Escuela Superior Politécnica del Litoral

Facultad de Ingeniería en Electricidad y Computación

Diseño de una red híbrida con seguridad perimetral, empleando criterios de seguridad informática, para una cadena de farmacias

Proyecto de Titulación

Previo la obtención del Título de:

Magíster en Seguridad Informática

Presentado por:

Lcdo. Adrián Arrieta Hernández

Ing. Tula Bolaños Pinela

Guayaquil – Ecuador

Año: 2025

Agradecimiento

A DIOS, que es el centro de mi vida, a mi esposa e hijos, mis padres quienes siempre me incentivaron a no detenerme en este camino de la vida, y hacer siempre las cosas con excelencia.

Adicional, agradecer a mi compañera de trabajo ya que hemos estado en una lucha ardua por no desistir en alcanzar los objetivos propuestos.

Ing. Adrián Arrieta Hernández

A Dios por haberme dado todas las herramientas necesarias para poder realizar esta maestría, a Mario, sin él no lo hubiera logrado, no hubiera tenido los bríos para al menos inscribirme.

Gracias a todas aquellas personas que de alguna manera aportaron con ánimos, conocimientos para que pudiera llegar a esta instancia.

Ing. Tula Angélica Bolaños Pinela

Dedicatoria

Para Tatiana, Adrián, Tadeo y Emiliano, mis motores y pilares que han aguantado mi sacrificio todo este tiempo para alcanzar metas.

Lcdo. Adrián Arrieta Hernández.

Para mis Palitas, por sacrificar su tiempo, para que mamá termine esta nueva meta, en el camino del crecimiento profesional y personal.

Ing. Tula Bolaños Pinela

Declaración Expresa

Nosotros Adrián Arrieta Hernández y Tula Bolaños Pinela acordamos y reconocemos que:

La titularidad de los derechos patrimoniales de autor (derechos de autor) del proyecto de graduación corresponderá a los autores, sin perjuicio de lo cual la ESPOL recibe en este acto una licencia gratuita de plazo indefinido para el uso no comercial y comercial de la obra con facultad de sublicenciar, incluyendo la autorización para su divulgación, así como para la creación y uso de obras derivadas. En el caso de usos comerciales se respetará el porcentaje de participación en beneficios que corresponda a favor de los autores.

La titularidad total y exclusiva sobre los derechos patrimoniales de patente de invención, modelo de utilidad, diseño industrial, secreto industrial, software o información no divulgada que corresponda o pueda corresponder respecto de cualquier investigación, desarrollo tecnológico o invención realizada por nosotros durante el desarrollo del proyecto de graduación, pertenecerán de forma total, exclusiva e indivisible a la ESPOL, sin perjuicio del porcentaje que nos corresponda de los beneficios económicos que la ESPOL reciba por la explotación de nuestra innovación, de ser el caso.

En los casos donde la Oficina de Transferencia de Resultados de Investigación (OTRI) de la ESPOL comunique los autores que existe una innovación potencialmente patentable sobre los resultados del proyecto de graduación, no se realizará publicación o divulgación alguna, sin la autorización expresa y previa de la ESPOL.

Guayaquil, 27 de agosto del 2025.

Firmado electrónicamente por:
ADRIAN ALBERTO ARRIETA HERNANDEZ
Validar únicamente con FirmaEC

Lcdo. Adrián Arrieta Hernández

Firmado electrónicamente por:
TULA ANGELICA BOLANOS PINELA
Validar únicamente con FirmaEC

Ing. Tula Bolaños Pinela

Evaluadores

Firmado electrónicamente por:
LENIN EDUARDO FREIRE COBO
Validar únicamente con FirmaEC

M.Sc. Lenin Eduardo Freire Cobo

Tutor

Firmado electrónicamente por:
JUAN CARLOS GARCIA PLUA
Validar únicamente con FirmaEC

M.Sc. Juan Carlos García Plúa

Revisor

Resumen

El presente trabajo de titulación se centra en el diseño de un esquema hibrido de red basándose en criterios de seguridad informática para una cadena de farmacias, buscando crear una estrategia de seguridad fuerte y adaptada a las necesidades particulares de la empresa, basada en un análisis de riesgos.

El presente incluye la identificación de amenazas tanto internas como externas, así como la evaluación de vulnerabilidades en la infraestructura física y digital de la empresa. Al abordar estos aspectos, este trabajo de titulación busca proporcionar una solución integral que no solo proteja los activos de la empresa, sino que también garantice la continuidad operativa y la confianza de los clientes y empleados. Además, explora el impacto económico de implementar estas medidas de seguridad y cómo se puede lograr un equilibrio entre costos y beneficios para asegurar una inversión sostenible en la protección de la empresa.

Se busca también, fomentar una cultura de seguridad en la organización, en la que todo el personal, a todos los niveles, esté al tanto de las políticas y procedimientos de seguridad, y sea capaz de actuar de forma proactiva ante cualquier eventualidad.

Palabras Clave: encriptación, amenaza, vulnerabilidad, infraestructura, redundante.

Índice General

Agradecimiento II
Dedicatoria II
Declaración Expresa IV
Evaluadores V
Resumen VI
Índice General VII
Índice de figuras IX
Índice de tablas X
Introducción XI
Capitulo I 1
Generalidades 1
1. Antecedentes 1
1.2 Descripción del Problema 1
1.3 Solución Propuesta 2
1.4 Objetivo General 7
1.5 Objetivos Específicos. 7
1.6 Metodología 7
Capítulo 2 9
Marco Teórico 9
2.1 Redes de Telecomunicaciones 9
2.1.1 Definición de Redes Híbridas 9
2.1.2 Componentes de una red Híbrida. 10
2.1.3 Diseño de una Red Híbrida en la nube. 11
2.1.4 Ventajas y desventajas de una Red Híbrida. 12
2.2 Seguridad Informática 15
2.2.1 Seguridad perimetral. 15
2.2.2 Herramientas de Seguridad Perimetral en Redes Híbridas 16
2.3 Servicios Cloud 18
2.3.1 Escalabilidad y Flexibilidad 18
Capítulo 3 21
Levantamiento De Información 21
3.1 Establecimiento del contexto de la organización 21
3.2 Identificación de activos de información de la empresa 22

3.3 Topología actual de la red....28
3.4 Identificación de Vulnerabilidades....29
Capítulo 4....33
Análisis y Tratamiento de Riesgo de la Nueva Red Híbrida....33
4.1 Criterios de seguridad informática, para la implementación de red híbrida. 33
4.1.1 Seguridad en el perímetro de la red....33
4.1.2 Seguridad en el acceso y autenticación. 34
4.2 Evaluación de riesgo....34
4.2.1 Identificación de Activos Críticos....34
4.2.2 Identificación de Amenazas y Vulnerabilidades....35
4.2.3 Análisis de Impacto y Probabilidad....36
4.3 Tratamiento de Riesgo de los activos....37
4.3.1 Mitigación de Riesgos....38
4.3.2 Aceptación de Riesgos....39
4.3.3 Eliminación de Riesgos....39
4.3.3 Transferencia de riesgos....40
4.4 Consideraciones éticas y legales....41
Capitulo 5....44
Acciones y Políticas para la Nueva Red Híbrida....44
5.1 Políticas de seguridad para la nueva red. 44
5.1.1 Control de Acceso....44
5.1.2 Protección Perimetral....45
5.1.3 Seguridad en la Nube....46
5.1.4 Concienciación y Capacitación....47
5.2 Diseño de las acciones dentro de los controles de seguridad de la nueva red híbrida. 49
5.2.1 Segmentación de la Red....49
5.2.2 Cifrado de Datos....50
5.2.3 Control de Acceso Basado en Roles....51
5.2.4 Planes de Respuesta ante Incidentes....52
Conclusiones Y Recomendaciones....57
Conclusiones....57
Recomendaciones....59
Limitaciones del Proyecto....61
Biliografia....62

Índice de figuras

Figura 1. Diagrama Arquitectónico General....20

Figura 2. Diseño de Red – Cadena de Farmacias....46

Figura 3. Mapa lógico de segmentación de red....50

Figura 4. Diagrama de control de acceso basado en roles (RBAC)....52

Figura 5. Flujo de respuesta ante incidentes de seguridad 53

Índice de tablas

Tabla 1. Activos de Información....28

Tabla 2. Resumen de Vulnerabilidades detectadas....31

Tabla 3. Elementos Críticos Identificados....35

Tabla 4. Matriz de Riesgo para la Red Híbrida....37

Tabla 5. Resumen del tratamiento de riesgos en la red híbrida....41

Tabla 6. Plan de concientización y capacitación del personal por área de la organización....48

Tabla 7. Ejemplos de acciones de seguridad alineadas a cada tipo de control implementado..54

Tabla 8. Resumen de las acciones implementadas en la red híbrida y su relación con los riesgos y políticas de seguridad. 55

Introducción

En la era tecnológica actual, las empresas, sin importar su tamaño, requieren estar conectadas con el mundo exterior, lo que ha generado una creciente dependencia de la tecnología. Esta necesidad de conexiones externas también ha incrementado la actividad de los ciber delincuentes, lo que obliga a todos los sectores a desarrollar e implementar medidas de seguridad que protejan los recursos que poseen.

En este marco, el presente estudio aborda el desafío específico de diseñar un plan completo de seguridad perimetral, basado en un análisis de riesgos, con el objetivo de reforzar la postura de seguridad de una mediana empresa ubicada en la ciudad de Guayaquil, teniendo en cuenta las particularidades de su entorno operativo. A través de un análisis detallado de los riesgos a los que se enfrenta, se pretende no solo identificar las amenazas posibles, sino también comprender las vulnerabilidades específicas que podrían ser aprovechadas por actores maliciosos.

La seguridad perimetral, entendida como la protección de los límites físicos y lógicos de una red, se presenta como un pilar fundamental para defenderse de amenazas externas. Sin embargo, el diseño de un enfoque integral y adaptado a las características particulares de una mediana empresa requiere una comprensión profunda de los riesgos asociados a su operación.

La relevancia de una gestión eficiente de riesgos en el campo de la seguridad informática es indiscutible. El panorama empresarial contemporáneo enfrenta amenazas que evolucionan de manera constante, desde ciberataques sofisticados hasta la vulnerabilidad inherente a los sistemas tecnológicos. Por ello, el diseño de un esquema integral de seguridad perimetral para una mediana empresa en Guayaquil se presenta como una respuesta estratégica para mitigar estos riesgos y asegurar la integridad, confidencialidad y disponibilidad de la información crítica.

Capitulo I

Generalidades

1. Antecedentes

Las redes de comunicación han evolucionado paulatinamente en las últimas décadas. Inicialmente, las empresas farmacéuticas dependían de redes locales (LAN) para conectar dispositivos y compartir recursos. Con el tiempo, la necesidad de conectar diferentes sucursales y permitir acceso remoto impulsó la integración de redes híbridas que combinan tecnologías locales y en la nube.

1.2 Descripción del Problema

El problema en la que se ve inmerso esta empresa dedicada a la venta de productos farmacéuticas, es que cada farmacia a nivel nacional se encuentra expuesta a pérdida de servicios, vulnerabilidades de red internas por no contar con una protección perimetral de su red interna.

Hace unos meses, la empresa se vio envuelta en un ataque de fuerza bruta a sus servidores de correos donde se tuvo afectación de servicio al momento de enviar correos electrónicos a sus clientes, debido a que el mail server no se encontraba en un DMZ (Zona Segura que permite que las empresas u organizaciones protejan su red interna), donde sufrieron afectación de los servicios en los cuales brindan a sus usuarios finales.

A nivel del área de IT no se tiene establecido, un plan de contingencia ante escenarios donde se vean afectado su producción, aunque conocen la importancia y lo vital que es para la empresa mantenerse operativo mientras sus sucursales estén atendiendo al publico en general.

Así como también, luego de verse expuestos a este ciberataque a su red interna, se tomaron medidas que no fueron efectivas, y se evidencia la falta de una red de datos con una disponibilidad para ofrecer sus productos a toda hora, ocasionando perdidas económicas y de prestigio la red de farmacia.

1.3 Solución Propuesta

La solución que se presenta a esta red de farmacias es ideal por varias razones, no solo que combina una interconexión entre todas las sucursales y la matriz de la empresa, a través de redes privadas y públicas sino que también incluye una protección de datos e información que garanticen una gestión eficiente del trafico en la red con disponibilidad para proveer sus productos a clientes finales.

Al integrar ésta solución con redes que viajen por internet y de forma privada por infraestructura MPLS (Combinación de etiquetas Multiprotocolo) lo que nos va a permitir una mayor flexibilidad, dado que se pueden elegir diferentes medios de comunicación en función de la criticidad del servicio.

Al momento de establecer una red híbrida, se garantizará la continuidad del negocio, minimizando los incidentes, así como también adaptando enlaces redundantes donde la red pueda gozar de contingencia y en caso de perdida de servicio por el enlace privado podrá ser dirigido por la red pública, para lo cual es crucial para una cadena de farmacias, donde la disponibilidad del sistema es vital para mantener las operaciones diarias.

Dentro del diseño, se propone integrar un Firewall donde se pueda incluir políticas de filtrado, inspección de trafico, prevención de intrusos y estar protegidos ante cualquier amenaza externa como interna, así mismo se creará una segmentación donde se pueda aislar los servidores de producción diferenciados a los usuarios finales, para así reducir los riesgos a vulnerabilidades.

El uso de una red híbrida puede optimizar los costos de operación, aunque las conexiones privadas suelen ser más costosas, sin embargo al combinarlas con redes públicas para servicios no críticos o tráfico menos sensible, se reduce la dependencia en enlaces dedicados de alto costo, en donde se realizará una inversión más eficiente sin comprometer la seguridad o la calidad del servicio.

Al poder poner en producción este diseño de red híbrida, la cadena de farmacias podrá gozar de una red escalable, conforme la empresa crezca, se añadirán sucursales que utilicen las mismas conexiones seguras y flexibles sin necesidad de una inversión posterior, dado que se ajustarán fácilmente a las condiciones ya establecidas en la solución inicial, sin poner en riesgo ningún servicio ni comprometer la información de la empresa.

Se tendrá una administración centralizada de toda la infraestructura de la red, facilitando así cualquier tipo de configuración que se requiera, esto es crucial para la empresa dado que al contar con diversas ubicaciones, se garantizará que cada sucursal cuente con todas las políticas de seguridad en la que los datos estén protegidos siempre y sólo con acceso restringido a personal autorizado.

Para terminar, se entregará una capacitación al personal de IT, siendo este factor de vital importancia al momento de operar la red y establecer las mejores políticas de seguridad en base a las necesidades de cada usuario que tenga acceso a toda la data de la empresa, así podremos ofrecer una red eficiente, rápida y segura priorizando la protección de accesos no autorizados y una estabilidad operativa.

En conclusión, la solución establecida de esta red híbrida con seguridad perimetral es ideal ya que proporciona una combinación equilibrada de

flexibilidad, seguridad, rendimiento con costos controlados, donde permite a la cadena de farmacias mantener operaciones eficientes y seguras, y se adapte fácilmente al crecimiento y proteja sus datos sensibles de manera efectiva.

Para realizar este análisis de riesgo, hemos optado por la norma ISO 27001:2013. Esta elección se basa en su reconocimiento internacional y respeto en el campo de la seguridad de la información, así como en su capacidad para cumplir con normativas y expectativas globales, lo que puede ser atractivo si la empresa tiene como objetivo futuro extender sus operaciones con clientes en el extranjero. Además, este estándar proporciona un enfoque integral para la gestión de la seguridad de la información, abarcando no solo aspectos técnicos, sino también organizativos, de personal y procesos, lo que garantiza una gestión completa de la seguridad.

Después de recopilar la información necesaria utilizando la norma ISO 27001:2013, procederemos a elaborar el análisis de riesgo siguiendo un proceso que analizará el estado actual de la empresa:

- Establecimiento del contexto
- Identificación de activos
- Identificación de amenazas
- Evaluación de vulnerabilidades
- Evaluación de riesgos

- Tratamiento de riesgos
- Documentación

A partir de este análisis de riesgo, desarrollaremos un diseño de seguridad perimetral con el objetivo de abordar y minimizar las brechas de seguridad identificadas. Un esquema de seguridad perimetral sólido y bien diseñado es fundamental para proteger a una empresa de las amenazas cibernéticas y asegurar su continuidad operativa, reputación y relaciones comerciales.

Este enfoque proactivo en la seguridad informática permitirá a la empresa fortalecer sus procesos internos, garantizando la confidencialidad, integridad y disponibilidad de la información y protegerá los intereses tanto de la empresa como de sus clientes.

Además, recalcar que en Ecuador, entidades como ARCOTEL y la Asociación Ecuatoriana de Seguridad Informática han advertido que los ciberataques generan pérdidas significativas en el sector privado, superando los dos millones de dólares anuales en promedio.

Estos datos reflejan una realidad preocupante que no solo afecta a grandes corporaciones, sino también a negocios medianos como las cadenas de farmacias. Un solo incidente de seguridad puede poner en riesgo su funcionamiento diario y, sobre todo, la confianza que los clientes depositan en ellas.

1.4 Objetivo General

Diseñar una infraestructura de red donde combina una red híbrida, física y en la nube; con diferentes tecnologías de conectividad para una cadena de farmacia asegurando sus telecomunicaciones y accesos a datos de manera más segura.

1.5 Objetivos Específicos.

1) Realizar un levantamiento de información de todos los recursos de red en producción dentro de las farmacias a nivel nacional.
2) Plantear el equipamiento óptimo donde el tráfico de información entre farmacias permita ser más eficiente.
3) Esquematizar un plan de seguridad perimetral y un plan de contingencia, de forma que se proteja de ataques externos a la red de farmacias.

1.6 Metodología

Para este trabajo se desarrollará un estudio transversal basado en entrevistas e información documentada. Estas entrevistas se llevarán a cabo sobre la población de interés la cual es el departamento de tecnología, siendo estos los administradores directos de la red, obteniendo de esta manera la información que se requiere de manera más ágil y confiable.

Como instrumento para la recopilación de datos haremos uso de entrevistas estructuradas. El protocolo de preguntas que presentaremos al personal de TI, contendrá entre otros,el estado actual de la red, requerimientos de la red,

consultas de vulnerabilidades en cuánto a la seguridad, eventos o incidentes que en la que la organización se haya visto expuesta. Así también se determinaran los retos de la organización, presupuestario entre otros. Adicionalmente se obtendrán sugerencias y expectativas de un nuevo diseño de red a proponer. Finalmente,la información levantada se contrastara con la información documentada proporcionada por el área a entrevistar.

Una vez recopilados los datos, se llevará a cabo un **análisis cualitativo** de la información obtenida, para llegar a Identificar temas claves relacionados para el diseño.

Posterior a este análisis se realizara el diseño propuesto y así lograr establecer recomendaciones para optimizar el diseño y mejorar la seguridad.

Capítulo 2

Marco Teórico

2.1 Redes de Telecomunicaciones

2.1.1 Definición de Redes Híbridas

Las redes híbridas son infraestructuras de comunicación que combinan características de diferentes tipos de redes, como redes públicas y privadas, cableadas e inalámbricas, o físicas y virtuales, para ofrecer una solución versátil que optimiza el rendimiento, la seguridad y la escalabilidad.

Este tipo de red es especialmente útil para organizaciones que requieren conectividad eficiente y segura en entornos distribuidos. [1]

Las redes híbridas permiten la integración de múltiples tecnologías de red, proporcionando flexibilidad y resiliencia al adaptarse a diversos requerimientos de conectividad y seguridad en tiempo real. [2].

2.1.2 Componentes de una red Híbrida.

Una red híbrida se compone de diversos elementos que permiten su funcionamiento, integración y escalabilidad. Estos componentes trabajan en conjunto para proporcionar una infraestructura eficiente, segura y flexible. [3]

Routers.-

Este equipo es el encargado de dirigir el tráfico entre redes locales y externas, incluyendo redes privadas y públicas. Es un componente esencial en cualquier red híbrida, ya que son los dispositivos responsables en decidir la mejor ruta para que los paquetes de datos lleguen a su destino de manera eficiente y segura. [3]

Switches.-

Permiten la conexión de dispositivos dentro de una misma red local, gestionando el tráfico interno, su función principal es recibir, procesar y reenviar datos a dispositivos específicos dentro de la red, optimizando el uso del ancho de banda y mejorando la eficiencia de la comunicación interna. [3]

Permiten la segmentación de redes, reduciendo la congestión.
Su uso de tablas MAC garantiza el envío eficiente de datos.

Facilitan la configuración de redes virtuales (VLANs) para mejorar la seguridad y la organización del tráfico. [4].

Redes Privadas Virtuales (VPNs).-

Es una tecnología que permite la creación de una conexión segura a través de una red pública, como Internet, utilizando técnicas de cifrado y autenticación para proteger la integridad y confidencialidad de los datos transmitidos. La VPN actúa como un túnel seguro entre el dispositivo del usuario y la red privada, lo que garantiza que el tráfico de datos esté protegido de accesos no autorizados. Este tipo de red es ampliamente utilizado por empresas y organizaciones para permitir el acceso remoto de los empleados a recursos internos de la empresa, manteniendo la seguridad de la información, incluso cuando se utiliza una red pública. [2]

Servicios en la nube.-

Se refieren a la entrega de recursos informáticos (como almacenamiento, procesamiento y software) a través de Internet, en lugar de mediante servidores o infraestructura local. Estos servicios se proporcionan bajo un modelo de pago por uso, lo que permite a las empresas y usuarios individuales acceder a recursos de manera flexible y escalable sin necesidad de poseer o gestionar la infraestructura física. [2]

Las ventajas de los servicios en la nubes son: Reducción de Costos, Mejora de la Colaboración, Seguridad y Respaldo, donde con un bajo presupuesto y menor inversión en infraestructura, tendremos fácil acceso a información y documentos dentro de la empresa. [2].

2.1.3 Diseño de una Red Híbrida en la nube.

Una red híbrida en la nube combina infraestructuras de TI locales con servicios de nube pública y privada, permitiendo la portabilidad de cargas de trabajo, una gestión unificada de los recursos y la optimización de costos y rendimiento. Este modelo ofrece flexibilidad para ejecutar aplicaciones en el entorno más adecuado según sus necesidades específicas, ya sea por razones de seguridad, cumplimiento normativo o capacidad de procesamiento. La integración entre los diferentes entornos se facilita mediante redes de área local (LAN), redes de área amplia (WAN), conexiones VPN. Además, las redes híbridas en la nube son esenciales para estrategias que requieren escalabilidad dinámica, recuperación ante desastres y adaptabilidad tecnológica. [5].

2.1.4 Ventajas y desventajas de una Red Híbrida.

Esta tecnologías han ganado popularidad debido a su capacidad para combinar lo mejor de los entornos locales y la nube, brindando flexibilidad, escalabilidad y seguridad a las organizaciones. permite que las empresas aprovechen los beneficios de ambos mundos, gestionando datos y aplicaciones de manera más eficiente mientras optimizan costos y recursos. Sin embargo, aunque las redes híbridas ofrecen muchas ventajas, también presentan ciertos desafíos en términos de complejidad y costos adicionales. A continuación, se describen las principales ventajas de adoptar una red híbrida en la nube.

Ventajas:

Escalabilidad y Flexibilidad.-

Las redes híbridas permiten a las organizaciones escalar sus recursos de manera eficiente según las necesidades de carga de trabajo, utilizando tanto infraestructura local como servicios en la nube. Esto permite una mejor adaptación a las fluctuaciones en la demanda y a las necesidades empresariales cambiantes. [6]

Optimización de costos

Utilizar una red híbrida permite a las organizaciones reducir costos al adoptar una infraestructura que solo consume recursos cuando es necesario. Además, pueden optimizar su inversión en la infraestructura existente y ampliar las capacidades de procesamiento mediante la nube cuando se requiera. [7]

Alta disponibilidad y recuperación ante desastres

La replicación de datos entre infraestructuras locales y la nube mejora la disponibilidad y garantiza la recuperación ante desastres. Las redes híbridas permiten a las organizaciones asegurar la continuidad del negocio, incluso en casos de fallos en los sistemas locales. [8]

Seguridad

La seguridad se puede gestionar de manera más eficiente, ya que las organizaciones pueden almacenar datos sensibles en sus propios servidores mientras aprovechan los servicios en la nube para otras aplicaciones. [5]

Acceso remoto y Disponibilidad.

La posibilidad de acceder a recursos tanto locales como en la nube desde cualquier lugar mejora la colaboración entre equipos distribuidos y facilita el acceso remoto a datos y aplicaciones. [9]

Desventajas

Costo Inicial de Implementación

La adquisición de hardware especializado, software y servicios para configurar una red híbrida con seguridad perimetral puede representar un gasto considerable. Este costo inicial puede ser una barrera significativa para pequeñas empresas que carecen de recursos financieros suficientes. Además, se debe considerar la inversión en capacitación del personal técnico para asegurar el manejo adecuado de la infraestructura. [10]

Complejidad de Gestión

Las redes híbridas exigen un nivel avanzado de conocimiento técnico, ya que involucran la integración de servicios locales y en la nube. Esto puede derivar en desafíos operativos si no se cuenta con un equipo capacitado para gestionar la configuración, monitoreo y actualización continua de la red. Además, la falta de un manejo adecuado podría dar lugar a vulnerabilidades de seguridad. [11]

Conectividad a Internet

Las redes híbridas dependen en gran medida de una conexión a internet confiable para acceder a los servicios en la nube. Una interrupción o una conexión lenta puede afectar significativamente la disponibilidad de aplicaciones críticas y la productividad de la organización. Esto es

especialmente problemático en áreas donde la conectividad no es estable. [12]

2.2 Seguridad Informática

En el ámbito de la tecnología y la gestión de la información, la Seguridad Informática es esencial al formar la primera línea de defensa contra las amenazas cibernéticas externas. Este enfoque estratégico se centra en la implementación de medidas y controles específicos destinados a proteger la integridad, confidencialidad y disponibilidad de los sistemas informáticos, comenzando desde el acceso inicial a la red de la organización.

2.2.1 Seguridad perimetral.

La seguridad perimetral es una estrategia diseñada para proteger los límites de una red corporativa, asegurando que cualquier interacción con la red desde el exterior esté controlada y monitoreada. En las redes híbridas, este enfoque resulta esencial debido a la combinación de infraestructura local y servicios en la nube, lo que amplía significativamente la superficie de ataque.

Los sistemas de seguridad perimetral utilizan tecnologías como firewalls avanzados, sistemas de detección y prevención de intrusos (IDS/IPS) y redes privadas virtuales (VPN). Estas herramientas trabajan en conjunto para identificar, mitigar y responder a posibles amenazas antes de que puedan acceder a la red interna. Además, las soluciones modernas incorporan inteligencia artificial y aprendizaje automático para detectar patrones anómalos en el tráfico de red y prevenir ataques avanzados. Ejemplo, los firewalls de próxima generación (NGFW) no solo realizan el

filtrado de paquetes tradicional, sino que también inspeccionan el contenido del tráfico, detectando malware o comportamientos sospechosos. Este nivel de análisis es crucial para prevenir ataques como ransomware o phishing dirigido. [13]

En redes híbridas, la seguridad perimetral también incluye herramientas específicas para proteger los puntos de integración con servicios en la nube, garantizando que los datos transferidos estén cifrados y que solo usuarios y dispositivos autorizados puedan acceder a ellos. [14]

2.2.2 Herramientas de Seguridad Perimetral en Redes Híbridas

A continuación, se detallan algunos elementos que integran las soluciones de seguridad perimetral.

Firewalls de Próxima Generación (NGFW)s. – Definimos que estos equipos son una evolución de los firewalls tradicionales, que ofrecen una capa adicional de seguridad al incorporar capacidades avanzadas de inspección y control. Mientras que los firewalls tradicionales operan principalmente a nivel de red (filtrado de direcciones IP y puertos), los NGFW operan a nivel de aplicaciones y pueden realizar un análisis profundo del tráfico. Esto les permite detectar y prevenir amenazas más complejas, como malware, ataques de día cero y otros tipos de intrusiones sofisticadas. [15].

Estos inspeccionan no solo los encabezados de los paquetes de red, sino también su contenido. Esta capacidad les permite identificar amenazas que se ocultan dentro del tráfico encriptado o en protocolos no estándar. [15], pueden identificar y gestionar el tráfico de aplicaciones específicas,

incluso si están ocultas dentro de otros protocolos. Esto permite bloquear aplicaciones no deseadas o riesgosas como juegos en línea o programas de descarga de archivos, que pueden ser vectores de malware. [15]

Sistemas IDS/IPS (Detección y Prevención de Intrusos) – Los sistemas de detección de intrusos (IDS) monitorean la actividad de la red para identificar comportamientos anómalos o patrones sospechosos que podrían indicar un intento de ataque. Por otro lado, los sistemas de prevención de intrusos (IPS) no solo detectan amenazas, sino que también bloquean automáticamente las conexiones maliciosas.
En una red híbrida, los IDS/IPS son esenciales porque:
Protegen la interacción entre la infraestructura local y los servicios en la nube.

Detectan y bloquean intentos de acceso no autorizado, como ataques de fuerza bruta.

Ayudan a mitigar ataques DDoS (Denegación de Servicio Distribuido) al identificar picos anómalos en el tráfico. [16]

En resumen, la implementación de sistemas IDS/IPS fortalece la postura de seguridad de una organización al brindar detección temprana y medidas preventivas contra posibles intrusiones.

Inspección de Tráfico Cifrado - Muchos ataques modernos se ocultan dentro del tráfico cifrado mediante HTTPS. Los NGFW tienen la capacidad de realizar inspección profunda de paquetes (DPI) incluso en conexiones cifradas, utilizando certificados de seguridad para descifrar, analizar y volver a cifrar el tráfico antes de enviarlo al destino. [13]

2.3 Servicios Cloud

Los servicios en el Cloud y en Data Centers (DC) desempeñan un papel esencial en las redes híbridas, al ofrecer herramientas avanzadas para el manejo de datos, operaciones empresariales, y estrategias de seguridad. La integración entre ambos entornos permite optimizar el rendimiento, garantizar la disponibilidad y proteger la información. [18]

2.3.1 Escalabilidad y Flexibilidad

Los servicios en la nube permiten ajustar recursos según la demanda en tiempo real. Esto es particularmente útil para gestionar picos de tráfico o proyectos temporales, sin necesidad de adquirir hardware adicional. [18]

Gestión de Identidades y Accesos (IAM)

La nube facilita la implementación de sistemas centralizados de autenticación y autorización, como Azure Active Directory y Google Identity. Estas herramientas fortalecen el control de accesos y reducen riesgos relacionados con cuentas comprometidas. [7]

Protección Contra Amenazas Avanzadas

Los proveedores de Cloud, como AWS y Microsoft Azure, integran sistemas basados en inteligencia artificial para detectar y mitigar amenazas en tiempo real. Estas plataformas se actualizan automáticamente con la última información sobre ciberseguridad global. [14]

Servicios en el Data Center (DC)

Control Total sobre la Infraestructura

Los DC locales permiten a las empresas mantener un control absoluto sobre los recursos físicos y virtuales, garantizando que los datos sensibles no salgan del entorno interno. [13]

Personalización de Sistemas de Seguridad

Los DC ofrecen la posibilidad de implementar configuraciones de seguridad específicas, como firewalls internos y segmentación de red avanzada. Esto permite a las organizaciones cumplir con normativas y estándares específicos. [19]

Resiliencia Local y Continuidad

El almacenamiento redundante dentro de un DC garantiza la disponibilidad de los datos en caso de fallos o desconexión de los servicios en la nube. Además, los DC permiten realizar pruebas de recuperación ante desastres de forma controlada. [11]

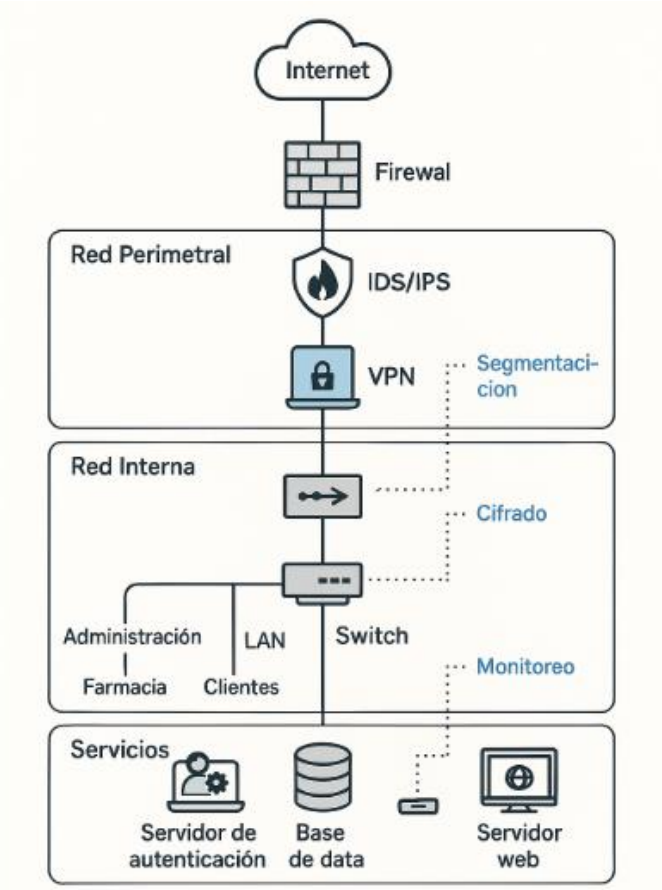

Figura 1. Diagrama Arquitectónico General

Capítulo 3

Levantamiento De Información

3.1 Establecimiento del contexto de la organización

Para llevar a cabo esta propuesta de diseño, se ha tomado como objeto de estudio una cadena de farmacias de mediano tamaño que tiene presencia en la región costa . Esta organización gestiona información sensible de los cliente. Por medio de una entrevista con el Gerente de TI se obtiene información importante de la necesidad de re diseñar su red de telecomunicaciones. El estudio se enfocara exclusivamente en los componentes actuales de la red, incluyendo tanto el hardware como el software, que integran la red de datos así como los dispositivos de seguridad perimetral.

3.2 Identificación de activos de información de la empresa

Proceso	Categoría del activo de información	Nombre del activo de información	Descripción del activo de información	Criticidad
Comercialización en línea de fármacos y suministros médicos - Gestión de recepción, preparación y envío de productos farmacéuticos	Información o datos	Sistema de información de inventarios, costos y precios en farmacia	Incluye los códigos de identificación de producto (SKU) para todos los fármacos y suministros médicos comercializados por la empresa, con sus precios y costos asociados.	**Alta**
Comercialización en línea de fármacos y suministros médicos	Aplicación	Sistema de gestión de inventarios farmacéuticos	Aplicación para la gestión de inventarios, precios y costos de productos farmacéuticos	**Alta**
Venta de	Información o	Código fuente de	Contiene los archivos de	**Alta**

productos y servicios por Internet	datos	la aplicación de escritorio de ventas	código fuente, recursos gráficos, videos, enlaces y demás componentes de la aplicación de escritorio de ventas.	
Venta de productos y servicios por Internet	Aplicación	Servicio web IIS para landing page de ventas	Aplicación de servicio web IIS diseñada como landing page para mostrar información relevante sobre productos y servicios de ventas por Internet.	**Alta**
Venta de productos y servicios por Internet	Servicio	Servicio de puntos de venta (POS) para ventas por Internet	Servicio que facilitación de compra de productos o servicios, e imprime comprobantes de pago, vinculando el método de pago utilizado (tarjeta, efectivo, consignación bancaria, etc.).	**Alta**

Vinculación, promoción y desvinculación de personal (Directo y tercero)	Información o datos	Base de datos personales y laborales de empleados	Incluye información personal de los empleados, tales como nombres, número de identificación, fecha de nacimiento, fecha de ingreso, salario, cargo, ubicación laboral, dirección residencial y teléfono.	**Alta**
Gestión de Seguridad de TI	Servicio	Acceso a Internet	Servicio de acceso controlado a Internet	**Medio**
Gestión de Seguridad de TI	Servicio	Seguridad de EndPoint	Servicio de Seguridad para equipos de cómputo y servidores, incluyendo antivirus y antispyware corporativo	**Medio**
Gestión de	Equipo Informático	Consola de Antivirus y	Consola de Antivirus y	**Alto**

Seguridad de TI		Antispyware corporativo	Antispyware corporativo	
Equipo de red o telecomunicaciones	Equipo de red o telecomunicaciones	Appliance para el filtrado de Virus de correo y SPAM	Appliance para el filtrado de Virus de correo y SPAM	**Medio**
Gestión de Infraestructura de TI	Servicio	Correo electrónico corporativo	El servicio de correo electrónico corporativo es esencial para la comunicación interna y externa, facilitando el intercambio seguro y eficiente de información entre empleados y con partes externas. Incluye funciones avanzadas de seguridad para proteger contra amenazas de malware y phishing, y está diseñado para garantizar la privacidad y la integridad de los datos	**Medio**

			corporativos.	
Gestión de Infraestructura de TI	Aplicación	Almacenamiento de archivos y carpetas compartidas	Este servicio ofrece una solución centralizada para el almacenamiento de documentos, permitiendo la colaboración eficiente entre equipos a través del acceso controlado y compartido a archivos y carpetas. Implementa rigurosas medidas de seguridad para asegurar la confidencialidad, integridad y disponibilidad de los datos corporativos esenciales.	**Alto**

Gestión de Infraestructura de TI	Suministro	Aire acondicionado Data Center	El sistema de aire acondicionado para el Data Center está diseñado para mantener una temperatura y humedad óptimas, crucial para proteger el hardware y garantizar el funcionamiento eficiente de los equipos. Incluye sistemas redundantes para asegurar la continuidad operativa ante fallos.	**Alto**
Gestión de Infraestructura de TI	Suministro	Energía eléctrica regulada Data Center	Este servicio consiste en proporcionar una fuente de energía eléctrica estable y continua al Data Center, esencial para el funcionamiento ininterrumpido y seguro de los equipos críticos.	**Alto**

Gestión de Infraestructura de TI	Equipo Informático	Terminales acceso ventas/archivos	PC escritorio, en cada farmacia por medio del cual se tiene acceso al sistema de inventario, y proceso de ventas	**Medio**

Tabla 1. Activos de Información

3.3 Topología actual de la red

La topología de la red del Data Center se organiza en un diseño híbrido que combina elementos de topologías en estrella y en malla para optimizar tanto la conectividad como la resiliencia. El núcleo de la red consiste en un conjunto de switches de alto rendimiento configurados en un esquema de malla completa, proporcionando múltiples rutas redundantes entre ellos para asegurar una alta disponibilidad y tolerancia a fallos.

Desde este núcleo, la red se ramifica en topologías en estrella hacia los distintos racks de servidores. Cada rack está equipado con switches de acceso de doble enlace ascendente, asegurando conexiones redundantes hacia el núcleo. Esto minimiza los puntos de falla y mantiene la operatividad del servicio incluso en caso de una desconexión.

Para la gestión del tráfico y la seguridad, se utilizan dispositivos de gateway redundantes que proporcionan firewall filtrado de contenido y servicios de detección y prevención de intrusiones. Estos gateways están estratégicamente ubicados en la periferia de la red para interceptar y analizar el tráfico entrante y

saliente, implementando políticas de seguridad antes de que los datos alcancen los servidores críticos o salgan al exterior.

La red también incluye un sistema de monitoreo proactivo que utiliza herramientas de análisis de tráfico y gestión de la red para detectar anomalías en tiempo real y ajustar automáticamente las rutas o el ancho de banda según sea necesario. Este sistema garantiza una respuesta ágil a los cambios en la demanda de la red o a posibles amenazas de seguridad.

Finalmente, para el soporte de aplicaciones críticas y almacenamiento de datos, se implementan conexiones dedicadas de alta velocidad entre los servidores de almacenamiento y los servidores de aplicaciones, garantizando un rendimiento óptimo y baja latencia para transacciones y procesos empresariales clave.

3.4 Identificación de Vulnerabilidades

La identificación de vulnerabilidades es un paso fundamental para comprender y gestionar los posibles eventos que puedan afectar sus operaciones y objetivos. Para identificar los riesgos a los cuáles están expuestos bajo la infraestructura actual,

realizar entrevistas con personal clave, revisar procesos y evaluar el entorno empresarial, se obtuvo el siguiente análisis de brecha el cual permite identificar escenarios de riesgo actuales, desde ciber amenazas, hasta factores externos como eventos.

Escaneo Automatizado.

Se Utilizan herramientas avanzadas de escaneo de vulnerabilidades tales como Nessus, Qualys, y Rapid7 para realizar escaneos regulares y sistemáticos de toda

nuestra red. Estas herramientas evalúan los sistemas en busca de vulnerabilidades conocidas, configuraciones incorrectas, y actualizaciones de software faltantes. El escaneo se programan para ejecutarse durante las horas de menor actividad para minimizar el impacto en la red.

Evaluación de Penetración.

Complementamos los escaneos automáticos con pruebas de penetración realizadas por un equipo interno especializado y, ocasionalmente, terceros. Este proceso implica intentar explotar activamente las vulnerabilidades para determinar la exposición real de la red ante posibles ataques. Estas pruebas ayudan a identificar debilidades que no siempre son evidentes en un escaneo pasivo.

Auditorías de Seguridad.

Regularmente realizamos auditorías de seguridad que incluyen la revisión de políticas de seguridad, prácticas de gestión de parches, y procedimientos de respuesta a incidentes. Estas auditorías ayudan a asegurar que las medidas de protección no solo están en su lugar, sino que también son efectivas y se adhieren a las mejores prácticas de la industria.

Inteligencia de Amenazas.

Mantenemos una subscripción a servicios de inteligencia de amenazas que nos proporcionan información actualizada sobre nuevas vulnerabilidades, exploits y tácticas de ataque. Esta información se utiliza para anticipar y mitigar posibles vectores de ataque antes de que sean explotados.

Formación y Concienciación.

Conscientes de que el factor humano a menudo es el eslabón más débil en la seguridad, proporcionamos formación continua a nuestros empleados sobre los principios básicos de la seguridad informática, reconocimiento de phishing, y buenas prácticas generales de seguridad.

ID	Vulnerabilidad Detectada	Herramienta / Método	Nivel de Riesgo	Activo Afectado	Recomendación
VUL-01	Puertos abiertos sin cifrado (Telnet, FTP)	Nessus / Qualys	Alto	Equipos de red y servidores	Deshabilitar servicios inseguros y usar SSH/FTPS
VUL-02	Software desactualizado con CVEs activas	Nessus	Crítico	Servidor de base de datos	Actualizar software a versiones seguras
VUL-03	Uso de credenciales por defecto	Pentesting manual	Alto	Routers y switches	Cambiar credenciales por contraseñas seguras
VUL-04	Falta de segmentación de red (acceso libre entre áreas)	Auditoría de red	Medio	LAN corporativa	Implementar VLANs según roles y funciones
VUL-05	Ausencia de RBAC en sistemas críticos	Revisión de políticas	Alto	Sistema de autenticación y ERP	Aplicar RBAC y limitar privilegios por usuario
VUL-06	No se implementa IDS/IPS para detección temprana	Análisis arquitectónico	Medio	Red perimetral e interna	Integrar IDS/IPS para monitoreo y respuesta oportuna
VUL-07	Comunicaciones internas sin cifrado	Análisis de tráfico	Medio	Comunicación entre servicios	Aplicar TLS/SSL para canales internos sensibles
VUL-08	Falta de plan de respuesta ante incidentes	Revisión documental	Medio	Toda la organización	Elaborar e implementar un plan de respuesta formal

Tabla 2. Resumen de Vulnerabilidades detectadas

Respuesta y Remediación.

Una vez identificadas las vulnerabilidades, clasificamos su severidad y aplicamos parches o remedios de acuerdo a la criticidad y al impacto potencial. Esto se maneja a través de un proceso de gestión de vulnerabilidades que asegura que las acciones correctivas se toman de manera oportuna.

Todo este proceso de escaneo, auditoría y revisión permitió no solo identificar vulnerabilidades técnicas específicas, sino también entender el origen de cada una dentro del contexto operativo de la organización. La estrategia de identificación se basó en un análisis sistemático de amenazas y debilidades, comparando el estado real de la infraestructura con el diseño ideal propuesto.

Esto permitió establecer relaciones claras entre las fallas detectadas y sus posibles consecuencias, lo que facilitó definir acciones concretas para reducir los riesgos y fortalecer la seguridad de la red.

Capítulo 4

Análisis y Tratamiento de Riesgo de la Nueva Red Híbrida.

4.1 Criterios de seguridad informática, para la implementación de red híbrida.

El diseño e implementación de una red perimetral híbrida debe basarse en principios y criterios de seguridad informática que garanticen la protección de los datos, sistemas y dispositivos conectados. Los criterios clave incluyen:

4.1.1 Seguridad en el perímetro de la red

La red híbrida debe contar con un perímetro de seguridad correctamente definido para poder controlar y monitorear el tráfico de datos. Para lograr establecer esta seguridad podemos realizarlo mediante:

Firewalls de última generación (NGFW - Next-Generation Firewall).- Implementación de firewalls con capacidad de inspección profunda de paquetes (DPI), prevención de intrusiones (IPS) y filtrado de contenido.

Sistemas de Prevención y Detección de Intrusos (IDS/IPS).- Implementación de mecanismos que detecten y bloqueen actividades maliciosas en tiempo real.

4.1.2 Seguridad en el acceso y autenticación.

El acceso a la red híbrida debe ser controlado rigurosamente para evitar accesos no autorizados:

Gestión de identidades (IAM - Identity and Access Management).-

Implementación de políticas de acceso basadas en roles (RBAC) para restringir permisos según funciones dentro de la organización.

VPN y túneles cifrados.-

Uso de VPNs seguras para conexiones remotas, evitando exposiciones innecesarias a la red pública.

4.2 Evaluación de riesgo

La evaluación de riesgos es un proceso clave para identificar, analizar y priorizar las amenazas que pueden afectar la seguridad de la red híbrida. Para ello, se aplican los siguientes pasos:

4.2.1 Identificación de Activos Críticos

Se deben identificar los activos tecnológicos esenciales para la operación de la cadena de farmacias, tales como:

Elemento	Descripción	Nivel de Criticidad (1 -3)
Servidores de bases de datos	Son esenciales para la operatividad y gestión de la cadena de farmacias.	3 (Alta)
Sistemas de gestión de	Aplicaciones y software	3 (Alta)

farmacias y Ventas	encargados del control de ventas, facturación, stock y pedidos en cada farmacia.	
Infraestructura de red	Incluye switches, routers y firewalls que permiten la comunicación entre dispositivos,	3 (Alta)
Sistemas de respaldo y almacenamiento en la nube	Plataformas utilizadas para realizar copias de seguridad y almacenar información crítica.	2 (Media)

Tabla 3. Elementos Críticos Identificados

4.2.2 Identificación de Amenazas y Vulnerabilidades

Las amenazas pueden ser tanto internas como externas. Algunas amenazas comunes incluyen:

Ataques de malware y ransomware: Software malicioso que cifra o destruye datos.

Ataques de phishing: Suplantación de identidad para obtener credenciales de acceso.

Fugas de información: Robo de datos por empleados internos o terceros.

Para cada amenaza identificada, se deben analizar vulnerabilidades

existentes en la red híbrida, como configuraciones incorrectas, software desactualizado o accesos inseguros.

4.2.3 Análisis de Impacto y Probabilidad

Nos ayuda a evaluar los riesgos de seguridad en la red híbrida, identificando cuáles representan una mayor amenaza para la operación de la cadena de farmacias. Veamos cómo afectaría en función de estos dos criterios:

Impacto (Grado de daño si ocurre el riesgo)

Evalúa qué tan grave sería la consecuencia de un incidente de seguridad. En tu caso, el impacto podría ser:

Alto (3): Interrupción total del negocio, pérdida de datos críticos o acceso no autorizado a información confidencial (Ejemplo: falla en servidores de bases de datos).

Medio (2): Afectación parcial de la operación, ralentización de procesos o necesidad de aplicar medidas de recuperación (Ejemplo: caída temporal del sistema de gestión de farmacias).

Bajo (1): Incidentes menores con soluciones rápidas y sin un impacto significativo (Ejemplo: falla en un switch de una farmacia individual).

Probabilidad (Posibilidad de que el riesgo ocurra)

Se evalúa qué tan probable es que un riesgo se materialice:

Alta (3): Ataques cibernéticos recurrentes, vulnerabilidades sin parches, configuraciones inseguras.

Media (2): Amenazas ocasionales o dependientes de factores externos.

Baja (1): Poco probable que ocurra, pero aún posible en ciertas condiciones.

Riesgo Identificado	Impacto (1-3)	Probabilidad (1-3)	Nivel de Riesgo (Impacto × Probabilidad)
Falla en servidores de bases de datos	3 (Alto)	2 (Media)	6 (Alto)
Ciberataque (phishing, ransomware, malware)	3 (Alto)	3 (Alta)	9 (Crítico)
Caída de la infraestructura de red (firewalls, switches, routers)	3 (Alto)	2 (Media)	6 (Alto)
Falla en sistema de respaldo y almacenamiento en la nube	2 (Medio)	2 (Media)	4 (Moderado)

Tabla 4. Matriz de Riesgo para la Red Híbrida

4.3 Tratamiento de Riesgo de los activos

El tratamiento de riesgos consiste en aplicar estrategias de mitigación, transferencia, aceptación o eliminación del riesgo identificado.

El análisis y tratamiento de riesgo en la red híbrida de la cadena de farmacias es un proceso fundamental para garantizar la seguridad y continuidad del negocio, evaluar riesgos de manera meticulosa y adoptar estrategias adecuadas de tratamiento de riesgos permite minimizar vulnerabilidades y mejorar la resiliencia ante ciberataques.

4.3.1 Mitigación de Riesgos

Consiste en implementar controles de seguridad para reducir la probabilidad de ocurrencia o el impacto de una amenaza:

Implementación de parches y actualizaciones: Mantener el software y harware actualizado para corregir vulnerabilidades conocidas.

Cifrado de datos sensibles Protección de información almacenada y en tránsito mediante cualquier tipo de cifrado (AES-256) y uso de protocolos seguros (TLS 1.3, IPsec, SSH) para la transmisión de datos.

Fortalecimiento de políticas de acceso: Uso de autenticación multifactor y control estricto de permisos, inserción de firewalls de última generación (NGFW) para inspección profunda de paquetes y bloqueo de amenazas.

Respaldo y continuidad del negocio : Implementación de copias de seguridad automatizadas con almacenamiento en la nube y local y definir un Plan de Recuperación ante Desastres (DRP) con procedimientos claros en caso de fallos.

4.3.2 Aceptación de Riesgos

En algunos casos, los riesgos tienen un impacto bajo o un costo de mitigación superior al daño potencial. En estos escenarios, la empresa puede aceptar el riesgo, pero debe monitorearlo.

La aceptación de riesgos debe ser una decisión informada y documentada en un Registro de Riesgos, con revisiones periódicas.

Riesgos con impacto mínimo que no afectan la operación general de la red (ejemplo: caída temporal de una conexión secundaria).

Sistemas heredados con soporte limitado, siempre que no manejen información crítica.

4.3.3 Eliminación de Riesgos

Cuando un riesgo es demasiado alto y no puede mitigarse de forma efectiva, la mejor solución es eliminar la vulnerabilidad subyacente.

1. Retiro de software obsoleto sin soporte ni actualizaciones (Ejemplo: versiones antiguas de Windows Server).
2. Desactivación de cuentas inactivas de empleados que ya no pertenecen a la empresa
3. Desconexión de dispositivos no seguros que no cumplen con los estándares de seguridad.

Con este diseño de red lo que tratamos, es de aplicar un plan de Seguridad Integral, combinando medidas preventivas con monitoreo continuo y respuestas rápidas ante incidentes.

4.3.3 Transferencia de riesgos

En ciertos escenarios, algunos riesgos pueden ser transferidos a un tercero a través de contratos, pólizas de seguro o servicios especializados. Aunque esta estrategia no elimina el riesgo, permite reducir su impacto financiero o técnico.

Ejemplos:

Contratación de servicios en la nube con proveedores certificados (SLA, ISO 27001).

Adquisición de seguros contra incidentes cibernéticos.

Tercerización de tareas críticas como respaldo o monitoreo.

En conclusión, el tratamiento de riesgos permite tomar decisiones estratégicas sobre cómo manejar las amenazas detectadas, de forma que se preserve la operatividad del negocio, se reduzcan vulnerabilidades y se mantenga la seguridad de la información. Aplicar estas estrategias adecuadamente fortalecerá la postura de seguridad de la cadena de farmacias y permitirá un crecimiento más robusto y confiable.

ID	Riesgo Identificado	Tipo de Tratamiento	Acción Aplicada	Justificación
R-01	Vulnerabilidades por software/hardware desactualizado	Mitigación	Aplicación de parches y actualizaciones	Reduce riesgos explotables conocidos mediante mantenimiento preventivo
R-02	Exposición de datos en tránsito o almacenados	Mitigación	Cifrado de datos (AES-256, TLS 1.3, IPsec, SSH)	Asegura la confidencialidad e integridad de la información
R-03	Accesos no autorizados a la red o a servicios internos	Mitigación	Autenticación multifactor, RBAC, NGFW	Fortalece el control de acceso y reduce la probabilidad de intrusiones

R-04	Pérdida de información ante fallos del sistema	Mitigación / Transferencia	Respaldos automatizados (local y nube) y DRP	Garantiza continuidad del negocio y recuperación rápida
R-05	Caídas temporales de conexiones secundarias	Aceptación	Registro en el Registro de Riesgos y monitoreo continuo	Impacto bajo, no afecta operaciones críticas
R-06	Sistemas heredados con soporte limitado	Aceptación	Supervisión periódica y aislamiento lógico si es posible	No manejan datos sensibles, costo de reemplazo es elevado
R-07	Uso de software obsoleto y sin soporte	Eliminación	Retiro completo de sistemas obsoletos	No pueden protegerse adecuadamente, representan alto riesgo
R-08	Cuentas de usuarios inactivos	Eliminación	Eliminación de cuentas de extrabajadores	Evita accesos no autorizados por cuentas olvidadas
R-09	Equipos no seguros o que no cumplen estándares	Eliminación	Desconexión o reemplazo de dispositivos inseguros	Reducen la superficie de ataque eliminando puntos vulnerables
R-10	Impacto económico o técnico ante incidentes mayores	Transferencia	Contratación de seguros cibernéticos y servicios especializados	Disminuye el impacto financiero y delega funciones críticas a expertos
R-11	Riesgos asociados a servicios tecnológicos tercerizados	Transferencia	Contratación de servicios certificados (cloud, respaldo, monitoreo)	Reduce exposición directa y mejora nivel de cumplimiento y respuesta

Tabla 5. Resumen del tratamiento de riesgos en la red híbrida

Fuente: Autor

4.4 Consideraciones éticas y legales

Más allá de lo técnico, este proyecto también contempla un aspecto fundamental: actuar de forma responsable con la información. Al diseñar una red híbrida para una cadena de farmacias, se manejan datos sensibles de clientes, colaboradores y procesos internos, por lo que es clave tener en cuenta tanto la ética como las leyes que protegen esos datos.

En este sentido, se ha tomado como referencia la Ley Orgánica de Protección de Datos Personales (LOPDP), vigente en Ecuador desde mayo de 2021. Esta ley establece que cualquier dato personal debe ser tratado con respeto, cuidado y con el consentimiento de quien lo entrega. Es decir, las personas tienen derecho a saber cómo se usa su información y a que esta se mantenga segura.

Durante el desarrollo de esta propuesta, se han considerado varios principios que la LOPDP promueve y que también reflejan buenas prácticas éticas en tecnología:

- **Confidencialidad:** Toda información personal o sensible debe mantenerse protegida y fuera del alcance de personas no autorizadas.
- **Uso claro y justificado:** Los datos solo deben utilizarse para lo que fueron solicitados, dentro del funcionamiento propio de la red.
- **Consentimiento:** El tratamiento de datos debe contar con la aprobación consciente de cada persona involucrada.
- **Seguridad:** La red incluye mecanismos de protección como segmentación, control de accesos, autenticación y cifrado, que ayudan a evitar filtraciones, accesos indebidos o ataques.

Cumplir con estas consideraciones no solo evita problemas legales, sino que también fortalece la confianza en el sistema y en la organización que lo implementa. Al final, la tecnología debe servir a las personas, y eso

implica cuidar de su información con el mismo compromiso con el que se diseña toda la red.

Capitulo 5

Acciones y Políticas para la Nueva Red Híbrida

5.1 Políticas de seguridad para la nueva red.

En este capítulo se presentan las acciones y políticas de seguridad que se implementarán en la red híbrida de la cadena de farmacias. El objetivo principal es garantizar una seguridad perimetral efectiva, proteger la integridad de los datos y reducir al mínimo las vulnerabilidades frente a amenazas cibernéticas.

Las políticas de seguridad sirven como marco normativo que regula el uso de la red, estableciendo lineamientos claros para preservar la confidencialidad, integridad y disponibilidad de la información. Estas políticas deben prevenir accesos no autorizados, proteger los datos sensibles y asegurar la continuidad operativa de la red.

A continuación, se detallan las principales políticas a aplicar:

5.1.1 Control de Acceso

- **Autenticación y autorización:** Implementar mecanismos de autenticación robustos (como contraseñas seguras, biometría o tarjetas inteligentes) y establecer roles y permisos según el principio de mínimos privilegios, para asegurarse de que cada usuario tenga acceso solo a los recursos necesarios.
- **Control de acceso basado en políticas (PBAC)**: Configurar políticas de acceso que garanticen que solo las personas adecuadas puedan acceder a áreas específicas de la red.
- **Identificación y autenticación en todos los niveles**: Es necesario que todo acceso a sistemas y servicios (internos y externos) esté sujeto a un proceso de autenticación, con revisiones periódicas de los privilegios de acceso para ajustarlos a las necesidades actuales del personal.

5.1.2 Protección Perimetral

- **Firewalls:** Implementar firewalls a nivel de red, tanto para a entrada como la salida, para bloquear tráfico no autorizado y asegurar que la red esté protegida contra amenazas externas. Los proxies ayudarán a filtrar y monitorear el tráfico.

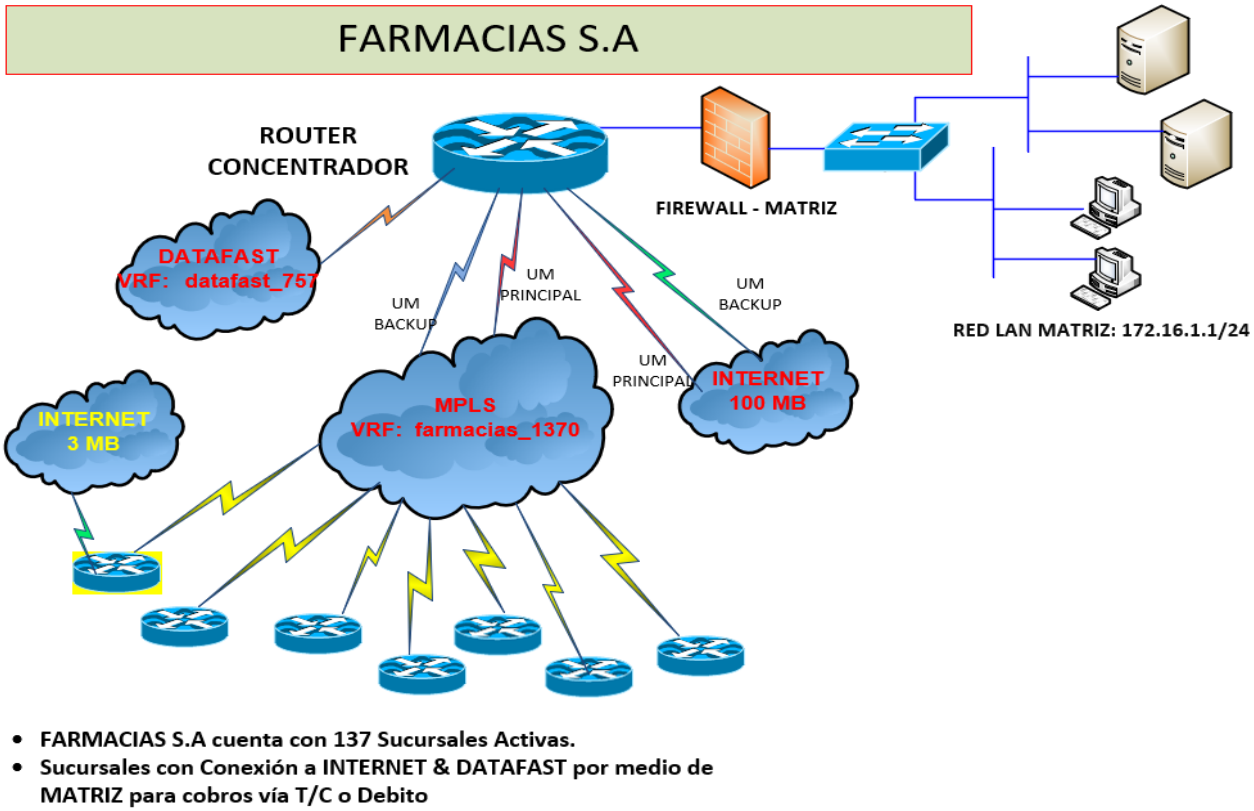

Figura 2. Diseño de Red – Cadena de Farmacias

Fuente. Autores

- **Sistema de detección y prevención de intrusiones (IDS/IPS)**: Utilizar estos sistemas para identificar y prevenir posibles ataques, como intentos de explotación de vulnerabilidades o accesos no autorizados, mediante la inspección en tiempo real del tráfico de la red.

- **Red privada virtual (VPN):** Asegurar que los usuarios remotos se conecten de manera segura a la red utilizando VPN, cifrando todo el tráfico que circula entre el usuario y la red corporativa.

5.1.3 Seguridad en la Nube

- **Acceso restringido y gestión de identidades:** Implementar controles de acceso y autenticación robustos en las plataformas en la nube, asegurando que solo los usuarios autorizados puedan acceder a los recursos críticos.
- **Protección de los centros de datos:** Los proveedores de la nube gestionan la seguridad física de sus centros de datos, incluyendo el acceso restringido a los edificios y equipos, así como las medidas contra desastres naturales.
- **Redundancia y disponibilidad**: Aseguran que sus servicios estén disponibles mediante una infraestructura redundante y resiliente (por ejemplo, respaldo de servidores, centros de datos distribuidos, etc.).
- **Cumplimiento de normativas y certificaciones de seguridad**: Los proveedores de la nube suelen obtener certificaciones de seguridad y cumplir con regulaciones de la industria (como ISO 27001.) para garantizar que sus prácticas de seguridad son sólidas y conformes con las normativas internacionales

5.1.4 Concienciación y Capacitación

En una red híbrida como la que se propone para Farmacias S.A., los dispositivos y las configuraciones son solo una parte de la solución. El otro componente —igual de importante— es el comportamiento de las personas que usan esa red a diario.

No basta con tener firewalls, políticas de acceso o servicios en la nube

seguros, si los usuarios internos no conocen los riesgos o no están preparados para enfrentarlos.

Un solo clic en un enlace malicioso, una contraseña débil o el uso de una red pública sin protección puede abrir la puerta a una amenaza grave.

Por esta razón, se plantea implementar un plan de concienciación y capacitación continua en seguridad informática. Esta iniciativa estará orientada a todos los niveles del personal, desde los colaboradores en puntos de venta hasta el personal administrativo y técnico.

Área	**Tipo de Capacitación**	**Frecuencia**
Ventas	Identificación de correos maliciosos	Trimestral
Administración	Manejo de información sensible	Semestral
TI	Protocolos de respuesta ante incidentes	Mensual
Todos los empleados	Buenas prácticas de ciberseguridad	Anual

Tabla 6. Plan de concientización y capacitación del personal por área de la organización

Fuente: Autor

El objetivo no es convertir a todos en expertos en ciberseguridad, sino crear una cultura organizacional consciente del valor de la información y de cómo cada persona tiene un rol en su protección.

Esta política de capacitación no solo reducirá riesgos operativos, sino que mejorará la respuesta ante incidentes y reforzará la confianza interna y externa en la red de Farmacias S.A.

5.2 Diseño de las acciones dentro de los controles de seguridad de la nueva red híbrida.

Al momento que ya se tienen establecidas las políticas de seguridad para la red, se procede a diseñar acciones especificas que se alineen a los controles de seguridad. Estas acciones aseguran la protección continua de la infraestructura de la red híbrida, gestionando riesgos y respondiendo a las amenazas en tiempo real.

5.2.1 Segmentación de la Red

La segmentación de la red es una acción crucial para mejorar la seguridad. Al dividir la red en diferentes segmentos, se limita el acceso a ciertas áreas de la red solo a usuarios o sistemas autorizados, reduciendo el riesgo de propagación de ataques.

- **Redes internas y externas**: Separar las redes internas (donde se almacenan los datos sensibles, servidores, etc) de las redes externas (que incluyen servicios de acceso remoto y conexiones de clientes o proveedores, usuarios que deben estar restringidos para información crucial de la compañia).

- **Subredes por función**: Crear subredes diferenciadas para funciones específicas dentro de la cadena de farmacias. Por ejemplo, una subred para area de ventas, otra para bases de datos, y una para servicios administrativos, aislando sistemas críticos de aquellos menos sensibles.

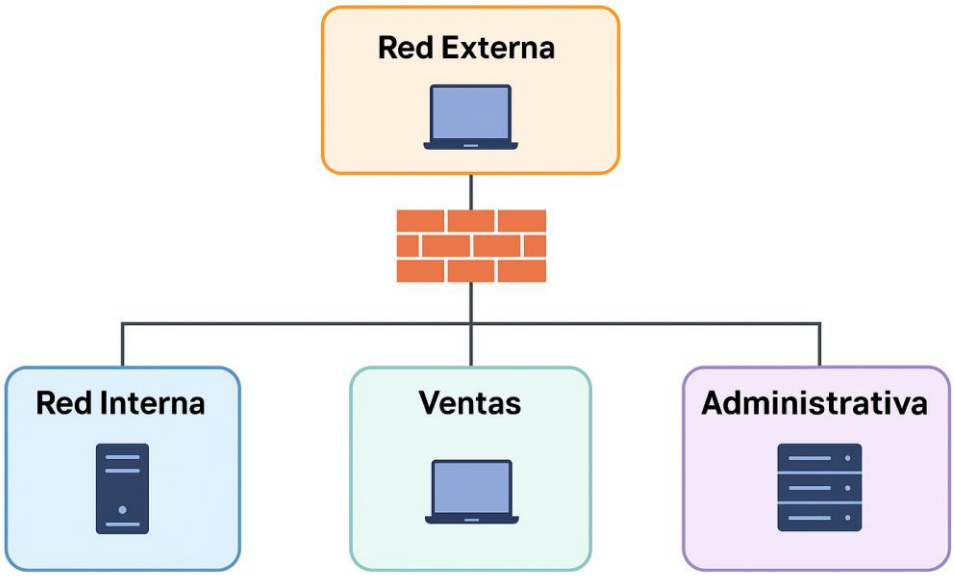

Figura 3. Mapa lógico de segmentación de red

Fuente: Autores

5.2.2 Cifrado de Datos

El cifrado de datos es una de las principales medidas de protección para la seguridad de la red híbrida. Proteger los datos mediante cifrado asegura que, incluso si un atacante obtiene acceso a los datos, no pueda interpretarlos sin la clave adecuada.

- **Gestión de claves**: Establecer un sistema centralizado para gestionar las claves de cifrado de manera segura. Las claves deben ser almacenadas de forma segura y no deben ser accesibles para usuarios no autorizados.
- **Cifrado en tránsito**: Asegurar que todo el tráfico de datos que circula entre los diferentes componentes de la red (servidores,

dispositivos, bases de datos, etc.) esté cifrado. Utilizar protocolos como HTTPS, TLS y VPNs para cifrar las comunicaciones.

- **Cifrado en reposo**: Implementar cifrado de datos en reposo para proteger la información almacenada en bases de datos y servidores. Esto es crucial especialmente para los datos sensibles, como los registros de clientes, datos financieros o cualquier información crítica relacionada con las farmacias.

5.2.3 Control de Acceso Basado en Roles

Nos permite gestionar quién tiene acceso a qué recursos dentro de la red híbrida, basándose en el rol y la función de cada usuario dentro de la organización. Esto refuerza la seguridad al limitar los privilegios de acceso de cada usuario a solo aquellos recursos que necesita para realizar su trabajo.

- **Definición de roles**: Crear roles y políticas de acceso específicas para diferentes tipos de usuarios (administradores, empleados de ventas, empleados de soporte, etc.) y asignarles privilegios adecuados a sus responsabilidades.
- **Separación de funciones:** Aplicar la separación de funciones para que ningún empleado tenga acceso completo a todas las partes críticas del sistema (por ejemplo, los empleados de ventas no deberían tener acceso a los registros financieros o a la configuración de seguridad de la red).
- **Revisión periódica de accesos:** Establecer revisiones regulares para verificar y ajustar los privilegios de acceso a medida que

cambian las responsabilidades del personal o cuando se agregan o eliminan roles dentro de la organización.

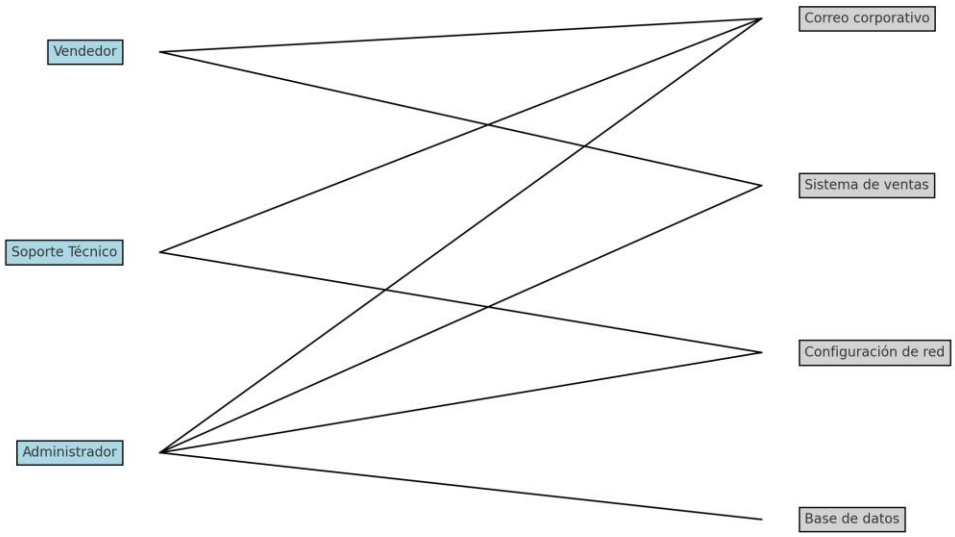

Figura 4. Diagrama de control de acceso basado en roles (RBAC)

5.2.4 Planes de Respuesta ante Incidentes

Tener un plan claro y bien definido de respuesta ante incidentes de seguridad es crucial para manejar cualquier brecha de seguridad o ataque que pueda ocurrir en la red híbrida.

- **Identificación de incidentes**: Desarrollar procedimientos claros para la identificación temprana de incidentes de seguridad, que incluyan análisis de logs, monitoreo en tiempo real, y patrones de comportamiento anómalo.
- **Comunicación y coordinación**: Asegurar que todos los departamentos involucrados en la respuesta ante incidentes (TI,

legal, comunicación, etc.) estén coordinados y tengan protocolos de comunicación claros durante un incidente.

- **Recuperación y restauración**: Establecer un proceso de recuperación para restaurar los servicios y sistemas comprometidos a su estado operativo lo más rápido posible, utilizando copias de seguridad y otros mecanismos de recuperación.

Figura 5. Flujo de respuesta ante incidentes de seguridad

El diseño de las acciones dentro de los controles de seguridad de la nueva red híbrida debe ser integral y basado en la colaboración entre todos los actores involucrados.

Desde la segmentación de la red hasta la respuesta ante incidentes, cada acción debe estar alineada con las políticas de seguridad y los riesgos específicos asociados a la infraestructura de la cadena de farmacias.

Control de Seguridad	Acción Específica	Objetivo
Segmentación de red	Separación de redes internas y externas	Limitar accesos no autorizados
Cifrado	Uso de TLS y VPN	Proteger información en tránsito
Control de accesos	Definición de roles por área	Restringir acceso a funciones críticas
Respuesta a incidentes	Plan de recuperación	Minimizar el tiempo fuera de operación

Tabla 7. Ejemplos de acciones de seguridad alineadas a cada tipo de control implementado.

Fuente: Autor

Al aplicar estas acciones, se garantiza una red híbrida robusta y resistente a los ciberataques, protegiendo tanto la información sensible como la operatividad continua del negocio.

Para que el diseño de la red híbrida no sea solo una propuesta técnica, sino una solución real frente a los riesgos detectados, fue necesario pensar en medidas concretas que respondan a esos problemas. La siguiente tabla resume de forma clara las acciones que se han considerado, explicando qué se busca lograr con cada una, qué tipo de riesgo se está abordando y a qué política de seguridad se relaciona. Esto permite ver cómo cada decisión dentro del diseño tiene un propósito que va más allá de lo técnico: proteger a la organización y su información.

Acción	Objetivo principal	Riesgo mitigado	Política relacionada
Segmentación de red	Limitar el movimiento lateral dentro de la red	Propagación de malware o intrusiones	Control de acceso
Cifrado de datos en tránsito	Proteger la información mientras se transmite	Intercepción de datos	Seguridad en la nube
Cifrado de datos en reposo	Asegurar datos sensibles almacenados	Robo de información confidencial	Seguridad en la nube
RBAC (control por roles)	Restringir accesos según funciones	Acceso no autorizado	Control de acceso
Revisión periódica de accesos	Ajustar privilegios al rol actualizado	Acumulación de privilegios innecesarios	Control de acceso
VPN y firewall perimetral	Asegurar conexiones remotas y filtrar tráfico	Intrusión externa	Protección perimetral
Plan de respuesta ante incidentes	Actuar rápidamente en caso de ciberataque	Pérdida de servicio o datos	Gestión de incidentes
Capacitación al personal	Reducir errores humanos y malas prácticas	Phishing, negligencia	Concienciación y capacitación

Tabla 8. Resumen de las acciones implementadas en la red híbrida y su relación con los riesgos y políticas de seguridad.

Fuente: Autor

Estas acciones no solo fortalecen el diseño de la red, sino que reflejan un enfoque consciente y estratégico frente a la seguridad. Cada medida ha sido pensada para que, en conjunto, respondan tanto a las amenazas más evidentes como a las más sutiles.

Vincularlas con políticas específicas asegura que el diseño no quede aislado, sino que forme parte de una cultura de seguridad sólida, pensada para crecer con la empresa y adaptarse a sus retos. Esta combinación de técnica y estrategia es lo que le da valor real a la propuesta.

Conclusiones Y Recomendaciones

Conclusiones

1. Tras culminar el desarrollo del proyecto titulado “Diseño de una Red Híbrida con seguridad perimetral, empleando criterios de seguridad informática, para una cadena de farmacias”, se llegaron a las siguientes conclusiones:

2. Diseñar una infraestructura de red donde combina una red híbrida, física y en la nube; con diferentes tecnologías de conectividad para una cadena de farmacia asegurando sus telecomunicaciones y accesos a datos de manera más segura.

3. Realizar un levantamiento de información de todos los recursos de red en producción dentro de las farmacias a nivel nacional.

4. Plantear el equipamiento óptimo donde el tráfico de información entre farmacias permita ser más eficiente.

5. Se realizó un levantamiento completo de todos los recursos de red en producción dentro de las farmacias a nivel nacional. Esta evaluación permitió identificar los principales elementos tecnológicos en uso, sus deficiencias y fortalezas, sentando las bases para la propuesta de red, con esto se cumplió el objetivo específico de levantar información de la infraestructura tecnológica.

6. Se identificó que la infraestructura tecnológica de la cadena de farmacias presentaba vulnerabilidades en su red, tanto en el acceso local como remoto, lo cual generaba riesgos de seguridad informática y ponía en peligro la continuidad del negocio, con

esto se cumplió el objetivo específico de diagnosticar los riesgos y vulnerabilidades existentes.

7. La evaluación de los equipos y conexiones permitió establecer la necesidad de una red híbrida que combine tecnología cableada y wireless, garantizando un mejor rendimiento, escalabilidad y disponibilidad del servicio, especialmente en entornos distribuidos como el farmacéutico.

8. Se determinó que la implementación de medidas de seguridad perimetral como firewalls, segmentación de red y políticas de acceso es fundamental para proteger la integridad, disponibilidad y confidencialidad de la información crítica de la organización, con esto se cumplió el objetivo específico de diseñar una red híbrida con seguridad perimetral.

9. El diseño propuesto considera buenas prácticas en seguridad informática, cumpliendo con estándares internacionales como la norma ISO/IEC 27001:2013, garantizando así una solución adaptable, segura y eficiente para las necesidades actuales y futuras de la empresa, con esto se cumplió el objetivo específico de diseñar una red híbrida con seguridad perimetral.

10. Se planteó un plan de seguridad perimetral y contingencia que incluye políticas de respaldo, continuidad de operaciones, y procedimientos ante incidentes. Este enfoque busca proteger la red frente a ataques externos, asegurar la recuperación oportuna, y fortalecer la resiliencia del entorno tecnológico, con esto se cumplió el objetivo específico de proponer un plan de contingencia ante posibles incidentes de seguridad.

11. Uno de los principales aportes del proyecto es la alineación entre la infraestructura tecnológica y los objetivos operativos de la empresa, permitiendo una red resiliente

que no solo responde a las amenazas, sino que también se adapta al crecimiento futuro de la organización.

12. Además, se evidenció que una red híbrida no solo mejora la seguridad, sino también la eficiencia de los procesos internos, al permitir conexiones seguras desde distintos puntos de venta, oficinas o incluso ubicaciones remotas, sin comprometer la confidencialidad de la información.

13. Finalmente, se concluye que la integración de soluciones tecnológicas no debe ser un fin en sí mismo, sino parte de una visión estratégica orientada a proteger el activo más valioso de cualquier organización moderna: la información.

Recomendaciones

1. Una vez desarrollado el presente proyecto, se proponen las siguientes recomendaciones, orientadas no solo a la implementación técnica, sino también a la sostenibilidad y mejora continua de la solución propuesta:

2. Se recomienda implementar el diseño de red híbrida planteado, respetando todas las consideraciones técnicas y de seguridad detalladas en este estudio. Este diseño no solo aborda las necesidades actuales de conectividad y protección, sino que también permite escalar con flexibilidad a medida que la empresa crezca.

3. Es fundamental establecer un plan de implementación progresivo, que permita evaluar el impacto de cada componente del diseño a medida que se lo pone en marcha. Esta estrategia minimiza riesgos y permite realizar ajustes sobre la marcha, asegurando una transición estable y efectiva.

4. Se aconseja realizar auditorías de seguridad periódicas, con el fin de identificar vulnerabilidades emergentes y evaluar la eficacia de los controles implementados.

Estas auditorías deben ir acompañadas de un plan de mejora continua, que permita mantener la infraestructura alineada con los estándares internacionales y las mejores prácticas en seguridad informática.

5. Resulta clave fomentar una cultura organizacional de seguridad, donde todos los colaboradores —no solo el personal técnico— comprendan los riesgos asociados al uso inadecuado de las tecnologías de información. Esto implica capacitar constantemente al personal en temas como prevención de ataques de ingeniería social, gestión de contraseñas y uso responsable de los recursos tecnológicos.

6. Se sugiere documentar todos los procesos, configuraciones y políticas relacionadas con la red y su seguridad, de forma que la gestión del conocimiento no dependa exclusivamente de individuos, sino que quede institucionalizada para futuras referencias y auditorías.

7. La empresa debe destinar un presupuesto anual para actualización tecnológica. Esto incluye no solo la renovación de hardware y licencias, sino también la contratación de servicios de soporte, consultoría y entrenamiento, garantizando así la vigencia de la solución implementada.

8. Se recomienda evaluar regularmente el rendimiento de la red híbrida mediante herramientas de monitoreo y análisis, que permitan anticiparse a cuellos de botella o incidentes, asegurando así una experiencia de usuario fluida y sin interrupciones.

9. Por último, se aconseja establecer un comité interno de seguridad, compuesto por personal de áreas clave (TI, operaciones, gerencia), que se encargue de revisar políticas, responder ante incidentes y tomar decisiones estratégicas relacionadas con la ciberseguridad y la infraestructura tecnológica.

10. Estas recomendaciones buscan no solo mantener segura y funcional la red diseñada, sino también integrar la seguridad como un pilar permanente en la operación y crecimiento de la empresa.

Limitaciones del Proyecto

Aunque el diseño propuesto se ajusta bien a las necesidades actuales de la organización, hay ciertos aspectos que no se abordaron por completo y que vale la pena considerar:

- **Resistencia al cambio y adaptación del personal:** Aunque el diseño propuesto contempla aspectos técnicos sólidos y controles de seguridad efectivos, su éxito en la práctica dependerá también de la disposición del personal a adoptar nuevas políticas, herramientas y formas de trabajo.
  Cambiar hábitos, cumplir protocolos y entender la importancia de la seguridad no siempre es inmediato. Esta dimensión humana, que escapa al diseño técnico, representa un reto potencial al momento de implementar la solución en toda la organización.

- **Dependencia de la conexión a Internet:** Al tratarse de una red híbrida que combina recursos locales con servicios en la nube, su correcto funcionamiento depende en parte de la estabilidad del Internet. Esto significa que, si llegaran a presentarse cortes o fallos prolongados en la conectividad externa, algunas funciones críticas podrían verse afectadas.

Biliografia

[1] Kumar, A., & Shukla, R. (2019). Network Architecture for Hybrid Systems: Bridging the Gap Between Cloud and On-Premise. Springer.

[2] Furht, B., Escalante, A., "Handbook of Cloud Computing", Springer, 2010, páginas referenciadas: Toda la obra.

[3] Tanenbaum, A. S., & Wetherall, D. J. (2011). Computer Networks. Pearson.

[4] Hucaby, D. (2020). Cisco Catalyst Switches Configuration Handbook. Cisco Press.

[5] Red Hat, "What is hybrid cloud?" http://www.redhat.com/es/topics/cloud- computing/what-is-hybrid-cloud, consulta: 22 de diciembre de 2024, páginas referenciadas: Sección introductoria y desarrollo.

[6] Goyal, P., "Cloud Computing: A Hybrid Approach to Cloud Integration", Wiley, 2021

[7] Mell, P., & Grance, T., "The NIST Definition of Cloud Computing", National Institute of Standards and Technology, 2011

[8] Arora, P., Soni, H., & Gupta, S., "Cloud Computing and Hybrid Cloud Architecture", Springer, 2020.

[9] Frost & Sullivan, "Global Cloud Computing Market Analysis", Frost & Sullivan, 2020

[10] López, M. (2019). Seguridad perimetral en redes empresariales. Revista de Ciberseguridad, 12(3), 45-59.

[11] García, F., & Pérez, R. (2021). Gestión de redes y su impacto en las PYMES. Universidad Técnica de Madrid.

[12] NIST (2020). Cybersecurity Framework. Disponible en: https://www.nist.gov

[13] Stallings, W. (2021). "Seguridad de redes y comunicaciones". Pearson

[14] Pfleeger, C. P., & Pfleeger, S. L. (2020). "Análisis y diseño de sistemas de seguridad". Springer

[15] Cisco Systems. (2023). "Guía práctica de seguridad empresarial". Cisco Press.

[16] Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems (3ra ed.). Wiley.

[17] Shackelford, M. (2022). Ciberseguridad en redes modernas. Wiley.

[18] González, L., & Martínez, P. (2021). *Computación en la nube: Modelos y aplicaciones*. Alfaomega.

[19] Whitman, M. E., & Mattord, H. J. (2022). *Principles of Information Security*. Cengage Learning.

[20] E. G. Little y G. L. Rogova, «An Ontological Analysis of Threat and Vulnerability», en 2006 9th International Conference on Information Fusion, 2006, pp. 1-8. doi: 10.1109/ICIF.2006.301716.

[21] ISO/IEC 27001:2013, «Information technology - Security techniques - Information security management systems - Requirements». 2013. [En línea]. Disponible en: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

[22] M. N. Aleksandrov, V. A. Vasiliev, y S. V. Aleksandrova, «Implementation of the Risk-based Approach Methodology in Information Security Management Systems», en 2021 International Conference on Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS), 2021, pp. 137-139. doi: 10.1109/ITQMIS53292.2021.9642767.

[23] M. A. Roumani, C. C. Fung, y P. Choejey, «Assessing economic impact due to cyber attacks with System Dynamics approach», en 2015 12th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), 2015, pp. 1-6. doi: 10.1109/ECTICon.2015.7207084.

[24] Z. Alimzhanova, A. Tleubergen, S. Zhunusbayeva, y D. Nazarbayev, «Comparative Analysis of Risk Assessment During an Enterprise Information Security Audit», en 2022 International Conference on Smart Information Systems and Technologies (SIST), 2022, pp. 1-6. doi: 10.1109/SIST54437.2022.9945804.

[25] A. Hapon, V. Fedorchenko, V. Martovytskyi, V. Rykun, O. Sievierinov, y I. Oleshko, «Measuring Vulnerabilities in Threat Modelling with Risk Matrix», en 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T), 2021, pp. 617-619. doi: 10.1109/PICST54195.2021.9772211.

[26] G. Castro Arica, «Introducción a la Ciberseguridad», 2021, abril de 2021. [En línea]. Disponible en: https://gerardokaztro.medium.com/introducci%C3%B3n-a-la-ciberseguridad-ff67eb3dff12

[27] D. P. F. Möller, H. Vakilzadian, y R. E. Haas, «Cybersecurity Certificate in Digital Transformation», en 2022 IEEE International Conference on Electro Information Technology (eIT), 2022, pp. 556-561. doi: 10.1109/eIT53891.2022.9813932.

[28] L. Gashi, A. Luma, y A. Aliu, «A comprehensive review of cybersecurity perspective for Wireless Sensor Networks», en 2022 International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), 2022, pp. 392-395. doi: 10.1109/ISMSIT56059.2022.9932788.

[29] N. Ismail, «What is digital transformation in business: everything you need to know», 2020, abril de 2020. [En línea]. Disponible en: https://www.information-age.com/what-is-digital-transformation-in-business-12365/

[30] «ISO/IEC 27001: What's new in IT security?», 25/10/2022, 2022.

[31] J. Jurgens y K. Bissell, «Global Cybersecurity Outlook 2022», enero de 2022.

[32] R. R. Branco y G. N. Barbosa, «Distributed malware analysis scheduling», en 2011 6th International Conference on Malicious and Unwanted Software, 2011, pp. 34-41. doi: 10.1109/MALWARE.2011.6112324.

[34] I. Sumantra y S. Indira Gandhi, «DDoS attack Detection and Mitigation in Software Defined Networks», en 2020 International Conference on System, Computation, Automation and Networking (ICSCAN), 2020, pp. 1-5. doi: 10.1109/ICSCAN49426.2020.9262408.

[35] F. Trishan, «¿Qué es la autenticación adaptativa y cuáles son sus retos y desafíos?» [En línea]. Disponible en: https://www.chakray.com/es/autenticacion-adaptativa-cuales-son-retos-desafios/

[36] A. Abrie, «¿Qué son los ataques DDoS y DoS?», 29 de septiembre de 2020. [En línea]. Disponible en: www.icm.es/2020/09/29/ddos-dos/

[37] Z. V. Altamirano Valarezo, Á. B. Pinto Astudillo, y J. D. C. Sánchez Guerrero, «Text mining aplicado a la clasificación y distribución automÁtica de correo electrónico y detección de correo SPAM», Escuela Superio Politecnica del Litoral, Guayaquil, 2007. [En línea]. Disponible en: https://www.dspace.espol.edu.ec/bitstream/123456789/3225/1/5744.pdf

[38] «Reporte de Tráfico Malicioso refleja aumento de ataques DoS en 2022», 19 de abril de 2023. [Https://itahora.com]. Disponible en: https://itahora.com/2023/04/19/reporte-de-trafico-malicioso-refleja-aumento-de-ataques-dos-en-2022/