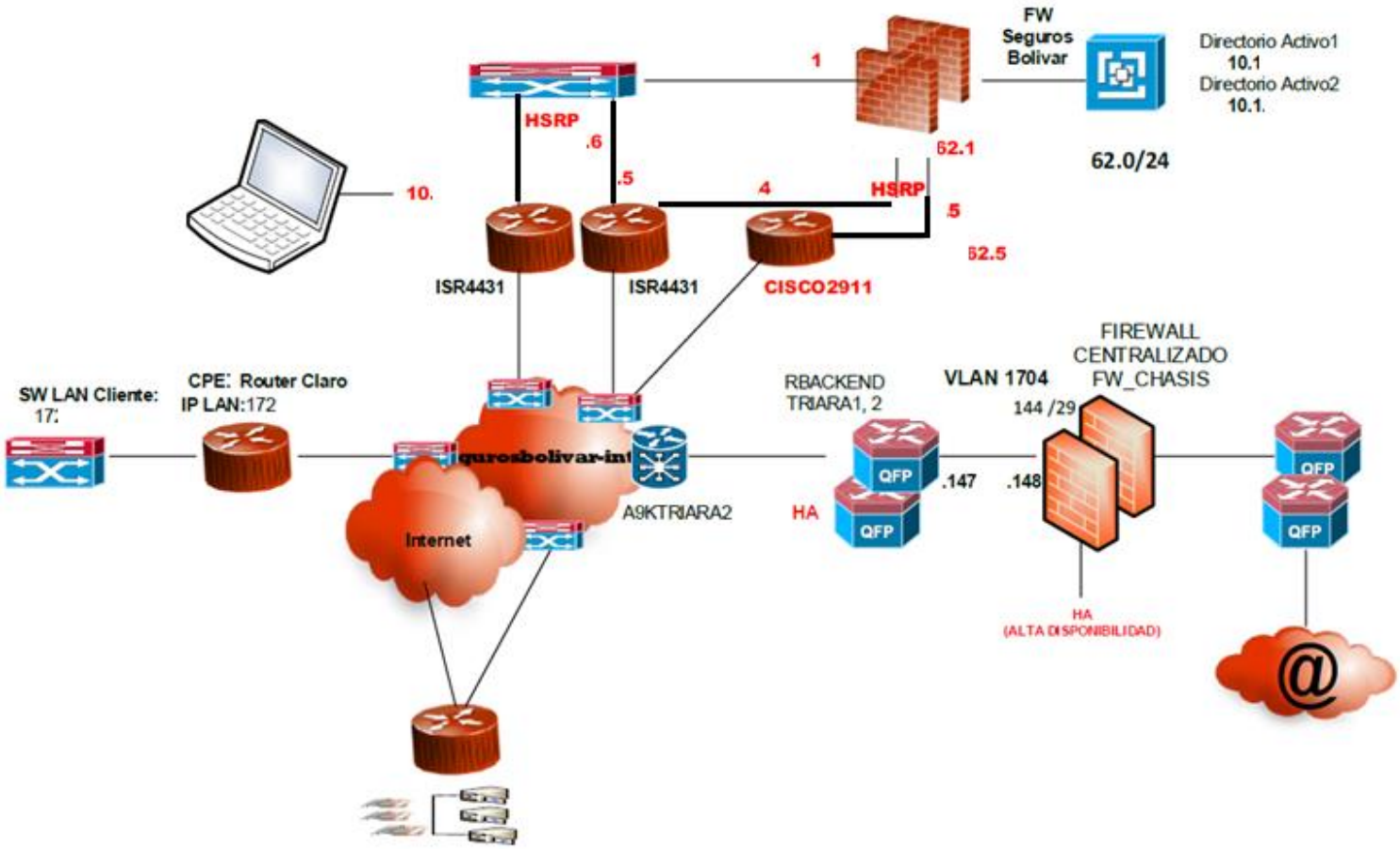
SABILLÓN, R., & Cano, J. J. Auditorías en Ciberseguridad: Un modelo de aplicación general para empresas y naciones. Revista Ibérica de Sistemas

e Tecnologías de Informação, [Sitio web], 2019 [Consultado 16 de abril 2022]. Disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/124326/1/Sabillon_RISTI_Auditorias_Ciberseguridad.pdf

UNAD. (s.f). Universidad Nacional Abierta y a Distancia. [Sitio web] Bogotá: ECBTI – Alternativas para grado. [Consulta 06 de abril 2022] Disponible en: https://academia.unad.edu.co/ecbti/oferta-academica/alternativas-para-grado

ANEXOS

Anexo A. Topología General de interconexión en datacenter de la red IWAN



Anexo B. Preguntas de entrevista.

Tabla Anexo B.

	Mejores Prácticas de Red	WAN	Corporative (Wifi, LAN)
1	Hay un proceso bien definido para revisar las opciones de arquitectura de redes para cada nuevo ciclo de inversiones observándose la mejor relación costo operacional, escalabilidad y consumo de instalaciones	3 – Sí, siempre	3 – Sí, siempre
2	El principal driver de adopción de nuevas inversiones nunca se basa únicamente en costo	3 – Sí, siempre	3 – Sí, siempre
3	Es una política el mantenimiento preventivo de equipos activos, módulos de control, tarjetas, SFPs, fuentes de potencia, módulos de refrigeración, etc … en duplicidad con los servicios de soporte y garantía	1 – No	1 – No
4	Existe un entorno y un proceso de homologación para nuevas soluciones, separadas del entorno productivo con el fin de estándarizar las tecnologías requeridas en producción	4 – No sé decir	4 – No sé decir
5	El espacio físico y la energía no son problemas o preocupaciones para nuestros entornos	3 – Sí, siempre	3 – Sí, siempre
7	Se tiene una estandarización de fabricantes para cada capa o función desempeñada en nuestra red	3 – Sí, siempre	3 – Sí, siempre
8	Tenemos una estandarización y tipificación de equipos activos para cada capa o función realizada en nuestra red	2 – La mayoría de las veces sí	2 – La mayoría de las veces sí
9	Tenemos una política de actualización de sistema operativo / firmware de equipos activos de red que analiza tendencias, históricos, problemas y se anticipa a futuros bugs y / o riesgos de seguridad	2 – La mayoría de las veces sí	2 – La mayoría de las veces sí
10	Tenemos una homogeneización de sistemas operativos que nos permite garantizar que nuestro ambiente tenga menos exposiciones a los riesgos de indisponibilidad por bugs o interoperabilidad	2 – La mayoría de las veces sí	2 – La mayoría de las veces sí
11	La red soporta la demanda existente y no tenemos puntos críticos de "cuellos de botella''	2 – La mayoría de las veces sí	3 – Sí, siempre

15	La latencia no es un problema para la red actual	2 – La mayoría de las veces sí	3 – Sí, siempre
16	Existe una arquitectura bien definida de Interconexión de redes que aísla dominios de capa 2 reduciendo el dominio de fallas	3 – Sí, siempre	3 – Sí, siempre
17	Existen procedimientos bien definidos para evitar Loops de Layer 2	3 – Sí, siempre	3 – Sí, siempre
18	Para cualquier nuevo proyecto de TI, el equipo de redes siempre está involucrado desde su concepción	1 – No	1 – No
19	Ninguna nueva tecnología de redes es puesta en producción, sin antes ser homologada y probada en entornos de prueba, separados de la red de producción	2 – La mayoría de las veces sí	2 – La mayoría de las veces sí
20	Hay una clara visión hacia dónde debemos llevar nuestra arquitectura de redes para obtener mejores resultados con menores costos	1 – No	1 – No
21	Todos los enlaces uplinks de la red LAN se mantienen activos gracias a la tecnología y la arquitectura utilizadas (abstracción de protocolo Spanning-Tree)	0 – No aplicable	3 – Sí, siempre
22	La sobresuscripción entre las capas de la arquitectura fue dimensionada pensando de en los niveles de tráfico este-oeste y norte-sur.	3 – Sí, siempre	3 – Sí, siempre
23	Hay una documentación actualizada y confiable de la topología física y lógica de nuestra red	2 – La mayoría de las veces sí	2 – La mayoría de las veces sí
24	La capa de ruteo entre Vlans está bien definida, documentada, y predice siempre la mejor trayectoria con la latencia más baja posible.	2 – La mayoría de las veces sí	2 – La mayoría de las veces sí
25	La arquitectura de firewalls está estandarizada, documentada y permite el crecimiento horizontal (cluster) si es necesario	3 – Sí, siempre	3 – Sí, siempre
27	El tráfico entre servidores es bien conocido y documentado para facilitar cualquier cambio en la configuración de firewalls y balanceadores.	0 – No aplicable	3 – Sí, siempre
34	La arquitectura de enrutamiento de la red interna está bien definida, documentada y permite que sólo se utilice un protocolo de enrutamiento	2 – La mayoría de las veces sí	3 – Sí, siempre
35	En la arquitectura de red LAN se consideran enlaces redundantes desde la capa de Acceso hacia los Switches de Agregación/Core	0 – No aplicable	3 – Sí, siempre

36	El uso de virtualización de tablas de rutas (VRF) siempre se utiliza para aislar entornos con overlaps de direcciones y todos en la organización saben utilizarlo	1 – No	1 – No
37	No hay entornos con enrutamiento asimétrico	3 – Sí, siempre	3 – Sí, siempre
39	Las técnicas de DdoS son fácilmente detectadas y las amenazas mitigadas	4 – No sé decir	4 – No sé decir
40	Existe una política de segmentación de Líneas de negocio y protección de perímetros protegidos por firewalls que a continuación se documenta y se conoce	3 – Sí, siempre	3 – Sí, siempre
41	La configuración de los elementos de firewall sigue una política formal de construcción de reglas	4 – No sé decir	4 – No sé decir
42	Hay una rutina bien definida para la limpieza, reordenación y consolidación de reglas de firewall	4 – No sé decir	4 – No sé decir
43	La arquitectura de protección perimetral está estandarizada, documentada y satisface las necesidades de escalabilidad y simetría del tráfico	2 – La mayoría de las veces sí	2 – La mayoría de las veces sí
44	Nuestro entorno de redes está preparado para satisfacer las futuras demandas de IPV6	1 – No	2 – La mayoría de las veces sí
45	La virtualización de elementos de red siempre se utiliza para optimizar el uso de recursos físicos (VDC, VRF, contextos, tenants, etc.)	2 – La mayoría de las veces sí	2 – La mayoría de las veces sí
46	Las segmentaciones en VLAN se documentan y no hay overlaps de identificadores (VLAN ID)	2 – La mayoría de las veces sí	2 – La mayoría de las veces sí
47	La versión de Spanning-tree usada está estandarizada, documentada, tiene el menor tiempo de convergencia posible y todos en la operación saben manipular	0 – No aplicable	2 – La mayoría de las veces sí
48	Cuando usamos STP, tenemos el control de Root Bridges/BPDU para mantener la mejor topología activa para el entorno	0 – No aplicable	4 – No sé decir
49	Cuando usamos el STP, tenemos el control de instancias distintas (PVST/MSTP) con diversos grupos Vlan para permitir que todos los trunks permanezcan activos	0 – No aplicable	4 – No sé decir
50	Nuestra arquitectura de red define claramente el límite de dominio de la Capa 2 y la Capa 3 y todo está documentado	2 – La mayoría de las veces sí	2 – La mayoría de las veces sí
51	Todo el tráfico de la Red WAN (MPLS, Internet) es cifrado y se utilizan VPN para la interconexión de sitios.	2 – La mayoría de las veces sí	0 – No aplicable

52	Una política de QoS está aplicada a todos los elementos y atiende las necesidades de trafico de las diversas necesidades de negocio y servicios corporativos	2 – La mayoría de las veces sí	1 – No
53	En la arquitectura de red WAN se considera el uso de doble enlace y también doble CPE en sitios que requieran Alta Disponibilidad	3 – Sí, siempre	0 – No aplicable
54	El nivel de broadcast y flooding está controlado o nunca ha sido responsable de la degradación de los servicios	4 – No sé decir	4 – No sé decir
55	Existe una red aislada para el tránsito entre DMZ's con interés de tráfico común	3 – Sí, siempre	3 – Sí, siempre
56	Nuestras herramientas de gestión están bien configuradas, con OID correctamente elegidos según las recomendaciones de cada fabricante de elementos de red	4 – No sé decir	4 – No sé decir
58	Algunas aplicaciones de negocio utilizan tráfico de Multicast, mientras la infraestructura de red y sus componentes están configurados para soportar este tipo de tráfico.	1 – No	1 – No
60	Tenemos una clara política de BYOD que está reflejada en el control de acceso a la información y el uso de dispositivos móviles	0 – No aplicable	1 – No
61	NAC y 802.1x son ampliamente difundidos en nuestra red corporativa y se adhieren a la política de seguridad	1 – No	1 – No
62	Cuenta con mecanismos de doble autenticación para los usuarios remotos, para el acceso a servicios y/o aplicaciones críticas	1 – No	1 – No
63	Los enlaces WAN están dimensionados para soportar el tráfico actual y cumplir los requisitos de negocio	2 – La mayoría de las veces sí	0 – No aplicable
64	El SLA de aplicaciones en oficinas remotas es medido y controlado para garantizar la mejor experiencia de los usuarios	1 – No	0 – No aplicable
65	El consumo de electricidad es monitoreado y siempre optimizado	1 – No	1 – No
66	Tenemos una arquitectura de DMZ exclusiva y protegida para conectar oficinas remotas a nuestro centro de datos	3 – Sí, siempre	0 – No aplicable
67	La infraestructura de red utiliza técnicas de overlay para virtualizar la red	1 – No	1 – No
68	Nuestro modelo de gestión operacional utiliza herramientas para	1 – No	1 – No

	aprovisionamiento / orquestación de recursos de red		
69	El tiempo de provisión de servicios de redes no es limitante para el lanzamiento de nuevos proyectos y servicios de áreas demandantes	2 – La mayoría de las veces sí	2 – La mayoría de las veces sí
70	La arquitectura de redes permite la interconexión entre las sucursales y DCs con los servicios públicos y privados de Cloud	3 – Sí, siempre	3 – Sí, siempre
72	La capa de acceso a la red solo tiene conectividad para elementos de servidor, impresoras, Wireless Aps y dispositivos de usuario final. (ningún otro elemento de red se conecta)	1 – No	1 – No
73	La distribución de bloques de direcciones IP permite resumir las tablas de enrutamiento IGP	4 – No sé decir	0 – No aplicable
74	La distribución de direcciones IP internas permite una segmentación de ambientes sin uso de traducciones por overlapping	3 – Sí, siempre	3 – Sí, siempre
75	Las tecnologías utilizadas actualmente le permiten escalar de forma segura en términos de MAC, rutas y VLAN	3 – Sí, siempre	3 – Sí, siempre
76	Los filtros de MAC / rutas y técnicas de manipulación manual de enrutamiento (PBR por ejemplo) se controlan y se utilizan como último recurso	3 – Sí, siempre	0 – No aplicable
77	La arquitectura de DC / LAN de la red actual o que se implementará en el futuro, sigue el concepto de Fabric-Networks y todos del equipo ya están preparados para soportarla	0 – No aplicable	1 – No
80	Tenemos una red Wifi con cobertura suficiente para satisfacer las necesidades de movilidad	0 – No aplicable	2 – La mayoría de las veces sí
81	Existen características aplicadas para contener broadcasts excesivos así como ofertas de DHCP indebidas	4 – No sé decir	4 – No sé decir
82	Hay una documentación de directiva de seguridad de redes basada en un Plan director de Seguridad, y estas políticas se reflejan en las mejores prácticas de configuración y protección por segmento de red	2 – La mayoría de las veces sí	2 – La mayoría de las veces sí
83	La red Wifi tiene segmento separado para visitantes y las redes Wifi-corporativas poseen filtros de tráfico y mecanismos de	0 – No aplicable	2 – La mayoría de las veces sí

	autenticación y encriptación adecuados para cada tipo de dispositivo		
84	Conocemos la base instalada y tenemos una política de cambio de equipos activos tan pronto como se encuentren en End-of-X.	2 – La mayoría de las veces sí	2 – La mayoría de las veces sí
85	La red WiFi tiene mecanismos de detección y mitigación de ataques específicos inalámbricos (WIPS) y presencia de Aps	0 – No aplicable	4 – No sé decir
86	La red tiene mecanismos de protección contra tráfico de comportamiento malintencionado, malware de red, correo electrónico spam, sitios web comprometidos y se realiza una administración BDA. (Antes, durante, después), permitiendo la identificación de ataques y el tratamiento rápido usando procedimientos y herramientas	1 – No	1 – No
87	La red de usuarios (Campus LAN) permite solamente el acceso de usuarios autorizados y hay control para el acceso de visitantes.	0 – No aplicable	1 – No
88	Los eventos y los registros de seguridad se supervisan y se almacenan para el análisis periódico, generando acciones correctivas y mejoras.	3 – Sí, siempre	3 – Sí, siempre
89	Existe una trazabilidad detallada (usuario, fecha, comando, equipo) para habilitar la auditoría de red.	1 – No	1 – No
90	El número de certificados digitales es grande (>100) y hay soluciones para automatizar la administración de CA, claves y certificados.	4 – No sé decir	0 – No aplicable
91	Los equipos de red se configuran constantemente para ser adecuados a un modelo de Hardening previamente definido.	1 – No	1 – No
92	El plan de direccionamiento Ipv4 actual está correctamente planificado, con subredes distribuidas según los segmentos lógicos/VLAN en uso y hay espacio para futuras expansiones	3 – Sí, siempre	3 – Sí, siempre
93	El uso de direcciones Ipv4 no presenta conflictos de direcciones incluso en la condición de direccionamiento estático, con documentación y control de uso.	2 – La mayoría de las veces sí	2 – La mayoría de las veces sí
94	El servicio DHCP se aplica a todos los segmentos de red excepto a los servidores	3 – Sí, siempre	3 – Sí, siempre

95	El plan de IP *adresses* hace uso de direcciones de dominio público RFC 1918	3 – Sí, siempre	3 – Sí, siempre
96	El control de la asignación y el uso de direcciones IP está automatizado e integrado con el servicio DHCP (IPAM)	3 – Sí, siempre	3 – Sí, siempre
97			
99	Nuestro objetivo es aprovechar el potencial de SDN utilizando continuamente nuestra capacidad de desarrollo interno y, por lo tanto, reducir los costos operativos	0 – No aplicable	0 – No aplicable
100	Los Beacons y los servicios de localización se utilizan como diferenciales en nuestras estructuras remotas, apoyando estrategias de campaña, fidelización y conocimiento del cliente	0 – No aplicable	0 – No aplicable
101	Se realizó un análisis de consolidación de infraestructura del entorno de TI (servidor, almacenamiento, red, Seguridad, movilidad) con el fin de optimizar y reducir la cantidad de equipos físicos y los respectivos costos de capex y opex.	1 – No	1 – No
102	El Proceso/Tiempo de configurar equipos de red para cumplir con nuevos sistemas no está afectando al negocio o se está habilitando de manera más ágil	1 – No	1 – No
103	Tenemos una política de renovación de equipos basada en fechas de End-of-Life/Support del fabricante	1 – No	1 – No
104	Nuestros sistemas analizan periódicamente las vulnerabilidades de red con la ayuda de herramientas adecuadas.	1 – No	1 – No
105	Nuestros protocolos de enrutamiento dinámico están protegidos por mecanismos de autenticación.	4 – No sé decir	4 – No sé decir
106	Entendemos que la política de reducción de costos CAPEX y OPEX la Red no debe comprometer la seguridad de esta y el desarrollo normal del negocio	3 – Sí, siempre	3 – Sí, siempre
107	Existen errores de aprovisionamiento pero no generan incidentes que afecten a nuestro SLA	2 – La mayoría de las veces sí	2 – La mayoría de las veces sí
108	Ya hay movimientos en otras áreas dirigidas a la adición de Software-Defined-Environment.	2 – La mayoría de las veces sí	1 – No
109	El uso de VNF (conectividad, L4-L7, etc.) es amplio y está dominado por los equipos de arquitectura, despliegue y operación	0 – No aplicable	0 – No aplicable
110	El Sponsor de TI líder y las áreas adyacentes de la red conocen y	1 – No	1 – No

	comprenden los beneficios de las soluciones SDN		
112	Los Equipos de conectividad existentes (Switches y Routers físicos y/o virtuales) admiten tecnologías SDN y se pueden aprovisionar a través de protocolos como OpenFlow, OpFlex y otros que están estandarizados	1 – No	1 – No
113	Los equipos de servicios L4-L7 existentes (Firewalls, Balanceadores de carga, físicos y/o virtuales y otros) admite tecnologías SDN que se pueden aprovisionar a través de protocolos como OpenFlow, OpFlex y otros estandarizados	0 – No aplicable	0 – No aplicable
114	Hay inspecciones de tráfico Este-oeste	0 – No aplicable	1 – No
115	El proceso de cambio está claro, bien documentado y seguido por las áreas involucradas	2 – La mayoría de las veces sí	2 – La mayoría de las veces sí
116	Existe un inventario de redes (elementos físicos y virtuales, acceso físicas y lógicas) y es actualizado periódicamente	2 – La mayoría de las veces sí	2 – La mayoría de las veces sí
117	Los SLAs de aprovisionamiento, rendimiento y disponibilidad de la infraestructura están definidos por ambiente / aplicación y son regularmente monitoreados (tiempo real y / o reportes)	2 – La mayoría de las veces sí	0 – No aplicable
118	Hay una política de control de acceso a la consola del equipo, con una fuerte autenticación y definición de niveles de privilegios adecuados para la operación	4 – No sé decir	4 – No sé decir
119	Utilizamos herramientas de gestión de aprovisionamiento para reducir los errores operativos y el tiempo de configuración de los routers en la WAN	1 – No	0 – No aplicable
120	Hay una plataforma unificada de gestión de la WAN que realiza la detección de fallas y la administración de rendimiento de los enlaces proporcionando visibilidad de los SLAs contratados (disponibilidad, jitter, latencia, packet)	2 – La mayoría de las veces sí	0 – No aplicable
121	La red WAN permite el uso simultáneo de enlaces y el tráfico de cada aplicación se asigna dinámicamente en cada enlace de acuerdo con el SLA de cada aplicación	1 – No	0 – No aplicable
122	Hay aplicaciones de vídeo en las Branches y utiliza políticas en la red WAN para controlar y prevenir el consumo excesivo de ancho de banda	1 – No	0 – No aplicable

123	Existe una libertad contractual junto a los proveedores actuales de enlaces y hoy cualquier tecnología de última milla puede ser utilizada	3 – Sí, siempre	0 – No aplicable
124	El acceso a Internet está disponible en las sucursales y existen soluciones de seguridad alineadas con el plan director de seguridad de la información (PDSI) para evitar accesos indebidos	3 – Sí, siempre	0 – No aplicable
125	Se utilizan soluciones de aceleración de aplicaciones para reducir el consumo de banda y la latencia y mejorar el tiempo de respuesta al usuario	1 – No	0 – No aplicable
126	Nuestra arquitectura de aplicaciones requiere servidores en sucursal, y utiliza soluciones para optimizar la infraestructura de TI remota, como la virtualización de servidores y los servicios de red	0 – No aplicable	0 – No aplicable
128	Utilizamos aplicaciones de virtualización de escritorio (VDI Citrix o VMware, por ejemplo) y la red tiene el tamaño y la configuración adecuada para transportar este tráfico (ancho de banda, latencia, QoS)	0 – No aplicable	0 – No aplicable
129	Se puede realizar la administración del CPE de las sucursales o branches, y cambiar la política de enrutamiento de forma ágil para satisfacer las necesidades del negocio	1 – No	0 – No aplicable
130	La convergencia de los servicios de medios de video remota utiliza la estructura de TI sin afectaciones en la red.	2 – La mayoría de las veces sí	0 – No aplicable
131	Se tiene control sobre los dispositivos de usuario a nivel navegación cuando están en trabajo remoto (Home Office)	4 – No sé decir	4 – No sé decir
132	La arquitectura de WLAN a través de un controlador central está estandarizada e integrada en los sistemas de autenticación y autorización corporativos	0 – No aplicable	1 – No
133	Nuestra red WLAN identifica y actúa sobre dispositivos indebidamente instalados	0 – No aplicable	1 – No
134	La información analítica de consumo WLAN (como la ubicación y el tiempo de uso) se utilizan para tomar decisiones de negocio y áreas de apoyo	0 – No aplicable	0 – No aplicable
136	Existen herramientas para la recolección de tráfico en la red LAN corporativa y que lo analizan con fines de capacidad de planificación y detección de anomalías	0 – No aplicable	1 – No

137	La red LAN corporativa tiene microsegmentación, controlando la política de acceso a cada aplicación basada en la identidad del usuario y en las características del dispositivo de acceso (modelo y ausencia de parches)	0 – No aplicable	1 – No
138	La microsegmentación en la LAN corporativa permite a los administradores gestionar las políticas de acceso a la red.	0 – No aplicable	1 – No
139	Existen soluciones de protección de contenido en el perímetro, incluyendo seguridad de correo electrónico corporativo y navegación Web (URL y DNS query)	3 – Sí, siempre	3 – Sí, siempre
140	La red del Data Center tiene protección en 2 capas de Firewall, usando diferentes fabricantes en cada capa	2 – La mayoría de las veces sí	2 – La mayoría de las veces sí
141	Existen IPS en la red protegiendo el perímetro externo del Data Center contra ataques externos conocidos de capa 7. También existen IPS internos para protección contra ataques internos	2 – La mayoría de las veces sí	2 – La mayoría de las veces sí
142	Existen *agentes* en los terminales corporativos y en los terminales BYOD que detectan la existencia de tráficos o archivos maliciosos, con capacidad de bloquearlos conforme a la política corporativa. Además de virus, detecta gusanos y malwares	0 – No aplicable	3 – Sí, siempre
143	Hay un Firewall entre la red LAN corporativa y la red del Data Center, protegiendo el Data Center de eventuales ataques internos	0 – No aplicable	3 – Sí, siempre
144	Existe una integración automatizada entre las distintas plataformas de seguridad (protección de contenido, Firewall / IPS, análisis de tráfico interno, clientes antimalware, centros globales de inteligencia, etc.) permitiendo la detección y protección contra ataques sofisticados como Ransomware modernos (SOC)	0 – No aplicable	2 – La mayoría de las veces sí
145	Existen productos para análisis históricos de ataques ocurridos, posibilitando entender el evento y localizar segmentos que aún pueden ser vulnerables	0 – No aplicable	1 – No
146	Utilizamos una herramienta de administración unificada para red cableada e inalámbrica.	0 – No aplicable	1 – No
147	Tenemos una documentación detallada del posicionamiento de los access-points	0 – No aplicable	1 – No

	instalados y documentación de site-survey pre o post implementación.		
148	Se realiza un site-survey para cada nueva implementación de Wifi.	0 – No aplicable	1 – No
149	Los 89ccess-points instalados poseen funcionalidad embebida de análisis de RF y permiten cambiar automáticamente de canal en caso de detección de interferencia en el canal de operación.	0 – No aplicable	4 – No sé decir
150	La mayoría de los clientes Wifi ya operan en 5 GHz.	0 – No aplicable	3 – Sí, siempre
151	Los 89ccess-points instalados ya soportan las tecnologías WiFI6 o WiFi6e?	0 – No aplicable	1 – No
152	El acceso Wifi de invitado se ofrece de forma segura mediante la creación del usuario invitado por un administrador de la empresa o a través de credenciales de redes sociales como Facebook, Google u otros.	0 – No aplicable	1 – No
157	La red LAN existente cumple con los requisitos de VoIP, como PoE y QoS	0 – No aplicable	3 – Sí, siempre

Fuente: "Elaboración Propia"