Análisis de la interconexión para el soporte de equipos de impresión en la zona Atlántico Norte de Colombia de la empresa RICOH utilizando Redes de Nueva Generación ARMS

Cristian Camilo Contreras Diaz

Director

Raúl Bareno Gutiérrez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería - ECBTI

Redes de Nueva Generación

2024

Resumen

El problema principal se centra en la evaluación y análisis de la infraestructura de interconexión utilizada para respaldar los equipos de impresión de la empresa RICOH, en la Zona Norte Atlántico de Colombia. La investigación se enfoca específicamente en la implementación de Redes de Nueva Generación ARMS, el objetivo es mejorar la eficiencia operativa y garantizar un soporte óptimo para los equipos de impresión de la organización.

La importancia de este estudio es abordar aspectos clave, como la topología de red, la capacidad de ancho de banda, la seguridad de la información y la interoperabilidad de los sistemas; seguido a esto, se realizó un análisis detallado de los beneficios potenciales que ofrecen las redes ARMS, destacando su capacidad para adaptarse a cambios en la demanda y optimizar la gestión de recursos. Además, se llevó a cabo una revisión exhaustiva de las tecnologías y protocolos involucrados en las Redes de Nueva Generación, con un enfoque en su aplicabilidad especificando el entorno de soporte en equipos de impresión RICOH.

La metodología de investigación es de tipo explorativa y descriptiva, el desarrollo de la evaluación de impactos estructurados, el uso del software ARMS permitirá reconocer la captación y velocidad de las Redes de Nueva Generación. Esto tiene como objetivo revisar y argumentar el impacto de las nuevas tecnologías en las empresas más reconocidas de la Zona Norte, Atlántico, Colombia.

Palabras clave:

Ciberseguridad

Interconexión

Topología de red

Abstract

The main problem focuses on the evaluation and analysis of the interconnection infrastructure used to support the printing equipment of the RICOH company, in the North Atlantic Zone of Colombia. The research focuses specifically on the implementation of New Generation ARMS networks, the objective is to improve operational efficiency and ensure optimal support for the organization's printing equipment.

The importance of this study is to address key aspects, such as network topology, bandwidth capacity, information security and systems interoperability; followed by this, a detailed analysis of the potential benefits offered by ARMS networks was carried out, highlighting their ability to adapt to changes in demand and optimize resource management. In addition, a comprehensive review of the technologies and protocols involved in New Generation Networks was carried out, with a focus on their applicability by specifying the support environment in RICOH printing equipment.

The research methodology is exploratory and descriptive, the development of the structured impact assessment, the use of ARMS software will allow recognizing the uptake and speed of New Generation Networks. This aims to review and argue the impact of new technologies on the most recognized companies in the Northern Zone, Atlántico, Colombia.

Keywords:

Cybersecurity

Interconnection,

NetworkTopology

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Planteamiento del Problema

En la actualidad, las empresas buscan constantemente mejorar sus procesos y servicios mediante la incorporación de tecnologías avanzadas. En este contexto, el soporte de equipos de impresión se ha vuelto esencial para el funcionamiento eficiente de las organizaciones. En la Zona Norte de Colombia, la empresa RICOH desempeña un papel crucial en la provisión de soluciones de impresión, así mismo el análisis de la interconexión para el soporte de equipos en esta región, revela desafíos tales como la inseguridad en las redes cibernéticas que afectan la eficacia y la eficiencia de los servicios ofrecidos por la empresa.

En este sentido, la implementación de Redes de Nueva Generación, específicamente las Redes de Móviles Avanzadas (ARMS), se presenta como una solución potencial para obtener una mejor conectividad y también un soporte técnico de calidad de los equipos de impresión de RICOH en la región. A pesar de la prometedora perspectiva de las ARMS en el ámbito de la interconexión, existen desafíos y problemáticas que deben ser abordados de manera integral para ofrecer seguridad en el éxito de la implementación.

La conectividad inestable y la falta de redundancia en las redes actuales pueden resultar en tiempos de inactividad significativos. Según Jones y García (2020), "los problemas de conectividad pueden obstaculizar la comunicación efectiva entre los equipos de impresión y los centros de soporte técnico, afectando la capacidad de respuesta y la resolución rápida de problemas".

El uso de Redes de Nueva Generación Adaptive Resource Management System (ARMS) es esencial para abordar los desafíos mencionados. Según Chen et al. (2021), "las redes ARMS ofrecen flexibilidad y adaptabilidad, permitiendo una gestión eficiente de los recursos de red para optimizar la calidad del servicio en entornos dinámicos".

Los problemas identificados en la interconexión y el soporte técnico de equipos de impresión pueden tener un impacto directo en la experiencia del cliente. Según Gutiérrez y Ramírez (2018), "una experiencia del cliente deficiente puede resultar en la pérdida de la satisfacción del cliente y, en última instancia, en la disminución de la lealtad hacia la marca".

La transmisión de datos sensibles a través de las ARMS plantea preocupaciones sobre la seguridad de la información. Investigaciones de García et al. (2018) indican que "la adopción de tecnologías de vanguardia requiere un enfoque integral de seguridad que considere la protección de datos y la privacidad como elementos fundamentales".

La zona Norte Atlántico de Colombia presenta condiciones geográficas y climáticas que afectan la estabilidad de las conexiones de red, esta inestabilidad puede impactar directamente en la eficiencia operativa de los equipos de impresión de RICOH.

Como lo señala Smith et al. (2019), "las condiciones adversas del entorno pueden influir significativamente en la confiabilidad de las conexiones inalámbricas, requiriendo estrategias específicas para mitigar estos efectos."

En este contexto, es imperativo realizar un análisis exhaustivo de la interconexión para el soporte de equipos de impresión en la Zona Norte de Colombia de la empresa RICOH, con el objetivo de identificar soluciones basadas en Redes de Nueva Generación ARMS que mejoren la eficiencia operativa y la experiencia del cliente.

Justificación

El análisis de la interconexión de los equipos de impresión permite identificar posibles cuellos de botella y optimizar la eficiencia operativa. La implementación de Redes de Nueva Generación ARMS va a facilitar la comunicación instantánea entre los equipos y el centro de soporte técnico, agilizando la resolución de problemas y minimizando el tiempo de inactividad.

La implementación de una infraestructura de red más avanzada va a contribuir a la reducción de costos operativos asociados al soporte técnico.

La adopción de Redes de Nueva Generación ARMS nos va a permitir que RICOH se mantenga a la vanguardia en cuanto a tecnologías emergentes, así mismo la capacidad de integrar soluciones innovadoras y aprovechar las funcionalidades avanzadas de estas redes la cual nos va a garantizar la competitividad de la empresa en un mercado en constante evolución.

La calidad del soporte técnico es un factor clave para la fidelización del cliente, al optimizar la interconexión de los equipos de impresión, RICOH garantiza una experiencia de cliente mejorada, ofreciendo servicios más rápidos, personalizados y eficientes.

La zona Norte de Colombia presenta desafíos geográficos y logísticos que pueden afectar la eficacia del soporte técnico. Una red de nueva generación ARMS nos va a facilitar la comunicación en tiempo real, superando obstáculos geográficos y permitiendo una gestión remota más efectiva de los equipos de impresión.

En conclusión, la monografía representa una inversión estratégica para RICOH, ya que este proyecto contribuye el fortalecimiento de la posición de RICOH en el competitivo y dinámico entorno empresarial de la región Norte del Atlántico en Colombia, brindando una experiencia excepcional al cliente.

Objetivos

Objetivo General

Implementar la arquitectura de interconexión para el soporte de equipos de impresión en la zona Norte Atlántico de Colombia de la empresa RICOH utilizando Redes de Nueva Generación

Objetivos Específicos

Validar las diferentes soluciones de interconexión de la región Norte Atlántico de Colombia para la definición de aspectos de conectividad y parámetros de calidad de servicio que permitan la conexión remota con los diferentes clientes a los que se les ofrece el servicio.

Instalar las herramientas de interconexión ARM**S** a nivel de accesos seguros vía VPN hacia la integración de la revisión en tiempo real de aspectos técnicos de operación de los diferentes equipos

Simular en un entorno controlado la operación e integración de la solución que permita validar los diferentes aspectos de ciberseguridad

Marco Conceptual, Teórico y Referencial

Implementar la arquitectura de interconexión para el soporte de equipos de impresión en la zona Norte Atlántico de Colombia de la empresa RICOH utilizando Redes de Nueva Generación

Marco Conceptual

ARMS: Un Sistema Móvil Remoto Avanzado (SMRA) en Redes de Nueva Generación se refiere a una tecnología o plataforma que permite el control, monitoreo y operación de dispositivos móviles y servicios a distancia utilizando las capacidades avanzadas de las Redes de Nueva Generación, como 5G. (Smith J. , 2021)

VPN: Una red privada virtual es una tecnología que crea una conexión de red segura y encriptada sobre una red pública, como Internet. las VPN en Redes de Nueva Generación no solo garantizan la seguridad de los datos, sino que también optimizan la gestión de tráfico y mejoran la eficiencia general de la red (Jones, 2021)

IPsec (Internet Protocol Security): es un conjunto de protocolos y servicios diseñados para asegurar la comunicación de datos a través de redes IP, proporcionando autenticación, integridad y confidencialidad. IPsec asegura la comunicación a través de una red IP mediante el cifrado y autenticación de cada paquete de IP en una sesión de comunicación." La implementación de IPsec es crucial en Redes de Nueva Generación debido a su capacidad para proteger la transferencia de datos en redes móviles y de nube, asegurando que la información sensible permanezca confidencial y protegida contra accesos no autorizados (NIST, 2021)

Marco de Internet de las Cosas (IoT): Explora cómo las redes 5G son fundamentales para habilitar la conectividad masiva de dispositivos IoT, lo que permite a este proyecto conocer la automatización, la recopilación de datos en tiempo real y la toma de decisiones más inteligentes

en una amplia gama de aplicaciones, como la gestión de recursos y la atención médica. (Banafa, 2021)

Marco de Transformación Industrial (Industria 4.0): Destaca cómo las redes 5G están impulsando la transformación de la industria al proporcionar conectividad confiable y de alta velocidad en entornos industriales, lo que facilita la automatización, la optimización de la cadena de suministro y la mejora de la productividad. (Suarez, 2019)

Marco Teórico

Se tomó como referente el proyecto titulado Redes de Nueva Generación y su Aplicación en el Soporte de Equipos de Impresión. El presente proyecto se trata de las Redes de Nueva Generación (NGN) las cuales son una arquitectura avanzada que facilita la convergencia de servicios y aplicaciones sobre una única infraestructura de red. Estas redes son altamente escalables, flexibles y capaces de soportar una amplia gama de servicios, incluyendo voz, datos y video. La implementación de NGN en el soporte de equipos de impresión puede optimizar la eficiencia operativa y reducir costos. Según un estudio de Cisco, la adopción de NGN puede mejorar significativamente la velocidad y la calidad de las comunicaciones internas y externas de una empresa, lo que es crucial para el mantenimiento y soporte técnico de equipos de impresión. (Systems, 2020)

Se tomó como referente el proyecto titulado Implementación de Redes ARMS en la Industria de la Impresión. Las redes ARMS son una solución avanzada para la gestión de recursos en redes complejas. Un artículo de la IEEE detalla cómo las redes ARMS pueden optimizar la asignación de recursos y mejorar la disponibilidad y confiabilidad de los servicios de impresión. La tecnología ARMS permite una monitorización continua y la capacidad de

ajustar automáticamente los recursos según las necesidades del momento, lo cual es fundamental para el mantenimiento preventivo y correctivo de equipos de impresión. (IEEE, 2021)

Se tomó como referente el proyecto titulado Estudio de Caso: Implementación de NGN y ARMS en una Empresa de Telecomunicaciones. Un estudio de caso realizado por la empresa Huawei en una gran empresa de telecomunicaciones demuestra los beneficios de la implementación de NGN y ARMS. La empresa logró reducir los tiempos de inactividad y mejorar la eficiencia operativa gracias a la capacidad de monitorización y ajuste en tiempo real de las redes NGN y ARMS. Estos resultados son aplicables a la industria de la impresión, donde la disponibilidad y la eficiencia son cruciales para el soporte técnico.

Marco Referencial

Se tomo como referente el siguiente proyecto titulado Análisis comparativo entre las redes 4g; 5g y su influencia en la parroquia urbana san lorenzo del cantón. El proyecto de investigación tiene como objetivo realizar un análisis comparativo de la influencia que tienen las redes 4G; 5G en los moradores de la parroquia urbana San Lorenzo, lo que nos permite dar a conocer cuán importante es, ya que deben ser justificados, en su mayoría los habitantes asumen que debe existir una mejor cobertura basándonos en los que se han presentado en el transcurso de este tiempo en pandemia, de esta manera favorecer a la parroquia y que exista una mejor conectividad (MARGARITA, 2021)

Se tomo como referente el siguiente proyecto titulado Migraciones de tecnologías compone el Trabajo de Fin de Grado correspondiente a la titulación Grado en Ingeniería de las Tecnologías de Telecomunicación por la Universidad de Sevilla, por lo cual se llevó a cabo la realización de un estudio de la red para migrar las tecnologías 2G/3G/4G a la nueva tecnología 5G. El objetivo del presente proyecto es conseguir una mayor velocidad de conexión con una

latencia más baja favoreciendo así una mejor comunicación entre miles de millones de dispositivos conectados a la red (BELTRAN, 2023)

En este trabajo se pretende analizar el uso de la red móvil 4G , las redes inalámbricas y los servicios IOT entendiendo que cada una de las generaciones (desde la primera hasta la cuarta generación) las cuales han traído consigo un avance importante en tecnología con respecto a sus antecesoras, ya que cada nueva tecnología presentada, ha logrado beneficiar a los proveedores de redes móviles en el país ya que tienen la posibilidad de ofrecer mejores servicios hacia los usuarios, al tener la posibilidad de disponer de mayor conectividad, mayor seguridad y confiabilidad en la navegación. (Figueroa, 2021)

Desarrollo de la Temática

Validar las diferentes soluciones de interconexión de la región Norte Atlántico de Colombia para la definición de aspectos de conectividad y parámetros de calidad de servicio

Tras un análisis exhaustivo de las necesidades de interconexión en la región Norte Atlántico de Colombia, se ha determinado que la implementación de una solución de red privada virtual (vpn) basada en ipsec es la opción más adecuada. Esto se debe a la necesidad de garantizar la seguridad y confidencialidad de los datos que se transmiten entre las distintas ubicaciones geográficas de la región. La solución ipsec proporciona un nivel de cifrado robusto y autenticación sólida que asegura la integridad de la información sensible.

Esta elección se fundamenta en la necesidad imperiosa de salvaguardar la seguridad y la confidencialidad de los datos que circulan entre las diversas ubicaciones geográficas de la zona. La solución ipsec se destaca por proporcionar un nivel de cifrado robusto y una autenticación sólida, elementos que garantizan la integridad de la información sensible que se transmite a través de la red.

El entorno empresarial moderno requiere una infraestructura de red confiable y segura para mantener la continuidad operativa y proteger los activos digitales de una organización. En la región Norte atlántico de Colombia, donde diversas entidades pueden tener la necesidad de intercambiar datos sensibles entre sí, la implementación de una vpn ipsec se convierte en una medida esencial para mitigar los riesgos asociados con posibles ataques cibernéticos y filtraciones de información.

El entorno geográfico de la región Norte Atlántico de Colombia presenta desafíos específicos en términos de seguridad de la información y protección de datos. La implementación de una solución vpn ipsec aborda directamente estas preocupaciones al

proporcionar un mecanismo seguro para la transmisión de datos sensibles, tanto dentro como fuera de la red corporativa. Esta tecnología garantiza que la comunicación entre sedes, sucursales o filiales permanezca encriptada y protegida contra posibles amenazas externas o internas.

Además, la elección de una vpn basada en ipsec ofrece flexibilidad y escalabilidad para adaptarse a las necesidades cambiantes de la organización en la región. Con la capacidad de establecer túneles seguros a través de Internet público, la vpn ipsec permite la interconexión de diferentes ubicaciones de manera eficiente y rentable, sin comprometer la seguridad de la información. Esta flexibilidad es crucial en un entorno empresarial dinámico como el de la región Norte atlántico de Colombia, donde las empresas buscan soluciones tecnológicas que puedan crecer y evolucionar con ellas.

En conclusión, la decisión de implementar una solución de interconexión vpn ipsec en la región Norte atlántico de Colombia se basa en la necesidad de garantizar la seguridad, confidencialidad e integridad de los datos empresariales en un entorno geográfico diverso y desafiante. La tecnología ipsec ofrece los niveles de protección necesarios para satisfacer estas demandas, al tiempo que proporciona la flexibilidad y escalabilidad requeridas para adaptarse a las necesidades cambiantes de las organizaciones en la región.

El protocolo ipsec (protocolo de seguridad de internet) ha demostrado ser una solución efectiva para establecer conexiones seguras a través de redes no confiables, como Internet. Su capacidad para proporcionar cifrado de extremo a extremo y autenticación de los participantes de la comunicación brinda un nivel adicional de protección que es fundamental en entornos donde la confidencialidad de los datos es una prioridad.

Además, en la región Norte Atlántico de Colombia, donde las organizaciones pueden estar sujetas a regulaciones estrictas en materia de protección de datos, la adopción de una

solución de vpn ipsec puede ayudar a cumplir con los estándares de seguridad requeridos y evitar posibles sanciones legales. En última instancia, la elección de implementar una vpn ipsec refleja el compromiso de las entidades con la protección de la información y la garantía de la integridad de las operaciones comerciales en la región.

La implementación de ipsec garantizará la integridad de la información sensible de las empresas de RICOH, mitigando los riesgos asociados con posibles ataques cibernéticos o filtraciones de datos. con una capa de seguridad adecuada en su infraestructura de red, RICOH podrá cumplir con las regulaciones de privacidad de datos y ofrecer tranquilidad a sus clientes y socios comerciales.

Tras un análisis exhaustivo de las necesidades de interconexión en la región Norte Atlántico de Colombia, las empresas clientes de RICOH tales como Bayer, tiendas D1 y Servientrega, han concluido que la implementación de una solución de red privada virtual (vpn) basada en ipsec es la opción más adecuada para satisfacer sus requerimientos. Esta decisión se basa en la necesidad imperante de salvaguardar la seguridad y confidencialidad de los datos que se intercambian entre las diversas ubicaciones geográficas de la región. La solución ipsec se ha destacado por ofrecer un nivel de cifrado robusto y autenticación sólida, lo que garantiza la integridad de la información sensible que circula a través de la red.

Además, la solución ipsec no solo ofrece un alto nivel de seguridad, sino que también es altamente adaptable a las necesidades específicas de la empresa Bayer en términos de escalabilidad y compatibilidad con su infraestructura existente. Esto significa que la implementación de esta solución no solo satisfará las demandas actuales de interconexión, sino que también estará preparada para adaptarse y crecer en respuesta a futuras expansiones o cambios en el entorno empresarial.

Así mismo la elección de una solución de vpn ipsec para la interconexión en la región Norte atlántico de Colombia por parte de Bayer se fundamenta en la necesidad de proteger la seguridad y confidencialidad de los datos empresariales. Esta decisión refleja el compromiso de la empresa con la seguridad de la información y su capacidad para adaptarse a las demandas cambiantes del entorno empresarial moderno.

La elección de la solución ipsec se justifica en su capacidad para brindar un nivel de cifrado robusto y una autenticación sólida, elementos cruciales para garantizar la integridad de la información de carácter sensible. En un entorno empresarial donde la protección de los datos es de vital importancia, la solución ipsec emerge como una alternativa confiable y efectiva para asegurar la confidencialidad y seguridad de las comunicaciones.

La adopción de una infraestructura basada en vpn ipsec ofrece una capa adicional de seguridad al proporcionar un túnel seguro a través del cual los datos pueden ser transmitidos de manera cifrada, protegiéndolos así de cualquier intento de interceptación o acceso no autorizado. Además, esta solución ofrece un alto grado de flexibilidad y escalabilidad, lo que permite adaptarse a las necesidades cambiantes de la empresa sin comprometer la seguridad de la red.

Lo que se puede observar en la tabla 1. Es un cuadro descriptivo de las diversas soluciones de interconexión que son de mucha importancia para lograr entender por qué se utilizan las adecuadas para este proyecto, sus ventajas y desventajas, entre otros factores.

Tabla 1

Descripción de las Diversas Soluciones

Cuadro Descriptivo				
Soluciones	Ventajas	Desventajas	Pro	Contras
Tecnologías Inalámbricas (4G LTE y 5G):	Rápida implementación y expansión. Mayor flexibilidad en términos de ubicación y movilidad. Menores costos de infraestructura inicial en comparación con la fibra óptica.	Menor velocidad y capacidad en comparación con la fibra óptica. La calidad de la señal puede verse afectada por la interferencia y la congestión. Posible limitación de datos y velocidades según el plan contratado.	Menor latencia: Especialmente en el caso del 5G, la latencia se reduce significativamente, lo que permite una mejor experiencia en tiempo real Mayor capacidad de red: Las tecnologías 4G LTE y 5G tienen una mayor capacidad para manejar un mayor número de dispositivos	Costo de implementación: Desplegar infraestructura 5G es costoso, lo que puede llevar a que los proveedores de servicios inalámbricos. Consumo de energía: La tecnología 5G puede consumir más energía tanto en los dispositivos como en las antenas de red,

Fibra Óptica	Alta velocidad de transmisión de datos. Mayor confiabilidad y estabilidad de la conexión. Baja latencia, ideal para aplicaciones sensibles al tiempo.	Costos de despliegue y mantenimiento elevados. Requiere infraestructura física extensa y compleja. La instalación puede ser lenta y requerir permisos y licencias.	Ancho de banda: La fibra óptica tiene un ancho de banda muy amplio Inmunidad a interferencias electromagnéticas: A diferencia de los cables de cobre. Menor atenuación: La señal óptica en la fibra óptica puede viajar distancias más largas con menos atenuación que las señales eléctricas Seguridad: La fibra óptica es difícil de interceptar porque no emite señales	Costo inicial: La instalación de redes de fibra óptica puede ser costosa. Compatibilidad: Aunque la fibra óptica ofrece muchas ventajas, no todos los dispositivos y redes son compatibles con esta tecnología Desafíos de instalación: La instalación de fibra óptica puede ser más difícil y llevar más tiempo que la instalación

Redes de Satélite	Cobertura amplia, incluso en áreas remotas. Rápida implementación sin necesidad de infraestructura terrestre. Menor susceptibilidad a desastres naturales que puedan afectar la infraestructura terrestre.	Mayor latencia en comparación con la fibra óptica y algunas redes inalámbricas. Costos operativos y de suscripción pueden ser elevados. Limitaciones de velocidad y capacidad en comparación con otras tecnologías.	Acceso Ubicuo: Los servicios satelitales pueden llegar a áreas donde las redes terrestres no están disponibles. Resiliencia: Las redes satelitales pueden ser más resistentes a desastres naturales Velocidad de Implementación.	Costo: La construcción, lanzamiento y mantenimiento de satélites puede ser extremadamente costoso. Interferencia: Las señales satelitales pueden ser susceptibles a interferencias. Capacidad Limitada: A pesar de los avances tecnológicos, las redes satelitales pueden tener una capacidad limitada.

VPN (Red Privada Virtual)	Seguridad: Las VPN proporcionan un nivel adicional de seguridad al cifrar el tráfico de datos entre dispositivos. Privacidad: Al ocultar la dirección IP real del usuario y enmascarar su ubicación geográfica Evitar la censura: Las VPN pueden eludir restricciones geográficas.	Velocidad: El uso de una VPN puede ralentizar la conexión a Internet debido al proceso de cifrado Costo: Algunos servicios de VPN pueden ser costosos, especialmente aquellos que ofrecen características avanzadas o un mayor ancho de banda. Complejidad: Configurar y mantener una VPN puede ser complicado.	Acceso remoto seguro: Las VPN permiten a los usuarios acceder a la red de forma segura Costo: Las VPN pueden ser una opción más económica en comparación con la instalación de infraestructura. Flexibilidad: Las VPN pueden ser fácilmente escalables y pueden adaptarse a las necesidades cambiantes de la organización.	Rendimiento: El rendimiento de una VPN puede verse afectado por factores como la velocidad de conexión Dependencia de la conexión a internet: Las VPN dependen de una conexión a internet estable y de alta velocidad Configuración y mantenimiento: Configurar y mantener una VPN correctamente.

VPN IPsec	Seguridad robusta: IPsec ofrece un alto nivel de seguridad mediante la autenticación y cifrado de los datos transmitidos a través de la VPN Compatibilidad: IPsec es compatible con una amplia gama de dispositivos y sistemas operativos, lo que facilita su implementación en diferentes entornos de red. Escalabilidad: Las redes VPN IPsec	Configuración complicada: La implementación y configuración inicial de una red VPN IPsec puede ser complicada y requerir experiencia técnica, especialmente para usuarios menos experimentados. Compatibilidad limitada con NAT: A veces, las redes VPN IPsec pueden tener problemas de compatibilidad con dispositivos que utilizan la	Integridad de datos: IPsec garantiza que los datos transmitidos a través de la VPN no sean modificados ni alterados durante la transmisión, proporcionando una capa adicional de seguridad contra ataques de manipulación de datos. Autenticación mutua: IPsec admite la autenticación mutua entre los dispositivos de la VPN, lo que significa que tanto	Overhead de Procesamiento: IPsec agrega un overhead de procesamiento a los dispositivos de red, ya que los paquetes deben ser cifrados y autenticados antes de ser transmitidos a través del túnel VPN. Esto puede afectar el rendimiento de la red, especialmente en dispositivos con recursos limitados. Posibles Problemas de

	son escalables y pueden adaptarse para soportar un gran número de usuarios de usuarios. Rendimiento: IPsec generalmente ofrece un buen rendimiento, especialmente en términos de velocidad de transferencia de datos.	traducción de direcciones de red (NAT), lo que puede dificultar la conexión en ciertos entornos de red. Posibles problemas de interoperabilidad: Debido a las diferentes implementaciones de IPsec por parte de los proveedores, pueden surgir problemas de interoperabilidad al conectar dispositivos.	el cliente como el servidor deben autenticarse entre sí antes de establecer la conexión, lo que mejora la seguridad general de la comunicación. Flexibilidad: IPsec es altamente configurable y puede adaptarse a una variedad de requisitos de seguridad y configuraciones de red, lo que lo hace adecuado para una amplia gama de casos de uso.	Interoperabilidad: Aunque IPsec es un estándar, pueden surgir problemas de interoperabilidad entre diferentes implementaciones de IPsec de diferentes fabricantes. Esto puede requerir pruebas exhaustivas y ajustes para garantizar una comunicación segura y confiable entre dispositivos de diferentes proveedores.

ARMS	Descentralización: Las redes ARMS están diseñadas para ser descentralizadas, lo que significa que no dependen de un servidor centralizado. Esto las hace más resistentes a ataques y fallos de red. Privacidad: Al no depender de un servidor central, las comunicaciones a través de una red ARMS pueden ser más privadas ya que no pasan a través de un punto	Complejidad: Configurar y mantener una red ARMS puede ser más complicado que una VPN tradicional debido a su naturaleza descentralizada. Menos velocidad: Debido a su estructura descentralizada, las redes ARMS pueden tener una velocidad más lenta en comparación con las VPN tradicionales, especialmente en	Confiabilidad: ARMS utiliza tecnología de radiofrecuencia para proporcionar conexiones inalámbricas, lo que puede ser beneficioso en áreas donde las conexiones físicas son difíciles de implementar o mantener. Rapidez de implementación: Al ser una solución inalámbrica, la implementación de ARMS puede ser más rápida que otras soluciones	Limitaciones de alcance: Aunque ARMS ofrece flexibilidad, su alcance podría verse limitado en áreas con obstrucciones físicas o interferencias, lo que podría afectar la calidad de la conexión. Posible interferencia: Debido a su dependencia de señales de radio, ARMS puede ser susceptible a interferencias externas que podrían afectar la

	central que pueda ser monitoreado. Resistencia a la censura: La arquitectura descentralizada de las redes ARMS puede dificultar la censura gubernamental o corporativa, ya que no hay un punto centralizado para bloquear.	redes grandes y congestionadas. Menor disponibilidad de servicios: Dado que las redes ARMS son relativamente nuevas y menos comunes que las VPN, es posible que haya menos servicios y aplicaciones compatibles disponibles.	que requieren la instalación de infraestructura física. Flexibilidad: ARMS puede adaptarse a diversas necesidades de conectividad, ya sea para empresas, instituciones educativas o usuarios residenciales.	estabilidad de la conexión. Costo inicial: La implementación inicial de ARMS puede requerir una inversión significativa en equipos y configuraciones especializadas.

Nota. En la tabla puede encontrar información de las ventajas, desventajas, pro y contras de los tipos de redes y protocolos de seguridad.

La identificación de soluciones de interconexión dependen de factores como la infraestructura local, proveedores de servicios de telecomunicaciones y tecnologías disponibles en la región Norte del Atlántico de Colombia, para ello es crucial realizar un análisis detallado de las necesidades específicas de la conectividad, así como considerar factores como el costo, la

disponibilidad de servicios y la infraestructura existente al seleccionar la solución de interconexión más adecuada para la región, las conexiones más comunes son las siguientes.

Fibra Óptica

La implementación de redes de fibra óptica ofrece altas velocidades de transmisión de datos y una baja latencia, lo que la convierte en una opción eficiente para la interconexión en áreas urbanas y suburbanas.

Redes Inalámbricas

Tecnologías como Wi-Fi y WiMAX proporcionan conectividad inalámbrica, siendo estas ideales para entornos donde la instalación de cables es difícil o costosa, creando mejores oportunidades de conectividad eficiente.

Satélite

Esta es considerada la mejor opción de conectividad para las áreas remotas o donde la infraestructura terrestre es limitada, las conexiones vía satélite pueden ser una opción viable para establecer la interconexión.

Redes Móviles 4G/5G

Las redes móviles de alta velocidad, como 4G y 5G, ofrecen una conectividad confiable y rápida, siendo una opción efectiva para entornos urbanos y rurales, creando seguridad en los procesos.

Redes de Nueva Generación ARMS

En el contexto específico del análisis de la interconexión para el soporte de equipos de impresión RICOH, las Redes de Nueva Generación ARMS (Advanced Remote Management System) pueden ser una solución específica para la gestión remota de los dispositivos, para mejorar la conexión y presentar mejores resultados en la investigación.

VPN (Redes Privadas Virtuales)

Implementar VPN permite establecer conexiones seguras a través de Internet, lo que puede ser útil para conectar oficinas remotas y facilitar el soporte remoto.

La compatibilidad de las soluciones de interconexión del soporte de los equipos de impresión de RICOH dependerá del ancho de banda, de la latencia, de la seguridad y de la estabilidad de la conexión, siendo esto fundamental para que se logre admitir las funciones avanzadas de las impresoras a color o impresiones de alta resolución, así mismo permitiendo realizar modificaciones e impresiones en tiempo real, garantizando la respuesta rápida de los equipos en las operaciones remotas.

Instalación de las Herramientas de Interconexión ARMS

Es fundamental tener presente la terminología bien especificada para conocer el funcionamiento y descripción de cada impresora RICOH, para conocer cual método es el requerido para la instalación de las herramientas ARMS, además de tener la suficiente capacitación y conocimiento para realizar la instalación de forma correcta para no limitar el equipo e implantar las herramientas básicas para mejorar los procesos en Servientrega S.A.S, Bayer y Tiendas D1. A continuación, se describe la terminología asociada a las impresoras RICOH.

La autenticación hace referencia al proceso de verificación de la identidad de un usuario que le permite acceder al sistema. Remote Communication Gate S incluye un sistema de autenticación integrado y admite varios sistemas de autenticación externos, tales como LDAP (Protocolo ligero de acceso a directorios) y ActiveDirectory. (Ricoh, 2022).

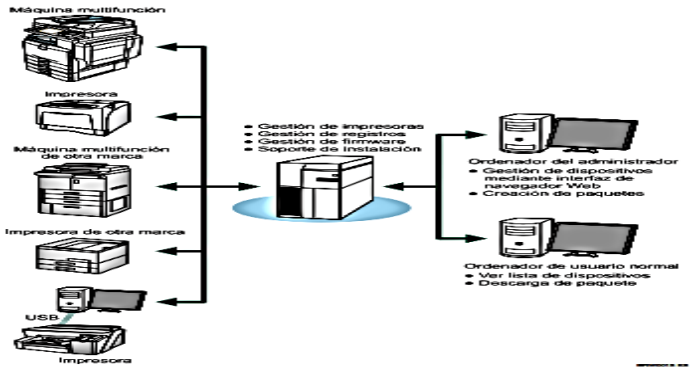
La localización hace referencia al proceso de detectar automáticamente dispositivos conectados a la red y dispositivos conectados a ordenadores a través de USB y registrarlos posteriormente en Remote Communication Gate S. (Ricoh, 2022).

Un paquete es un archivo ".exe" que incluye todos los archivos y ajustes necesarios para instalar un driver de un dispositivo. Los paquetes se utilizan para distribuir drivers de dispositivos a los usuarios. Todo el contenido registrado en un paquete se instala mediante la ejecución del archivo ".exe". Para crear paquetes hay que descargar la aplicación Package del servidor de Remote Communication Gate S e instalarla en un ordenador (Ricoh, 2022).

Puede realizar diversos ajustes en el servidor Remote Communication Gate S. Se pueden realizar ajustes en el Menú de configuración relacionado con la red, vistas, gestión de grupos, notificaciones, así como ajustes de registros y personalización individual en el servidor Remote Communication Gate S. (Ricoh, 2022)

Figura 1

Instalación de Equipos



Nota. Se describe el proceso de instalación de la siguiente manera, debido a que hay diversas redes de instalación de software a través de las conexiones en red o USB se mencionan todas. Adaptado de (Ricoh, 2022)

Conexión USB

1. Antes de instalar el software (Preparación de los elementos necesarios)
2. Instalación rápida para USB (Instalación del software)

Conexión en Red (Entorno IPv4)

1. Antes de instalar el software (Preparación de los elementos necesarios)
2. Selección del tipo y método de configuración de dirección IP
3. Conexión del ordenador y la máquina
4. Impresión de una lista de ajustes de red
5. Instalación rápida en red (Instalación del software)
6. Después de la instalación del software (Comprobación de la dirección IP)

Conexión en Red (Entorno IPv6)

1. Antes de instalar el software (Preparación de los elementos necesarios)
2. Selección del tipo y método de configuración de dirección IP
3. Conexión del ordenador y la máquina
4. Impresión de una lista de ajustes de red
5. Configuración de la dirección IPv6 a través del Web Image Monitor
6. Instalación rápida en red (Instalación del software) (Consulte pág.9)
7. Después de la instalación del software (Comprobación de la dirección IP)

Es importante contar con las siguientes instrucciones para los computadores en el momento de la instalación

1.CPU: compatible con Pentium a 500 MHz o superior

2.Memoria: 200 MB

3. Espacio mínimo disponible en el disco duro: el mismo que el mínimo recomendado para el sistema operativo

4. Requiere uno de los siguientes entornos: El equipo en el que desea instalar Remote Communication Gate S debe ser miembro del dominio.

5. Dominio de Windows NT

6. Dominio de Windows 2000 Active Directory (modo mixto, modo permitido de acceso compatible con NT)

7. Dominio de Windows 2003 Active Directory (modo mixto, intermedio)

8. Dominio de Windows Server 2008 Active Directory (Ricoh, 2022)

Dado a que se trata de equipos de impresión, la seguridad de la red es fundamental, las soluciones de interconexión deben incorporar medidas de seguridad robustas, como cifrado de datos, autenticación segura y protección contra amenazas cibernéticas, para garantizar la integridad y confidencialidad de la información de la impresión, asegurarse de que las soluciones de interconexión sean compatibles con los protocolos de comunicación utilizados por los equipos, esto puede incluir protocolos estándar de la industria o protocolos específicos de RICOH.

Es esencial realizar pruebas piloto y colaborar estrechamente con el equipo de soporte técnico de RICOH y los proveedores de servicios de interconexión para garantizar que la solución seleccionada satisfaga adecuadamente las necesidades específicas de soporte remoto, para equipos de impresión en la región Norte del Atlántico de Colombia.

Cliente Servientrega S.A.S

El cliente SERVIENTREGA S.A.S ubicado en la zona Norte de atlántico en la ciudad de Soledad, en la cual se instalará las herramientas de interconexión ARMS en 4 de los equipos

ubicados en esta zona, con el propósito de verificar como está el funcionamiento de los equipos en el cliente, para generar la seguridad en la red y a su vez monitorear en tiempo real el estado actual de los equipos instalados.

Cliente Bayer

Bayer es una empresa multinacional con una amplia presencia global y una destacada operación en Barranquilla, Atlántico. La implementación de Redes de Nueva Generación ARMS y VPN IPsec en las impresoras de RICOH es una estrategia clave que refleja el compromiso de la empresa con la eficiencia operativa y la seguridad de la información.

La elección de estas tecnologías para las impresoras de RICOH en Bayer Barranquilla responde a varios factores estratégicos:

Eficiencia operativa: Las redes ARMS permiten una gestión remota avanzada de los dispositivos de impresión, lo que facilita la supervisión y el mantenimiento de las impresoras desde una ubicación central. Esto reduce la necesidad de intervenciones físicas en cada impresora, optimizando los recursos y minimizando el tiempo de inactividad.

Seguridad de la información: En un entorno empresarial como el de Bayer, donde la protección de datos confidenciales es crucial, la implementación de VPN IPsec en las impresoras de RICOH garantiza una comunicación segura y cifrada entre los dispositivos y la red corporativa. Esto protege la integridad y la confidencialidad de los documentos que se imprimen, así como de cualquier información sensible que pueda transmitirse a través de las impresoras.

Adaptación a la era digital: En un mundo cada vez más interconectado, es fundamental que las empresas implementen tecnologías que les permitan mantenerse al día con las demandas del mercado y las tendencias tecnológicas. La integración de Redes de Nueva Generación en las impresoras de RICOH demuestra el compromiso de Bayer Barranquilla con la innovación y la

transformación digital, lo que contribuye a mejorar la productividad y la competitividad de la empresa en el mercado.

Así mismo, la implementación de redes ARMS y VPN IPsec en las impresoras de RICOH en Bayer Barranquilla es una decisión estratégica destinada a mejorar la eficiencia operativa, garantizar la seguridad de la información y promover la innovación tecnológica en la empresa, consolidando así su posición como líder en su sector.

Cliente D1

Tiendas D1, una cadena de supermercados ubicada en Barranquilla, Atlántico, es reconocida por su compromiso con la calidad y la eficiencia en la atención al cliente. Con una sólida presencia en el mercado local, la empresa se esfuerza constantemente por mantenerse a la vanguardia en términos de tecnología para mejorar sus operaciones y ofrecer un mejor servicio.

En un mundo donde la seguridad y la conectividad son aspectos críticos para el éxito empresarial, Tiendas D1 ha tomado la decisión estratégica de implementar Redes de Nueva Generación ARMS y VPN IPsec en sus impresoras de la marca RICOH. Esta iniciativa demuestra el compromiso de la empresa con la modernización y la optimización de sus procesos internos.

La implementación de redes ARMS permite a Tiendas D1 administrar de manera remota sus impresoras RICOH, lo que facilita la gestión y el monitoreo de los dispositivos desde cualquier ubicación. Esto se traduce en una mayor eficiencia operativa, ya que el personal de TI puede realizar actualizaciones, diagnosticar problemas y realizar mantenimiento sin necesidad de intervenir físicamente en cada impresora, lo que ahorra tiempo y recursos.

Por otro lado, la adopción de VPN IPsec garantiza la seguridad de la red y la protección de los datos sensibles de la empresa. Esta tecnología cifra la comunicación entre las impresoras

RICOH y los servidores de la empresa, lo que minimiza el riesgo de intrusiones o pérdida de información confidencial. Con la implementación de VPN IPsec, Tiendas D1 asegura la integridad y confidencialidad de sus datos, lo que contribuye a fortalecer la confianza de los clientes y socios comerciales en la marca.

En conclusión, la decisión de Tiendas D1 de implementar redes ARMS y VPN IPsec en sus impresoras RICOH demuestra su compromiso con la innovación tecnológica y la seguridad empresarial. Estas medidas no solo mejoran la eficiencia operativa, sino que también protegen los activos digitales de la empresa, lo que contribuye a su crecimiento y éxito continuo en el competitivo mercado de supermercados.

Parámetros del servicio Qos: En el contexto actual de las redes de comunicación, la calidad del servicio (QoS) juega un papel fundamental en la satisfacción del usuario y el rendimiento de las aplicaciones. La ejecución efectiva de QoS se convierte en un desafío crucial para garantizar una experiencia de usuario óptima en entornos cada vez más exigentes. En este caso se centra en mejorar el servicio QoS, mediante el uso de soluciones de interconexión basadas en la arquitectura ARM. La adopción de estas herramientas proporciona una plataforma versátil y eficiente para optimizar el flujo de datos, ayudando a gestionar los recursos de red de una manera más rápida, lo que resulta en una mejora significativa en la entrega de servicios y una experiencia de usuario mejorada.

La calidad del servicio o más conocido como QoS es un factor crítico en cualquier implementación del software, especialmente cuando se trata de sistemas de gestión remota como el ARMS en impresoras. La instalación del software ARMS tiene un impacto directo en la eficiencia operativa y el rendimiento de los equipos de impresión, por lo que la consideración de la calidad del servicio es esencial.

En primer lugar, la instalación del software ARMS implica la configuración de parámetros específicos que determinarán cómo se asignan los recursos de red para garantizar la prioridad de los servicios críticos. El QoS en este contexto se centra en garantizar la entrega oportuna y confiable de la información de gestión entre las impresoras y el sistema central, minimizando posibles demoras y optimizando la eficiencia operativa (Zhang, 2020)

En segunda instancia, la calidad del servicio sobre la instalación del ARMS aborda la gestión de ancho de banda, asegurando que las comunicaciones entre las impresoras y el sistema central no compitan con otros flujos de datos críticos. La asignación eficiente de recursos se traduce en una mayor capacidad de respuesta y una menor probabilidad de interrupciones en la transmisión de datos de gestión (Choudhary, 2020)

Otro aspecto clave de la calidad del servicio en la instalación del software ARMS es la gestión de la latencia. La comunicación en tiempo real entre el sistema central y las impresoras requiere una baja latencia para garantizar una interacción fluida y una toma de decisiones rápida en caso de eventos críticos o actualizaciones de firmware (Mohan, 2020)

La seguridad juega un papel crucial en la calidad del servicio durante la instalación del ARMS. La implementación de medidas de seguridad robustas, como la encriptación de datos y la autenticación segura, no solo protege la integridad de la información transmitida, sino que también contribuye a la confiabilidad general del sistema (Karmakar, 2019)

Finalmente, la calidad del servicio sobre la instalación del software ARMS en impresoras se centra en la optimización de recursos, la gestión de ancho de banda, la minimización de la latencia y la garantía de la seguridad de la comunicación, todos elementos cruciales para maximizar la eficiencia y la confiabilidad del sistema.

Esta iniciativa se orienta hacia la integración de la revisión en tiempo real de aspectos técnicos de operación de los diversos equipos que componen nuestro entorno tecnológico, por medio de la implementación de esta solución la cual permitirá no solo una supervisión más eficiente, sino también una respuesta inmediata a posibles incidencias, asegurando así la continuidad y eficacia de las operaciones. Este paso estratégico hacia la conectividad segura, contribuirá significativamente a la mejora continua de los procesos, garantizando un entorno tecnológico robusto y eficiente.

En la empresa Servientrega S.A.S sucursal Norte atlántico, se realizó la instalación de las herramientas de interconexión ARMS por medio de software y personal capacitado, el cual permitirá contar con una mayor visibilidad y control sobre los sistemas, facilitando así la detección y respuesta ante posibles incidencias, asegurando la continuidad de los servicios con los más altos estándares de calidad y seguridad.

A continuación, se presenta el registro detallado de la implementación inicial del sistema ARMS en la máquina láser Ricoh 6503, ubicada estratégicamente en la zona de masivos en las instalaciones de Servientrega S.A.S.

Este proceso incluye exhaustivas especificaciones de instalación que abarcan desde los requisitos técnicos hasta los procedimientos detallados, con el propósito de garantizar una configuración óptima. Además, se proporciona información detallada sobre el modelo de uso específico para esta máquina, destacando las capacidades y funcionalidades que ofrece en el contexto de las operaciones.

El paso inicial en la incorporación de ARMS a la maquinaria láser no solo representa un avance tecnológico significativo, sino que también establece una base sólida para aprovechar al máximo las capacidades de monitoreo y gestión en tiempo real que esta herramienta proporciona

en el entorno de producción masiva; La primera instalación se implementó en la maquina RICOH MP 6503 ubicada en la zona de masivos en la sede de Servientrega S.A.S

Modelo: RICOH MP6503

Serial: G657L300051

Ubicación: Masivos

Figura 2

Maquina Servientrega S.A.S

Nota. Impresora MP6503, blanco y negro, de la empresa Servientrega. Fuente. Creación propia.

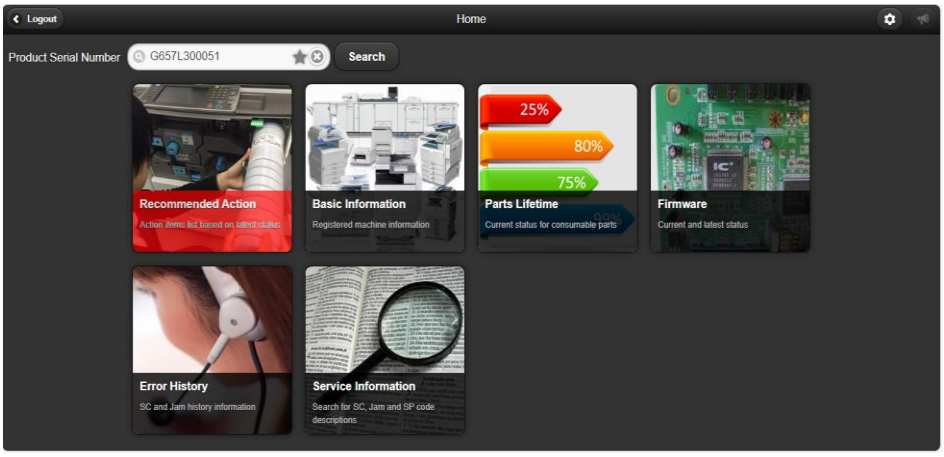
Página Principal

La página principal de la instalación del ARMS ofrece una visión integral y centralizada de todo el proceso de implementación de esta herramienta en la infraestructura, en primer lugar, proporciona una descripción general del proyecto, destacando los objetivos y beneficios clave que se esperan lograr con la integración de ARMS en nuestro entorno tecnológico, así mismo presenta un mapa visual del progreso de la instalación, indicando claramente las etapas completadas y las pendientes.

Asimismo, se incluye información detallada sobre las máquinas y dispositivos específicos que ya han sido equipados con ARMS, proporcionando detalles sobre las características técnicas y funcionalidades adicionales que se han habilitado en cada caso. Esto permite a los usuarios familiarizarse con las capacidades mejoradas de sus equipos y comprender cómo integrar eficientemente ARMS en sus flujos de trabajo diarios.

Figura 3

Página Principal del Sistema ARMS



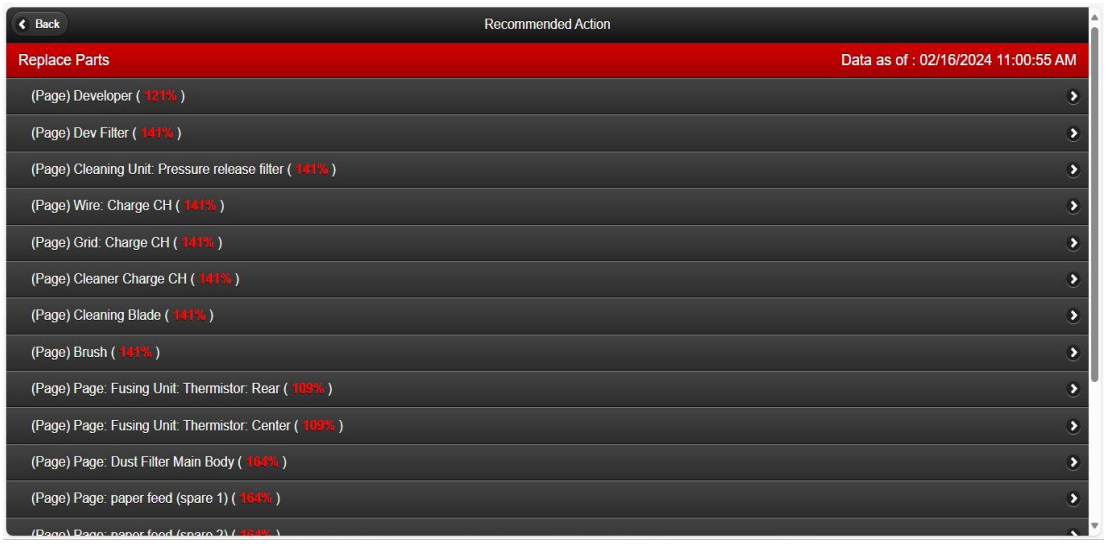
Nota. Página principal del sistema ARMS donde se detalla sus diferentes funciones. Fuente. Creación propia.

Página de Recomendaciones

Las páginas de recomendaciones desempeñan un papel fundamental debido a que se presentan como un recurso integral que guía a los usuarios a lo largo de la configuración y optimización de ARMS en sus entornos específicos. En estas páginas, se pueden encontrar sugerencias detalladas sobre las mejores prácticas de instalación, configuración y personalización para asegurar un despliegue eficiente, adaptado a las necesidades particulares. Así mismo, estas recomendaciones abarcan aspectos cruciales como la gestión de recursos, la seguridad, la integración de los sistemas existentes, proporcionando una referencia valiosa para garantizar el rendimiento óptimo y la estabilidad del sistema.

Figura 4

Página de Recomendaciones del Sistema ARMS



Nota. Página de información y recomendación de las partes del equipo de impresión, en él se puede ver porcentaje de cada unidad instalada, cuando está en rojo nos indica que ya se debe cambiar. Fuente. Creación propia.

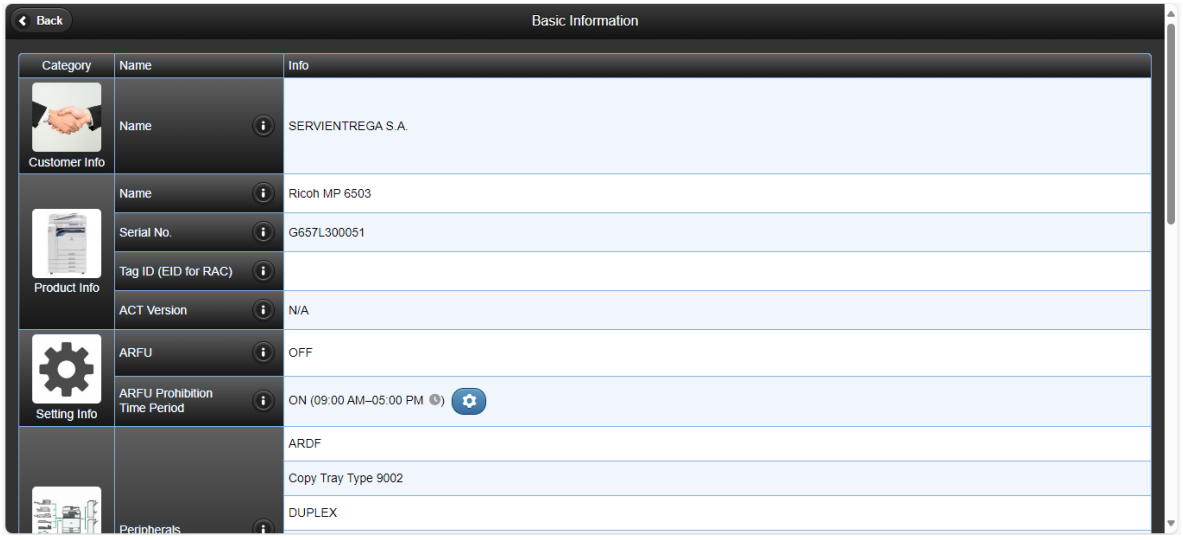
Información Básica

La Información Básica para Servientrega de ARMS se centra en proporcionar una comprensión esencial del funcionamiento, este sistema integra datos clave y herramientas analíticas avanzadas para ofrecer a los usuarios una visión integral de los recursos disponibles, permitiendo una toma de decisiones informada y estratégica. La información básica es importante para conocer sobre la asignación de recursos, seguimiento de actividades y análisis de tendencias, lo que permite adaptarse ágilmente a los cambios en el entorno operativo.

Las ARMS se convierten en una herramienta fundamental para mejorar la planificación y ejecución de tareas, promoviendo así la eficacia y el éxito en diversas áreas de aplicación.

Figura 5

Información Básica del Sistema ARMS



Nota. Página de información básica sobre el sitio de instalación del equipo de impresión, donde podemos ver el nombre del cliente, el modelo del equipo, el número de serial. Fuente. Creación propia.

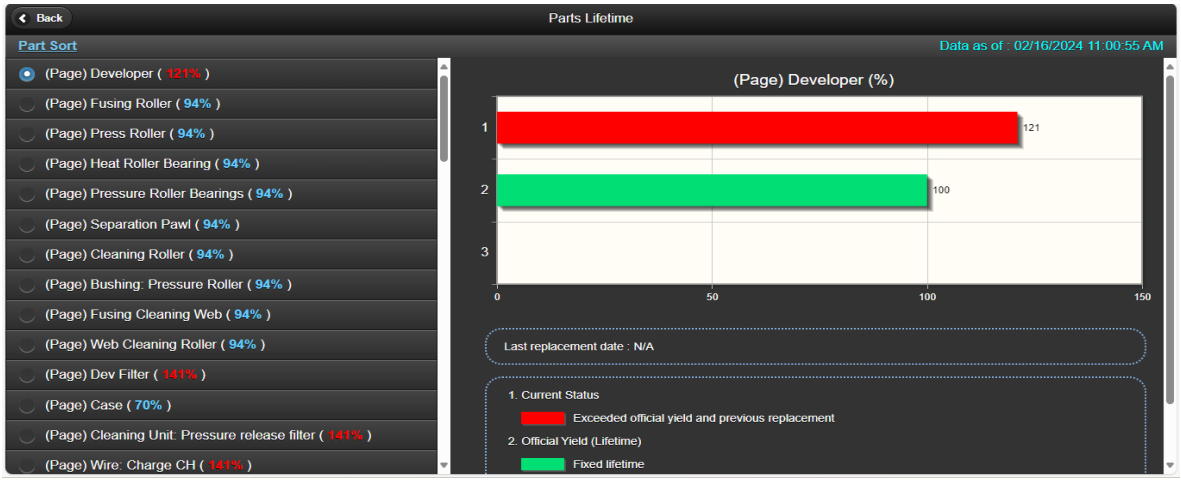
Tiempo de Vida de las Partes

El Tiempo de Vida de las Partes emerge como un factor crítico para garantizar la continuidad y eficiencia operativa de la maquina gracias a la longevidad y el rendimiento que cada componente desempeña, por el papel fundamental en la capacidad del ARMS para gestionar eficazmente los recursos y optimizar las operaciones logísticas de Servientrega S.A.S. Lo que muestra es una elección de partes y componentes con una durabilidad adecuada, así como la implementación de prácticas de mantenimiento preventivo, por lo que se vuelven esenciales para maximizar el tiempo de vida útil del sistema ARMS.

Esta estrategia no solo asegura una operación continua y sin interrupciones, sino que también contribuye a la rentabilidad a largo plazo, a minimizar los costos asociados con reparaciones y reemplazos frecuentes.

Figura 6

Tiempo de Vida de las Partes del Sistema ARMS



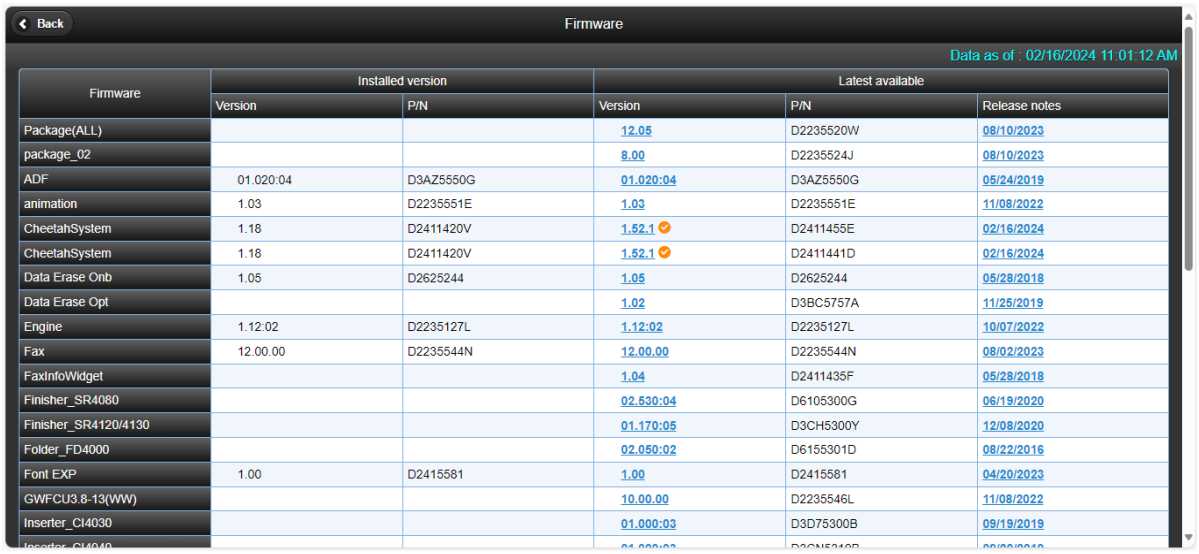
Nota. Página de información y recomendación de las partes del equipo de impresión, en él se puede ver porcentaje de cada unidad instalada, cuando está en rojo nos indica que ya se debe cambiar. Fuente. Creación propia.

Firmware

El firmware en el contexto de ARMS, consiste en un software integrado en el hardware de las armas, no solo controla aspectos básicos como la seguridad y la precisión, sino que también permite la personalización y actualización de características específicas. Servientrega S.A.S se benefician del firmware del ARMS al tener la capacidad de ajustar la configuración de sus armas para adaptarse a diferentes situaciones o mejorar su eficacia. Además, las actualizaciones periódicas del firmware pueden proporcionar mejoras en la seguridad, la velocidad de respuesta y la integración con tecnologías emergentes, garantizando que el usuario tenga acceso a lo último en innovación para maximizar la eficiencia y la seguridad en el uso de estas tecnologías avanzadas.

Figura 7

Firmware del Sistema ARMS



Firmware	Installed version		Latest available		
	Version	P/N	Version	P/N	Release notes
Package(ALL)			12.05	D2235520W	08/10/2023
package_02			8.00	D2235524J	08/10/2023
ADF	01.020:04	D3AZ5550G	01.020:04	D3AZ5550G	05/24/2019
animation	1.03	D2235551E	1.03	D2235551E	11/08/2022
CheetahSystem	1.18	D2411420V	1.52.1	D2411455E	02/16/2024
CheetahSystem	1.18	D2411420V	1.52.1	D2411441D	02/16/2024
Data Erase Onb	1.05	D2625244	1.05	D2625244	05/28/2018
Data Erase Opt			1.02	D3BC5757A	11/25/2019
Engine	1.12:02	D2235127L	1.12:02	D2235127L	10/07/2022
Fax	12.00.00	D2235544N	12.00.00	D2235544N	08/02/2023
FaxInfoWidget			1.04	D2411435F	05/28/2018
Finisher_SR4080			02.530:04	D6105300G	06/19/2020
Finisher_SR4120/4130			01.170:05	D3CH5300Y	12/08/2020
Folder_FD4000			02.050:02	D6155301D	08/22/2016
Font EXP	1.00	D2415581	1.00	D2415581	04/20/2023
GWFCU3.8-13(WW)			10.00.00	D2235546L	11/08/2022
Inserter_CI4030			01.000:03	D3D75300B	09/19/2019

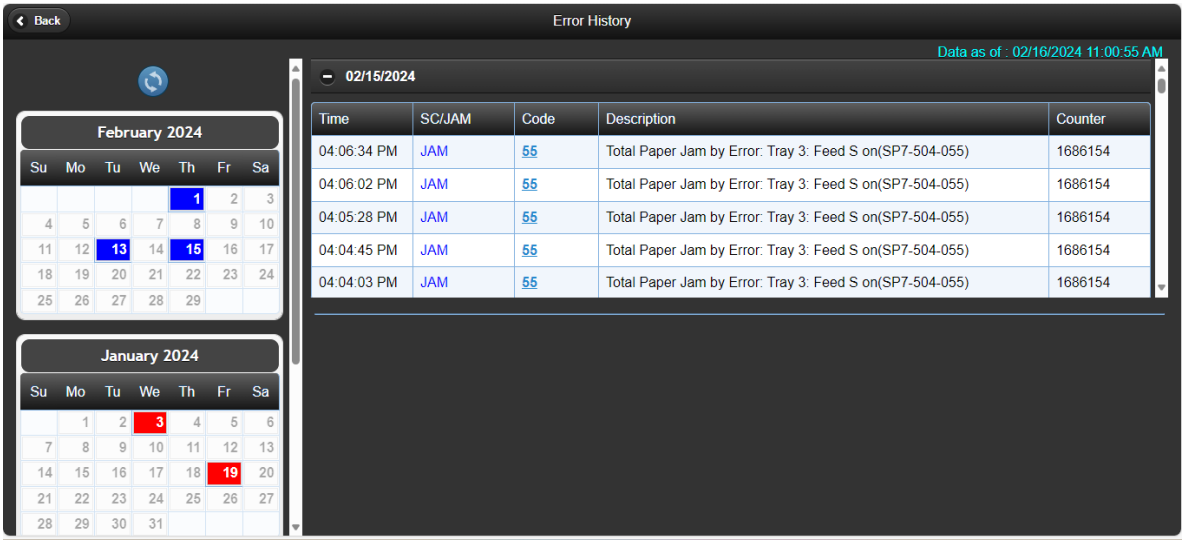
Nota. Página de información y recomendación de las partes del equipo de impresión, en él se puede ver porcentaje de cada unidad instalada, cuando está en rojo nos indica que ya se debe cambiar. Fuente. Creación propia.

Historial de Errores

El Historial de Errores es una herramienta crucial para Servientrega S.A.S debido a que proporciona un registro detallado de los inconvenientes encontrados durante el uso del sistema, este historial no solo actúa como una guía para diagnosticar problemas, sino que también ofrece insights valiosos para mejorar la estabilidad y el rendimiento del software. Cada entrada en el historial es una ventana al pasado, permitiendo al usuario analizar patrones recurrentes, identificar tendencias y aplicar soluciones efectivas. A través de la revisión regular del Historial de Errores se puede optimizar la experiencia de ARMS al abordar proactivamente cualquier problema potencial, garantizando así un funcionamiento más eficiente y confiable del sistema.

Figura 8

Historial de Errores del Sistema ARMS



Nota. Página de historial de errores del sistema ARMS donde nos indica las fechas donde el equipo presentó atascos o códigos de bloqueo; También nos indica una breve descripción sobre el error que presentó. Fuente. Creación propia.

Servicio de Información

El Servicio de Información para Servientrega se presenta como una herramienta integral y accesible diseñada para satisfacer las necesidades informativas de todos los operarios que cuentan con el servicio. Con un enfoque centrado en la transparencia y la eficiencia, este servicio proporciona una fuente confiable de datos relacionados con ARMS, ofreciendo detalles sobre actualizaciones, políticas, y cualquier cambio relevante en el sistema. Además, se destaca por su capacidad para responder rápidamente a las consultas de los usuarios, brindando asistencia oportuna y garantizando una experiencia satisfactoria. Con el compromiso de mantener al cliente informado y empoderado, el Servicio de Información para los usuarios de ARMS juega un papel crucial en fortalecer la relación entre la plataforma y su comunidad de usuarios.

Figura 9

Servicio de Información

Nota. Página de servicio de información, donde podemos filtrar y buscar de forma más específica los códigos o atascos que haya presentado el equipo, también podemos ingresar al modo SP y obtener más información sobre el equipo de impresión. Fuente. Creación propia.

La segunda instalación se implementó en la maquina RICOH MP4055 ubicada en el pasillo bajando las escaleras en la sede de Servientrega S.A.S

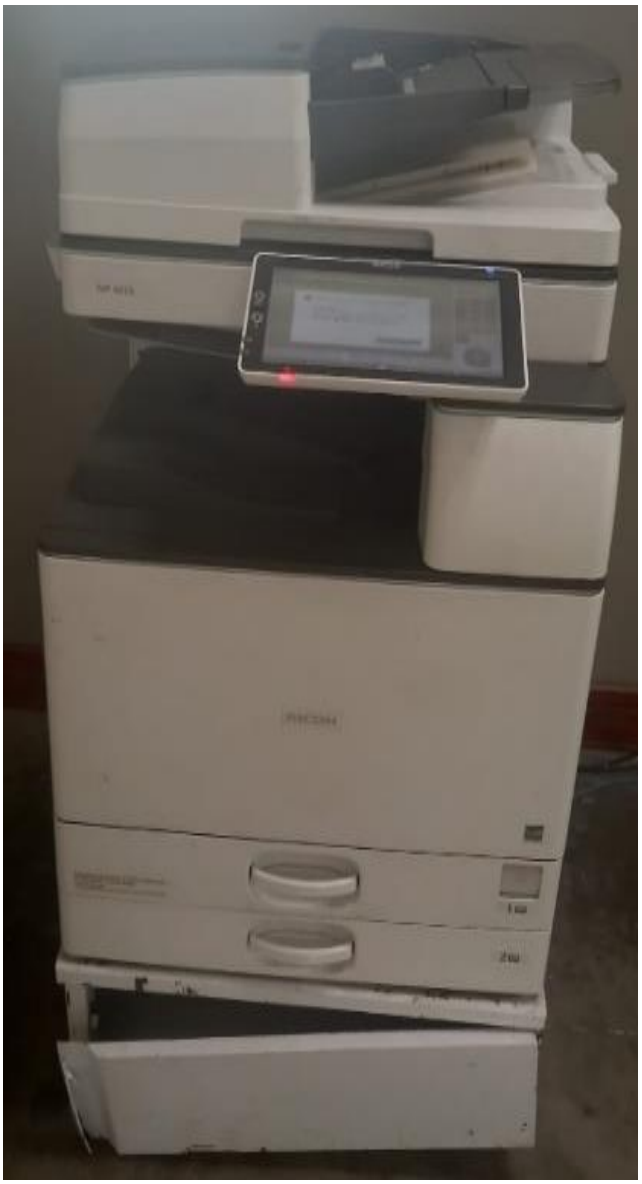
Modelo: RICOH MP4055

Serial: C329R700675

Ubicación: Pasillo Bajando las Escaleras

Figura 10

Máquina de Servientrega S.A.S



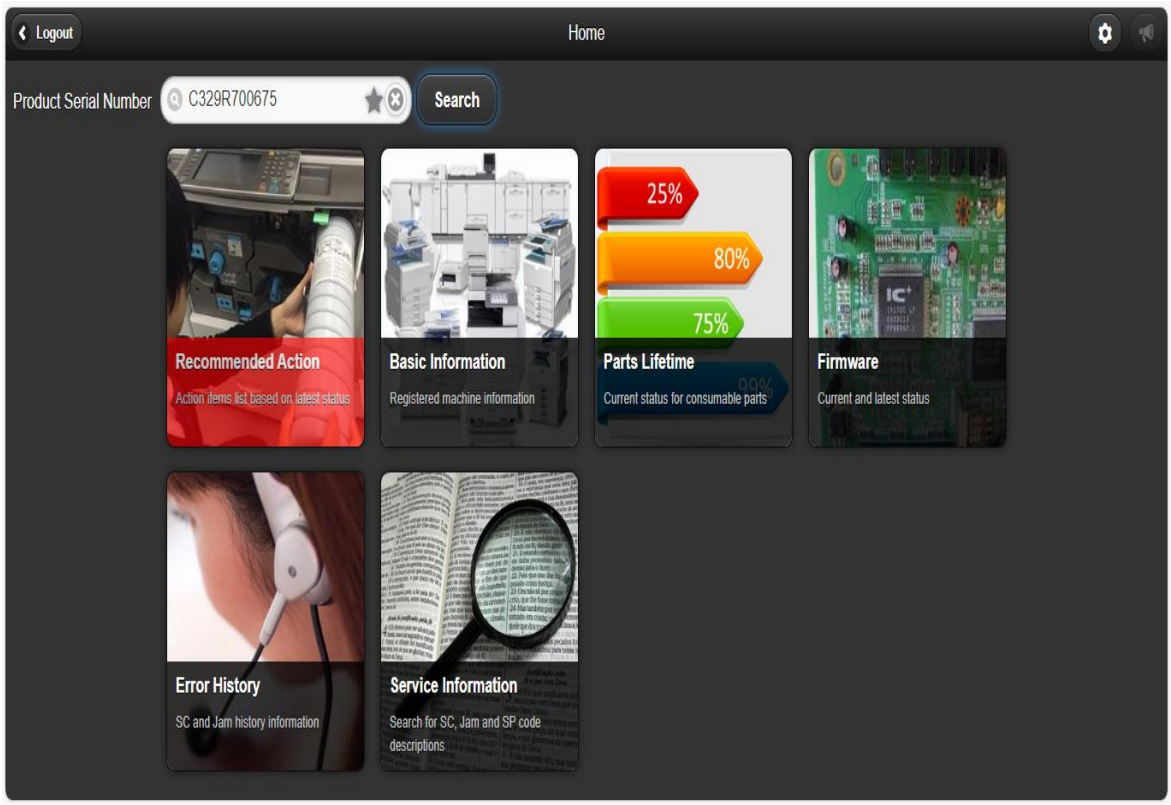
Nota. Impresora MP4055, blanco y negro, de la empresa Servientrega. Fuente. Creación propia.

Página Principal

Como se logra apreciar en Servientrega S.A.S se instaló la segunda maquina RICOH con el monitoreo ARMS, el cual permite conocer cómo está el funcionamiento de la maquina si es viable o no su ubicación de trabajo, además de presentar al cliente un reporte detallado del tiempo de vida de las partes, permitiendo así que el monitoreo por parte de los técnicos RICOH sea más eficiente y presten de manera rápida un servicio ágil.

Figura 11

Página Principal del Sistema ARMS



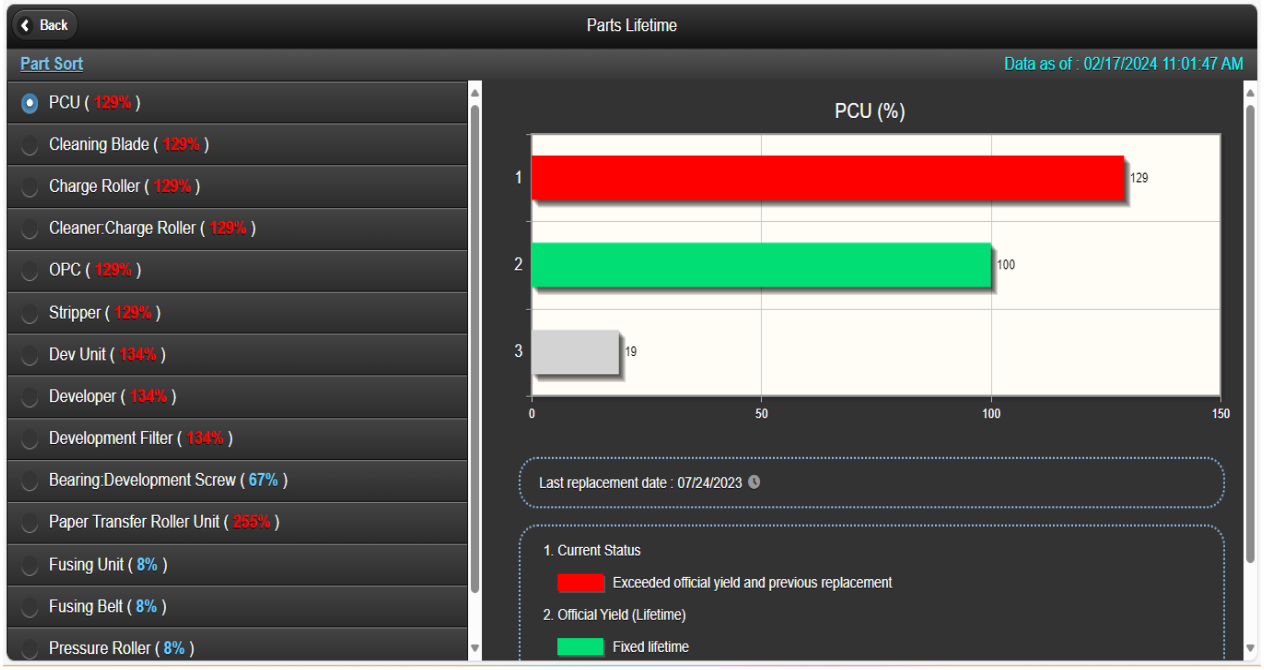
Nota. Página principal del sistema ARMS donde se detalla sus diferentes funciones. Fuente. Creación propia.

Tiempo de Vida de las Partes

Como se mencionaba anteriormente la implementación del ARMS en Servientrega S.A.S, permitiendo operar de manera precisa los problemas e inconvenientes que se presenta en la máquina, como se puede apreciar en la siguiente imagen muestra el porcentaje real de cómo está la vida útil del repuesto, tal como la OPC que se encuentra en un porcentaje del 129%, esto demostrando que se debió pedir el repuesto cuando estaba en el 80% y no esperar que este sobre pasando el límite de la parte.

Figura 12

Tiempo de Vida de las Partes del Sistema ARMS



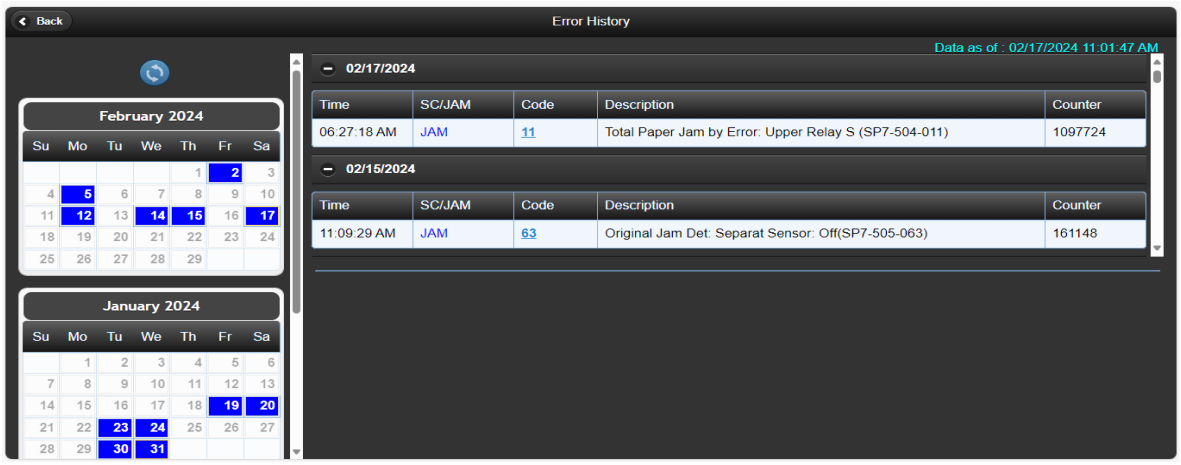
Nota. Página de información y recomendación de las partes del equipo de impresión, en él se puede ver porcentaje de cada unidad instalada, cuando está en rojo nos indica que ya se debe cambiar. Fuente. Creación propia.

Historial de Errores

El historial de errores de esta máquina presenta mayor supervisión por parte de los técnicos de RICOH realizando acciones preventivas sobre las emergencias o errores que no se puedan solucionar de una vez, como se logra observar en el calendario se están realizando mantenimientos de forma secuencial de la maquina ubicada en el pasillo, debido a su gran uso por la ubicación estratégica.

Figura 13

Historial de Errores del Sistema ARMS



Nota. Página de historial de errores del sistema ARMS donde nos indica las fechas donde el equipo presentó atascos o códigos de bloqueo; También nos indica una breve descripción sobre el error que presentó. Fuente. Creación propia.

La tercera instalación se implementó en la maquina RICOH MPC 307 ubicada en la zona piso 1 laboratorio en la sede de BAYER S.A.S

Modelo: RICOH MPC307

Serial: C508P902240

Ubicación: Piso 1 laboratorio

Figura 14

Máquina de Bayer S.A.S

Nota. Impresora MPC307, a color, de la empresa Bayer ubicada en la zona de laboratorio. Fuente. Creación propia.

La cuarta instalación se implementó en la maquina RICOH MPC 307 ubicada en la zona Piso 1 área de ingeniería en la sede de BAYER S.A.S

Modelo: RICOH MPC307

Serial: C508P902258

Ubicación: Piso 1 área de ingeniería

Figura 15

Máquina de Bayer S.A.S

Nota. Impresora MPC307, a color, de la empresa Bayer ubicada en el piso 1 de la zona de ingeniería. Fuente. Creación propia.

La quinta instalación se implementó en la maquina RICOH MP7503 ubicada en la zona Piso 1 área logística en la sede de D1 S.A.S

Modelo: RICOH MP7503

Serial: G667L800435

Ubicación: Piso 1 área logística

Figura 16

Máquina de D1 S.A.S

Nota. Impresora MP7503, blanco y negro, de la empresa D1 ubicada en el piso 1 del área de logística. Fuente. Creación propia.

La sexta instalación se implementó en la máquina RICOH IM7000 ubicada en la zona piso 2 área de ventas en la sede de D1 S.A.S

Modelo: RICOH IM7000

Serial: 4021C700466

Ubicación: piso 2 área de ventas

Figura 17

Máquina de D1 S.A.S

Nota. Impresora IM7000, blanco y negro, de la empresa D1 ubicada en el piso 1 del área de logística. Fuente. Creación propia.

La implementación de una red privada virtual (VPN) para la instalación del ARMS (Advanced Routing and Management System) en impresoras RICOH añade una capa adicional de seguridad y gestión de datos, debido a esto se presentan los parámetros clave que deben considerarse al configurar una VPN para esta finalidad:

Protocolo VPN

Seleccionar un protocolo VPN seguro es esencial. IPSec (Protocolo de seguridad de Internet) y OpenVPN son opciones comunes, IPSec es altamente seguro y se integra bien con sistemas de gestión remota, mientras que OpenVPN es conocido por su flexibilidad y compatibilidad multiplataforma.

Modo de Operación

Permite definir el modo de operación de la VPN, ya sea en modo túnel (toda la comunicación entre impresoras y el sistema central está encapsulada) o en modo transporte (solo los datos están cifrados). El modo túnel suele ser preferido para una mayor seguridad.

Autenticación

Establecer un método sólido de autenticación para garantizar que solo dispositivos autorizados accedan a la red. Las opciones incluyen certificados digitales, nombres de usuario/contraseñas seguras o autenticación multifactorial.

Encriptación

Configurar el nivel de encriptación para proteger los datos transmitidos. Se recomienda utilizar algoritmos de encriptación fuertes como AES (Estándar de cifrado avanzado) con claves de longitud adecuada para garantizar la seguridad de la comunicación.

Direcciones IP y Subredes

Asignar rangos de direcciones IP para las impresoras y el sistema central en la VPN. Definir las subredes correspondientes y asegurarse de que no entren en conflicto con otras redes existentes para evitar problemas de conectividad.

Al considerar estos parámetros al configurar una VPN para la instalación del ARMS en impresoras RICOH, se establecerá una infraestructura segura y eficiente que facilitará la gestión remota y la comunicación fluida entre los dispositivos de impresión y el sistema central.

Comandos de configuración para accesos seguros, destacando los parámetros de la VPN en relación con la autenticación, integridad y confidencialidad.

En un entorno cada vez más digitalizado, la seguridad de la información es de suma importancia. La implementación de redes privadas virtuales (VPN) es una de las estrategias más

efectivas para garantizar la seguridad en las comunicaciones, permitiendo el acceso seguro a recursos desde ubicaciones remotas. En este proyecto, exploraremos los comandos de configuración para asegurar el acceso mediante VPN, enfocándonos en los parámetros relacionados con la autenticación, integridad y confidencialidad, también conocidos como los principios de la CIA (Confidencialidad, Integridad y Disponibilidad).

Configuración de la VPN

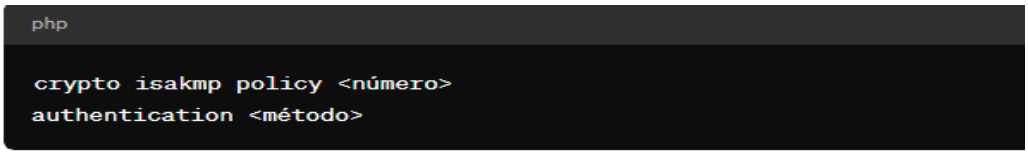
La configuración de una VPN implica una serie de pasos, entre los que se encuentran la selección de protocolos, algoritmos y parámetros de seguridad.

Autenticación

La autenticación asegura que los usuarios y dispositivos sean quienes dicen ser antes de permitirles el acceso a la red. En una VPN, esto se logra mediante la implementación de métodos de autenticación robustos. Algunos comandos relevantes para la configuración de la autenticación incluyen:

Figura 18

Protocolo de Autentificación en las Redes VPN



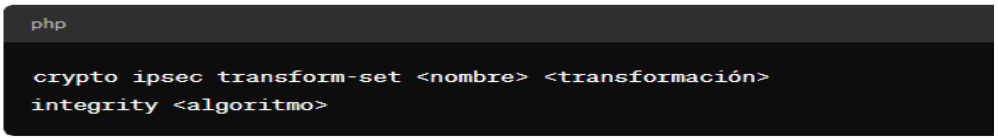
Nota. Se muestra imagen de la ejecución del protocolo de isakmp. Fuente. Creación propia.

Integridad

La integridad garantiza que los datos no sean modificados ni alterados durante la transmisión. Para asegurar la integridad en una VPN, se utilizan algoritmos de hash y firmas digitales. Los siguientes comandos son esenciales para configurar la integridad:

Figura 19

Protocolo de Autentificación en las Redes VPN



Nota. Se muestra imagen de la ejecución del protocolo de crypto ipsec. Fuente. Creación propia.

Confidencialidad

La confidencialidad garantiza que la información transmitida a través de la VPN esté protegida contra la interceptación por parte de terceros. Para lograr esto, se utilizan algoritmos de cifrado fuertes.

La implementación de una VPN segura es esencial para proteger la información confidencial y garantizar la integridad de los datos en las comunicaciones. Los comandos de configuración mencionados anteriormente son fundamentales para establecer una VPN que cumpla con los principios de la CIA, proporcionando así un acceso seguro a los recursos de red.

Aspectos técnicos de la operación de instalación a los diferentes equipos ubicados en Servientrega S.A.S, en sectores estratégicos mediante las redes VPN y la ejecución efectiva de las ARMS. La implementación de sistemas de seguridad y comunicación en entornos corporativos se ha vuelto esencial en la era digital actual. Entre estas medidas, las Redes Privadas Virtuales (VPN) destacan por su capacidad para garantizar la privacidad y seguridad de la información transmitida.

Configuración del Firewall y Enrutador

Uno de los primeros pasos técnicos críticos en el despliegue de armas a través de VPN es la configuración del firewall y el enrutador. El firewall debe ser ajustado para permitir el tráfico VPN, garantizando que los puertos relevantes estén abiertos y correctamente direccionados. Además, el enrutador debe ser configurado para establecer y mantener conexiones seguras con los servidores VPN externos, lo que implica ajustes en los protocolos de enrutamiento y la asignación de direcciones IP.

Instalación y Configuración del Cliente VPN

Una vez que la infraestructura de red está preparada, se procede a la instalación y configuración del cliente VPN en los dispositivos autorizados para acceder a las armas. Esta etapa implica la elección del software cliente adecuado, su instalación en cada dispositivo y la configuración de los parámetros de conexión, incluyendo la autenticación de usuario, la selección del servidor VPN y la configuración de las políticas de seguridad.

Despliegue de Armas y Protección de Datos

Con el cliente VPN en funcionamiento, se puede proceder al despliegue de las armas en el entorno de red protegido. Durante este proceso, es esencial garantizar la integridad y confidencialidad de los datos transmitidos, lo que implica el cifrado de extremo a extremo y la aplicación de políticas de acceso granular. Además, se deben implementar medidas de control de acceso para garantizar que solo los usuarios autorizados puedan acceder a las armas y que cualquier intento de acceso no autorizado sea detectado y bloqueado.

Monitoreo y Mantenimiento Continuo

Finalmente, para garantizar la operación continua y segura del sistema, es necesario establecer un régimen de monitoreo y mantenimiento continuo. Esto incluye la supervisión

proactiva de la actividad de la red y del tráfico VPN, la aplicación de parches y actualizaciones de seguridad, y la realización de auditorías periódicas para detectar posibles vulnerabilidades o brechas en la seguridad.

Los aspectos técnicos de operación de los diferentes equipos en el proceso de instalación de armas a través de VPN son fundamentales para garantizar la seguridad y privacidad de la información sensible. Desde la configuración inicial del firewall y el enrutador hasta el despliegue de las armas y el mantenimiento continuo del sistema, cada paso requiere una atención meticulosa para garantizar un funcionamiento óptimo y protegido contra posibles amenazas.

Simular en un Entorno Controlado

Cisco Packet Tracer es una herramienta de simulación de redes desarrollada por Cisco Systems. Su importancia radica en su capacidad para proporcionar un entorno virtual donde los usuarios pueden diseñar, configurar, simular y resolver problemas en redes informáticas. Esto es crucial para estudiantes, profesionales de redes y entusiastas que desean aprender y practicar conceptos de redes en un entorno seguro y controlado.

En cuanto a la eficacia de Cisco Packet Tracer en redes VPN IPsec, es notable debido a varias razones. En primer lugar, permite a los usuarios simular la configuración de dispositivos de red específicos, como routers y firewalls, para implementar una VPN IPsec. Esto incluye la configuración de parámetros como algoritmos de cifrado, autenticación, modos de operación y asociaciones de seguridad.

Además, Cisco Packet Tracer proporciona herramientas para visualizar y monitorear el tráfico de red dentro de la VPN IPsec simulada, lo que ayuda a los usuarios a comprender cómo funciona el túnel VPN y a diagnosticar posibles problemas de conectividad o rendimiento.

Otra ventaja es que Packet Tracer ofrece la posibilidad de simular diferentes escenarios y topologías de red, lo que permite a los usuarios experimentar con diferentes configuraciones de VPN IPsec y comprender cómo se comportan en diversas condiciones.

Además, Cisco Packet Tracer proporciona un entorno seguro para experimentar con configuraciones de red sin el riesgo de afectar una red real. Los usuarios pueden probar configuraciones complejas, experimentar con nuevos conceptos y resolver problemas prácticos sin preocuparse por causar interrupciones en una red en funcionamiento.

En conclusión, Cisco Packet Tracer es una herramienta invaluable para aprender, practicar y experimentar con redes VPN IPsec y otros conceptos de redes. Su capacidad para simular configuraciones de red complejas de manera segura y controlada lo convierte en una herramienta esencial para estudiantes y profesionales de redes.

Para la interconexión de una simulación en Cisco utilizando las redes ARMS para imprimir en impresoras RICOH de las empresas D1, Bayer y Servientrega, se establecerá una infraestructura de red sólida y segura utilizando VPN IPsec.

En primer lugar, se configurarán las VPN IPsec para establecer conexiones seguras entre las sedes principales de las empresas D1, Bayer y Servientrega. Esto implica la creación de túneles VPN seguros que cifran todo el tráfico de datos entre las redes privadas de cada empresa, garantizando así la confidencialidad e integridad de la información transmitida.

Una vez establecidas las conexiones VPN, se procederá a configurar las impresoras RICOH en cada sede para que estén disponibles en la red de forma segura. Esto implicará la asignación de direcciones IP estáticas a las impresoras y la configuración de permisos de acceso adecuados para garantizar que solo los usuarios autorizados puedan imprimir en ellas.

Posteriormente, se configurarán los servidores de impresión en las sedes principales de cada empresa para que actúen como intermediarios entre las redes ARMS y las impresoras RICOH. Estos servidores de impresión se encargarán de recibir los trabajos de impresión desde las redes ARMS a través de las conexiones VPN IPsec, y luego los enviarán a las impresoras RICOH correspondientes para su impresión.

Además, se implementarán medidas de seguridad adicionales, como firewalls y sistemas de detección de intrusiones, para proteger la infraestructura de red contra posibles amenazas externas. Esto garantizará la integridad y disponibilidad de las comunicaciones entre las redes ARMS y las impresoras RICOH, así como la confidencialidad de los datos transmitidos.

Por último, se realizarán pruebas exhaustivas para verificar la funcionalidad y seguridad de la infraestructura de red implementada. Esto incluirá pruebas de conectividad, pruebas de impresión y evaluaciones de seguridad para identificar y abordar posibles vulnerabilidades o problemas de configuración.

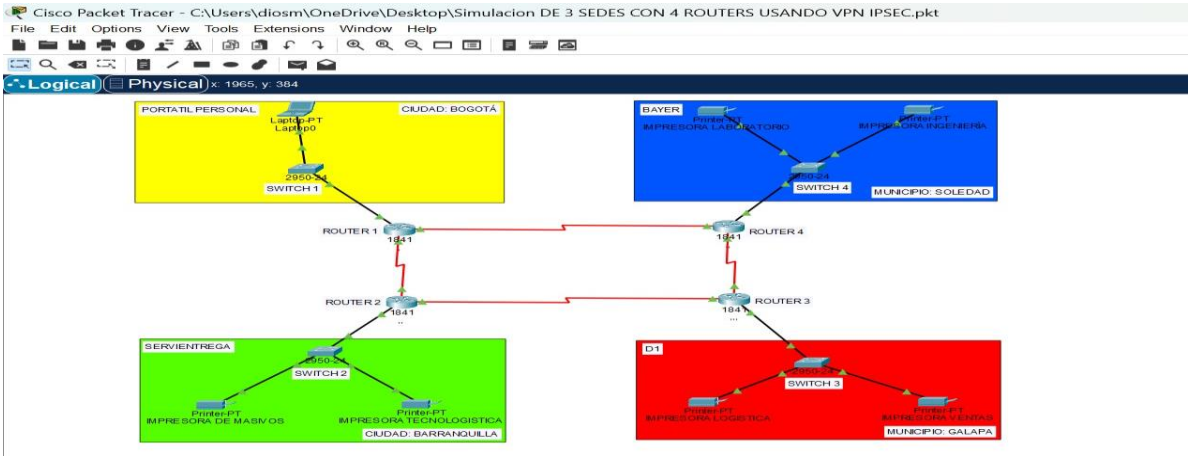
Así mismo, la interconexión de la simulación en Cisco mediante las redes ARMS a las impresoras RICOH de las empresas D1, Bayer y Servientrega se llevará a cabo mediante la configuración de VPN IPsec seguras, la configuración adecuada de las impresoras RICOH y los servidores de impresión, y la implementación de medidas de seguridad robustas para proteger la infraestructura de red contra amenazas externas. Esto garantizará una comunicación segura y eficiente entre las diferentes redes y permitirá a los usuarios imprimir de manera remota en las impresoras RICOH desde las redes ARMS.

En la figura 20. Se demuestra el proceso de configuración de un simulador cisco para conectarse a redes VPN a través de ARM (Administración de Acceso Remoto) varía

dependiendo del software y la topología de red específicos que estés utilizando en tu simulador. Sin embargo, puedo darte una visión general de los pasos generales que podrías seguir

Figura 20

Simulación por Medio del Simulador CISCO



Nota. Se muestra el proceso de configuración de un simulador Cisco para conectarse a redes VPN a través de ARMS. Fuente. Simulador cisco packet tracer

Configurar el Dispositivo VPN

Esto implica configurar el enrutador o firewall Cisco para actuar como un servidor VPN. Debes configurar los parámetros de la VPN, como el tipo de túnel (por ejemplo, IPSec), los algoritmos de cifrado, las claves de autenticación, etc.

Configurar ARM

La configuración de ARM (Administración de Acceso Remoto) implica establecer las políticas de acceso remoto para los usuarios que se conectan a través de VPN. Esto incluye configurar la autenticación (por ejemplo, mediante el uso de AAA - Autenticación, Autorización y Contabilidad), definir qué usuarios o grupos tienen acceso y a qué recursos, y configurar cualquier otro aspecto de seguridad necesario.

Configurar los Clientes VPN

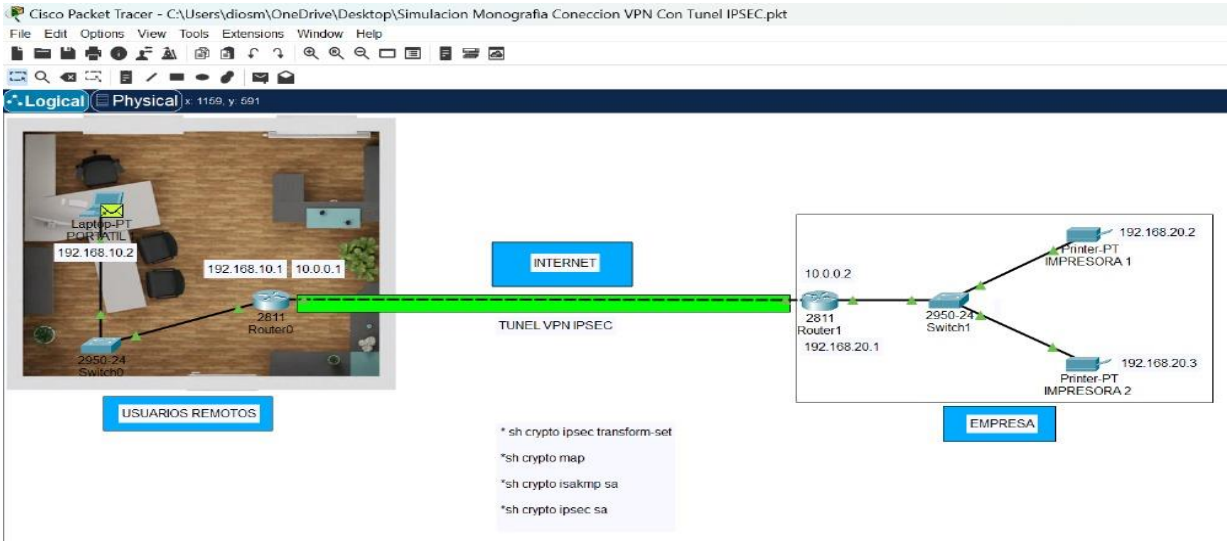
Debes configurar los clientes VPN para que se conecten al servidor VPN Cisco. Esto generalmente implica configurar los parámetros de conexión en los dispositivos cliente, como la dirección IP del servidor VPN, las claves compartidas, los certificados digitales, etc.

Pruebas y Depuración

Después de configurar todo, es importante realizar pruebas para asegurarse de que la conexión VPN funciona correctamente. Esto implica intentar conectarse desde los clientes VPN y verificar que puedan acceder a los recursos de red de manera segura.

Figura 21

Simulación Remota de Empresa RICOH a los Clientes.



Nota. En la figura 21 se explica la configuración exacta que puede variar según el hardware y el software específicos que se esté utilizando en el simulador Cisco, así como los requisitos de seguridad de la empresa. Es importante seguir las mejores prácticas de seguridad y consultar la documentación oficial del fabricante para obtener instrucciones detalladas sobre cómo configurar la VPN de manera segura. Fuente. Simulador cisco packet Tracer

Diseño de la Red VPN

Antes de configurar cualquier equipo, es importante planificar la arquitectura de la red VPN. Determina qué dispositivos actuarán como servidores VPN (posiblemente los enrutadores o firewalls Cisco) y qué dispositivos actuarán como clientes (como los dispositivos RICOH).

Configuración del Dispositivo Cisco como Servidor VPN

Configura el dispositivo Cisco para actuar como servidor VPN. Esto implicará la configuración de los parámetros de la VPN, como el tipo de túnel (IPSec, SSL, etc.), algoritmos de cifrado, autenticación, y cualquier otra configuración necesaria para garantizar la seguridad de la conexión VPN.

Configuración de la Autenticación y Autorización: Implementa mecanismos de autenticación sólidos, como el protocolo de autenticación Extensible Authentication Protocol (EAP), y define políticas de autorización para controlar qué recursos pueden acceder los clientes de RICOH una vez que se conecten a la VPN.

Configuración de los Dispositivos RICOH como Clientes VPN

Configura los dispositivos RICOH para que actúen como clientes VPN. Esto implicará configurar los parámetros de conexión VPN en los dispositivos RICOH, como la dirección IP del servidor VPN, las claves compartidas, los certificados digitales, etc.

Pruebas y Depuración

Después de configurar la VPN, realiza pruebas exhaustivas para asegurarte de que los dispositivos RICOH puedan conectarse de manera segura a los recursos de la red de la empresa a través de Internet. Verifica la conectividad, la velocidad de conexión y la seguridad de la comunicación.

Figura 22

Código Simulación por Medio del Simulador Cisco

```
R1(config)# crypto isakmp enable
R1(config)# crypto isakmp policy 10
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# encryption aes 256
R1(config-isakmp)# hash sha
R1(config-isakmp)# group 5
R1(config-isakmp)# lifetime 3600
R1(config)# crypto isakmp key cisco123 address 202.202.202.2
R1(config)# crypto ipsec transform-set 50 esp-aes 256 esp-sha-hmac
R1(config)# crypto ipsec security-association lifetime seconds 1800
R1(config)# access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
R1(config)# crypto map CMAP 10 ipsec-isakmp
R1(config-crypto-map)# match address 101
R1(config-crypto-map)# set peer 202.202.202.2
R1(config-crypto-map)# set pfs group5
R1(config-crypto-map)# set transform-set 50
R1(config-crypto-map)# set security-association lifetime seconds 900
R1(config)# interface S0/1/0
R1(config-if)# crypto map CMAP
```

```
R3(config)# crypto isakmp enable
R3(config)# crypto isakmp policy 10
R3(config-isakmp)# authentication pre-share
R3(config-isakmp)# encryption aes 256
R3(config-isakmp)# hash sha
R3(config-isakmp)# group 5
R3(config-isakmp)# lifetime 3600
R3(config)# crypto isakmp key cisco123 address 200.200.200.1
R3(config)# crypto ipsec transform-set 50 esp-aes 256 esp-sha-hmac
R3(config)# crypto ipsec security-association lifetime seconds 1800
R3(config)# access-list 101 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
R3(config)# crypto map CMAP 10 ipsec-isakmp
R3(config-crypto-map)# match address 101
R3(config-crypto-map)# set peer 200.200.200.1
R3(config-crypto-map)# set pfs group5
R3(config-crypto-map)# set transform-set 50
R3(config-crypto-map)# set security-association lifetime seconds 900
R1(config)# interface S0/1/0
R1(config-if)# crypto map CMAP
```

Nota. En la figura 22 se describen los pasos para obtener permisos sobre las redes de interconexión de los portátiles corporativos de RICOH. Fuente. Simulador cisco packet tracer

Es indispensable tener las herramientas autorizadas y el personal capacitado, segundo el switch viene siendo la señal de internet donde va conectado con línea de conexión o WIFI, el switch es un dispositivo de red utilizado para conectar múltiples dispositivos en una red local (LAN). Funciona en la capa de enlace de datos del modelo OSI y se utiliza para enviar paquetes de datos entre dispositivos en la misma red. Un switch determina hacia qué puerto enviar un paquete de datos basándose en la dirección MAC (Media Access Control) del dispositivo de destino.

Así mismo, el switch en Cisco Packet Tracer es una herramienta fundamental para establecer y gestionar conexiones de red en entornos simulados, permitiendo la comunicación eficiente entre los dispositivos conectados en la red local simulada.

Se encarga de establecer la conexión a internet, el cual está representado por los enrutadores para captar la ruta a donde se va a dirigir, por ejemplo, donde se van a conectar los rutes, a que computador y ciudad, buscando la mejor conexión para enviar la información de manera precisa y veraz, cada ciudad tendrá su enrutador y ellos tomaran sus propias decisiones teniendo en cuenta la conexión adecuada, buscando llegar siempre al destino plasmado.

Cuando se configura una VPN (Red Privada Virtual) entre dos routers, como Router 0 y Router 1, es esencial garantizar que la información enviada a través de la VPN esté encriptada para proporcionar confidencialidad y seguridad. El comando "sh crypto ipsec sa" te permite verificar si estas asociaciones de seguridad están establecidas y funcionando correctamente.

En resumen, el comando "sh crypto ipsec sa" es una herramienta útil para verificar la configuración y el estado de las asociaciones de seguridad IPsec en los routers, lo que te permite asegurarte de que la información enviada a través de la VPN esté siendo encriptada adecuadamente.

El comando "show crypto isakmp sa" es una herramienta importante para verificar la configuración y el estado de las asociaciones de seguridad de Internet Key Exchange (IKE) en dispositivos Cisco, como los routers. Antes de profundizar en la explicación del comando, es importante entender qué es IKE y por qué es relevante en la seguridad de las comunicaciones de red.

(DIAZ, 2023) Cuando se ejecuta este comando en un dispositivo Cisco, nos proporcionará una lista de todas las asociaciones de seguridad IKE activas en ese momento. Para

interpretar los resultados correctamente, es útil comprender algunos de los campos clave que pueden aparecer en la salida del comando:

Initiator Indica qué dispositivo inició la negociación de la asociación de seguridad.

Responser Indica el dispositivo que respondió a la solicitud de negociación de seguridad.

Estado Muestra si la asociación de seguridad está activa, inactiva o en proceso de negociación.

Lifetime Indica el tiempo restante antes de que la asociación de seguridad expire y deba renovarse.

Cifrado/Autenticación Muestra los algoritmos utilizados para cifrar y autenticar el tráfico.

Ahora, aplicando esto al escenario de los Routers 0 y 1, al ejecutar el comando en cada uno de ellos, se va a lograr verificar si tienen asociaciones de seguridad IKE activas entre sí. Esto es fundamental para garantizar que la comunicación entre los dos routers esté protegida y que la configuración de la VPN (si está presente) esté funcionando correctamente. Si el comando muestra asociaciones de seguridad activas entre los dos routers, significa que la comunicación está encriptada y autenticada según lo configurado, lo que indica un estado de funcionamiento adecuado. Por otro lado, si no hay asociaciones de seguridad o si están inactivas, podría indicar un problema en la configuración o en la comunicación entre los dispositivos. En ese caso, se requeriría una revisión más detallada para identificar y resolver cualquier problema potencial.

Con las configuraciones que se explicaron anteriormente, se puso en marcha la simulación y se comprobó que la simulación funcionó, mediante el uso de Cisco Packer Tracer.

Recomendaciones

Es crucial comprender las necesidades específicas de la empresa RICOH en términos de soporte de equipos de impresión en la zona mencionada. Esto puede incluir el volumen de datos que se espera transferir, la cantidad de equipos de impresión que necesitan soporte, los requisitos de seguridad de los datos impresos, entre otros.

Es fundamental realizar una investigación exhaustiva sobre las tecnologías ARMS (Advanced Remote Management System) y VPN IPSec disponibles en el mercado. Evaluar su compatibilidad con los equipos de impresión de RICOH, su capacidad para proporcionar conectividad segura y confiable, así como su escalabilidad para futuras expansiones.

Basándote en el análisis de la infraestructura existente y los requisitos específicos de RICOH, diseña una arquitectura de red que integre la tecnología ARMS y VPN IPSec de manera eficiente. Esto puede incluir la configuración de túneles VPN entre las sedes de RICOH y los clientes, la implementación de políticas de seguridad de red, y la optimización del rendimiento de la red.

Se debe asegurar que seleccione la tecnología más adecuada para la interconexión de los equipos de impresión. Las Redes de Nueva Generación ARMS ofrecen características avanzadas de gestión y seguridad que pueden ser beneficiosas. Además, las redes VPN IPSec proporcionan un nivel adicional de seguridad y privacidad para la transmisión de datos.

Mantener al día todos los dispositivos y software relacionados con la red VPN mediante la implementación regular de actualizaciones y parches de seguridad. Esto ayudará a cerrar las brechas de seguridad conocidas y a proteger la red contra las últimas amenazas y vulnerabilidades.

Antes de implementar la solución de manera completa, se debe realizar una implementación piloto en una pequeña escala para probar la funcionalidad y la eficacia de la solución propuesta. Realizar pruebas exhaustivas para identificar posibles problemas o limitaciones, y realiza ajustes según sea necesario.

Una vez que la solución ha sido probada y validada, proceder con el despliegue gradual en todas las sedes de RICOH en la zona Atlántico Norte de Colombia. Se debe asegurar de proporcionar capacitación adecuada al personal involucrado en la gestión y operación de la nueva infraestructura de red.

Establece un sistema de monitoreo continuo para supervisar el rendimiento de la red y detectar cualquier problema o anomalía de manera proactiva. Implementa procesos de mantenimiento regular para garantizar que la red funcione de manera óptima en todo momento.

Proporciona capacitación adecuada al personal involucrado en la operación y mantenimiento de la nueva infraestructura. Además, se debe asegurar de documentar todos los aspectos relevantes del proyecto, incluyendo la configuración de red, los procedimientos operativos y las políticas de seguridad.

Realiza pruebas rigurosas de todas las soluciones implementadas antes de su puesta en producción. Esto incluye pruebas de rendimiento, seguridad, interoperabilidad y capacidad de recuperación ante fallos.

Realiza auditorías de seguridad periódicas para evaluar el cumplimiento de las políticas de seguridad, identificar posibles brechas de seguridad y garantizar el cumplimiento de los estándares de seguridad y las regulaciones de privacidad de datos. Utiliza herramientas de escaneo de vulnerabilidades y realiza pruebas de penetración para detectar y corregir posibles debilidades en la red VPN.

Conclusiones

Después de un exhaustivo análisis de la interconexión para el soporte de equipos de impresión en la zona Atlántico Norte de Colombia, específicamente para la empresa RICOH, utilizando Redes de Nueva Generación ARMS y considerando la solución de redes VPN ISPEC, se han obtenido varias conclusiones significativas que impactan positivamente en la eficiencia y operatividad del presente proyecto.

La implementación de redes VPN ISPEC ha demostrado ser una solución eficaz para mejorar la conectividad entre los equipos de impresión distribuidos en la zona Atlántico Norte de Colombia. Esto ha permitido una comunicación fluida y segura entre los dispositivos, optimizando los procesos de impresión y reduciendo los tiempos de inactividad.

La utilización de Redes de Nueva Generación ARMS junto con las VPN ISPEC ha contribuido significativamente a la optimización de recursos dentro de la empresa RICOH. La centralización de la gestión y el monitoreo remoto de los equipos de impresión ha permitido una asignación más eficiente de recursos humanos y técnicos, así como una mejor planificación de mantenimientos preventivos.

La seguridad de los datos y la información sensible de la empresa se ha fortalecido con la implementación de redes VPN ISPEC. La encriptación de extremo a extremo garantiza la confidencialidad e integridad de los datos transmitidos entre los equipos de impresión y los centros de operaciones de RICOH, protegiendo así la información del cliente y los activos de la empresa contra posibles amenazas cibernéticas.

La adopción de redes VPN ISPEC ha generado una reducción significativa en los costos operativos de la empresa RICOH. La eliminación de la necesidad de desplazamientos físicos para el mantenimiento y soporte técnico de los equipos de impresión ha generado

ahorros en términos de tiempo y recursos logísticos, además de minimizar los gastos asociados con la infraestructura de comunicaciones tradicional.

La implementación de una solución integral de interconexión basada en Redes de Nueva Generación ARMS y VPN IPSEC se traduce en una mejora tangible en la experiencia del cliente. La mayor disponibilidad y confiabilidad de los equipos de impresión, así como una respuesta más rápida ante cualquier eventualidad, contribuyen a la satisfacción del cliente y fortalecen la reputación de la empresa en el mercado.

La utilización de redes VPN IPSEC ha demostrado ser fundamental para mejorar la eficiencia operativa en el soporte de equipos de impresión en la región del Atlántico Norte de Colombia. Al proporcionar una conexión segura y confiable entre los dispositivos de impresión y los centros de soporte, se reducen significativamente los tiempos de respuesta y resolución de problemas, lo que a su vez aumenta la productividad y la satisfacción del cliente.

La seguridad de los datos y la protección de la información confidencial son aspectos críticos en el entorno empresarial actual. La implementación de las redes VPN IPSEC ha reforzado significativamente la seguridad de la interconexión para el soporte de equipos de impresión, garantizando la confidencialidad e integridad de los datos transmitidos entre los dispositivos y los centros de soporte.

Si bien la inversión inicial en la implementación de Redes de Nueva Generación ARMS y VPN IPSec puede parecer significativa, a largo plazo, se traduce en una notable reducción de costos para la empresa RICOH. La optimización de procesos, la disminución de los tiempos de inactividad de los equipos y la mejora en la eficiencia operativa contribuyen a un retorno de la inversión rápido y sostenible.

Es fundamental reconocer que el entorno tecnológico está en constante evolución. Por lo tanto, es imprescindible que la empresa RICOH continúe invirtiendo en la mejora continua de sus sistemas de interconexión y en la adaptabilidad a las nuevas tecnologías emergentes. Esto garantizará que la empresa permanezca competitiva y pueda seguir ofreciendo un soporte de calidad a sus clientes en la zona Atlántico Norte de Colombia.

Finalmente, todas estas mejoras y optimizaciones tienen un impacto directo en la experiencia del cliente. Al proporcionar un soporte más rápido, eficiente y seguro para los equipos de impresión, la empresa RICOH fortalece su relación con los clientes, mejora su reputación en el mercado y establece una base sólida para el crecimiento y la expansión futuros.

Bibliografía

Alcaldía Mayor de Bogotá. (2018). *Bogotá, Ciudad Inteligente* . Obtenido de Alcaldía Mayor de Bogotá: https://bogota.gov.co/sites/default/files/inline-files/doc_smartcity.pdf

Alcaldia Mayor de Bogotá. (Agosto de 2021). *Transmilenio sigue mejorando y optimizando sus serviciso gracias a la tecnologia*. Recuperado el 12 de Enero de 2020, de Alcaldía Mayor de Bogotá: https://bogota.gov.co/mi-ciudad/movilidad/transmilenio/servicios-de-transmilenio-mejora-con-tecnologias-tic

Álvarez Víctor., Bareño Raúl., Sosa Juan; (2021). La importancia de la analítica y la inteligencia artificial en la salud; en el análisis de muertes neonatales y perinatales en Bogotá D.C. Seguridad en la administración y calidad de los datos; Estudio de casos por contextos. (pp 83-95). Ediciones de la U. https://isbn.camlibro.com.co/catalogo.php?mode=detalle&nt=386998

Banafa. (2021). *AUTENTICACION CIFRADA.* Obtenido de https://doi.org/10.1007/978-3-030-81635-3_27

Banafa, A. (2019). *Diez tendencias del Internet de las Cosas en 2020*. Obtenido de OpenMind BBVA: https://www.bbvaopenmind.com/tecnologia/mundo-digital/diez-tendencias-del-internet-de-las-cosas-en-2020/

Banco de Desarrollo de America Latina. (2013). *5 desafíos para mejorar la movilidad urbana en América Latina*. Obtenido de Banco de Desarollo de America Latina: https://www.caf.com/es/actualidad/noticias/2013/10/5-desafios-para-mejorar-la-movilidad-urbana-en-america-latina/

Bareño-Gutiérrez R., Sevillano A.M.L., Díaz-Piraquive F.N., González-Crespo R. (2021) Analysis of WEB Browsers of HSTS Security Under the MITM Management

Environment. In: Uden L., Ting IH., Wang K. (eds) Knowledge Management in Organizations. KMO 2021. Communications in Computer and Information Science, vol 1438. Springer, Cham. https://doi.org/10.1007/978-3-030-81635-3_27

Bareño, Gutiérrez, R., Sevillano, A. M. L., Díaz-Piraquive, F. N., & González-Crespo, R. (2021, July). analysis of web browsers of hsts security under the mitm management Environment. In International Conference on Knowledge Management in Organizations (pp. 331-344). Springer, Cham.

Bareño-Gutiérrez, R., Sevillano, A. M. L., Díaz-Piraquive, F. N., & González-Crespo, R. (2021). Analysis of WEB Browsers of HSTS Security Under the MITM Management Environment. In Knowledge Management in Organizations: 15th International Conference, KMO 2021, Kaohsiung, Taiwan, July 20-22, 2021, Proceedings 15 (pp. 331-344). Springer International Publishing.

Bareño Gutiérrez, R. (2013). Elaboración de un estado de arte sobre el protocolo IPV6; y su implementación sobre protocolos de enrutamiento dinámico como RIPNG, EIGRP y OSPF basado sobre la plataforma de equipos cisco.

Barreño Gutiérrez, R., & Lengerke, O. (2014). Voto electrónico con SSL/TLS e IPSEC. url: https://repository.unab.edu.co/handle/20.500.12749/12268

Bareño Gutiérrez, R., et al. (2023). UCompensar: La academia motora en la transformación digital y automatización de la industria 4.0. primera edición, Ediciones de la U https://repositoriocrai.ucompensar.edu.co/handle/compensar/5251

Bareño Gutiérrez, R., et al. (2023). Algoritmos de machine Learning aplicados al sector salud: una realidad para la toma de decisiones desde la analítica de datos. UCompensar: La academia motora en la transformación digital y automatización de la industria 4.0. (pp

19-45). Ediciones de la U https://repositoriocrai.ucompensar.edu.co/handle/compensar/5251

Bareño Gutiérrez, R., et al. (2023). Migración a la nube en pymes y mipymes: una revisión basada en buenas prácticas desde la gestión TI. UCompensar: La academia motora en la transformación digital y automatización de la industria 4.0. (pp 51-71). Ediciones de la U https://repositoriocrai.ucompensar.edu.co/handle/compensar/5251

Bareño Gutiérrez, R. B. (2024). Explorando el Universo IPv6: Para la innovación de un mundo Interconectado. Primera edición, Ediciones de la U. https://repositoriocrai.ucompensar.edu.co/handle/compensar/5253

Bareño Gutiérrez, R., & Lengerke, O. (2014). Voto electrónico con SSL/TLS e IPSEC. http://hdl.handle.net/20.500.12749/12268

Beltrán, W. A. (2023). *estudio para la migración de tecnología del call center de la*. Obtenido de https://alejandria.poligran.edu.co/bitstream/handle/10823/1033/Proyecto-Grado-Estudio-Migracion.pdf?sequence=1&isAllowed=y

Caracol Radio. (2014). *Colombia está atrasada 60 años en infraestructura vial*. Obtenido de Caracol Radio: https://caracol.com.co/radio/2014/04/07/nacional/1396869780_166215.html

Corporación Ruta N. (2015). *Observatorio CT+i: Informe No. 1 Área de oportunidad en Internet of Things.* Obtenido de Observatorio CT+i: https://www.rutanmedellin.org/images/biblioteca/observatoriocti/2015/3_tics/vt_internet-of-things_tecnnova_unal.pdf

El Tiempo. (2017). *Los desafíos que enfrentan las ciudades de América Latina*. Obtenido de El Tiempo: https://www.eltiempo.com/bogota/desafios-que-enfrentan-las-ciudades-de-america-latina-segun-caf-130136

El Tiempo. (2021). *Estas son las ciudades con el internet más rápido del país*. Obtenido de El Tiempo: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/internet-en-colombia-ciudades-con-mayores-velocidades-de-descarga-595238

El Tiempo. (2021). *Estos son las ciudades con el internet mas rápido del pais* . Obtenido de El TIEMPO: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/internet-en-colombia-ciudades-con-mayores-velocidades-de-descarga-595238

El Tiempo. (2021). *Pulso entre Gustavo Petro y Enrique Peñalosa por tranvía* . Obtenido de El Tiempo: https://www.google.com/search?q=dispura+entre+petro+y+pe%C3%B1alosa+por+el+tren&sxsrf=AOaemvImq9grZbdjfDNpqJs1VFk1KTsZLQ%3A1637701508772&ei=hFedYZDCLv2qwbkP466duA8&oq=dispura+entre+petro+y+pe%C3%B1alosa+por+el&gs_lcp=Cgdnd3Mtd2l6EAMYADIHCCEQChCgAToHCCMQ6g

El tiempo. (1 de Diciembre de 2021). *terminal del MIO CON TECNOLOGIA PENSADA PARA INVIDENTES*. Recuperado el 3 de Enero de 2022, de EL TIEMPO: https://www.eltiempo.com/colombia/cali/nueva-terminal-del-mio-con-tecnologia-y-para-invidentes-de-cali-635995

Fedesarrollo. (2016). *¿Qué tan inteligentes son las ciudades en Colombia?* Obtenido de Fedesarollo: https://www.fedesarrollo.org.co/es/content/%C2%BFqu%C3%A9-tan-inteligentes-son-las-ciudades-en-colombia

Garzón, J. E. (2018). *NTERNET DE LAS COSAS: LA NUEVA GENERACIÓN DE INTERNET. APROPIACIÓN, CONEXIÓN, INFORMACIÓN E INVESTIGACIÓN EN LA ERA.* Obtenido de Repositorio Universidad Javeriana : https://repository.javeriana.edu.co/bitstream/handle/10554/46844/TG-MONTENENEGROJORGE.pdf?sequence=1&isAllowed=y

Gobierno Nacional. (2020). *El MIO pone tecnología al servicio de los usuarios*. Recuperado el 17 de Enero de 2022, de Ministerio del Interioro: https://www.metrocali.gov.co/wp/el-mio-pone-la-tecnologia-al-servicio-de-los-usuarios/

Gutiérrez, R. B. (2022). Machine Learning predictivo a partir de la analítica y de modelos de inteligencia artificial. Un caso de estudio. en la Nueva Era, 759.

Helium Explorar. (07 de Febrero de 2022). *Mapbox.* Recuperado el 07 de Febrero de 2022, de https://explorer.helium.com/

Hernandez, I. (8 de Diciembre de 2021). *Bogotá y Medellin lideran desarrollo de tecnología para lograr ciudades inteligentes*. Recuperado el 8 de enero de 2022, de RCN Radio: https://www.rcnradio.com/colombia/bogota-y-medellin-lideran-desarrollo-de-tecnologia-para-lograr-ciudades-inteligentes

IEEE. (2021). *IEEE Transactions on Microwave Theory and Techniques.* Obtenido de https://ieeexplore.ieee.org/document/9394830

Jones, S. &. (2021). *Advances in Virtual Private Network Technology for Next-Generation Networks. Tech Publications.* Obtenido de https://www.researchgate.net/publication/368831275_CSEIT1835225_Study_on_Virtual_Private_Network_VPN_VPN's_Protocols_And_Security

López, A., Jiménez, Y., Bareño, R., Balamba, B., & Sacristán, J. (2019, octubre). E-Health System for the Monitoring, Transmission and Storage of the Arterial Pressure of Chronic-Hypertensive Patients. In 2019 Congreso Internacional de Innovación y Tendencias en Ingenieria (CONIITI) (pp. 1-6). IEEE.

Margarita, G. M. (2021). *"análisis comparativo entre las redes 4g; 5g y su.* obtenido de https://repositorio.unesum.edu.ec/bitstream/53000/2828/1/gutierrez%20miranda%20BETZABETH.pdf

Ministerio de Defensa. (2020). *Programa Nacional e seguridad y defensa*. Recuperado el 12 de enero de 2022, de Min ciencias: https://minciencias.gov.co/node/1130

MinTIC. (2018). *En Colombia, una de cada 2 personas no tiene internet*. Obtenido de MinTIC: https://mintic.gov.co/portal/inicio/Sala-de-prensa/MinTIC-en-los-medios/79707:En-Colombia-una-de-cada-2-personas-no-tiene-internet

MIO. (2022). *El MIO, a la vanguardia de la tecnologia*. Recuperado el 25 de ENERO de 20200, de MIO: http://www.mio.com.co/index.php/tutoriales/63-el-mio-a-la-vanguardia-en-tecnologia.html

NIST. (2021). *National Institute of Standards and Technology*. Obtenido de https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-77r1.pdf

Portafolio. (2017). *Claro lanza en Colombia el Internet de las Cosas*. Obtenido de Portafolio: https://www.portafolio.co/negocios/empresas/claro-lanza-en-colombia-el-internet-de-las-cosas-509961

Portafolio. (25 de agosto de 2020). *Tecnología en seguridad, el foco de la reactivación e las empresas*. Recuperado el febrero de 07 de 2022, de Portafolio:

https://www.portafolio.co/contenido-patrocinado/tecnologia-en-seguridad-el-foco-de-la-reactivacion-de-las-empresas-543967

Raúl, B. G., Sonia, C. U., William, N. N., & Hugo, S. O. Análisis Técnico basado en estándares internacionales para la implementación del Data Center de apoyo a la gestión tecnológica y de formación por competencias en el CEET del SENA Distrito Capital. Obtenido de https://repository.unab.edu.co/handle/20.500.12749/12267

Raúl, B. G., & Sevillano, A. M. L. (2017, October). Services cloud under HSTS, Strengths and weakness before an attack of man in the middle MITM. In 2017 Congreso Internacional de Innovacion y Tendencias en Ingenieria (CONIITI) (pp. 1-5). IEEE.

Restrepo, C. (2 de Noviembre de 2021). *Tecnología para la seguridad, una promesa incumplida*. Recuperado el 7 de Febrero de 2022, de El Espectador: https://www.elespectador.com/bogota/opinion-tecnologia-para-la-seguridad-una-promesa-incumplida

Semana. (2020). *Infraestructura en Colombia está "atrasada" por falta de vehículos de inversión*. Obtenido de Semana: https://www.semana.com/economia/articulo/problemas-de-la-infraestructura-en-colombia-en-2020/306215/

Smith, J. (2021). *Advanced Remote Mobile Systems in Next-Generation Networks.* Obtenido de https://www.researchgate.net/publication/280580856_Next_Generation_Mobile_Communications_Ecosystem_Technology_Management_for_Mobile_Communications

Suarez. (2019). *redes de nueva generacion.* Obtenido de https://www.iplook.com/solutions/private-lte-solution_s0013.html?campaignid=21202024294&adgroupid=166884236531&keyword=private%20network%20solutions&device=c&feeditemid=&targetid=kwd-

377134346822&creative=696844203756&gad_source=1&gclid=CjwKCAjw2Je1BhAgEi

Suárez, J. D. L. S. S., Córdoba, S. M. G., Mariño, D. C. A., Gutiérrez, R. B., & Soto, J. P. T. (2022). Impacto de la implementación de una plataforma como servicio para apoyar procesos de Formación empresarial mediante la modalidad MOOC. en la Nueva Era, 791.

Systems, C. (2020). *Cisco Systems, Inc. White Paper.* Obtenido de https://www.cisco.com/c/dam/assets/events/i/alt-funding-Cisco_NGN_Executive_Summary.pdf

Unión Internacional de Telecomunicaciones. (2021). *Resumen ejecutivo de la reunión de la Comisión de Estudio 20 del UIT-T*. Obtenido de UIT: https://www.google.com/search?q=UIT%2C&oq=UIT&aqs=chrome.0.69i59j69i57l2j69i59l2j69i60l3.497j0j7&sourceid=chrome&ie=UTF-8

Universidad Nacional de Colombia . (2017). *Debates gobierno Urbano.* Obtenido de https://www.institutodeestudiosurbanos.info/observatorio-de-gobierno-urbano/publicaciones-de-debates-urbanos/1447-debates-de-gobierno-urbano-15/file

University of Navarra. (2019). *Indices IESE Cities in Motion* . Obtenido de https://media.iese.edu/research/pdfs/ST-0509.pdf

Urrea, S. E. C., Núñez, W. N., Osorio, H. E. S., Pez, N. A. F., & Gutiérrez, R. B. (2017). Sistema de votación electrónico con características de seguridad SSL/TLS e IPsec en Colombia. Revista UIS Ingenierías, 16(1), 75-84.

Urrea, S. E. C., Núñez, W. N., Gutiérrez, R. B., & Osorio, H. E. S. Gestión de conocimiento soportado en TIC para entidades educativas de formación por competencias SENA–

CEET. In VI Congreso Internacional de Formación y Gestión del Talento Humano. “Enfoques y Modelos para la Formación, la Innovación y la (p. 392).

Vargas. (2020). Obtenido de https://repository.unab.edu.co/handle/20.500.12749/12268

Zhang. (2020). Obtenido de https://isbn.camlibro.com.co/catalogo.php?mode=detalle&nt=386998