UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR

POSGRADOS

Maestría en
SEGURIDAD DE LA INFORMACIÓN

RPC-SO-28-NO.669-2021

Opción de Titulación:

Proyecto de titulación con componentes de investigación aplicada y/o de desarrollo

Tema:

Análisis de la ciberseguridad a la infraestructura tecnológica de la empresa SEÑAL X

Autor:

Christopher Junior Pesántez Ávila

Director:

Juan Carlos Domínguez Ayala

CUENCA – Ecuador
2023

Autor:

Christopher Junior Pesántez Ávila
Ingeniero Electrónico.
Candidato a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
Christopher.pesantez@gmail.com

Dirigido por:

Juan Carlos Domínguez Ayala
Ingeniero en Sistemas.
Magister en Redes de Comunicaciones.
jdominguez@ups.edu.ec

CUENCA – ECUADOR – SUDAMÉRICA
CHRISTOPHER JUNIOR PESÁNTEZ ÁVILA
Análisis de la ciberseguridad a la infraestructura tecnológica de la empresa SEÑAL X

DEDICATORIA

Mi hija es el mejor regalo que haya podido recibir de parte de Dios. Eres mi mayor tesoro y también la fuente más pura de mi inspiración; por eso quiero agradecerte cada momento de felicidad con el que colmas mi vida. Te doy las gracias, hija mía, por darle sentido a mi vida y permitirme ser cada día mejor padre junto a ti.

Eres el mayor tesoro de mi vida y mi fuente de motivación. Gracias a ti he podido cumplir con todas mis obligaciones académicas necesarias, pues de otra manera este proyecto no hubiera culminado con el mismo éxito

AGRADECIMIENTO

Querida Jessica

Quiero expresarte mi profundo agradecimiento por todo el apoyo incondicional que me brindaste durante mi proceso de investigación y escritura de mi tesis de magister. Tus palabras de aliento, paciencia y comprensión me ayudaron a superar los momentos de incertidumbre y frustración, y me motivaron a seguir adelante en momentos en los que pensé en abandonar.

También quiero agradecer a nuestra hija Daniela, quien ha sido una fuente constante de alegría y motivación durante todo este proceso. Sus risas y sonrisas me recordaron constantemente la importancia de mantener un equilibrio en mi vida y me dieron la fuerza necesaria para seguir adelante.

Gracias a ustedes dos, he logrado culminar mi tesis de magister y estoy muy orgulloso de compartir este logro con ustedes. Sin su amor, apoyo y paciencia, esto no habría sido posible.

Tabla de Contenido

Índice de Figuras

Análisis de la ciberseguridad a la infraestructura tecnológica de la empresa Señal X

Autor(es):

Christopher Junior Pesántez Ávila

Resumen

Entre los hechos destacables que se han producido en todo el mundo en los últimos años se encuentra un aumento significativo de los ataques a la seguridad de la información, el activo más importante de continuidad del negocio. Los ataques cibernéticos pueden lanzarse desde adentro (usuarios, redes y aplicaciones) o desde fuera de la organización, pero las nuevas tendencias corporativas como el teletrabajo o la computación en la nube han expuesto brechas en los controles de seguridad ya que gran parte de la política se enfoca en la protección del perímetro. y se basa en la definición de una zona de confianza donde los usuarios de los dispositivos pueden utilizar los dispositivos conectados a la red interna y utilizar los servicios con las menores restricciones posibles, entendiendo este comportamiento como una violación a la protección de los activos de información. Por lo tanto, el presente trabajo pretende identificar medidas emergentes de remediación con el afán de tomar el camino hacia una arquitectura Zero Trust y las consideraciones de su posible implementación en la organización Señal X. De esta forma, es posible dar una visión general sobre la importancia de crear un conjunto óptimo de medidas que puedan reducir el riesgo de ataques informáticos y su posible impacto en la estructura empresarial de la organización. Por lo tanto, un modelo de seguridad de confianza cero se define como una política responsable de identificar, validar y automatizar los principios de seguridad dentro de una organización que se aplicarán a los recursos técnicos y, en última instancia, a los usuarios. Para llevar a cabo este propósito, el modelo se basa en tres principales fundamentales: acceso seguro a todos los recursos independientemente de la ubicación, política de menor privilegio y el monitoreo constante. Para la elaboración de este trabajo se realizara las técnicas de revisiones bibliográficas, visita en sitio para determinar las superficies de protección y la consulta a expertos para hacer uso de las herramientas de ciberseguridad actuales que posee la empresa, para terminar con una propuesta de implementación en donde se garantice la seguridad de la información teniendo siempre como objetivo mantener seguros los 3 pilares fundamentales de la seguridad de la información: Confidencialidad, Integridad y disponibilidad.

Palabras clave:

Ciberseguridad, Zero Trust, seguridad de la información

Abstract

Among the notable developments worldwide in recent years has been a significant increase in attacks on information security, the most important business continuity asset. Cyber attacks can be launched from within (users, networks and applications) or from outside the organization, but new corporate trends such as teleworking or cloud computing have exposed gaps in security controls as much of the policy is focused on perimeter protection. and is based on the definition of a zone of trust where device users can use devices connected to the internal network and use services with the least possible restrictions, understanding this behavior as a violation of the protection of information assets. Therefore, this paper aims to identify emerging remediation measures in order to take the path towards a Zero Trust architecture and the considerations of its possible implementation in the Signal X organization. In this way, it is possible to give an overview of the importance of creating an optimal set of measures that can reduce the risk of cyber attacks and their potential impact on the business structure of the organization. Therefore, a zero trust security model is defined as a policy responsible for identifying, validating and automating security principles within an organization that will be applied to technical resources and, ultimately, to users. To accomplish this purpose, the model is based on three main fundamentals: secure access to all resources regardless of location, least privilege policy and constant monitoring. For the elaboration of this work the techniques of bibliographic reviews, site visit to determine the protection surfaces and consultation with experts to make use of the current cybersecurity tools that the company has, to finish with an implementation proposal where the security of the information is guaranteed always having as objective to maintain safe the 3 fundamental pillars of the security of the information: Confidentiality, Integrity and availability.

Key Words:
Cybersecurity, Zero Trust, information security

1. Introducción

En toda organización tener unas herramientas sólidas sobre las que se estructure una infraestructura tecnológica puede traducirse en un aumento de la eficiencia operativa, mayor capacidad de respuesta, simplificación de mantenimiento y soporte, reducción de costos y por ende en un aumento de la productividad. De esta manera, destinar presupuestos al área de Ciberseguridad es también invertir en calidad para toda la empresa y sus clientes. De la Ciberseguridad dependen numerosos elementos del funcionamiento empresarial y su correcto uso puede ser determinante para el desarrollo de cualquier actividad.

Según un estudio de 2021 realizado por IBM y Ponemon Institute, encontraron que el costo promedio de una filtración de datos en América Latina fue de $2,56 millones, y el tiempo promedio para identificar y contener una filtración fue de 287 días. Esto se compara con un aumento promedio de costos del 52% (1.68) en 2020 [1].

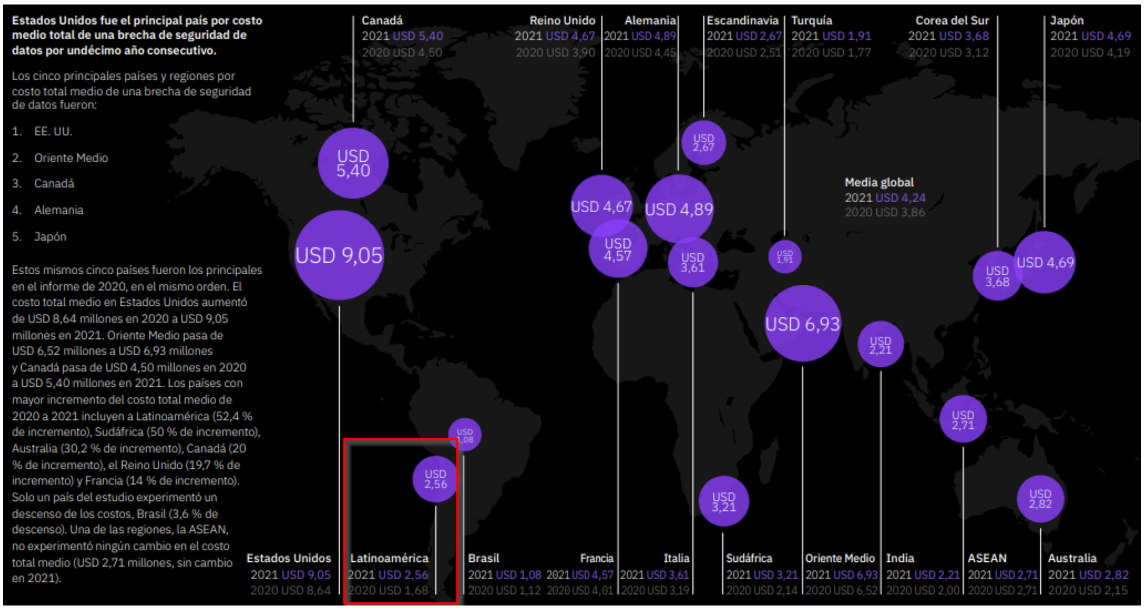

Figura 1. Costo promedio por brecha de datos en Latinoamérica [1]

Adicionalmente, nuestro país ha sufrido varios ataques cibernéticos en algunas instituciones del gobierno, como lo fue recientemente la estructura tecnológica del Municipio de Quito, dejando inhabilitados algunos de sus servicios como: matriculación, citas, pagos, consultas de placas entre otros [2]. El ataque fue ocasionado por un malware de tipo ransomware, pero que el municipio alego que se preservo la integridad de toda la información.

Figura 2. Comunicado AMT Quito [2]

La empresa de ciberseguridad reconocida a nivel mundial ESET, también realizo algunas aseveraciones con respecto a las vulnerabilidades encontradas en Latinoamérica durante el año 2020, “Entre los exploits más detectados se destacan aquellos que explotan vulnerabilidades como la CVE-2012-0143 (con el 70% de las detecciones de exploits), CVE-2017-11882 y CVE-2017-0144 (correspondiente al exploit Double Pulsar). En los tres casos, estos fallos de seguridad permiten al atacante tomar control del sistema afectado” [3]. Esto con el afán de destacar la falta de actualizaciones a nivel de SO, y la constante adquisición de programas “piratas” que se utilizan en Latinoamérica.

Por otra parte, con la aparición de nuevas tendencias como BYOD (bring your own device) y el teletrabajo, acrecentado en gran medida por la pandemia del COVID-19, los colaboradores necesitan cada vez más tener acceso a los recursos de las organizaciones, desde cualquier lugar y en cualquier momento. Esto conlleva a las organizaciones a ofrecer una infraestructura dimensionada para los picos de trabajo, ya que las conexiones se harán desde fuera de la oficina.

Para resolver algunos de estos problemas, las empresas han optado por direccionar algunos de sus servicios a la nube, ya que la misma solventa varias medidas de seguridad implícitas en la mayoría de los servicios que oferta. Además, se pueden describir varias ventajas de poseer una infraestructura híbrida (sistemas on-premise y nube privada o pública), tales como [4]:

- Agilidad
- Flexibilidad
- Seguridad
- Control
- Costo-Beneficio

En el pasado, el enfoque de la infraestructura tecnológica y su seguridad estaba en asegurar, mantener y controlar el perímetro del centro de datos, pero gracias a la nueva realidad, los perímetros ya no existen. La forma en que diseñamos, implementamos, integramos y administramos la tecnología de la información está cambiando drásticamente. Las nubes públicas e híbridas redistribuyen las responsabilidades de cumplimiento y seguridad de datos entre diferentes proveedores de servicios.

En este contexto, las organizaciones ecuatorianas necesitan mejorar la gestión de la seguridad. Por ejemplo, migrar a la gestión de confianza cero. Este modelo difiere de los enfoques que se enfocan en la seguridad perimetral basados en la premisa de confianza y verificación, Zero Trust se basa en la idea de que por defecto una organización no debe confiar en ninguna entidad interna o externa que ingrese a su perímetro, de ahí el nombre [5]. Dada la mayor superficie de ataque de un híbrido en funcionamiento, no puede colocar todos sus recursos de seguridad en el perímetro y confiar en todo lo que hay dentro.

Es importante que las empresas acepten medidas diseñadas no solo para garantizar la privacidad y seguridad de la información de sus usuarios, sino también para tener disponibles sistemas de seguridad para proteger la infraestructura informática de la empresa, así como el desarrollo de protocolos operativos. Prevenir dichos riesgos y actuar cuando se produzcan.

2. Determinación del Problema

De acuerdo con los puntos elaborados anteriormente se optará por realizar el análisis de la línea base de la infraestructura tecnológica actual de la empresa SEÑAL X para la identificación de las medidas emergentes de remediación a implementase, bajo la arquitectura de seguridad Zero Trust.

Esta arquitectura está diseñada para reducir el riesgo de ciberseguridad al eliminar la confianza implícita en la infraestructura de TI bajo el modelo "nunca confíes, siempre revisa" [6]. Lo cual asegura los accesos tanto remotos como de infraestructura local de los usuarios hacia los recursos de la empresa.

La seguridad Zero Trust se apoya en tecnologías ya existentes, brindando a las empresas [7]:

- Protección avanzada contra al acceso de usuarios remotos
- Mayor autenticación
- Acceso seguro desde cualquier lugar
- Protección de datos garantizada
- Reducción de infracciones y daños
- Mejora la agilidad mediante el uso seguro de soluciones móviles y en la nube

Este modelo considera toda actividad de la red como potencialmente dañina hasta que se demuestre lo contrario, esto conlleva a que la capacidad de los atacantes para propagarse a lo largo de la red se reduzca drásticamente. Un estudio realizado en 2021 por Okta descubrió que el 82% de las compañías a nivel mundial planean permitir al menos el trabajo remoto parcial después de la pandemia, y el 47% permitirá que los empleados trabajen permanentemente desde casa a tiempo completo [8]. Con esto en mente, es imperativo que las empresas ecuatorianas empiecen a trabajar en proyectos de transición hacia una seguridad de Zero Trust como lo han ido realizando a lo largo de los años empresas reconocidas como: Microsoft, Google y Cisco.

La seguridad Zero Trust ha ganado popularidad en los últimos años, ya que se vuelve necesaria para defender los entornos modernos de trabajo desde cualquier lugar. Este modelo de seguridad también puede ser implementado en la pequeña y mediana empresa ya que actualmente estas empresas cuentan con las tecnologías necesarias para poder realizarlo, debido a las constantes nuevas amenazas, varias instituciones se han visto en la obligación de adquirir Firewalls de próxima generación, así como protecciones de usuario final (Endpoint Protection), el cual ya es un paso importante para establecer el camino a seguir en el afán de obtener una seguridad Zero Trust.

En el reporte titulado "Zero Trust Impact Report" [9], en donde han participado alrededor de 1000 profesionales de TI de 8 países, una de las principales conclusiones obtenidas, es que para el 33% de los lideres de ciberseguridad el modelo Zero Trust es una prioridad. Por otra parte, en este estudio, también se concluyó que el 85% de las organizaciones dijo haber implementado o estar en proceso de implementación de Zero Trust [9]. Es por ello, que de acuerdo con las cifras y beneficios aquí planteados se establece que una seguridad Zero trust es el futuro de la ciberseguridad.

2.1. Objetivos (general y específicos)

Objetivo general

Analizar la línea base de la infraestructura tecnológica actual de la empresa SEÑAL X para la identificación de las medidas emergentes de remediación a implementarse con el afán de tomar el camino hacia una arquitectura de zero trust.

Objetivos Específicos

- Definir las teorías de la ciberseguridad en una arquitectura Zero Trust
- Diagnosticar el estado actual de la infraestructura tecnológica en la empresa Señal X, para determinar la viabilidad de desarrollar la arquitectura Zero Trust
- Presentar un modelo de arquitectura zero trust realizada a medida y que pueda ser utilizado por la empresa, ocupando sus recursos actuales en cuanto a ciberseguridad.

3. Metodología

Para obtener los beneficios del modelo Zero Trust se necesita conocer cada componente de la infraestructura actual. Esto nos permitirá identificar donde están nuestros principales recursos, principales riesgos y vulnerabilidades, por lo que se iniciara determinando cual es el diagrama de red actual, que activos críticos forman parte de esta, que áreas de comunicación posee la red y cuáles son los activos de seguridad que la empresa ocupa actualmente, y con esta información definida, se procederá a identificar las superficies de protección.

Se deberán también definir el comportamiento de los usuarios y la integridad de los dispositivos, ya que estos son indicadores importantes cuando se busca establecer confianza en la seguridad de los sistemas, y a su vez estos serán los delimitantes de los mecanismos de las políticas. Las políticas de soporte se crearán con la utilización del método Kipling, que responde sobre quien, que, cuando, donde, por qué y cómo.

Dado que Zero Trust se basa en la microsegmentación o segmentación, el perímetro de seguridad se dividirá en pequeñas áreas para mantener el acceso separado a las diferentes partes de la red. De este modo, nos aseguramos de que un recurso se comunique con otro, las reglas específicas deben autorizar este tráfico y el firewall de próxima generación proporcionará el más alto nivel de seguridad transparente para el usuario final.

En cuanto al mejoramiento de políticas de autenticación de usuario, se incorporará el uso de la autenticación por medio de un directorio activo, en donde se generarán directivas de grupo tanto de usuario como de equipo, que posteriormente serán sincronizadas con la nube de Azure por medio de un agente, y de esta manera se obligara al usuario a utilizar estas directivas tanto on-premise como fuera de ella.

Por otra parte, la utilización de la autenticación doble factor es primordial en un modelo Zero Trust para garantizar el acceso a los sistemas que serán ocupados por los usuarios. En este ámbito, Azure ofrece este tipo de autenticación el cual será revisado más a detalle para compaginar las directivas del directorio activo local con el de la nube.

Debido a que la empresa actualmente cuenta con una suscripción activa de Office365, se realizara la investigación respectiva en cuanto al uso de sus políticas de acceso para recursos en la nube y posterior planteamiento de un modelo que pueda ser utilizado a futuro por la organización.

Para desarrollar los fundamentos teóricos se aplicará el método Analítico-Sintético que de acuerdo al autor Cesar Bernal: "Estudia los hechos, partiendo de la descomposición del objeto de estudio en cada una de sus partes para estudiarlas en forma individual (análisis), y luego se integran esas partes para estudiarlas de manera holística e integral (síntesis)." que servirá para analizar las teorías, desglosar y con propias concepciones sintetizar la información. Se aplicará la técnica de la revisión bibliográfica analizando revistas de alto impacto, artículos científicos y artículos académicos referentes al tema de estudio.

Para determinar el estado actual de la empresa en cuanto a infraestructura tecnológica se refiere, se realizara una visita de campo para obtener la información exacta de los activos que posee actualmente la empresa señal X y se aplicará un cuestionario bien estructurado en el cual se obtendrá toda la información necesaria para desarrollar el correcto dimensionamiento de la arquitectura Zero Trust a implementarse.

Para la elaboración del modelo Zero Trust se aplicará la investigación tecnológica para hacer uso de las plataformas tecnológicas, haciendo uso del método Kippling con el propósito de determinar los accesos de usuarios a los servicios de la empresa, además, se aplicará la técnica de consulta a expertos debido a los diferentes proveedores de ciberseguridad que actualmente posee la empresa.

4. Marco teórico referencial

La infraestructura de una empresa típica se ha vuelto cada vez más compleja. Una empresa puede gestionar múltiples redes internas, oficinas remotas con infraestructura local propia, servicios personales y/o móviles y servicios en la nube. Esta complejidad va más allá de los enfoques tradicionales de ciberseguridad basados en el perímetro, ya que las empresas no tienen un único perímetro fácilmente identificable. La seguridad cibernética basada en el perímetro también ha demostrado ser insuficiente porque el movimiento lateral no se inhibe cuando los atacantes violan el perímetro. Fruto de este complejo trabajo se ha desarrollado un nuevo modelo de ciberseguridad denominado "Zero Trust" (ZT). El enfoque de ZT se centra principalmente en la protección de datos y servicios, pero puede y debe ampliarse para incluir todos los activos empresariales (dispositivos, componentes de infraestructura, aplicaciones, componentes virtuales y en la nube) y sujetos (usuarios finales, aplicaciones y otras entidades no humanas que solicitan información de recursos).

Los modelos de seguridad Zero Trust suponen que un atacante está presente en el entorno y que un entorno que es propiedad de la empresa no es diferente que cualquier entorno que no sea propiedad de la empresa. En este nuevo paradigma, una empresa debe asumir que no hay confianza implícita y analizar y evaluar continuamente los riesgos para sus activos y funciones de negocio y luego promulgar protecciones para mitigar estos riesgos. En Zero Trust, estas protecciones suelen implicar la minimización del acceso a los recursos (como los datos y recursos informáticos y aplicaciones o servicios) a sólo aquellos sujetos y activos identificados para este acceso, así como autenticar y autorizar continuamente la identidad y la postura de seguridad de cada solicitud de acceso. De acuerdo con las pautas NIST SP 800-207, Zero Trust es un término para un conjunto en evolución de paradigmas de seguridad cibernética que cambia la protección de los perímetros estáticos de la red a los usuarios, activos y recursos. Zero Trust Architecture (ZTA) utiliza los principios de Zero Trust para diseñar flujos de trabajo e infraestructura empresarial e industrial. Zero Trust asume que no existe una confianza implícita en los activos o cuentas de usuario basada únicamente en la ubicación física o de red (es decir, LAN frente a Internet) o la propiedad de los activos (empresariales o personales).

La autenticación y la autorización (sujeto y dispositivo) son funciones discretas que se realizan antes de que se establezca una sesión en un recurso empresarial. Zero Trust es una respuesta a las tendencias en las redes empresariales, incluidos los usuarios remotos, BYOD y los activos basados en la nube que no se encuentran dentro de los límites de la propia red de la empresa.

La confianza cero se centra en proteger los recursos, usuarios y activos individualmente, sin importar quien los posee, debido a que la ubicación de la red ya no se considera el componente principal para la postura de seguridad del recurso.

4.1. Principios de un enfoque Zero trust [11]

- Los servicios informáticos y las fuentes de datos se consideran recursos.
- La comunicación es segura sin importar la ubicación.
- El acceso a los recursos individuales de la empresa se ortorga por sesión.
- Las políticas dinámicas, incluida la identidad del cliente, el estado observable de la aplicación/servicio y los activos solicitados, y posiblemente otros atributos ambientales y de comportamiento, determinan el acceso a los recursos.
- La empresa supervisa y mide la integridad y la postura de seguridad de todos los activos propios y asociados.
- Antes de permitir el acceso, se aplican estrictamente todas las autorizaciones de recursos.
- Las empresas recopilan la mayor cantidad de información posible sobre el estado actual de los activos, la infraestructura de red y las comunicaciones y utilizan esa información para mejorar su postura de seguridad.

4.2. Supuestos básicos para la conectividad de la red para cualquier organización que utilice ZT en la planificación y el despliegue de la red. [11]

- Toda la red privada de la empresa no se considera una zona de confianza implícita.
- Los dispositivos de la red pueden no ser propiedad de la empresa o no ser configurables.
- Ningún recurso es intrínsecamente fiable.
- No todos los recursos de la empresa están en la infraestructura de la empresa.
- Los sujetos y activos empresariales remotos no pueden confiar plenamente en su conexión de red
- Los activos y los flujos de trabajo que se mueven entre la infraestructura empresarial y no empresarial deben tener una postura y una política de seguridad coherentes.

Para encaminar a la empresa Señal X hacia un modelo Zero Trust se deben tomar en consideración los elementos de ciberseguridad que actualmente posee en su infraestructura interna para posteriormente realizar una propuesta de implementación que vaya de acuerdo a sus necesidades.

Se realizó una visita de campo al establecimiento con el afán de realizar un mapeo en conjunto con al administrador de los servicios tecnológicos para así delimitar todos los elementos de ciberseguridad que la empresa posee actualmente. Algunos de ellos son:

- Firewall de nueva generación
- Antimalware de nueva generación con cifrado de discos
- Suscripción a office365 (Acceso condicional en el portal de azure)

- Suscripción de OpenDNS (consultas DNS seguras)

Además de estos elementos se propone la implementación de un directorio activo local, el cual, en conjunto con el servicio de Azure en la nube puede ayudarnos con el aseguramiento de acceso a recursos, así como al manejo de usuarios y dispositivos remotos, así como locales. Las principales ventajas de la implementación de un directorio activo serían las siguientes:

- Establecimiento de políticas de contraseñas, longitud, caducidad centralizada
- Manejo de usuarios, equipos y grupos de una manera centralizada y con capacidad para ser sincronizada con la nube de azure
- Autenticación de usuarios a ciertos equipos de la red en caso de administrar sus servicios
- Integración con aplicaciones de terceros para mantener el uso de las credenciales sobre otras plataformas de servicios
- Directivas de usuario y computador centralizado
- Establecer sincronización con la plataforma de office365, para garantizar el acceso condicional a las aplicaciones.
- Comunicación bidireccional entre on-premise y la nube de Azure, para gestionar las políticas por medio de directivas locales y de Intune cuando los usuarios remotos no se comuniquen con el dominio local

Una de las principales ventajas de este sistema es la sincronización que se puede realizar con la infraestructura de Microsoft, para esto se debe realizar la instalación de un agente llamada Azure AD Connect, el cual provee varias bondades como son [12]:

- Sincronización de hash de contraseñas, método de inicio de sesión que sincroniza el has de contraseña con office365
- Autenticación de paso a través, donde la autenticación en la nube debe ser autorizado por el dominio local, para ello se debe instalar un agente de autenticación para tener la comunicación bidireccional

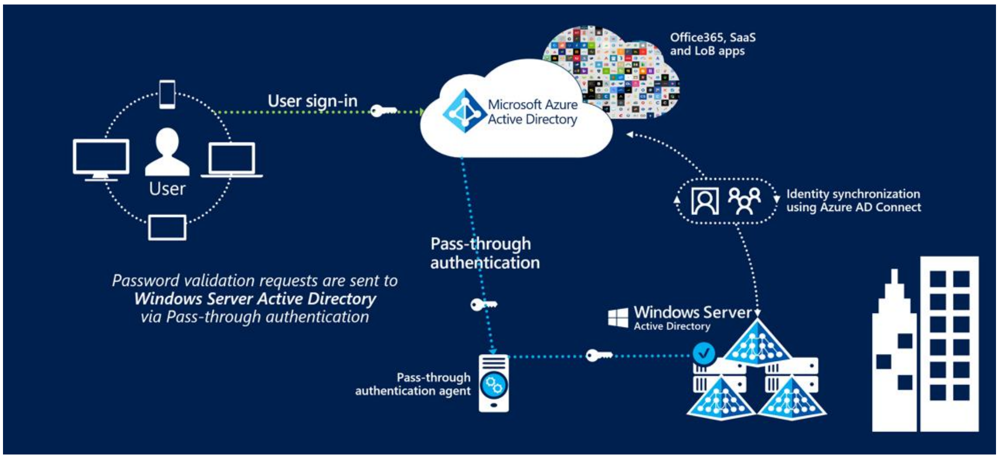

Figura 3. Esquema de flujo para agente PTA [12]

- Sincronización, dedicado a la creación de usuarios, grupos y otros objetos desde el entorno local a la nube
- Reescritura de contraseñes, ofrece la bidireccionalidad cuando se realizan cambios de clave y mantiene las políticas locales con la nube, es decir que una vez que el usuario realice un cambio de clave en la nube, esta será sincronizada con el dominio local

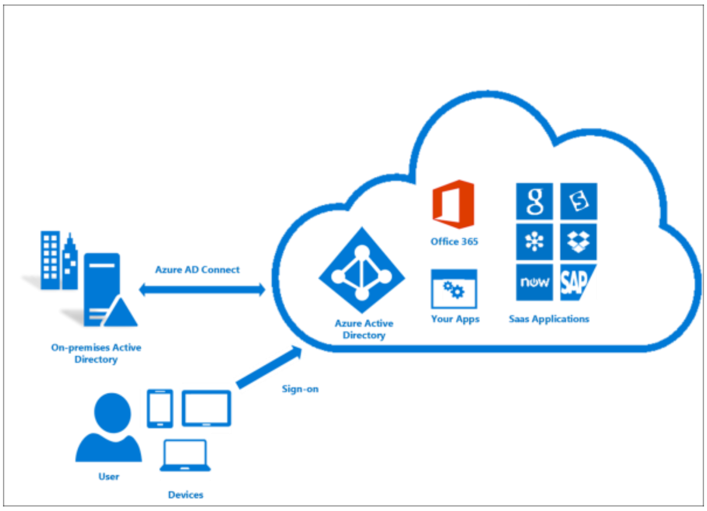

Figura 4. Esquema de flujo de conexión para reescritura de contraseñas [12]

El Firewall que actualmente utiliza la empresa es de la marca Sophos, el cual ofrece una protección de ciberseguridad de próxima generación, con varios módulos para asegurar el tráfico que debe manejar el equipo, entre ellos se pueden utilizar el control de aplicaciones, antivirus dual, control web, protección de correo electrónico, IPS de primera categoría para la protección contra amenazas avanzadas, capacidad de sincronización con directorio activo para el uso de VPNs de acceso de usuarios y generación de OTP (One Time Password) administrados en el propio equipo. Las firmas IPS identifican amenazas y especifican una acción recomendada cuando el firewall encuentra tráfico coincidente. Las firmas son específicas de aplicaciones, servicios o plataformas. El firewall incluye firmas predefinidas y también puede crear firmas personalizadas [13]. El equipo que mantiene la empresa actualmente es Sophos XG125 que posee las siguientes características:

Product Matrix

Model		Tech. Specs				Throughput[1]				
	Revision #	Form Factor	Ports/Slots (Max Ports)	w-model*	Swappable Components	Firewall (Mbps)	IPsec VPN (Mbps)	NGFW (Mbps)	Threat Protection (Mbps)	Xstream SSL (Mbps)
XG 86(w)	1	desktop	4	Wi-Fi 5	n/a	3,100	225	350	145	75
XG 106(w)	1	desktop	4	Wi-Fi 5	opt. ext. Power	3,550	330	400	150	75
XG 115(w)	3	desktop	4	Wi-Fi 5	opt. ext. Power	4,000	560	1,000	375	130
XG 125(w)	3	desktop	9/1 (9)	Wi-Fi 5	opt. ext. Power, 3G/4G	7,000	1,500	1,275	400	170
XG 135(w)	3	desktop	9/1 (9)	Wi-Fi 5	opt. ext. Power, 3G/4G, Wi-Fi**	7,500	1,700	1,800	600	210
XG 210	3	1U	8/1 (16)	n/a	opt. ext. Power	29,000	1,920	3,200	800	230

Figura 5. Especificaciones de firewall Sophos xg 125 [13]

Para mantener un solo proveedor de ciberseguridad, la empresa también posee un antimalware de la misma marca (Sophos Intercept X Advanced with XDR), el cual ofrece seguridad a nivel de máquinas de usuarios en los siguientes apartados [14]:

Features	Intercept X Advanced	Intercept X Advanced with XDR
ATTACK SURFACE		
Web Security	✓	✓
Download Reputation	✓	✓
Web Control / Category-based URL Blocking	✓	✓
Peripheral Control	✓	✓
Application Control	✓	✓
BEFORE IT RUNS ON DEVICE		
Deep Learning Malware Detection	✓	✓
Anti-Malware File Scanning	✓	✓
Live Protection	✓	✓
Pre-execution Behavior Analysis (HIPS)	✓	✓
Potentially Unwanted Application (PUA) Blocking	✓	✓
Intrusion Prevention System	✓	✓
STOP RUNNING THREAT		
Data Loss Prevention	✓	✓
Runtime Behavior Analysis (HIPS)	✓	✓
Antimalware Scan Interface (AMSI)	✓	✓
Malicious Traffic Detection (MTD)	✓	✓
Exploit Prevention	✓	✓
Active Adversary Mitigations	✓	✓
Ransomware File Protection (CryptoGuard)	✓	✓
Disk and Boot Record Protection (WipeGuard)	✓	✓
Man-in-the-Browser Protection (Safe Browsing)	✓	✓
Enhanced Application Lockdown	✓	✓

DETECT		
Live Discover (Cross Estate SQL Querying for Threat Hunting & IT Security Operations Hygiene)		✓
SQL Query Library (pre-written, fully customizable queries) Suspicious Events Detection and Prioritization		✓
Suspicious Events Detection and Prioritization		✓
Fast Access, On-disk Data Storage (up to 90 days)		✓
Cross-product Data Sources e.g. Firewall, Email (Sophos XDR)		✓
Cross-product Querying (Sophos XDR)		✓
Sophos Data Lake Cloud Storage		30 days
Scheduled Queries		✓
INVESTIGATE		
Threat Cases (Root Cause Analysis)	✓	✓
Deep Learning Malware Analysis		✓
Advanced On-demand Sophos X-Ops Threat Intelligence		✓
Forensic Data Export		✓
REMEDIATE		
Automated Malware Removal	✓	✓
Synchronized Security Heartbeat	✓	✓
Sophos Clean	✓	✓
Live Response (remotely investigate and take action)		✓
On-demand Endpoint Isolation		✓
Single-click "Clean and Block"		✓

Figura 6. Bondades de producto endpoint intercept X advanced con EDR [14]

Además de estas capacidades, posee una consola de administración en línea en Sophos Central, en donde el firewall también puede ser anclado y administrado activando las capacidades de "Synchronized Security" en donde toda la información tanto del endpoint como del firewall puede ser comunicada entre sí para obtener una mejor visibilidad de seguridad ya que los productos de Sophos trabajan juntos de forma activa a través de un “Security Heartbeat”, respondiendo automáticamente a los incidentes y proporcionando información de seguridad mejorada, posibilitando la sincronización de la seguridad.

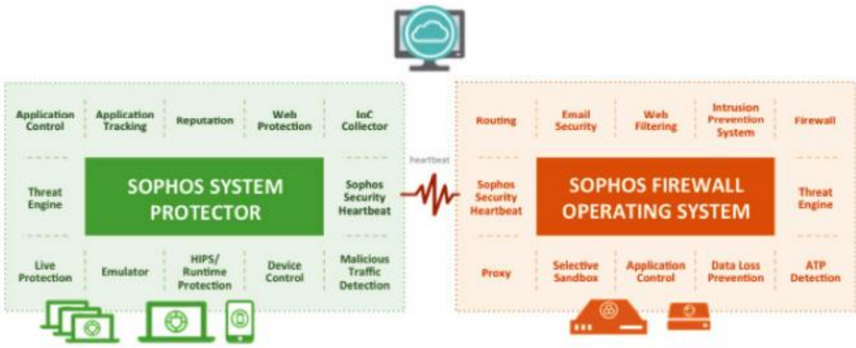

Figura 7. Esquema heartbeat con Sophos XG

Al implementar Sophos Security Heartbeat, las organizaciones pueden detectar amenazas sofisticadas antes de que causen algún daño en su infraestructura, identificar automáticamente los sistemas infectados, automatizar la respuesta a incidentes y ver el estado de seguridad de los endpoints en tiempo real. El security heartbeat posee 3 niveles de salud que se muestran por colores, rojo, amarillo y verde que desencadenan automáticamente la toma de decisiones de seguridad, además de enviar información detallada al panel de control del firewall de red, permitiendo al personal conocer el estado de salud actual de sus endpoints [15].

Posibles desencadenantes de alertas	Rojo	Amarillo	Verde
Aplicación maliciosa detectada	X - activo	X - inactivo	
Aplicaciones no deseadas		X - detectado	
Tráfico de red malicioso	X – Comunicación desde una estación de trabajo a un host malicioso o sospechoso de serlo		
El software de seguridad de Sophos no funciona correctamente	X - El sistema puede carecer de protección		
No se detecta nada, el software de seguridad funciona correctamente			X

Figura 8. Estado de protección con heartbeat [15]

La empresa también cuenta con una suscripción al servicio OpenDNS perteneciente a Cisco, el cual brinda ciertas bondades para la resolución de nombres y las consultas DNS de usuarios desde la infraestructura interna, así como de los usuarios remotos. Esta herramienta aumenta la velocidad de navegación por los sitios web y evita el acceso involuntario a sitios de phishing y malware, así como a cualquier contenido web que se configure como restringido. Para los usuarios remotos, se puede configurar la opción de roaming client, el cual es un agente que se instala en el equipo final de usuario que protege a los empleados remotos incluso cuando no están trabajando con una conexión VPN, y la consola recibe visibilidad inmediata de los dispositivos de todos los usuarios, independientemente de dónde estén trabajando. Esto proporciona una protección rápida y eficaz contra el malware, el phishing y las devoluciones de llamada de comando y control donde quiera que vayan sus usuarios, además de ofertar información granular sobre la aplicación de políticas y la elaboración de informes sobre la identidad específica del equipo o incluso del usuario de Active Directory que ha iniciado sesión [16].

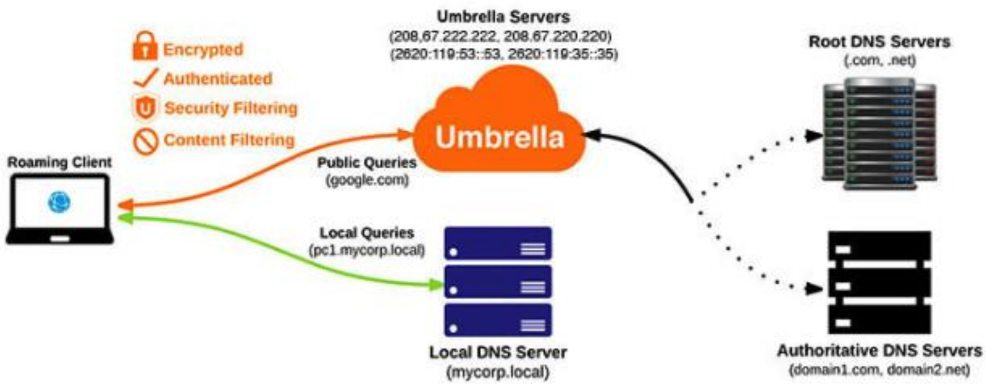

Figura 9. Modo de operación de umbrella roaming client [16]

Señal X actualmente posee una suscripción en office 365 para el uso de ofimática, debido a las bondades que la misma suministra a cualquier negocio, ya que ahora los usuarios pueden acceder a la información donde quiera que vayan. La eficiencia es muy importante para las empresas. Cualquier organización que sea capaz de comunicarse y colaborar es más eficaz. Tener acceso a herramientas de productividad que permiten a las personas hacer su trabajo desde cualquier lugar agiliza las organizaciones y les permite competir en su industria. Office 365 es la suite de productividad de Microsoft con herramientas como Word, Exchange, Excel, SharePoint, Teams y mucho más [17]. Por ello, se han considerado 7 ventajas claves del uso de esta plataforma:

- Acceder a los archivos desde cualquier lugar, ya que cada usuario cuenta con un almacenamiento definido entregado por defecto con el licenciamiento de la cuenta
- Almacenamiento seguro en la nube, Office 365 es un entorno totalmente seguro con sólidas medidas de seguridad, como la autenticación de dos factores, que garantiza que las personas no autorizadas no puedan acceder a información que no les corresponda
- Comunicación mejorada, con la ayuda de Outlook y Microsoft teams puedes estar en constante contacto entre departamentos, así como entre empresas
- Gastos predecibles
- Continuidad del negocio, a pesar de que algo ocurra con los equipos físicos, el correo electrónico, archivos y datos están a salvo en la nube, siempre y cuando se tenga activada la opción de sincronización de OneDrive
- Actualizaciones automáticas
- Colaboración centralizada, se pueden compartir buzones de correo para mantener al equipo correspondiente siempre comunicado, se pueden crear sitios colaborativos en share point que pueden ser compartidos con tan solo un link, o incluso una intranet para la empresa

Además de estos beneficios, la suscripción de office 365 también provee de acceso al portal de Azure en donde se pueden configurar seguridades adicionales de acceso por medio del acceso condicional y complementarlo con políticas intune que deben si o si cumplir los dispositivos. Es decir, se puede forzar el uso de un MFA para todos los usuarios, y tener una política que únicamente permita el acceso a los recursos a equipos que pertenezcan a la organización, siempre y cuando cumplan con la política base para los equipos, forzando a los clientes a cumplir ciertos criterios de seguridad para poder acceder la información [18].

El servicio de intune, provee la implementación de políticas que no son tan granulares como las directivas de grupo del dominio local, pero al trabajar en conjunto en los dispositivos, estas se complementan, asegurando tanto equipos en el dominio local como aquellos que se mantienen en teletrabajo. Microsoft Intune es una solución de gestión de equipos de usuario final basada en la nube. Gestiona el acceso de los usuarios y simplifica la administración de aplicaciones en todos sus dispositivos, incluidos dispositivos móviles, equipos de escritorio y equipos virtuales [19].

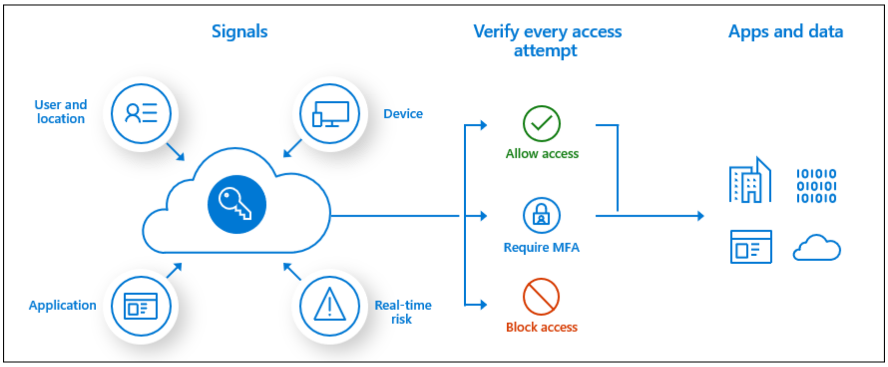

Figura 10. Esquema de acceso condicional [19]

Una arquitectura Zero Trust, se basa en la verificación de la identidad como requisito previo al acceso, por lo tanto, se debe definir una aplicación de doble autenticación que será usada por los usuarios críticos dentro de la empresa, como por ejemplo, el administrador de la infraestructura actual así como los cargos de altos rangos debido al tipo de información que manejan. En este caso se ha optado por la opción de DUO Security, ya que el mismo ofrece una versión gratuita de hasta 10 licencias que pueden servir para que los usuarios se acostumbren al uso de la misma cada que acceden a su equipo de trabajo. Esta aplicación provee un MFA muy amigable con el usuario ya que la autorización de acceso se realiza mediante la aprobación de una notificación push que llega a la aplicación del celular Duo Mobile, su consola de administración también se encuentra en la nube de cisco, y su proceso de enrolamiento es muy fácil de ejecutar. Mediante este método de autenticación se puede confirmar que el usuario en realidad es quien dice ser antes de poder acceder al recurso que necesita, en este caso puede ser su computador o un servidor que sea administrado por el usuario [20]. Además, se debe forzar a todos los usuarios a hacer el uso del MFA de office365 y azure con su aplicación Microsoft authenticator.

Por otra parte, un complemento del acceso condicional que se puede configurar es el permiso de acceso a los recursos de Microsoft desde ciertas ips públicas, en este caso se ocuparan las ips de los proveedores actuales, por lo tanto, los usuarios remotos deberán mantener una conexión VPN con el firewall que enrute el tráfico hacia Microsoft para que puedan tener acceso a los mismos, la VPN que se utilizara es una SSL, ya que en la misma se pueden configurar ciertos parámetros que garantizan la confidencialidad y autenticación de cada uno de los usuarios para poder acceder a los recursos de la red. Para este tipo de VPN, también se puede utilizar un OTP que provee el mismo equipo (Sophos XG), el cual es generado automáticamente cuando el usuario hace login en el portal de usuario, y que debe ser utilizado cuando se realiza la conexión VPN, de lo contrario se denegará el acceso.

En cuanto al sistema ERP que la empresa maneja actualmente, el mismo se encuentra alojado en la infraestructura de Digital Ocean y se encuentra publicado al mundo. Se ejecuta bajo una distribución Linux (Ubuntu), con el sistema odoo y es el encargado de manejar toda la producción, ventas, contabilidad, reportes y demás de la empresa Señal X. Actualmente es manejado por un proveedor externo quien se encarga de su mantenimiento, manejo y configuración. El sistema también puede ser integrado con una autenticación LDAP con el directorio activo para garantizar que cada usuario mantenga un perfil de su pertenencia y se pueda tener una mejor visibilidad en logs de auditoria en caso de necesitarlos.

Señal X es una empresa dedicada netamente al trabajo de publicidad empresarial con presencia en 3 ciudades del Ecuador, Cuenca, Quito y Guayaquil, siendo la primera la sucursal matriz en donde se elaboran la mayor parte de la manufactura. De acuerdo a la visita de campo realizada en la infraestructura de Señal X, se pudieron definir los siguientes componentes de red que posee la empresa, para exponer de mejor manera este punto se cuenta con un diagrama de red (Figura 11) previamente autorizado por la empresa.

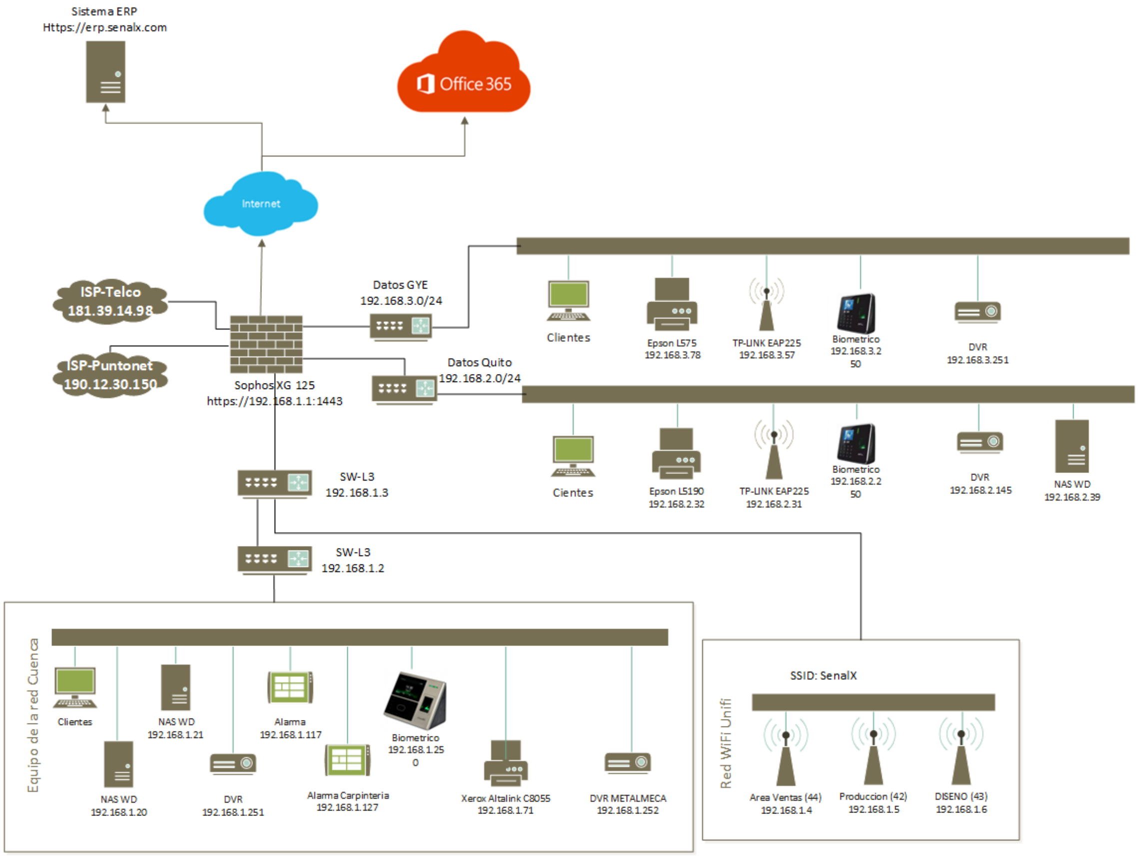

Figura 11. Diagrama de red actual

En el diagrama se pueden identificar los siguientes componentes de red:

- RED LAN Y REDES DE DATOS
- ISP
- FIREWALL SOPHOS XG 125
- COMPUTADORES DE USUARIO FINAL
- COMPUTADORES PARA REALIZAR IMPRESIONES Y TRABAJOS DE PUBLICIDAD
- ACCES POINTS
- SERVIDORES
- NAS
- IMPRESORAS WIFI
- RELOJES BIOMETRICOS
- RED WIFI
- SWITCH ADMINISTRABLES

De acuerdo al diagrama de red se puede observar que Señal X actualmente posee una red plana , misma que no mantiene segmentaciones de ningún tipo, por lo tanto todos los equipos tienen la capacidad de verse entre sí, ya sean equipos de producción o de usuarios administrativos de la empresa, en cuanto a la red WiFi también se pudo constatar que la red de invitados y la red empresarial se encuentran en el mismo segmento de red , compartiendo de esta manera servicios de impresión, acceso a servidores, y servicios locales que únicamente deberían ser accedidos por personal de la empresa.

Otro punto a destacar también es que poseen 2 contratos de internet comerciales, el principal con Telconet, en el cual se posee comunicación tanto a Quito y Guayaquil por una red de datos implementada por el mismo proveedor, y el otro enlace perteneciente a Puntonet el cual sirve como backup. De acuerdo a la entrevista llevada a cabo con el administrador de la red y servicios de Señal X se pudo obtener la información que mantienen una suscripción de Office365 en el cual manejan únicamente el servicio de correo electrónico a pesar de tener un licenciamiento que les otorga acceso a la mayoría de servicios de Microsoft como son:

- Microsoft Teams
- Outlook
- Sharepoint
- OneDrive

Conforme con lo expresado por el administrador, no se han realizado capacitaciones al personal para el uso de las demás herramientas que otorga Office365 así como las seguridades que podrían ser implementadas por medio del portal de Azure que podrían garantizar de gran manera el acceso exclusivo a la información de únicamente los colaboradores de la empresa.

Por otra parte, se me informo que actualmente la empresa no posee políticas de acceso a internet o de ningún tipo que garanticen la seguridad de la información o la seguridad de acceso hacia los servicios tecnológicos que posee la empresa. A pesar de contar con un software antimalware de próxima generación (Sophos Intercept X) las políticas para este software no han sido implementadas teniendo en cuenta el giro del negocio sino se han aplicado políticas por defecto implementadas por el mismo proveedor (Telconet). Además, la infraestructura actual posee varios equipos con sistema operativos obsoletos tales como Windows Vista, Windows XP y Windows 7, que no han sido tomados en consideración para llevar a cabo una migración hacia un sistema operativo actual o en su defecto aplicar una política de mínimo acceso interno o hacia internet. Entre los servidores que se encuentran en la red existen dos que son exclusivamente para realizar consultas, ya que corresponden a sistemas ERP que ya no son utilizados por la empresa, pero contienen información contable (cartera vencida), estos servidores tienen una versión Windows Server 2008 también obsoleta y que se encuentra en CPUs normales de usuario. Actualmente Señal X, trabaja con un sistema ERP montado en la nube de Digital Ocean, en el cual se generan todas las ventas, así como las ordenes de producción, pero que se mantiene publicado al mundo sin restricciones.

También, se pudo verificar que los usuarios hacen el uso de dos NAS (WD), los cuales no se encuentran segmentados y son alcanzables por cualquier usuario, y que además ya no cuentan con espacio para guardar los artes que produce el área de diseño, obligándolos a compartir estos artes a las diferentes áreas por medio de un disco duro externo.

El administrador actual, posee una gestión compartida con el proveedor de internet Telconet sobre el firewall que administra tanto la red local como el acceso de las redes de Quito y Guayaquil por medio de la red de datos. De acuerdo con la versión del firewall actual, el mismo tiene varias capacidades de nueva generación como es el sd-wan, VPN-SSL para acceso remoto, control de aplicaciones, control de acceso web, creación y manejo de vlans, IPS, entre otros. Al poseer el antimalware y firewall de la misma marca se realizó una investigación de las bondades que podría otorgar a la seguridad de equipos e infraestructura de la empresa, entre los más importantes se pudo encontrar los siguientes:

- Gestión centralizada desde Sophos Central

- Capacidad de uso de heartbeat (latido) en cada regla de firewall implementada
- Aislación automática de equipos en la red con un nivel de heartbeat en rojo
- Sincronización de usuarios con Directorio Activo para asignación de políticas
- Sincronización de aplicaciones utilizadas por los equipos que ayudan en la toma de decisiones
- Opción del uso de un OTP para hacer una conexión VPN a la red interna

De entre todas estas opciones la más destacable es el uso del heartbeat para garantizar el acceso a la red. Esta funcionalidad ayuda a que exclusivamente equipos que posean el endpoint (antimalware) puedan tener acceso a los recursos de red mediante una regla de firewall únicamente cuando su estado de salud este en verde, haciendo referencia a que si el equipo cumple con las políticas de seguridad implementadas en el antimalware el mismo tiene permiso para acceder al servicio que solicita de manera segura a través del firewall.

4.3. Superficies de protección

En un modelo Zero Trust, resulta más conveniente definir las superficies de protección que contiene los datos, activos, aplicaciones y servicios (DAAS) más cruciales y valiosos de la red. De este modo solo se incluyen en esta zona los componentes cruciales para las operaciones de la organización, ya que la superficie que hay que proteger es de menor magnitud que la superficie de ataque y siempre se puede conocer.

En el caso de Señal X las superficies de protección serían las siguientes:

- Sistemas ERP actual y anteriores
- Repositorio local y en la nube de artes de producción
- Respaldos de información de usuarios desvinculados de la empresa
- Acceso a servicios de office365
- Directorio activo local (debe ser implementado)

Con el establecimiento de las superficies de protección, se procede a realizar la segmentación correspondiente sobre los mismos, ya que se necesita tener una visibilidad pormenorizada del tráfico y aplicar capas adicionales de inspección basándonos en el método kipling, que define la política Zero Trust delimitando el quien, el que, el cuándo, el dónde, por qué y el cómo. Esta política determina quien puede transitar por este perímetro definido en un momento dado, vetando a los usuarios no autorizados el acceso a la superficie de protección.

5. Propuesta de implementación

Como primera instancia se propone realizar la segmentación del acceso a los servicios internos de la empresa, así como segmentar las máquinas de producción ya que las mismas en su gran mayoría poseen sistemas operativos obsoletos. Esta opción es plenamente viable ya que la infraestructura actual posee switches de capa 3 con capacidad para el manejo de VLANs. Para este caso también se propone realizar la virtualización de los 2 servidores de sistemas antiguos ERP en un hypervisor que de momento no está siendo utilizado y con la inspección realizada posee los recursos necesarios para realizar esta migración, la cual facilitaría de gran manera la gestión de accesos a estos servidores. Además, se debe reestructurar la manera de cómo se encuentran conectados físicamente los switches con el firewall ya que la conexión actual no posee ninguna configuración adicional para garantizar la alta disponibilidad en el tráfico de red. De la misma manera se debe también segmentar las superficies de protección tanto de la infraestructura interna como de los servicios en la nube, el sistema ERP debería conectar una VPN sitio a sitio con el firewall para así poder garantizar una conexión cifrada y segura, y por último el acceso a office 365 deberá poseer una política de acceso que autoriza las ips publicas actuales de Señal X.

Es importante recalcar también que, se deben generar políticas de mínimo acceso para las áreas de la empresa, ya que mediante esto se puede garantizar el ancho de banda que actualmente posee, así como el acceso indebido a sitios no permitidos que no vayan acorde al giro del negocio, estas políticas pueden ser implementadas tanto a nivel de firewall como a nivel de endpoint. El firewall Sophos xg tiene la capacidad de brindar acceso a los usuarios definiendo puertos de destino, control de aplicaciones autorizadas

por la empresa y acceso a paginas web por medio de categorización de las mismas facilitando las políticas de mínimo acceso para cada departamento de la empresa.
De acuerdo a la carga de trabajo del área de diseño que se pudo constatar es primordial la adquisición de un NAS con escalabilidad para soportar toda la carga de trabajo que se realiza, ya que actualmente los equipos que se encuentran dentro de la red (NAS WD) ya no poseen espacio utilizable, este equipo debería ser implementado en un segmento separado para garantizar el tráfico permitido hacia el equipo, además, se debe configurar su interfaz de red con un link aggregation para que pueda soportar la alta disponibilidad para la compartición de archivos a las áreas de producción de toda la empresa.
El directorio activo que se propone debe ser montado también en un segmento separado de red en el hypervisor disponible que mantiene la empresa bajo el dominio senalx.local para que no intervenga en la resolución de nombres cuando se requieran conexiones al dominio senalx.com, en este se deberán implementar políticas de grupo para asegurar los sistemas operativos Windows y habilitar la opción de MDM para también registrar los equipos en la nube de azure bajo un estado Hybrid AD join, de esta manera las políticas intune se podrán también aplicar sobre estos equipos. La instalación del agente Azure AD Connect se deberá implementar en este servidor y activar las opciones de autenticación de paso a través, así como la reescritura de contraseñas para sincronizar los equipos y usuarios a la nube de azure y de esta manera utilizar las credenciales de acceso tanto on-premise como en la nube. Una vez realizada la sincronización, se deben implementar políticas de acceso condicional sobre la infraestructura de azure en el cual los equipos y usuarios deben cumplir cada parámetro establecido para su acceso exitoso a los recursos en la nube. Esto también comprende el forzado del registro de dos métodos de autenticación, Microsoft App y correo electrónico para cuando los usuarios deseen cambiar sus credenciales lo puedan realizar, siempre y cuando confirmen ser quien dicen ser por medio de los dos métodos de autenticación que serían obligatorios. Y, por último, se debe hacer uso de la autenticación con MFA para el acceso a cualquier recurso de office 365.
El directorio activo deberá ser sincronizado con el firewall, para que así los usuarios puedan gestionar el acceso VPN con sus credenciales de dominio. Como se estableció anteriormente, esta VPN también deberá constar de un OTP para verificar la identidad

del usuario que quiere hacer la conexión. Las configuraciones de seguridad para la VPN SSL se deben realizar en el firewall para garantizar la confidencialidad del tráfico que pasa por esta conexión.

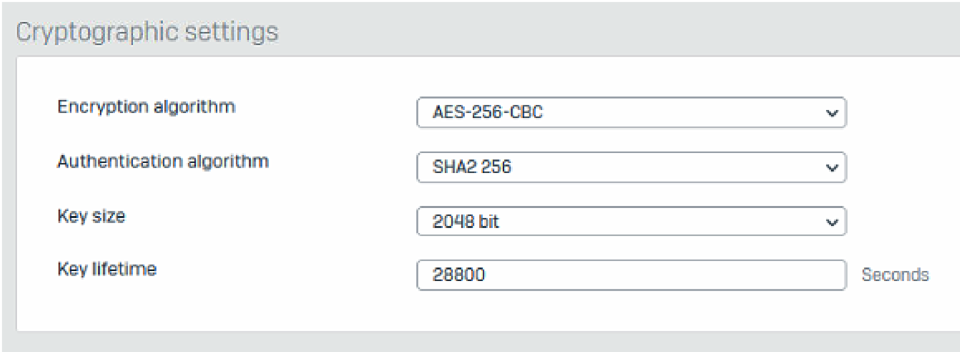

Figura 12. Configuración criptográfica para VPN SSL

Por otra parte, se deberá generar una política de aseguramiento de equipos en el cual se tiene que delimitar el software autorizado, así como el anclaje al directorio activo con las directivas de grupo pertenecientes al equipo, y asegurarse que el dispositivo este enrolado en Azure AD como Hybrid AD Join para posteriormente establecer también las políticas Intune. Bajo este mismo apartado se deberá realizar la instalación del agente de Open DNS roaming client para tener una visibilidad y protección de las consultas DNS que se realizan, tanto dentro como fuera de la institución.

Para los equipos considerados críticos, se deberá también realizar la instalación del agente DUO login con el afán de brindar acceso únicamente a los usuarios posterior a la confirmación de ser quien dicen ser por medio de un MFA adicional que se ejecuta cuando el usuario trata de ingresar en su equipo. Para lograr este objetivo se propone el siguiente esquema de red:

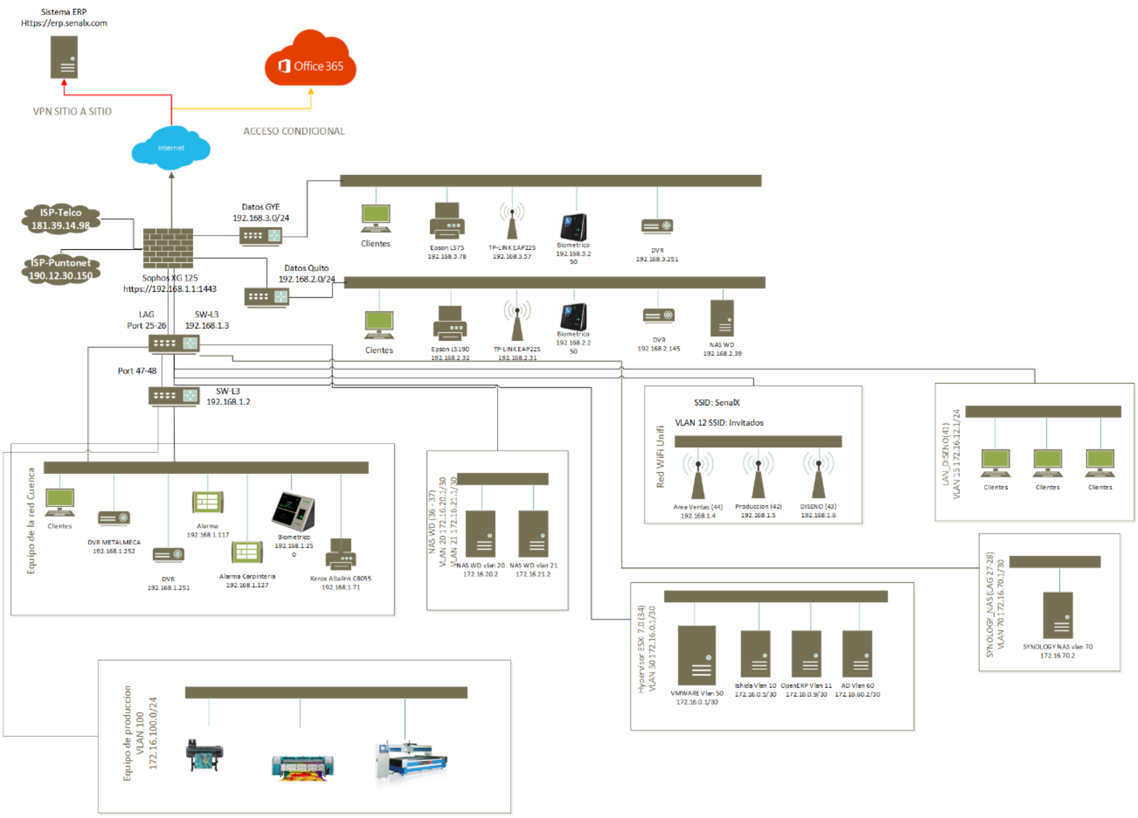

Figura 13. Diagrama de red propuesto

Bajo este nuevo esquema de red se logra garantizar en todo momento la cobertura de los activos de información tanto locales como remotos, gracias a la segmentación realizada, obligando al firewall a hacer uso de cada una de sus prestaciones en el tráfico desde y hacia los servicios internos y externos, logrando así tener un mayor control sobre el tráfico de red.

De la misma manera, se deberán crear unidades organizacionales en el directorio activo en donde se divida cada departamento, con el afán de que, al ser sincronizado con el firewall, se puedan generar reglas dirigidas a cada uno de ellos sobre las VPNs a establecerse manteniendo siempre una segmentación segura de acceso a los servicios.

De acuerdo con el diagrama de red actual (figura 11), las redes de datos envían todo su tráfico hacia la agencia matriz (Cuenca), en donde se realiza el filtrado y acceso de tráfico hacia los diferentes servicio locales y remotos, esto conlleva una falta de seguridad ya que al momento cualquier cliente que se pueda conectar a las redes de las sucursales tendría acceso abierto a los servicios locales. Por lo tanto, se propone, además, que cada sucursal deba cumplir con los siguientes aspectos en cuanto a infraestructura tecnológica para posteriormente realizar una VPN sitio a sitio tolerante a fallos, con equipos de seguridad perimetral de la misma marca que el de la matriz (SOPHOS XG), para de igual manera realizar segmentación de los departamentos o equipos de trabajo, estableciendo políticas de mínimo acceso.

Equipos mínimos necesarios para la infraestructura de una sucursal actual y/o adicional:

- Equipos de seguridad perimetral (de preferencia Sophos XG)
- 2 proveedores de internet, 1 principal y 1 de backup
- 1 switch administrable

Con la configuración mínima, se puede manejar de mejor manera tanto el tráfico local de cada sucursal como el tráfico que debe llegar a la agencia matriz por medio de una VPN sitio a sitio. Debido a que la infraestructura tecnológica se manejaría con una misma marca, la administración de la misma puede ser centralizada en la nube, haciendo uso del orquestador de SOPHOS (Sophos central), en donde se logra tanto administrar como monitorear la infraestructura y seguridad de todas las agencias de la empresa Señal X. Además, el uso de dos proveedores se hace imprescindible para poder realizar una conexión VPN sitio a sitio tolerante a fallos en donde la conexión se mantenga a pesar de que uno de los proveedores falle. Para una mejor comprensión se adjunta un diagrama de conexión.

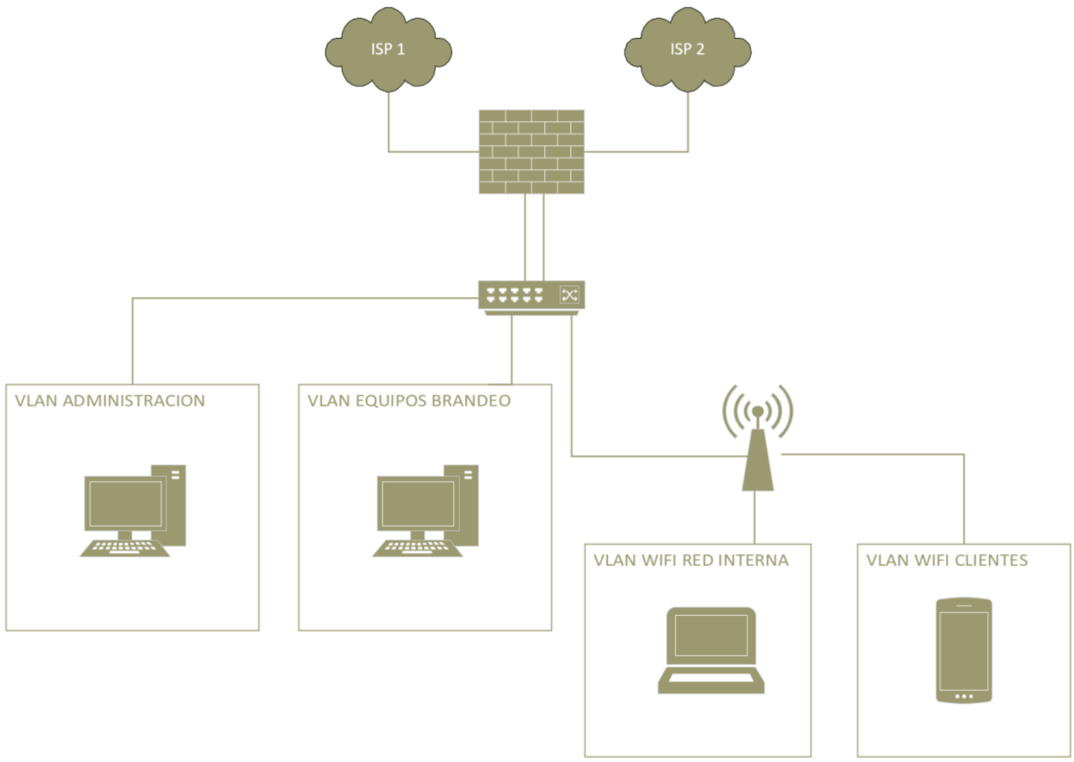

Figura 14. Equipos mínimos necesarios para una sucursal de la empresa

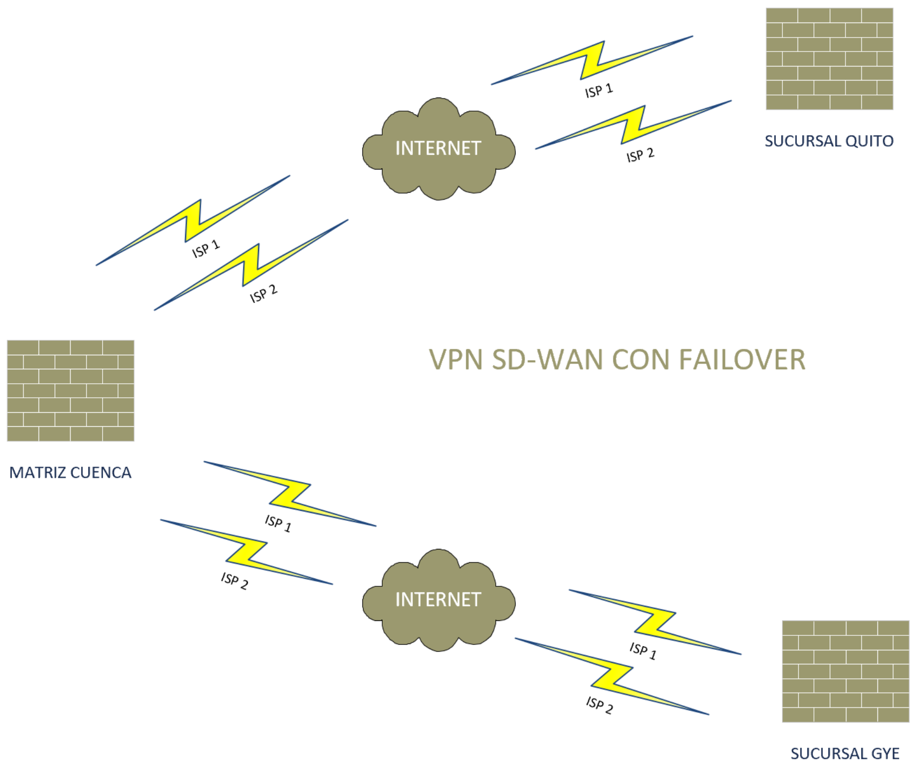

Figura 15. VPN sitio a sitio SD-WAN con failover

6. CONCLUSIONES

Un modelo de seguridad de confianza cero garantiza el control efectivo de la información y los sistemas críticos para el negocio, asegurando que las personas adecuadas tengan acceso a los datos correctos en el momento correcto. Basado en el principio de "nunca te confíes nunca, compruébale todo", Zero Trust ayuda a proteger los recursos de la empresa eliminando dispositivos desconocidos y no administrados y limitando el movimiento lateral.

Zero Trust proporciona políticas integrales en todo el proceso de desarrollo, incluidas las identidades, la infraestructura, los dispositivos, los datos, las aplicaciones y las redes. Para lograr un verdadero modelo Zero Trust, todos estos elementos deben ser validados y verificados para la confianza.

Aunque implementar un modelo de confianza cero puede ser difícil, es un elemento esencial de un plan de modernización a largo plazo. Cualquier organización que desee adoptar la confianza cero debe comenzar con un enfoque gradual de controles de seguridad, en lugar de intentar aplicar muchos controles grandes a la vez, es importante que una organización comience con un pequeño conjunto de controles de seguridad y los implemente de manera efectiva. Esto permitirá a la organización evaluar los resultados y aprender de las lecciones que se pueden aplicar a medida que se avanza en la implementación de controles adicionales.

Además, es importante que una organización se asegure de que sus controles de seguridad sean escalables y adaptables a medida que crece y cambia. La confianza cero es un enfoque a largo plazo y requiere un compromiso continuo para asegurarse de que los datos de la organización estén protegidos de manera efectiva.

En resumen, la implementación gradual de controles de seguridad es esencial para una estrategia de confianza cero efectiva y sostenible. Al comenzar con un pequeño conjunto de controles y adaptarlos a medida que la organización crece y cambia, se puede construir una estrategia de confianza cero sólida y efectiva a largo plazo.

7. RECOMENDACIONES

Realizar en lo posible informes quincenales de las distintas herramientas de ciberseguridad como: firewall, antimalware, consultas dns, autenticación MFA, entro otros, con la finalidad de determinar los comportamientos de los usuarios, y realizar cambios que aseguren una política de acceso mínimo necesario

Una arquitectura Zero Trust de acuerdo con la documentación y en experiencia propia es un proceso continuo, ya que las nuevas tecnologías obligan a ir creando, manteniendo y cambiando ciertas políticas de acceso, por lo que se deben realizar informes periódicos para determinar cuáles son las nuevas tendencias de los usuarios, así como entender cuáles son los accesos que los mismos necesitan, y de esta manera ir optimizando la arquitectura propuesta. Por último, es esencial evaluar y probar regularmente la seguridad; es importante realizar evaluaciones regulares de seguridad y pruebas de penetración para identificar posibles vulnerabilidades y brechas de seguridad en el sistema

REFERENCIAS

[1] I. C. PONEMON INSTITUTE, "Cost of a Data Breach Report 2020", IBM SECURITY, 2020.

[2] Metro Ecuador. "Infraestructura tecnológica del Municipio de Quito sufrió ataque informático". Metro Ecuador. https://www.metroecuador.com.ec/noticias/2022/04/18/infraestructura-tecnologica-del-municipio-de-quito-sufrio-ataque-informatico/

[3] "Infraestructura TI más segura de la mano de ESET - Prensario Tila". Prensario Tila. https://prensariotila.com/infraestructura-ti-mas-segura-de-la-mano-de-eset/

[4] infobae. "Qué es la nube híbrida y cuáles son las ventajas para los empresarios". infobae. https://www.infobae.com/america/tecno/2022/03/17/que-es-la-nube-hibrida-y-cuales-son-las-ventajas-para-los-empresarios/

[5] Akamai. "Modelo de seguridad Zero Trust: ¿Qué es Zero Trust?" akamai.com. https://www.akamai.com/es/our-thinking/zero-trust/zero-trust-security-model.

[6] I. IT. "Arquitectura de seguridad Zero Trust | Beneficios, Tecnologías e Implementación". International IT. https://www.internationalit.com/post/arquitectura-de-seguridad-zero-trust-beneficios-tecnologías-e-implementación?lang=es

[7] "Beneficios de adaptar una estrategia Zero Trust - Grupo Korporate". Grupo Korporate. https://grupokorporate.com/beneficios-de-adaptar-una-estrategia-zero-trust/

[8] Okta, "The State of Zero Trust Security 2021", OKTA, junio de 2021.

[9] John Grady y Adam DeMattia, "Zero Trust Impact Report", ESG Research Insights Paper, junio de 2022.

[10] C. A. Bernal, Metodología de la investigacion, 3a ed. PEARSON EDUCACIÓN, 2010.

[11] "SP 800-207, Zero Trust Architecture | CSRC". NIST Computer Security Resource Center | CSRC. https://csrc.nist.gov/publications/detail/sp/800-207/final

[12] "¿Que es Azure AD Connect y Connect Health? - Microsoft Entra". Microsoft Learn: Build skills that open doors in your career. https://learn.microsoft.com/es-es/azure/active-directory/hybrid/whatis-azure-ad-connect

[13] "IPS policies - Sophos Firewall". Service and Support. https://docs.sophos.com/nsg/sophos-firewall/18.5/Help/en-

us/webhelp/onlinehelp/AdministratorHelp/IntrusionPrevention/IPSPolicies/index.html#turn-on-ips-protection
[14] https://www.sophos.com/en-us/products/endpoint-antivirus/tech-specs
[15] https://www.sophos.com/es-es/medialibrary/PDFs/marketing%20material/sophos-security-heartbeat-wpna.pdf?la=es-ES#:~:text=Una%20solución%20creada%20para%20funcionar,de%20complejidad%20o%20costes%20adicionales.
[16] "Introduction". Umbrella User Guide. https://docs.umbrella.com/deployment-umbrella/docs/1-introduction-1
[17] "The 7 Key Benefits of Using Office 365 for Business". Core Technology Systems. https://www.core.co.uk/blog/blog/the-7-undeniable-benefits-of-using-office-365-for-business
[18] "Plan an Azure Active Directory Conditional Access deployment - Microsoft Entra". Microsoft Learn: Build skills that open doors in your career. https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/plan-conditional-access
[19] "What is Microsoft Intune". Microsoft Learn: Build skills that open doors in your career. https://learn.microsoft.com/en-us/mem/intune/fundamentals/what-is-intune
[20] "Guide to Two-Factor Authentication · Duo Security". Guide to Two-Factor Authentication · Duo Security. https://guide.duo.com/