Instituto Tecnológico y de Estudios Superiores de Occidente

Reconocimiento de validez oficial de estudios de nivel superior según acuerdo secretarial 15018, publicado en el Diario Oficial de la Federación del 29 de noviembre de 1976.

Departamento de Electrónica, Sistemas e Informática

Maestría en Informática Aplicada

Implementación de herramientas Zero-Trust

TRABAJO RECEPCIONAL que para obtener el **GRADO** de
MAESTRO EN INFORMÁTICA APLICADA

Presenta: **OLIVER ADRIAN LANDEROS ARIAS**

Tutor **MTRO. LUIS DANIEL SOUZA RODRÍGUEZ**

Tlaquepaque, Jalisco. 17 de junio de 2024.

Dedicatoria

A mis queridos padres Fortunato y Angélica, por su amor incondicional, su apoyo constante y por inculcarme los valores de la perseverancia y el esfuerzo. Sin su guía y aliento, no habría llegado hasta aquí.

A mis hijos Iñaki y André, quienes son mi fuente de inspiración diaria. Sus sonrisas y su curiosidad por el mundo me han motivado a superarme y a dar lo mejor de mí en cada momento.

A mi esposa Mafer, gracias por estar a mi lado en cada paso de este camino, por creer en mí y por brindarme el amor y la fuerza que necesitaba para alcanzar este logro.

A todos ustedes, les dedico esta maestría con todo mi corazón.

Resumen

Este documento ofrece una visión detallada del proyecto de implementación de Tailscale, *Single Sign-On (SSO)* y tecnologías de autenticación sin contraseña en nuestra infraestructura tecnológica.

En primer lugar, se aborda la integración de Tailscale, una solución moderna para redes privadas virtuales (VPN) que utiliza el protocolo *WireGuard*. Tailscale simplifica la configuración y gestión de redes seguras, permitiendo la creación de conexiones privadas entre dispositivos de manera eficiente y sin complicaciones tradicionales. El documento explora cómo Tailscale ha mejorado la conectividad, eliminando las barreras de firewalls y NAT, y reduciendo el tiempo de configuración de redes distribuidas.

En segundo lugar, se describe la implementación de *Single Sign-On (SSO),* una tecnología que unifica el proceso de autenticación, permitiendo a los usuarios acceder a múltiples aplicaciones con una sola credencial. Se detalla cómo SSO ha optimizado la experiencia del usuario al reducir la necesidad de gestionar múltiples contraseñas y cómo ha fortalecido la seguridad mediante la centralización y estandarización de los controles de acceso. Además, se discuten los beneficios operativos, incluyendo la simplificación en la administración de usuarios y la implementación de políticas de seguridad coherentes.

Finalmente, el documento explora la adopción de tecnologías de autenticación sin contraseña, que incluyen métodos avanzados como la autenticación biométrica. Estas tecnologías han elevado el nivel de seguridad al eliminar las contraseñas, reduciendo significativamente los riesgos de phishing y robo de credenciales. Se destaca cómo la autenticación sin contraseña ha mejorado la experiencia del usuario final, ofreciendo un acceso más rápido y sin fricciones.

A lo largo del documento, se proporcionan perspectivas sobre el impacto positivo de estas tecnologías en la infraestructura de la organización, mejorando tanto la seguridad como la eficiencia operativa. Además, se comparten las lecciones aprendidas y las mejores prácticas adoptadas durante el proceso de implementación, ofreciendo una guía valiosa para otras organizaciones que consideren la adopción de soluciones similares.

Palabras clave: Ciberseguridad, *Zero-Trust*, Tailscale, Inicio de sesión único, Autenticación sin contraseña

Contenido

Introducción

Este caso de estudio describe cómo una empresa emergente de seguridad informática con más de 15 años de experiencia y una sólida reputación implementó un programa de mejora de la seguridad informática para satisfacer los requisitos de sus nuevos inversores y clientes.

En los últimos cuatro años, la empresa experimentó un rápido crecimiento en términos de empleados y operaciones, duplicando el número de empleados en los dos últimos años hasta llegar a un promedio de 500. Este crecimiento fue impulsado por la aceptación de los clientes, las recomendaciones directas y la llegada de nuevos inversores.

Los nuevos inversores de la empresa se han fijado ambiciosos objetivos de crecimiento para la generación de negocio y el crecimiento del personal en todos los departamentos. Para lograr estos objetivos, la empresa debe mantener sus altos estándares de gobernanza y seguridad.

Como resultado de su crecimiento, la empresa comenzó a atraer la mirada de compañías trasnacionales para adquirir sus servicios. Estos nuevos clientes tienen requerimientos mínimos para poder realizar la contratación de servicios, como lo es, que la empresa obtenga y mantenga certificaciones comerciales como: SOC 2 Type II, ISO 27001 y Google A2LA.

La empresa cuenta con una plantilla de alrededor de 500 colaboradores y contratistas, la cultura de la empresa radica en “primero remoto” por lo cual todos los usuarios trabajan de manera remota. Si bien existen dos oficinas, el asistir a estas no es obligatorio. Esto detona una mayor atención en la parte de herramientas necesarias para mantener a los usuarios siempre conectados y seguros a las herramientas internas y externas de la organización.

La empresa emergente en cuestión utilizaba una solución de VPN de código abierto llamada *OpenVPN*. Aunque esta solución había sido efectiva en el pasado, ya no resultaba adecuada para satisfacer las necesidades actuales de la empresa, especialmente debido al crecimiento de su plantilla. Como resultado, surgieron los siguientes desafíos con esta solución:

El problema se centra en la insuficiencia de recursos humanos y capacitación dentro del equipo de soporte de TI para realizar tareas como la emisión o renovación de certificados para usuarios, así como la revocación y bloqueo de usuarios en el *firewall* en caso de salida de la organización. Esta limitación también se refleja en la falta de personal para instalar o actualizar agentes, certificados y solucionar problemas generales.

Detención de múltiples vulnerabilidades de seguridad en sus diferentes versiones tanto en el *firmware* de la caja central (*PfSense*) como en cada uno de los clientes/agentes instalados en los equipos del usuario final.

Por otro lado, la autenticación de la cuenta principal del usuario (*email* y herramientas ofimática) se realizaba a través de usuario y contraseña con un segundo factor de autenticación utilizado en cualquier aplicación que el usuario elija. Si bien esto cubría los estándares mínimos de seguridad, no era la opción más segura y actual en cuanto a seguridad y facilidad de uso.

Además, la empresa ya poseía las herramientas y licencias necesarias para implementar el inicio de sesión único con diversas aplicaciones de terceros. A pesar de esto, dicha funcionalidad no había sido activada. Esta omisión resultaba en la gestión de múltiples conjuntos de credenciales por parte de los usuarios, lo que incrementaba la carga administrativa y de seguridad. En ausencia del inicio de sesión único, la responsabilidad de salvaguardar los datos de la empresa y los clientes recaía en gran medida en el usuario final, lo que aumentaba el riesgo de vulnerabilidades y errores en la gestión de accesos.

Para abordar estos desafíos, implementamos las siguientes herramientas que cubren las necesidades al momento previo de la implementación:

- **Tailscale:** Una solución de red de confianza cero que proporciona acceso remoto seguro a infraestructura y aplicaciones sin necesidad de *VPN* ni reglas de firewall complejas, además que no requiere certificados individuales para cada usuario.
- **Autenticación sin contraseña:** Una solución que permite a los usuarios iniciar sesión sin necesidad de recordar una contraseña, que funciona en conjunto la autenticación biométrica y la autenticación de dos factores (*2FA*).
- **Inicio de sesión único (*SSO*):** Una solución que permite a los usuarios iniciar sesión en múltiples aplicaciones con un solo conjunto de credenciales.

Como Ingeniero de Infraestructura Senior de la empresa, mis funciones para este proyecto son las siguientes:

- Análisis de herramientas: Evaluar las diferentes opciones disponibles para cumplir con los requisitos del proyecto.
- Implementación: Instalar y configurar las herramientas seleccionadas.
- Generación de documentación necesaria: Documentar el proceso de implementación, así como la administración y uso de las herramientas.

Los siguientes son algunos de los beneficios asociados con las herramientas:

Seguridad mejorada: Tailscale, la autenticación sin contraseña y el *SSO* pueden ayudar a la empresa a mejorar su postura de seguridad al reducir el riesgo de filtraciones de datos y ataques de phishing.
Cumplimiento mejorado: Estas herramientas también ayudaron a la organización a cumplir con las regulaciones y estándares de la industria, como *SOC 2 TYPE II*, ISO 27001 y Google A2LA.
Mayor eficiencia y productividad: Al simplificar su arquitectura de red y reducir la necesidad de que los usuarios administren múltiples contraseñas, estas herramientas pueden ayudar a la empresa a mejorar la eficiencia y la productividad.

La implementación de las tres herramientas fue satisfactoria y se cumplieron todos los objetivos planteados. A lo largo de este documento se describen los aciertos, errores, posibles mejoras y lecciones aprendidas durante el proceso de implementación.

Como todo en el ámbito de TI no es un proyecto estático, se tendrán que actualizar para mantener la empresa no con los requerimientos mínimos, si no a la vanguardia para salvaguardar la información interna como de los clientes y mejorar la experiencia del usuario final.

CAPITULO 1

Antecedentes y significado

La protección basada en el perímetro, en la que históricamente se ha confiado para proteger las redes corporativas, opera bajo el supuesto de que las entidades dentro del perímetro de la red son de confianza, mientras que las que están fuera se consideran no confiables. Sin embargo, con la proliferación de los servicios en la nube, el trabajo remoto y los dispositivos móviles, el perímetro de la red tradicional se ha vuelto cada vez más poroso, lo que hace que las medidas de seguridad basadas en el perímetro sean inadecuadas para defenderse contra amenazas cibernéticas sofisticadas.

Por el contrario, *Zero Trust Architecture* adopta un enfoque fundamentalmente diferente al asumir confianza cero, independientemente de si las entidades están dentro o fuera del perímetro de la red. *ZTA* opera según el principio de "nunca confiar, siempre verificar", lo que requiere autenticación y autorización continuas para cada usuario, dispositivo y aplicación que intenta acceder a los recursos. Al aplicar estrictos controles de acceso basados en la identidad, la posición del dispositivo, la ubicación y otros factores contextuales, *ZTA* minimiza la superficie de ataque y reduce el riesgo de movimiento lateral por parte de actores maliciosos dentro de la red. Este enfoque se alinea con los principios de privilegio mínimo y confianza mínima, garantizando que los derechos de acceso se otorguen según sea necesario y que los privilegios se ajusten dinámicamente en función de los factores de riesgo cambiantes.

La transición de la protección basada en perímetro a la arquitectura *Zero Trust* representa un cambio de paradigma en la estrategia de ciberseguridad, que permite a las organizaciones adaptarse a la naturaleza dinámica de los entornos de TI modernos y mitigar eficazmente las amenazas cibernéticas en evolución. Al adoptar *ZTA*, las organizaciones pueden mejorar su postura de seguridad, mejorar la visibilidad y el control sobre el tráfico de la red y proteger mejor los activos de datos confidenciales contra amenazas internas y externas. Sin embargo, la implementación exitosa de *ZTA* requiere un enfoque holístico que abarque tecnología, procesos y cambios culturales, así como un monitoreo y adaptación continuos a las amenazas y tecnologías emergentes.

Las empresas en la industria de la tecnología enfrentan un conjunto distinto de desafíos en su viaje, particularmente en los ámbitos de la gobernanza y las certificaciones relacionadas con la seguridad, el cumplimiento y la protección de datos. A medida que estas empresas emergentes amplían sus operaciones y manejan datos cada vez más confidenciales, la necesidad de marcos de gobernanza sólidos se vuelve primordial. Estos marcos deben alinearse perfectamente con las mejores prácticas de la industria y los mandatos regulatorios.

La gobernanza, en este contexto, abarca el conjunto de procesos, políticas y procedimientos que orquestan la toma de decisiones, la gestión de riesgos y la conducta general de la organización. Este esfuerzo multifacético implica establecer estructuras claras de rendición de cuentas, delinear roles y responsabilidades e implementar controles estrictos para salvaguardar la confidencialidad, integridad y disponibilidad de los datos. Un marco de gobernanza eficaz permite a las nuevas empresas identificar, evaluar y mitigar los riesgos de forma eficaz, salvaguardando sus operaciones, activos intelectuales e información de los clientes.

Certificaciones como SOC 2 TYPE II, ISO 27001 y Google A2LA son evidencia concreta de que una empresa emergente ha implementado diligentemente un conjunto integral de controles, políticas y procedimientos diseñados para proteger la información confidencial y mantener un entorno operativo seguro. Estas certificaciones brindan garantía a las partes interesadas (incluidos clientes, socios e inversores) de que la empresa cumple con estándares de seguridad reconocidos, cumple con los requisitos reglamentarios y mantiene un sólido compromiso con la protección de datos.

En los últimos años, el panorama tecnológico ha sido testigo del surgimiento de herramientas y tecnologías innovadoras diseñadas específicamente para apoyar a las nuevas empresas en sus esfuerzos de gobernanza y certificación. Estas herramientas incluyen:

Tailscale: una herramienta de conectividad de red segura que permite a las empresas establecer conexiones seguras entre sistemas al tiempo que aplica estrictos controles de acceso.

Autenticación sin contraseña: esta tecnología elimina la necesidad de contraseñas tradicionales, lo que reduce el riesgo de ataques basados en credenciales y mejora la experiencia del usuario.

Las contraseñas siguen siendo omnipresentes en la autenticación de usuarios, pero son vulnerables a muchos ataques. Por lo tanto, hacen poco para que la toma de control de cuentas (ATO) y otros riesgos de identidad digital estén dentro de la tolerancia al riesgo de una organización. Las contraseñas comprometidas representan más del 60% de las brechas de *hacking*. (Ant, 2021)

Inicio de sesión único (SSO): al optimizar la gestión del acceso, simplificar el aprovisionamiento de usuarios y elevar la seguridad general, el SSO se ha convertido en una herramienta fundamental para modernizar los procedimientos de autenticación.

Comprender los antecedentes y el papel fundamental de estas herramientas en el contexto de la gobernanza es esencial. El objetivo de este trabajo es proporcionar una inmersión profunda en estas herramientas, dilucidando sus ventajas, desafíos y estrategias de implementación precisas para obtener las certificaciones SOC 2 TYPE II, ISO 27001 y Google

A2LA. Al analizar meticulosamente las implicaciones y los aspectos prácticos asociados con estas herramientas, fortaleciendo así sus prácticas de gobernanza y posicionándose para una ventaja competitiva dentro de la industria.

Desafíos actuales que enfrenta la empresa

Conforme la evolución de la empresa, su infraestructura abarca una combinación de herramientas gratuitas, desarrolladas internamente y de pago, cada una con distintos niveles de soporte. Si bien estas herramientas fueron suficientes durante la fase inicial, ahora están viéndose limitadas e insuficientes por satisfacer las mayores demandas provocadas por el crecimiento exponencial, impulsadas por rondas de inversión exitosas y los requisitos de nuevos clientes que exigen estricta seguridad y cumplimiento para forjar relaciones comerciales.

Un punto crítico radica en la naturaleza descentralizada de la autenticación, donde cada herramienta emplea un método de autenticación y un conjunto de credenciales distintos. Este enfoque descentralizado supone un inconveniente para los usuarios y presenta un gran riesgo de seguridad, ya que los usuarios tienden a reutilizar las credenciales en múltiples sistemas. Además, la carga para el personal de TI encargado de administrar estas plataformas dispares se ha vuelto abrumadora.

Por estos desafíos, la empresa debe modernizar sus procesos de autenticación, reforzar la seguridad y garantizar su cumplimiento según continúa su trayectoria de crecimiento y éxito.

Planteamiento del Problema

El problema que enfrenta la empresa se puede definir como la falta de una infraestructura segura que satisfaga las demandas del crecimiento exponencial. A medida que la empresa evoluciona, la combinación de herramientas utilizadas resulta limitada e insuficiente para manejar las nuevas exigencias generadas por el éxito financiero y la necesidad de cumplimiento de los nuevos clientes. En consecuencia, la empresa se enfrenta a la necesidad urgente de modernizar sus procesos para reforzar la seguridad y garantizar el cumplimiento, a fin de mantener su crecimiento y éxito continuo. Esto se divide en los siguientes 3 puntos:

1. El problema se plantea con la inminente expiración del certificado de la solución actual de VPN. Esta situación requiere una reinstalación tanto en el firewall central como en cada dispositivo de usuario. Sin embargo, este proceso se enfrenta a limitaciones debido a la carga de trabajo que supera la capacidad del personal actual del área de TI. Además, la solución actual exhibe múltiples vulnerabilidades de seguridad, las cuales han sido cada vez más recurrentes en los últimos meses, a pesar de las actualizaciones implementadas en los

agentes. Por último, el proceso manual de incorporación y salida de empleados y contratistas agrega una carga adicional al sistema.

2. Actualmente, no se dispone de una solución de autenticación universal para toda la organización. En su lugar, existen varias opciones, como acceso mediante usuario y contraseña, autenticación multifactorial a través de llamadas telefónicas, SMS y tokens en aplicaciones. La diversidad de opciones y excepciones en este sistema genera un entorno altamente vulnerable al phishing, lo que pone en riesgo la información propietaria de la organización y los datos confidenciales y sensibles de los clientes.

3. La falta de integración de aplicaciones de terceros con el proveedor de identificación actual (Entra ID) significa que cada usuario debe administrar al menos 10 conjuntos diferentes de credenciales. Esto lleva a que se reutilicen con frecuencia las mismas credenciales para distintas herramientas y aplicaciones, lo que representa un gran riesgo para la seguridad de la organización.

El desafío central: certificación y expansión global

Aunque el objetivo principal es abordar los problemas mencionados anteriormente, es importante destacar un objetivo secundario: asegurar que las herramientas y mejoras seleccionadas para resolver estos problemas cumplan completamente con los puntos de control asociados para obtener tres certificaciones clave: SOC 2 TYPE II, ISO 27001 y Google A2LA. Estas certificaciones son requisitos indispensables para atraer y retener una creciente base de clientes internacionales que buscan estándares establecidos en sus relaciones comerciales.

La obtención de estas certificaciones refleja el compromiso de la empresa con la seguridad sólida de los datos, el cumplimiento de rigurosos estándares internacionales y la construcción de una reputación confiable en el mercado global. Estos estándares son fundamentales para establecer la confianza de los clientes y garantizar la integridad de las operaciones comerciales en un entorno cada vez más exigente en términos de seguridad y cumplimiento normativo.

Migración e implementación de herramientas y procesos críticos

La obtención de estas certificaciones va más allá de un simple trámite; implica una transformación significativa en diversos aspectos de las operaciones de la empresa. El proceso de certificación demanda la migración e implementación de herramientas y procesos meticulosamente diseñados, ejecutados y aplicados para fortalecer tanto la seguridad como la eficiencia operativa de la organización

1. Evolución de VPN: La próxima expiración del certificado central de la solución VPN actual cobra gran importancia y amenaza con interrumpir la capacidad de la empresa para

conectar de forma segura a su fuerza laboral global. El proceso de renovación, cargado de complejidades, plantea una carga administrativa considerable para el ya sobrecargado departamento de TI. Encontrar una solución VPN adecuada, escalable y segura es una necesidad critica.

2. Autenticación sin contraseña: a medida que la empresa se expande y maneja datos cada vez más confidenciales, la dependencia de las contraseñas tradicionales se convierte en una vulnerabilidad evidente. La implementación de MFA se vuelve primordial, ya que proporciona una capa adicional de seguridad que protege contra ataques basados en credenciales y garantiza a los clientes el compromiso de la empresa con la protección de datos.

3. Revolución del inicio de sesión único (SSO): el panorama actual de autenticación descentralizada, caracterizado por métodos y políticas de credenciales dispares en todas las herramientas, plantea un grave riesgo de seguridad. También supone una carga para el personal de TI encargado de gestionar esta complejidad. La adopción de una solución SSO estandarizada y de alta seguridad no solo simplifica el acceso de los usuarios, sino que también aplica protocolos de seguridad sólidos que se alinean con las mejores prácticas de la industria.

Satisfacer las exigencias del crecimiento y la expansión global

Estrechamente vinculada a este desafío se encuentra la acelerada trayectoria de crecimiento de la compañía, impulsada por rondas de inversión exitosas y las crecientes demandas de los clientes transnacionales. La necesidad de ampliar las operaciones manteniendo al mismo tiempo los más altos estándares de seguridad y cumplimiento subraya la urgencia de este esfuerzo.

En esencia, la capacidad de la empresa para cumplir los requerimientos para obtener certificaciones y transformación de herramientas/procesos determinará su eficiencia operativa inmediata y su capacidad a largo plazo para prosperar en un entorno empresarial global competitivo, interconectado y consciente de la seguridad. Es un momento decisivo, en el que las decisiones estratégicas correctas darán forma al destino de la empresa y asegurarán su posición como socio confiable para clientes transnacionales.

Objetivos

General

Establecer un entorno robusto, resiliente y adaptativo que proteja la integridad de los datos y la privacidad del usuario, al tiempo que brinde una interfaz de usuario intuitiva y eficiente, elevando así la calidad global de nuestros sistemas y servicios.

Los beneficios esperados de esto son:

Seguridad mejorada: Las herramientas seleccionadas ayudarán a la empresa a mejorar su postura de seguridad al reducir el riesgo de filtraciones de datos y ataques de phishing.
Cumplimiento mejorado: Este proyecto ayudará a la organización a cumplir con las regulaciones y estándares de la industria, como *SOC 2 TYPE II*, ISO 27001 y Google A2LA.
Mayor eficiencia y productividad: Las herramientas ayudarán a la empresa a mejorar la eficiencia y la productividad de todos sus colaboradores.

Particulares

Los objetivos de este trabajo están diseñados para proporcionar una comprensión integral de cómo herramientas como Tailscale, la autenticación sin contraseña y SSO pueden ayudar a las empresas tecnológicas emergentes medianas a mejorar sus prácticas de gobierno y obtener certificaciones como SOC 2 TYPE II, ISO 27001 y Google A2LA. Los objetivos específicos de la investigación incluyen:

1. Analizar los beneficios y limitaciones de herramientas como Tailscale, autenticación sin contraseña y SSO para mejorar la gobernanza: este objetivo se enfoca en comprender las ventajas específicas que ofrece cada herramienta para fortalecer el marco de gobernanza de una empresa emergente:
    i. Examinará cómo Tailscale facilita la conectividad de red segura.
    ii. Cómo la autenticación sin contraseña mejora el control de acceso.
    iii. Cómo SSO agiliza los procesos de autorización y autenticación de usuarios.

    La investigación también identificará cualquier limitación o desafío potencial asociado con la implementación de estas herramientas.
2. Evaluar la aplicabilidad y eficacia de las herramientas Tailscale, autenticación sin contraseña y *Single Sign-On (SSO)* para cumplir con los requisitos de certificaciones reconocidas a nivel global, como SOC 2 TYPE II, ISO 27001 y Google A2LA. Se desarrollará cómo estas herramientas contribuyen a la implementación de los criterios específicos de seguridad, privacidad y gestión de información exigidos por cada certificación respectiva.

3. Desarrollar estrategias prácticas de implementación y mejores prácticas: este objetivo tiene como objetivo encontrar pautas prácticas para implementar Tailscale, autenticación sin contraseña y SSO. Se deberá identificar las consideraciones clave, los desafíos y los enfoques recomendados para la adopción e integración exitosas de estas herramientas.
4. Ejecución práctica de la implementación de Tailscale, la autenticación sin contraseña y SSO en la organización. Se buscará no solo comprender los beneficios y limitaciones teóricos de estas herramientas, sino también traducir ese conocimiento en acciones tangibles. La implementación abordará los siguientes aspectos clave:
    - Configuración y despliegue de Tailscale para garantizar una conectividad de red segura y eficiente.
    - Integración de la autenticación sin contraseña para mejorar el control de acceso, considerando la diversidad de usuarios y roles dentro de la organización.
    - Despliegue de *SSO* para agilizar los procesos de autorización y autenticación de usuarios, mejorando así la experiencia general del usuario.
    - Identificación y solución proactiva de desafíos y limitaciones que puedan surgir durante la implementación.

    Esta fase de implementación no solo busca obtener un conocimiento práctico y en tiempo real de las herramientas, sino también sentar las bases para una adopción exitosa que contribuya al fortalecimiento de la gobernanza y al cumplimiento de las certificaciones SOC 2 TYPE II, ISO 27001 y Google A2LA.

Preguntas por responder

Para abordar los objetivos descritos anteriormente, las siguientes preguntas de investigación guiarán nuestro trabajo:

1. ¿Cuáles son los beneficios y las limitaciones de herramientas como Tailscale, la autenticación sin contraseña y SSO para mejorar las prácticas de gobierno de las empresa?

2. ¿Cómo contribuye la implementación de Tailscale al cumplimiento de los requisitos de las certificaciones SOC 2 TYPE II, ISO 27001, Google A2LA?

3. ¿Qué estrategias prácticas de implementación y mejores prácticas se pueden recomendar para las empresas tecnológicas que buscan aprovechar Tailscale, la autenticación sin contraseña y SSO para fortalecer sus prácticas de gobierno?

Estas preguntas servirán como base para explorar la compleja relación entre la gobernanza, las herramientas para mejorar la seguridad y la gestión del acceso, y los requisitos de certificación.

Justificación

La seguridad informática se ha convertido en una preocupación primordial frente a la escalada de ciber amenazas. Las medidas tradicionales de seguridad perimetral y los cortafuegos ya no son suficientes para combatir el panorama digital en constante evolución. En consecuencia, la adopción de herramientas de "confianza cero" ha ganado un impulso significativo debido a su eficacia comprobada para proteger los sistemas contra las amenazas actuales. El objetivo es hacer visible la necesidad urgente de integrar herramientas de "confianza cero", el inicio de sesión único (*SSO*) y Tailscale, al tiempo que se demuestran las múltiples ventajas que otorgan a los administradores y los usuarios finales.

El término "confianza cero" encapsula una filosofía de seguridad cimentada en la desconfianza hacia cualquier entidad no verificada, ya sea un individuo o un dispositivo. En pocas palabras, cualquier solicitud de acceso a recursos requiere autenticación y autorización completas. Esta filosofía se basa en la noción de que todos los recursos, incluso aquellos que se ubican dentro de los límites de la red de una empresa, deben considerarse potencialmente inseguros. Por lo tanto, se deben instituir medidas de seguridad adicionales para proteger los activos y datos corporativos confidenciales.

En el modelo de la implementación de confianza cero, la autenticación sin contraseña se ha convertido en un ideal cada vez más favorecido. Al aprovechar los mecanismos de autenticación biométrica, como las huellas dactilares o el reconocimiento facial, la autenticación sin contraseña elimina la necesidad de que los usuarios recuerden contraseñas complejas. Esto disminuye el riesgo de contraseñas comprometidas o débiles, que con frecuencia son explotadas por actores malintencionados.

Otra faceta indispensable del marco de confianza cero es el inicio de sesión único (SSO), que permite a los usuarios acceder a múltiples aplicaciones y recursos utilizando un único conjunto de credenciales. Esto no solo mejora la comodidad del usuario, sino que también refuerza la seguridad al minimizar la cantidad de credenciales que deben almacenarse y protegerse. Okta, una importante empresa de seguridad digital realizó un estudio que reveló que la implementación de SSO reduce los requisitos de inicio de sesión de los empleados en un 60%, lo que alivia la carga administrativa y aumenta la productividad de los empleados. (Okta, 2019)

El acceso con privilegios mínimos representa otra herramienta indispensable de confianza cero, que implica la concesión de permisos únicamente esenciales a los usuarios para ejecutar sus tareas designadas. Esta práctica mitiga el riesgo de acceso no autorizado a los recursos, lo que fortalece la postura de seguridad y reduce la probabilidad de infracciones. El informe sobre el estado de la seguridad de la información de 2021 de Verizon destaca que el 61 % de las infracciones de seguridad involucraron credenciales robadas o comprometidas. La implementación del acceso con privilegios mínimos sirve para reducir las repercusiones que surgen de las credenciales comprometidas. (Verizon, 2021)

Por último, Tailscale, una herramienta de confianza cero, facilita la conectividad segura a los recursos empresariales desde cualquier ubicación geográfica. Aprovechando la tecnología de red privada virtual (VPN), Tailscale establece una red privada segura a través de Internet. Esto brinda una mayor flexibilidad a los empleados que requieren acceso a los recursos de la empresa desde entornos remotos, como trabajar desde casa. Además, Tailscale emplea sólidas técnicas de encriptación para mantener la confidencialidad e integridad de las comunicaciones, asegurando así la protección continua de los datos corporativos. (Pennarun, 2020)

La incorporación de herramientas de "confianza cero", que abarcan SSO, autenticación sin contraseña y Tailscale, genera una gran cantidad de beneficios tanto para los administradores como para los usuarios finales. En primer lugar, estas herramientas mejoran la seguridad al reducir el volumen de credenciales que requieren almacenamiento y protección, al mismo tiempo que garantizan que los usuarios estén restringidos a los recursos pertinentes exclusivamente. En segundo lugar, mejoran la productividad de los empleados al agilizar el proceso de inicio de sesión y permitir el trabajo desde cualquier lugar. Finalmente, estas herramientas agilizan los procesos de gestión de la seguridad y

alivian la carga de trabajo administrativo. (The National Institute of Standards and Technology, 2020)

En conclusión, la implementación de herramientas de "confianza cero" es imprescindible para garantizar la protección de los recursos corporativos y los datos confidenciales dentro del dinámico panorama digital. Herramientas como SSO, autenticación sin contraseña y Tailscale representan activos invaluables en esta búsqueda, fortaleciendo la postura de seguridad, reforzando la productividad y simplificando la administración de seguridad.

CAPITULO 2

Marco teórico

Mapa Mental

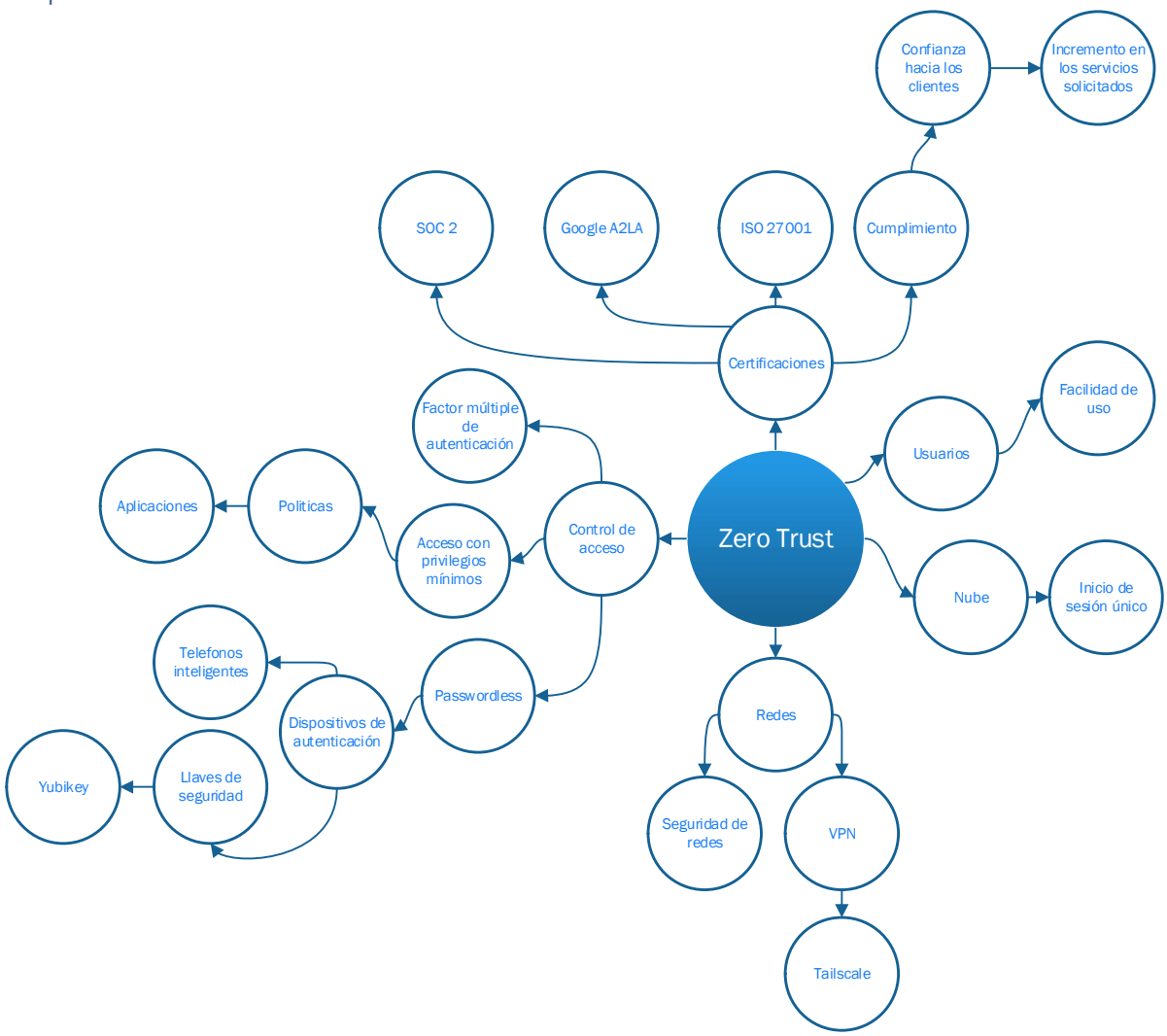

Ilustración 1. Mapa mental Zero trust

Zero Trust es un enfoque de seguridad que desconfía automáticamente de cualquier intento de acceso, ya sea dentro o fuera de la red corporativa, y requiere verificación continua de la identidad y la seguridad antes de permitir el acceso a recursos y datos. Aquí hay una explicación más detallada de los puntos mencionados y sus conexiones:

1. Certificaciones: Estas son acreditaciones de terceros que verifican que una organización cumple con estándares específicos de seguridad y cumplimiento. Las certificaciones como SOC 2, Google A2LA e ISO 27001 indican que una organización

ha implementado prácticas de seguridad sólidas y está comprometida con la protección de datos.

2. Confianza hacia los clientes: Zero Trust implica un cambio en la mentalidad de confiar en los usuarios internos y externos. Al adoptar este enfoque, las organizaciones pueden mejorar la seguridad al reducir la superficie de ataque y limitar el acceso solo a aquellos servicios y recursos necesarios para cada usuario. (The National Institute of Standards and Technology, 2020)
3. Control de acceso: Este aspecto se refiere a las medidas implementadas para verificar la identidad de los usuarios y regular su acceso a sistemas y datos. El uso de factores múltiples de autenticación y la concesión de privilegios mínimos son prácticas comunes en el marco Zero Trust. (Saltzer & Schroeder, 1975)
4. Políticas de aplicaciones: Las políticas de acceso a las aplicaciones definen quién tiene acceso a qué recursos y en qué condiciones. La autenticación sin contraseña (*passwordless*) es una técnica que elimina la necesidad de contraseñas tradicionales y aumenta la seguridad al utilizar métodos de autenticación más fuertes.
5. Dispositivos de autenticación: Estos son los medios utilizados para verificar la identidad del usuario. Los smartphones, llaves de seguridad como YubiKey y redes seguras son ejemplos de dispositivos utilizados en el contexto de Zero Trust para garantizar que solo usuarios autorizados accedan a los recursos. (Yubico, 2022)
6. Usuarios y Facilidad de Uso: Aunque la seguridad es fundamental, también es importante considerar la experiencia del usuario. Zero Trust busca equilibrar la seguridad con la facilidad de uso para garantizar que los usuarios puedan acceder a los recursos de manera eficiente y segura. (Paloalto, 2020)
7. Nube e Inicio de Sesión Único (SSO): La nube ofrece una plataforma flexible para implementar soluciones de seguridad basadas en Zero Trust. El inicio de sesión único permite a los usuarios acceder a múltiples aplicaciones y recursos con una sola autenticación, lo que mejora la experiencia del usuario y simplifica la gestión de acceso para los administradores. (Okta, 2021)

Revisión del estado del arte

Gobernanza en empresas tecnológicas. La gobernanza juega un papel fundamental en las empresas tecnológicas emergentes, especialmente a medida que crecen y manejan datos confidenciales. Establecer marcos de gobierno sólidos es fundamental para garantizar el cumplimiento de las normas, gestionar los riesgos y proteger los activos de la empresa.

En el contexto de las empresas tecnológicas emergentes, la gobernanza se refiere a los procesos, políticas y estructuras que guían la toma de decisiones, la gestión de riesgos y la responsabilidad dentro de la organización. Abarca varios aspectos, incluida la planificación estratégica, la gestión financiera, el cumplimiento de los requisitos legales y reglamentarios y la protección de datos. Las prácticas de gobernanza eficaces ayudan a las empresas emergentes a mantener la transparencia, la integridad y la responsabilidad, que son cruciales para generar confianza entre las partes interesadas y atraer inversiones.

Las empresas tecnológicas emergentes se enfrentan a desafíos específicos de gobernanza debido a su naturaleza acelerada y en rápida evolución. Algunos de los desafíos clave incluyen:

1. Falta de marcos de gobernanza formalizados: las empresas pequeñas o medianas suelen operar en un entorno dinámico, centrándose en la innovación y el crecimiento. Como resultado, es posible que no cuenten con marcos de gobernanza bien definidos. Esto puede dar lugar a una toma de decisiones ad hoc, una gestión de riesgos inadecuada y dificultades para garantizar el cumplimiento.

2. Recursos y experiencia limitados: las empresas pequeñas o medianas suelen tener recursos limitados, tanto en términos financieros como de personal. Es posible que carezcan de equipos dedicados de gobernanza y cumplimiento, lo que dificulta la asignación de recursos y experiencia a las actividades relacionadas con la gobernanza. Esto puede resultar en brechas en la implementación de los controles y procesos necesarios.

3. Complejidades del cumplimiento normativo: las empresas de tecnología están sujetas a una gran cantidad de regulaciones y requisitos de cumplimiento, según su industria y los países en los que operan. Navegar por estos complejos panoramas regulatorios puede ser desalentador, especialmente sin la orientación o la experiencia adecuadas.

4. Inquietudes sobre la privacidad y la seguridad de los datos: las empresas a menudo manejan datos confidenciales, incluida la información del cliente, la propiedad intelectual y las tecnologías patentadas. El mantenimiento de la privacidad de los datos y la implementación de medidas de seguridad sólidas son cruciales para proteger esta información del acceso no autorizado, las infracciones y el daño potencial a la reputación.

Para abordar estos desafíos, las empresas tecnológicas deben establecer prácticas de gobierno que se alineen con las mejores prácticas de la industria y los requisitos reglamentarios. La implementación de marcos como SOC 2 Type II *(American Institute of Certified Public Accountants*) o ISO 27001 (Sistema de Gestión de la Seguridad de la Información) puede proporcionar una base sólida para la gobernanza. Estos marcos enfatizan la evaluación de riesgos, los controles internos y la gestión del cumplimiento.

Además, empresas pueden beneficiarse del aprovechamiento de herramientas y tecnologías innovadoras para mejorar sus prácticas de gobierno. Herramientas como Tailscale, autenticación sin contraseña y SSO brindan oportunidades para fortalecer la seguridad, optimizar la administración de acceso y facilitar el cumplimiento de los requisitos de certificación.

***Zero Trust*.** El concepto *Zero Trust* es un paradigma y no una herramienta como erróneamente lo quieren hacer ver algunos proveedores de servicio. “Zero trust es un paradigma de seguridad cibernética centrado en la protección de los recursos y la premisa de que la confianza nunca se otorga implícitamente, sino que debe evaluarse continuamente.” (Rose, Borchert, Michell, & Connelly, 2020). Implementar Zero Trust implica una serie de herramientas y prácticas. El objetivo principal es proteger los datos y los recursos empresariales limitando los permisos de acceso únicamente a lo necesario para las actividades específicas de cada usuario. En este caso en particular nos centraremos en una VPN, la implementación de autenticación sin contraseñas, la autenticación de inicio único.

Uno no presta juramento y queda protegido por Zero Trust. Es un viaje que requiere objetivos, una hoja de ruta, hitos, métricas y validación. El cambio tecnológico puede no ser menor, y el cambio cultural bien puede ser importante. (Information Security Media Group, 2020)

Existen numerosos componentes lógicos que conforman una implementación de ZTA en una empresa. Estos componentes pueden operarse como un servicio local o mediante un servicio basado en la nube. El modelo de marco conceptual en la Ilustración 3 muestra la relación básica entre los componentes y sus interacciones. Tenga en cuenta que este es un modelo ideal que muestra componentes lógicos y sus interacciones. En la Ilustración 2, el punto de decisión de políticas (PDP) se divide en dos componentes lógicos: el motor de

políticas y el administrador de políticas (definido a continuación). Los componentes lógicos de ZTA utilizan un plano de control separado para comunicarse, mientras que los datos de la aplicación se comunican en un plano de datos. (The National Institute of Standards and Technology, 2020)

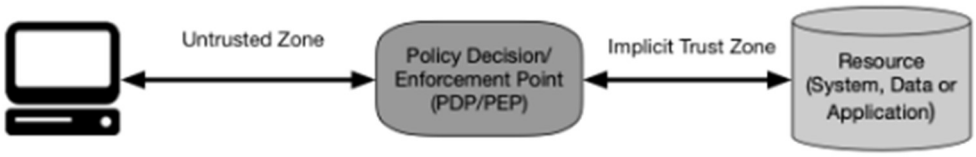

Ilustración 2. Acceso Zero trust (Rose, Borchert, Michell, & Connelly, 2020)

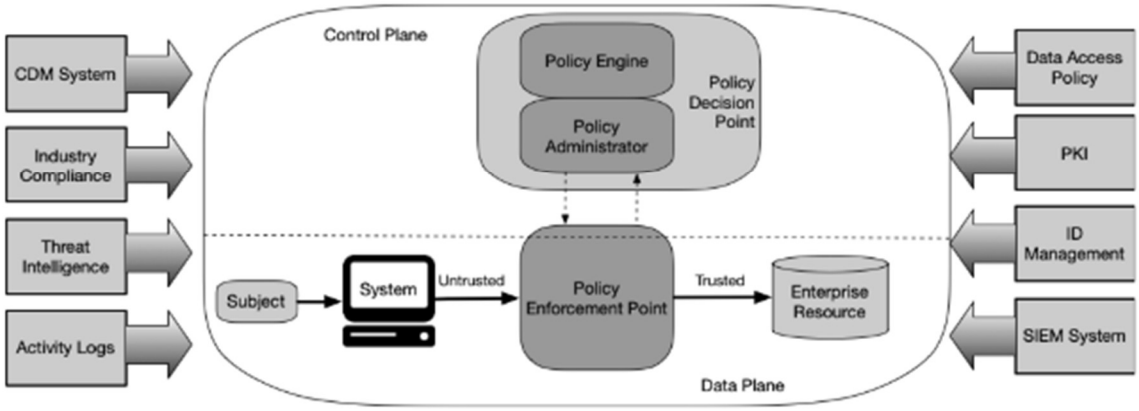

Ilustración 3. Componentes lógicos Core de Zero trust (Rose, Borchert, Michell, & Connelly, 2020)

El objetivo principal es proteger los datos y los recursos empresariales otorgando únicamente los permisos mínimos necesarios para realizar las respectivas actividades de cada usuario en particular.

Zero Trust es un enfoque estratégico de la ciberseguridad que protege a una organización al eliminar la confianza implícita y validar continuamente cada etapa de una interacción digital. Arraigado en el principio de "nunca confíes, siempre verifica", Zero Trust está diseñado para proteger los entornos modernos y permitir la transformación digital mediante el uso de métodos de autenticación sólidos, aprovechando la segmentación de la red, evitando el movimiento lateral, proporcionando prevención de amenazas de capa 7 del modelo OSI y simplificando las políticas de "acceso mínimo". (Paloalto, 2020)

Zero Trust es una estrategia de seguridad. No es un producto o un servicio, sino un enfoque para diseñar e implementar el siguiente conjunto de principios de seguridad:

PRINCIPIO	DESCRIPCION
Verificar explícitamente	Siempre autenticar y autorizar en función de todos los puntos de datos disponibles.
Utilice acceso con privilegios mínimos	Limite el acceso de los usuarios con acceso justo a tiempo y suficiente (JIT/JEA), políticas adaptativas basadas en riesgos y protección de datos.
Suponga una brecha	Minimice el radio de la explosión y el acceso al segmento. Verifique el cifrado de extremo a extremo y utilice análisis para obtener visibilidad, impulsar la detección de amenazas y mejorar las defensas.

(Microsoft, 2022)

Forrester y varios implementadores, como Palo Alto Network, se han estandarizado en un proceso de cinco pasos para implementar la arquitectura de confianza cero:

- Identificar la superficie de protección.
- Mapear flujos de transacciones.
- Cree una arquitectura de confianza cero.
- Crear una política de confianza cero.
- Supervisar y mantener.

Autenticación sin contraseña. Este concepto tiene ya bastante tiempo como tema principal de la seguridad de los datos dentro de las empresas. Ya desde el año 2004, Bill Gates comentaba en la conferencia RSA Security que las contraseñas tradicionales iban a terminar por dejar de usarse ya que no cumplían el desafío de mantener segura la información. Esto ha evolucionado el día de hoy a diversas formas de poder implementarlo. (Kotadia, 2004)

Con MFA, puede eliminar el riesgo de utilizar contraseñas como única forma de autenticación de usuario y reducir el riesgo de robo de credenciales al requerir un segundo método de verificación de identidad que un atacante no pueda robar fácilmente de forma remota. (DUO, 2021)

Este es un esquema que usa factores de posesión los más utilizados son: teléfonos inteligentes, llaves de seguridad; y factores de inherencia como datos biométricos ejemplos de esto son: el escaneo de huellas o rostros.

El objetivo de la autenticación sin contraseña es reducir los riesgos cibernéticos asociados con el uso de contraseñas. En la actualidad la mayoría de las brechas de seguridad involucran algún tipo de robo de contraseña.

Actualmente hay dos grandes vertientes, la implementación a través de aplicaciones en los teléfonos inteligentes utilizando métodos biométricos para la autenticación múltiple; como el uso de dispositivos físicos USB que requieren la interacción de un humano para la autenticación.

Autenticación multifactorial. "La autenticación multifactorial (MFA) es un enfoque en capas para asegurar el acceso físico y lógico donde un sistema requiere un usuario para presentar una combinación de dos o más autenticadores diferentes para verificar la identidad de un usuario para iniciar sesión. MFA aumenta la seguridad porque incluso si un autenticador se ve comprometido, los usuarios no autorizados no podrán cumplir el segundo requisito de autenticación y no podrá acceder al espacio físico objetivo o al sistema informático." (Cybersecurity & Infrastructure Security Agency, 2020)

Software criptográfico multifactorial. Un autenticador criptográfico de software multifactorial es una clave criptográfica almacenada en un disco o en algún otro medio *"soft"* que requiere activación a través de un segundo factor de autenticación. La autenticación se logra demostrando la posesión y control de la clave. La salida del autenticador depende en gran medida del protocolo criptográfico específico, pero generalmente es algún tipo de mensaje firmado. El autenticador criptográfico de software multifactorial es algo que usted tiene y DEBE ser activado por algo que usted sabe o por algo que es. El uso de la biometría (algo que usted es) en la autenticación incluye tanto la medición de características físicas (por ejemplo, huellas dactilares, iris, características faciales) como características de comportamiento (por ejemplo, cadencia de escritura). (NIST Special Publication 800-63B, 2017)

En esta implementación se tendrán un par de escenarios para cumplir con la autenticación multifactorial:

- Uso de aplicación *Microsoft Authenticator*. Con el desafío numérico y la utilización de datos biométricos de cada usuario implementados en el teléfono inteligente.

VPN. Por sus siglas en ingles es una "Red privada virtual" para el encapsulamiento de la trasmisión de datos entre dispositivos a través de redes públicas o compartidas. Es decir, brinda privacidad en línea a un usuario creando una conexión cifrada entre dispositivos. Utiliza protocolos de tunelización para cifrar datos confidenciales de un remitente, transmitirlos y luego descifrarlos en el extremo del receptor. Forma parte de la capa 2 del modelo OSI.

En este caso en particular se estará trabajando con Tailscale que es una VPN basada en WireGuard. “WireGuard crea un conjunto de túneles encriptados extremadamente livianos entre su computadora, VM o contenedor y cualquier otro nodo en su red.” (Pennarun, 2020)

La gran diferencia de este modelo es que se evita la creación o utilización de un concentrador para la trasmisión de todas las comunicaciones dentro de la VPN, de tal manera que cada nodo se conecta directamente a nodo destino sin intermediarios, haciendo más rápido, seguro y eficiente su funcionamiento.

Inicio de sesión único. Nace a principios de la década de 2000s, ante el escenario donde es necesario tener autenticación para diversos sistemas de diferentes proveedores por lo que se convirtió un problema para los usuarios el llevar control de cada una de estas. Por lo que se desarrolló diferentes metodologías para unificar/centralizar el acceso a las herramientas usando un solo sistema de autenticación. (My1Login, 2022)

“Las organizaciones pueden compartir su identidad de manera fácil y segura, se mejora la información y la seguridad al eliminar la posibilidad de cuentas compartidas. La experiencia del usuario es mejorada al eliminar nombres de usuario adicionales y contraseñas, lo que también permite menos llamadas al servicio de asistencia y costos administrativos.” (Lewis & Lewis, 2009)

En esta implementación se utilizarán Entra ID como proveedor de Identidad haciendo uso del protocolo SAML 2.0

Estándares de Certificación. Las certificaciones brindan un marco valioso para que las empresas tecnológicas emergentes demuestren su compromiso con la seguridad, el cumplimiento y la protección de datos. Validan que la empresa ha implementado controles y procesos sólidos en línea con los estándares aceptados por la industria.

1. SOC 2 TYPE II (System and Organization Controls 2): SOC 2 TYPE II es una certificación ampliamente reconocida desarrollada por el Instituto Americano de CPAs (AICPA). Se enfoca en auditar e informar sobre los controles relacionados con la seguridad, la disponibilidad, la integridad del procesamiento, la confidencialidad y la privacidad (los Criterios de Servicios de Confianza). La certificación SOC 2 TYPE II brinda garantías a los clientes, socios y partes interesadas de que una empresa emergente ha implementado controles efectivos para proteger sus datos y mantener operaciones seguras. (American Institute of CPAs (AICPA), s.f.)

2. ISO 27001: ISO 27001 es un estándar internacional para sistemas de gestión de seguridad de la información (SGSI). Proporciona un enfoque sistemático para

administrar información confidencial de la empresa y del cliente, asegurando su confidencialidad, integridad y disponibilidad. La certificación ISO 27001 demuestra que una empresa emergente ha establecido un marco integral de gestión de la seguridad de la información y se adhiere a las mejores prácticas para gestionar los riesgos. (International Organization for Standardization (ISO), 2013)

3. Google A2LA: Google A2LA (Evaluación y acreditación para aplicaciones de laboratorio) es un programa de certificación específico para empresas emergentes que operan en el entorno de Google Cloud. Se enfoca en evaluar los controles de seguridad y privacidad implementados por las empresas emergentes que utilizan los servicios de Google Cloud. La certificación Google A2LA demuestra el compromiso de la empresa emergente de cumplir con los estrictos requisitos de seguridad y privacidad de Google.

Lograr estas certificaciones demuestra un compromiso con la seguridad y el cumplimiento, mejora la reputación de la empresa e infunde confianza entre los clientes, socios e inversores.

SOC 2 TYPE II. Desarrollado por el Instituto Americano de CPA (AICPA), el SOC 2 TYPE II define los criterios para administrar los datos de los clientes en función de cinco principios: seguridad, disponibilidad, integridad de procesamiento, confidencialidad y privacidad. (American Institute of CPAs (AICPA), 2018)

- Seguridad. El principio de seguridad impone la protección de datos y sistemas, contra el acceso no autorizado. Con ese fin, es necesario implementar algún tipo de control de acceso, como, listas de control de acceso o sistemas de gestión de identidad.
    - Firewall tanto aplicativos como de redes
    - Factor doble de autenticación
    - Detección de intrusos
- Disponibilidad. Los sistemas deben cumplir con los SLA (acuerdo de nivel de servicio) de disponibilidad en todo momento. Esto requiere construir sistemas inherentemente tolerantes a fallas, que soporten una carga alta. También requiere que las organizaciones inviertan en sistemas de monitoreo de red y tengan planes de recuperación ante desastres.
    - Monitoreo de rendimiento
    - Recuperación de desastres

    - Manejo de incidentes de seguridad
- Integridad de procesamiento. Todos los sistemas siempre deben funcionar según el diseño, sin demoras, vulnerabilidades, errores o fallas. Las aplicaciones y procedimientos de aseguramiento de la calidad y monitoreo del desempeño son cruciales para lograr la adhesión a este principio.
    - Aseguramiento de calidad
    - Monitoreo de procesamiento
- Confidencialidad. Los datos califican como confidenciales si solo un grupo específico de personas debe acceder a ellos. Esto puede incluir el código fuente de la aplicación, nombres de usuario y contraseñas, información de tarjetas de crédito o planes comerciales, etc.
    - Encriptación
    - Controles de acceso
    - Firewall tanto aplicativos como de redes
- Privacidad. La recopilación, el almacenamiento, el procesamiento y la divulgación de cualquier información de identificación personal (PII) deben cumplir con la política de privacidad y uso de datos de la organización, junto con las condiciones definidas por AICPA, en los Principios de privacidad generalmente aceptados (GAPP).
    - PII es cualquier información que se puede utilizar para identificar de forma única a una persona, por ejemplo: nombre, edad, número de teléfono, información de tarjeta de crédito o número de seguro social, etc. Una organización debe aplicar controles rigurosos para proteger la PII del acceso no autorizado.
    - Control de acceso
    - Encriptación
    - Factor doble de autenticación

Con la obtención de esta certificación conlleva varias ventajas como lo son:

a) Poder trabajar con clientes que requieren cumplimiento de SOC 2 TYPE II como parte del contrato.
b) Incrementar la reputación de la empresa.
c) Asegurar a los clientes que se tienen todos los controles necesarios implementados para poder proteger sus datos procesados.

ISO 27001. Es un estándar reconocido internacionalmente para sistemas de gestión de seguridad de la información (SGSI). Proporciona un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar los controles de seguridad de la información de una organización. La certificación ISO 27001 demuestra que la

organización ha implementado un conjunto integral de controles y prácticas para proteger la información confidencial y administrar los riesgos de seguridad de la información de manera efectiva.

El proceso de certificación ISO 27001 implica varios pasos clave, que incluyen:

Análisis de brechas: la empresa evalúa sus prácticas de seguridad de la información existentes e identifica brechas en comparación con los requisitos de la norma ISO 27001.

1. Evaluación de riesgos: Se realiza una evaluación de riesgos exhaustiva para identificar y evaluar los riesgos de seguridad de la información para los activos de la organización.

2. Implementación de controles: con base en los riesgos identificados, se implementa los controles apropiados para mitigar los riesgos y garantizar el cumplimiento de los requisitos de la norma ISO 27001.

3. Documentación: Se desarrolla y mantiene documentación, incluida una política de seguridad de la información, informes de evaluación de riesgos y documentación de implementación de control.

4. Auditoría Interna: La organización realiza auditorías internas para verificar la efectividad de los controles implementados e identificar áreas de mejora.

5. Auditoría de certificación: un organismo de certificación acreditado realiza una auditoría independiente para evaluar el cumplimiento de la organización con los requisitos de la norma ISO 27001.

La certificación ISO 27001 brinda varios beneficios a las nuevas empresas, incluida la protección de datos mejorada, la gestión de riesgos mejorada y una mayor confianza de los clientes y socios comerciales.

Google A2LA. Es una certificación otorgada por Google que se centra en garantizar la seguridad de Google Play y el ecosistema de aplicaciones más amplio. App Defense Alliance se centra en proteger a los usuarios evitando que las amenazas lleguen a sus dispositivos y mejorando la calidad de las aplicaciones en todo el ecosistema. (App Defence Alliance, s.f.)

OWASP (el Proyecto Abierto de Seguridad de Aplicaciones Web) se ha establecido como un estándar industrial muy respetado para la seguridad de aplicaciones móviles. Su conjunto publicado de requisitos de seguridad, el Estándar de verificación de seguridad de aplicaciones móviles (MASVS), proporciona un conjunto de criterios de seguridad básicos para los desarrolladores. Junto con su conjunto de criterios de prueba publicado, MASTG (Guía de prueba de seguridad de aplicaciones móviles), OWASP ofrece un medio objetivo para que los desarrolladores evalúen sus aplicaciones según un estándar común. Los desarrolladores pueden trabajar directamente con un socio de laboratorio autorizado de Google para iniciar la evaluación de seguridad. A través de MASA, Google reconocerá a los desarrolladores cuyas aplicaciones hayan sido validadas de forma independiente según un conjunto de requisitos de nivel 1 de MASVS.

Beneficios:

Realizar pruebas de seguridad a aplicaciones de Google o terceros que son publicadas en la Google Play Store. Al ser un laboratorio certificado y aprobado por Google esto significa ser una de las 6 únicas entidades autorizadas a nivel global, para otorgar el sello de seguridad MASA, lo cual otorga un reconocimiento de seguridad y genera mayor confianza por parte de los usuarios finales

Privilegio Mínimo. “Cada programa y cada usuario del sistema debe operar utilizando el conjunto mínimo de privilegios necesarios para completar el trabajo. Principalmente, este principio limita el daño que puede resultar de un accidente o error. También reduce al mínimo el número de posibles interacciones entre programas privilegiados para un funcionamiento correcto, de modo que es menos probable que se produzcan usos de privilegios involuntarios, no deseados o inadecuados. Así, si surge una duda relacionada con el mal uso de un privilegio, se minimiza el número de programas que deben ser auditados.” (Saltzer & Schroeder, 1975)

Herramientas para una mejor gobernanza. La gobernanza eficaz en las empresas de tecnología emergentes depende de la implementación de herramientas y tecnologías que agilicen los procesos, mejoren la seguridad y faciliten el cumplimiento. Esta sección explora tres herramientas clave (Tailscale, autenticación sin contraseña e inicio de sesión único (SSO)) que pueden contribuir significativamente a mejorar las prácticas de gobernanza.

1. Tailscale: Es una herramienta de conectividad de red segura diseñada para simplificar la administración de la red y mejorar la seguridad, especialmente para sistemas distribuidos. Crea conexiones cifradas entre dispositivos, lo que ayuda a las empresas emergentes a establecer redes seguras y de confianza cero.
   Beneficios para la gobernanza:
   a. Seguridad mejorada: Tailscale proporciona conexiones seguras y cifradas, lo que reduce el riesgo de acceso no autorizado y violaciones de datos.

b. Control de acceso simplificado: ofrece un control de acceso detallado, lo que permite a las empresas emergentes aplicar políticas y permisos de acceso fácilmente.
c. Cumplimiento mejorado: Tailscale ayuda a cumplir con las normas de seguridad y privacidad al proporcionar una conectividad de red segura.

2. Autenticación sin contraseña: Elimina la necesidad de inicios de sesión tradicionales basados en contraseñas. En cambio, aprovecha otros factores como la biometría, los códigos de acceso de un solo uso o la autenticación basada en dispositivos para la verificación del usuario.

   Beneficios para la gobernanza:

   a. Riesgos reducidos relacionados con las contraseñas: la autenticación sin contraseña mitiga los riesgos asociados con contraseñas débiles, la reutilización de contraseñas y los ataques basados en credenciales.
   b. Experiencia de usuario mejorada: simplifica el proceso de inicio de sesión para los usuarios manteniendo una seguridad sólida.
   c. Control de acceso mejorado: la autenticación sin contraseña permite la autenticación multifactorial, lo que mejora aún más la seguridad.

3. Inicio de sesión único (SSO): Es un proceso de autenticación que permite a los usuarios acceder a múltiples aplicaciones o servicios con un único conjunto de credenciales de inicio de sesión. Agiliza la gestión de acceso y mejora la seguridad.

   Beneficios para la gobernanza:

   a. Control centralizado: SSO centraliza el control de acceso de los usuarios, lo que permite a los administradores gestionar los permisos de los usuarios y las políticas de acceso desde un único panel.
   b. Seguridad mejorada: SSO puede imponer métodos de autenticación sólidos y reducir el riesgo de acceso no autorizado.
   c. Pistas de auditoría: las soluciones SSO a menudo proporcionan pistas de auditoría, que son valiosas para fines de cumplimiento y gobernanza.

CAPITULO 3

Metodología

Para lograr los objetivos y responder a las preguntas, se empleará una metodología de investigación sistemática. Para este trabajo se propone la siguiente metodología:

1. Revisión de literatura: Se llevará a cabo un exhaustivo análisis de la literatura existente para obtener una comprensión profunda de los desafíos de gobernanza y los requisitos de certificación. Se examinarán documentos académicos pertinentes, informes de la industria, estudios de casos y directrices de mejores prácticas con el objetivo de establecer un sólido marco teórico para la investigación.

2. Recopilación de datos: Se recopilarán datos primarios y secundarios para respaldar la implementación. Los datos primarios se obtendrán a través de entrevistas y encuestas con profesionales que trabajan dentro de la empresa, expertos de la industria y auditores de certificación internos. Los datos secundarios incluirán documentación de la empresa, pautas de certificación e información disponible públicamente sobre la implementación de herramientas y la obtención de certificaciones.

3. Análisis comparativo: se realizará un análisis comparativo para evaluar los beneficios, las limitaciones y la eficacia de Tailscale, la autenticación sin contraseña y el SSO en el contexto de la gobernanza y las certificaciones. Este análisis implicará examinar cómo cada herramienta se alinea con los requisitos específicos de las certificaciones SOC 2 TYPE II, ISO 27001 y Google A2LA.

4. Desarrollo de estrategias de implementación: con base en los hallazgos de la revisión de la literatura y el análisis comparativo, se desarrollarán estrategias prácticas de implementación y mejores prácticas. Estas estrategias brindarán orientación sobre cómo aprovechar de manera efectiva Tailscale, la autenticación sin contraseña y SSO para mejorar las prácticas de gobernanza y lograr las certificaciones deseadas.

Es importante tener en cuenta que la metodología pudo ajustarse o refinarse a medida que avanza la implementación, según la disponibilidad de datos, los conocimientos emergentes y las consideraciones prácticas.

Este proyecto conlleva varios pasos a cumplirse para obtener una correcta implementación y obtener los resultados deseados, a continuación, se enumeras las principales tareas y manera propuesta de realizarlas.

- Conformación de equipo para definir las políticas de seguridad necesarias para la implementación de las herramientas propuestas, este grupo deberá estar conformado por al menos una persona de cada uno de los siguientes departamentos: Seguridad Informática, Ingeniería, Redes, Infraestructura, Soporte.

Este grupo deberá crear las siguientes políticas:

  - Generación de lista de usuarios con privilegios administrativos.
  - Definición de reglas de acceso a los diferentes sistemas internos.
  - Definición de los tiempos para autenticación de los usuarios, así como la rotación de llaves del cifrado de punto a punto para la VPN.

- Evaluación de al menos dos soluciones de VPN en el mercado que cumplan con el paradigma “Zero-Trust”. El equipo encargado de esta evaluación lo integrarán al menos un miembro de estos departamentos: Redes, Infraestructura, Seguridad Informática.

- Definición de tiempos y fechas para ejecutar la implementación en cada una de sus fases, así como la asignación de responsables de cada actividad, especificando los costos de cada una de las actividades teniendo en cuenta tanto los costos de inversión en equipamiento/software, así como el costo de las horas necesarias para completar el proyecto. Aquí es necesario contar con un Project Manager además de los gerentes de los siguientes departamentos: Seguridad informática, Soporte, Infraestructura.

- Obtención de la aprobación del proyecto, esto se llevará a cabo presentando todo el análisis de viabilidad y costos necesarios para ejecutar el proyecto, ante los *“stakeholders”,* los cuales son el director de Finanzas, director de Operaciones, director de Tecnología.

- Creación de la documentación necesaria de la arquitectura de las soluciones implementadas, así como manuales de usuario correspondientes y comunicados institucionales necesarios. Esta actividad será llevada a cabo por un equipo confirmado por al menos un integrante de los siguientes departamentos: Soporte, Infraestructura.

- Al terminar el proyecto, se tendrán sesiones de lecciones aprendidas que contarán con la presencia de los involucrados en cada fase. Así como la entrega de los reportes de cada uno de los grupos y un informe final presentado a los *"stakeholders"* por el *Project Manager*.

Análisis comparativo

En esta sección nos embarcamos en un análisis comparativo, profundizando en la eficacia de nuestras medidas de seguridad implementadas. Nuestro enfoque gira en torno a: Tailscale, autenticación sin contraseña e inicio de sesión único (SSO) integrados perfectamente con Entra ID que actúa como proveedor de identidad (IdP). A través de este análisis, nuestro objetivo principal es evaluar el impacto de estos métodos en aspectos críticos: solidez de la seguridad, mejoras en la experiencia del usuario y la eficiencia organizacional general.

En el panorama de la seguridad digital en rápida evolución, elegir las herramientas adecuadas es primordial. Cada herramienta aporta fortalezas y desafíos únicos. Tailscale promete capacidades de automatización y cifrado de extremo a extremo. La autenticación sin contraseña simplifica el acceso de los usuarios al tiempo que desafía las vulnerabilidades de las contraseñas tradicionales. SSO con Entra ID centraliza el control y promete un acceso optimizado a múltiples aplicaciones. Comprender estos matices no es simplemente un ejercicio teórico; es una necesidad estratégica. Guía nuestras decisiones, garantizando que nuestra infraestructura digital siga siendo sólida, fácil de usar y operativamente eficiente.

Al analizar las fortalezas y debilidades de Tailscale, la autenticación sin contraseña y el SSO con Entra ID, elaboramos un camino hacia decisiones informadas. Este análisis no se trata sólo de comprender el presente; es una guía para nuestras futuras implementaciones y optimizaciones. En esta exploración, buscamos comprender las complejidades de cada sistema y descubrir estrategias para aprovechar sus fortalezas y mitigar sus debilidades de manera efectiva.

A través de este análisis integral, creamos el camino hacia un futuro digitalmente seguro dentro de los límites actuales, fácil de usar y operativamente eficiente. Esto nos brindara el conocimiento para tomar decisiones que refuercen la postura de seguridad de nuestra

organización y la satisfacción del usuario, impulsándonos hacia un futuro donde la eficiencia y la innovación prosperan de la mano.

Comparación de seguridad

TAILSCALE

Fortalezas:

- Cifrado de extremo a extremo: el cifrado de extremo a extremo de Tailscale garantiza que los datos permanezcan confidenciales durante el tránsito, proporcionando una sólida capa de seguridad contra interceptaciones y escuchas ilegales.
- Modelo de confianza cero: al operar con un modelo de confianza cero, Tailscale aplica estrictos controles de acceso en todos los niveles, eliminando la suposición de confianza dentro de la red y mejorando la seguridad.
- Controles de acceso estrictos: Los estrictos controles de acceso de Tailscale garantizan que solo los usuarios y dispositivos autorizados puedan acceder a recursos específicos, fortaleciendo la red contra intrusiones no autorizadas.

Debilidades:

- Vulnerabilidades de configuración: la seguridad de Tailscale depende en gran medida de la configuración adecuada. Una configuración inadecuada o una mala gestión podrían introducir vulnerabilidades, lo que enfatiza la necesidad de prácticas de configuración meticulosas.
- Desafíos de escalabilidad: si bien es sólido, Tailscale podría enfrentar desafíos para manejar una gran cantidad de usuarios y dispositivos de manera eficiente, lo que podría afectar el rendimiento y la capacidad de respuesta a escala.

En la ilustración 4, podemos ver el ejemplo de como se ve una red de malla utilizada por tailscale, en donde la comunicación se realiza de punto a punto sin la necesidad de un punto concentrador por lo cual la seguridad se eleva de manera significativa.

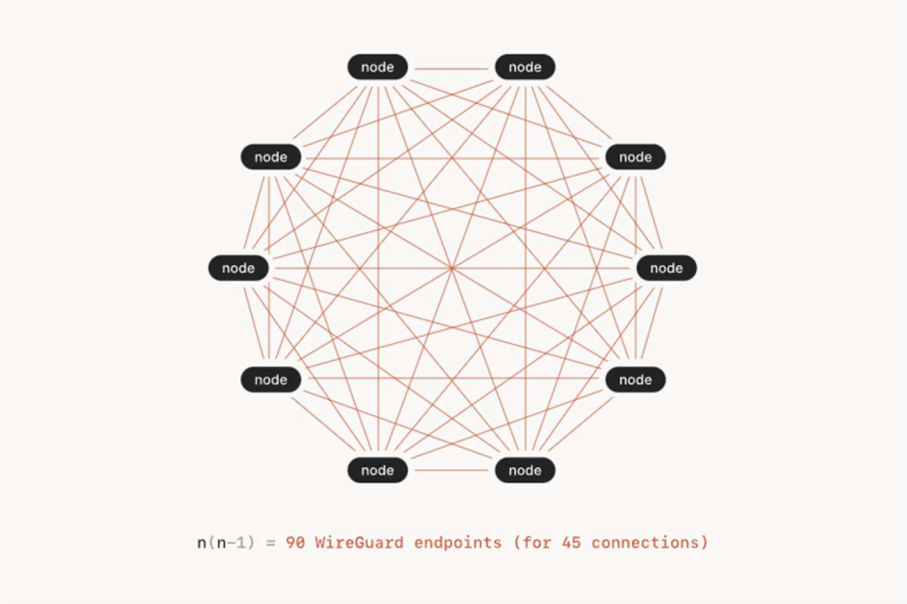

Ilustración 4. Ejemplificación de la red de malla de Tailscale. (Pennarun, 2020)

AUTENTICACION SIN CONTRASEÑA

Fortalezas:

- Eliminación de riesgos de contraseñas: la autenticación sin contraseña erradica las vulnerabilidades asociadas con las contraseñas tradicionales, lo que reduce significativamente el riesgo de ataques basados en credenciales.
- Autenticación de usuario sólida: Los métodos sin contraseña, como la biometría, brindan una autenticación de usuario sólida, lo que mejora la seguridad al garantizar que solo las personas autorizadas obtengan acceso.
- Seguridad mejorada: los métodos de autenticación sin contraseña refuerzan la seguridad general, proporcionando un enfoque de múltiples capas que fortalece los protocolos de autenticación.

Debilidades:

- Impacto en la calidad del dispositivo: La efectividad de la biometría y otros métodos puede variar según la calidad de los dispositivos utilizados, lo que podría introducir variabilidad en la precisión y confiabilidad de la autenticación.
- Desafíos de aceptación del usuario: La implementación inicial de la autenticación sin contraseña puede enfrentar resistencia debido a los desafíos de aceptación y comprensión del usuario. La formación y la comunicación adecuadas son vitales para superar estos obstáculos de forma eficaz.

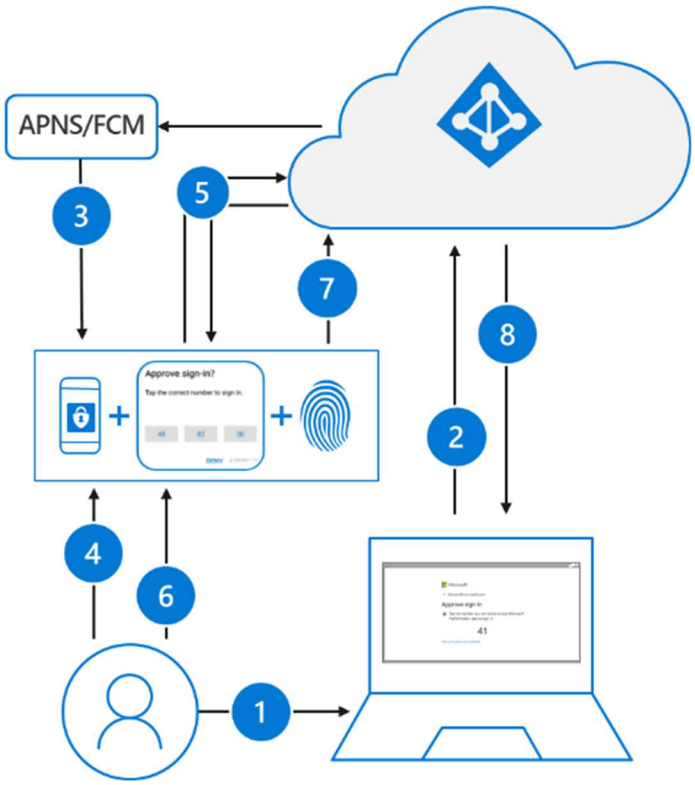

Ilustración 5. Flujo de autenticación sin contraseña usando dispositivo móvil. (Microsoft, 2023)

A continuación, la descripción del flujo plasmado en la figura anterior:

1. Un usuario inicia sesión en Windows mediante un gesto biométrico o PIN. El gesto desbloquea la clave privada de *Windows Hello* para empresas y se envía al proveedor de soporte de seguridad de autenticación en la nube, denominado proveedor de AP en la nube.
2. El proveedor de Cloud AP solicita un *nonce* (un número arbitrario aleatorio que se puede usar una vez) de Microsoft Entra ID.
3. Microsoft Entra ID devuelve un *nonce* válido durante 5 minutos.
4. El proveedor de Cloud AP firma el *nonce* utilizando la clave privada del usuario y devuelve el *nonce* firmado al ID de Microsoft Entra.
5. Microsoft Entra ID valida el *nonce* firmado utilizando la clave pública registrada de forma segura del usuario con la firma del *nonce*. Microsoft Entra ID valida la firma y luego valida el *nonce* firmado devuelto. Cuando se valida el *nonce*, Microsoft Entra ID crea un token de actualización principal (PRT) con una clave de sesión que se cifra con la clave de transporte del dispositivo y lo devuelve al proveedor de AP en la nube.
6. El proveedor de Cloud AP recibe el PRT cifrado con la clave de sesión. El proveedor de Cloud AP utiliza la clave de transporte privada del dispositivo para descifrar la clave de sesión y protege la clave de sesión mediante el Módulo de plataforma segura (TPM) del dispositivo.
7. El proveedor de Cloud AP devuelve una respuesta de autenticación exitosa a Windows. Luego, el usuario puede acceder a Windows y a las aplicaciones locales y en la nube sin necesidad de autenticarse nuevamente (SSO).

SSO CON ENTRA ID

Fortalezas:

- Control de acceso centralizado: el inicio de sesión único (SSO) centraliza el control de acceso, garantizando procesos de autenticación de usuario consistentes y optimizados en varias aplicaciones, mejorando tanto la seguridad como la experiencia del usuario.
- Integración con Entra ID: las sólidas funciones de seguridad y las políticas de acceso condicional de Entra ID brindan una capa adicional de seguridad, aumentando la resiliencia general del sistema contra posibles amenazas.
- Simplificación de la experiencia del usuario: SSO simplifica la experiencia del usuario al eliminar la necesidad de múltiples credenciales, lo que reduce la complejidad y los posibles puntos de falla en el proceso de autenticación.

Debilidades:

- Punto único de falla: si no se configura correctamente, SSO puede convertirse en un punto único de falla. Los mecanismos adecuados de redundancia y conmutación por error son esenciales para mitigar este riesgo de forma eficaz.
- Dependencia del tiempo de actividad de Entra ID: La dependencia del tiempo de actividad de Entra ID plantea riesgos potenciales. Se necesitan medidas adecuadas, como métodos de autenticación de respaldo y planes de contingencia, para garantizar el acceso ininterrumpido en caso de interrupciones del servicio Entra ID.

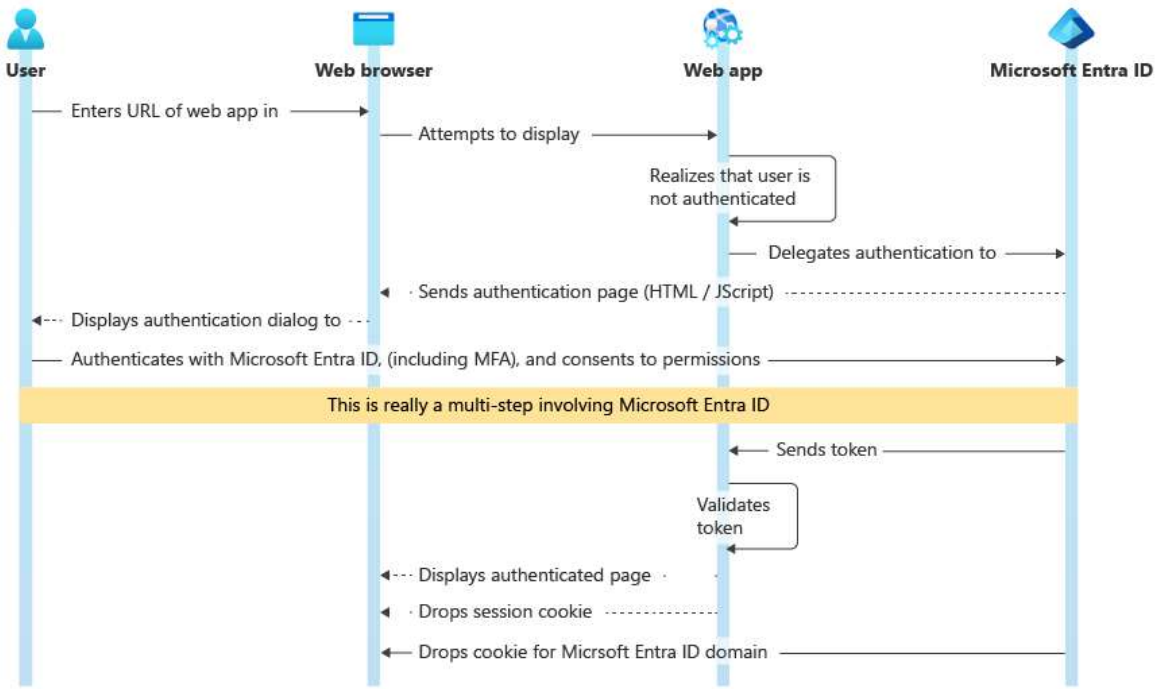

Ilustración 6. Flujo de autenticación con SSO. (Microsoft, 2023)

A continuación, la descripción del flujo de una autenticación satisfactoria plasmada en el diagrama superior:

1. La plataforma de identidad de Microsoft envía un token a la aplicación web.
2. Se guarda una cookie, asociada a un dominio de Microsoft Entra, que contiene la identidad del usuario en el contenedor de cookies del navegador. La próxima vez que una aplicación utilice el navegador para navegar hasta el punto final de autorización de la plataforma de identidad de Microsoft, el navegador presenta la cookie para que el usuario no tenga que iniciar sesión nuevamente. Esta es también la forma en que se logra el SSO. La cookie es generada por Microsoft Entra ID y solo puede ser entendida por Microsoft Entra ID.
3. Luego, la aplicación web valida el token. Si la validación tiene éxito, la aplicación web muestra la página protegida y guarda una cookie de sesión en el contenedor de cookies del navegador. Cuando el usuario navega a otra página, la aplicación web sabe que el usuario está autenticado en función de la cookie de sesión.

Comparación de la experiencia del usuario

TAILSCALE

Fortalezas:

- Acceso seguro y fluido: el sello distintivo de Tailscale es su capacidad de ofrecer no solo un acceso a la red seguro sino también fluido. Los usuarios pueden conectarse sin esfuerzo, lo que garantiza una experiencia consistente y sin complicaciones independientemente de su ubicación o condiciones de red.
- Flexibilidad y accesibilidad: el diseño de Tailscale se adapta a varios dispositivos y plataformas, ofreciendo a los usuarios la libertad de conectarse desde sus dispositivos preferidos, mejorando su flexibilidad y productividad.

Debilidades:

- Mitigación de la complejidad: la configuración inicial puede plantear desafíos para los usuarios no técnicos. La implementación de asistentes de configuración fáciles de usar y guías intuitivas puede mitigar significativamente esta complejidad, haciendo que el proceso de incorporación sea más fluido y accesible.
- Mejora de la asistencia al usuario: si bien Tailscale es generalmente fácil de usar, abordar problemas de conectividad podría requerir conocimientos técnicos avanzados. Ofrecer recursos sólidos de soporte al usuario y servicios de asistencia receptivos puede cerrar esta brecha de conocimiento, garantizando que los usuarios se sientan respaldados en caso de que necesiten solucionar problemas.

AUTENTICACION SIN CONTRASEÑA

Fortalezas:

- Experiencia de inicio de sesión intuitiva: la autenticación sin contraseña ofrece una experiencia de inicio de sesión intrínsecamente intuitiva, erradicando la frustración asociada con la administración de contraseñas tradicional. Los usuarios son recibidos con un proceso de autenticación fluido, lo que mejora significativamente su satisfacción y productividad.
- Eficiencia y velocidad: los métodos sin contraseña a menudo dan como resultado tiempos de inicio de sesión más rápidos, lo que contribuye a una mayor eficiencia durante el acceso de los usuarios. Esta velocidad no solo reduce los tiempos de espera, sino que también impacta positivamente en la continuidad del flujo de trabajo.

Debilidades: Es posible que se requiera compatibilidad del dispositivo y capacitación del usuario para que los usuarios se adapten a los nuevos métodos de autenticación.

SSO CON ENTRA ID

Fortalezas:

- Soporte de adaptación del dispositivo: algunos usuarios pueden necesitar capacitación para adaptarse a nuevos métodos o dispositivos de autenticación. Proporcionar una formación integral a los usuarios, junto con canales de soporte de fácil acceso, puede cerrar esta brecha de adaptación y garantizar una transición sin problemas para todos los usuarios.
- Garantía de compatibilidad del dispositivo: Garantizar la compatibilidad del dispositivo es crucial. Actualizar periódicamente las listas de compatibilidad y realizar encuestas a los usuarios puede ayudar a identificar problemas potenciales desde el principio, lo que permite soluciones proactivas y una experiencia de usuario ininterrumpida.

Comparación de eficiencia organizacional

TAILSCALE

Fortalezas:

- Reducción de la carga de trabajo: el modelo de confianza cero y las capacidades de automatización de Tailscale reducen significativamente la carga de trabajo del equipo de TI. Al automatizar el control de acceso, se minimizan las intervenciones manuales, lo que permite a los profesionales de TI centrarse en tareas más estratégicas y de valor añadido, mejorando la eficiencia general del equipo.
- Operaciones optimizadas: Las operaciones optimizadas de Tailscale se traducen en una reducción de tareas repetitivas. Con la gestión de acceso automatizada, el equipo de TI puede dedicar su tiempo y experiencia a la innovación y a medidas de seguridad proactivas, contribuyendo a la agilidad organizacional.

Debilidades:

- Equilibrio entre seguridad y automatización: si bien la automatización es una fortaleza, requiere una planificación meticulosa para lograr un equilibrio entre eficiencia y seguridad. Una configuración cuidadosa es fundamental para evitar posibles lagunas de seguridad, lo que requiere monitoreo y ajustes continuos para una eficiencia óptima sin comprometer la integridad de la seguridad.

AUTENTICACION SIN CONTRASEÑA

Fortalezas:

- Reducción de las solicitudes de soporte: la autenticación sin contraseña reduce drásticamente las solicitudes de soporte relacionadas con contraseñas. Esta reducción de tareas mundanas y que consumen mucho tiempo libera recursos de TI, permitiéndoles invertir su energía en iniciativas estratégicas que impulsan el crecimiento y la innovación organizacionales.
- Centrarse en tareas estratégicas: la disminución de las tareas de soporte relacionadas con contraseñas permite a los profesionales de TI dedicar su experiencia a proyectos

estratégicos, mejorando la eficiencia organizacional general y elevando la contribución del departamento de TI a los objetivos de la empresa.

Debilidades:

- Desafíos de la transición: La implementación inicial y la capacitación de los usuarios exigen un esfuerzo sustancial. Para abordar estos desafíos de manera efectiva se requiere un programa de capacitación integral que garantice que los usuarios sean expertos en los nuevos métodos de autenticación. Además, un enfoque proactivo para identificar y resolver fallas técnicas durante la fase de transición es vital para una implementación sin problemas.

SSO CON ENTRA ID

Fortalezas:

- Control centralizado: SSO con Entra ID centraliza el control de acceso de los usuarios, simplificando los procesos de incorporación y autenticación de usuarios. Esta centralización reduce la complejidad administrativa, acelera la incorporación de usuarios y mejora la eficiencia organizacional general.
- Seguimientos de auditoría detallados: Entra ID proporciona seguimientos de auditoría detallados, que ofrecen información detallada sobre las actividades de los usuarios y los patrones de acceso. Esta visibilidad proporciona a los administradores datos valiosos para la toma de decisiones estratégicas, garantizando que los controles de acceso se alineen con las políticas organizacionales y las necesidades de seguridad.

Debilidades:

- Complejidad de las políticas: la configuración de políticas de acceso condicional complejas puede requerir conocimientos especializados. Se debe asignar capacitación y recursos adecuados a los profesionales de TI para garantizar el dominio de estas complejidades, garantizando una gestión eficiente de las políticas sin interrupciones.
- Conciencia de dependencia: la dependencia excesiva del SSO puede plantear desafíos si Entra ID experimenta un tiempo de inactividad. Un enfoque proactivo implica un plan de contingencia, que garantice que existan métodos de autenticación alternativos para garantizar operaciones organizativas ininterrumpidas durante tales casos.

Cada sistema implementado tiene fortalezas distintivas, diseñadas para enfrentar desafíos específicos de seguridad y usabilidad. Tailscale se destaca por su destreza en la entrega de conectividad de red reforzada, enfatizando la seguridad hermética en cada punto de conexión. Paralelamente, la autenticación sin contraseña aparece como precursor del acceso fácil de usar, liberando a los usuarios de las complejidades de las contraseñas tradicionales. A una escala más amplia, SSO con Entra ID emerge como el acceso optimizado a las aplicaciones y un control administrativo elevado, simplificando la complejidades que implica la autorización del usuario.

Al contemplar el futuro de la gestión de acceso seguro, resulta evidente que la sinergia de estos sistemas presenta una buena oportunidad. Al combinar las fortalezas de la conectividad de red segura de Tailscale, la simplicidad intuitiva de la autenticación sin contraseña y el control centralizado que ofrece SSO con Entra ID, la organización puede crear un ecosistema resistente a las amenazas de seguridad y al mismo tiempo defender la experiencia del usuario. Esta integración holística genera un entorno caracterizado no solo por una sólida fortificación sino también por la facilidad con la que los usuarios navegan en el ámbito digital.

El eje de la eficacia perpetua reside en la adaptabilidad. A medida que el panorama digital evoluciona continuamente, también debe hacerlo nuestro enfoque de la seguridad. Por tanto, el viaje no concluye con la implementación; se extiende al ámbito de la observación atenta y la adaptación dinámica. La supervisión continua y el ajuste meticuloso en respuesta a los cambios de las necesidades de seguridad son los pilares sobre los que descansa una postura de seguridad óptima. Al adoptar este espíritu, la organización no sólo salvaguarda su presente, sino que también fortalecen su futuro frente a los desafíos que nos esperan.

Cumplimiento de puntos de control de las certificaciones

SOC 2 Type II

Tailscale

En el contexto de la certificación SOC 2 TYPE II, Tailscale puede contribuir a varios criterios de servicios de confianza:

Seguridad: el cifrado, el modelo de confianza cero y las políticas de control de acceso de Tailscale se alinean con los requisitos de seguridad de SOC 2 TYPE II, lo que ayuda a las empresas emergentes a proteger datos y sistemas confidenciales.

Disponibilidad: las conexiones de red seguras y confiables proporcionadas por Tailscale respaldan la disponibilidad de sistemas y datos, un criterio clave para la certificación SOC 2 TYPE II.

Confidencialidad y privacidad: los controles de acceso y cifrado de Tailscale ayudan a mantener la confidencialidad y privacidad de los datos, que son componentes integrales del cumplimiento de SOC 2 TYPE II.

Autenticación sin contraseña

En el contexto de la certificación SOC 2 TYPE II, la autenticación sin contraseña se alinea con varios criterios de servicios de confianza:

Seguridad: los métodos de autenticación sin contraseña mejoran la seguridad al eliminar los riesgos relacionados con las contraseñas y aplicar una autenticación más sólida, lo que contribuye directamente a los requisitos de seguridad de SOC 2 TYPE II.

Control de acceso: una autenticación más sólida garantiza que solo los usuarios autorizados puedan acceder a sistemas y datos confidenciales, lo que respalda los principios de control de acceso de SOC 2 TYPE II.

Monitoreo de la actividad del usuario: muchos sistemas de autenticación sin contraseña ofrecen seguimiento sólido de la actividad del usuario y pistas de auditoría, que son esenciales para demostrar el cumplimiento de los requisitos de seguimiento e informes de SOC 2 TYPE II.

SSO

En el contexto de la certificación SOC 2 TYPE II, SSO se alinea con varios criterios de servicios de confianza:

Seguridad: SSO contribuye a la seguridad al aplicar fuertes controles de autenticación y acceso, mitigando el riesgo de acceso no autorizado y violaciones de datos.

Control de acceso: SOC 2 TYPE II enfatiza los controles de acceso como un componente fundamental de la seguridad. SSO facilita políticas de control de acceso granulares y garantiza que solo las personas autorizadas puedan acceder a sistemas y datos confidenciales.

Monitoreo e informes: soluciones SSO son integrales de monitoreo e informes, generando pistas de auditoría y registros de eventos cruciales para cumplir con los requisitos de monitoreo e informes de SOC 2 TYPE II.

Puntos de control

El siguiente es un listado de puntos de control dentro de la auditoria los cuales fueron cubiertos por las herramientas implementadas:

AA1 - ID únicos y contraseñas seguras - Infraestructura: **Autenticación sin contraseña, SSO**
AA2 - ID únicas y contraseñas seguras – Aplicaciones: **Autenticación sin contraseña, SSO**
AA3: Autenticación multifactorial (MFA): **Autenticación sin contraseña**
AC1 - Aprovisionamiento y aprobación de acceso: **Autenticación sin contraseña, SSO, Tailscale**
AC2 - Revocación de Acceso: **SSO**
AC3 - Acceso administrativo/privilegiado: **Autenticación sin contraseña, SSO, Tailscale**
AC4 - Revisiones de acceso de usuarios: **Tailscale**
DP16 - Uso de Información Personal: **Tailscale**
PI1 - Acceso a datos de salida: **Tailscale**
SO6 - Cifrado de datos en tránsito: **Tailscale**
SO15 - Cortafuegos del Sistema: **Tailscale**

ISO 27001

Tailscale

Tailscale también puede apoyar a las empresas emergentes que buscan la certificación ISO 27001:

> **Gestión de riesgos:** las funciones de seguridad de Tailscale contribuyen a una gestión de riesgos eficaz al reducir la probabilidad de incidentes de seguridad, lo que ayuda a las empresas emergentes a cumplir con los requisitos de control y evaluación de riesgos de ISO 27001.
>
> **Control de acceso:** ISO 27001 enfatiza el control de acceso como un aspecto fundamental de la seguridad de la información. Las políticas de control de acceso de Tailscale se alinean con los principios de gestión de acceso de ISO 27001.
>
> **Monitoreo continuo:** las capacidades de registro y monitoreo de Tailscale facilitan el monitoreo continuo, un requisito para la certificación ISO 27001.

Autenticación sin contraseña

La autenticación sin contraseña también puede ser beneficiosa para las empresas emergentes que buscan la certificación ISO 27001:

> **Control de acceso:** ISO 27001 enfatiza el control de acceso como un aspecto fundamental de la seguridad de la información. La autenticación sin contraseña se alinea con los principios de gestión de acceso de ISO 27001.
>
> **Reducción de riesgos:** al eliminar los riesgos relacionados con las contraseñas, la autenticación sin contraseña reduce la probabilidad de incidentes de seguridad, lo que respalda los requisitos de control y evaluación de riesgos de ISO 27001.
>
> **Concienciación y capacitación del usuario**: ISO 27001 otorga importancia a la concientización y capacitación del usuario. La autenticación sin contraseña simplifica la autenticación del usuario, lo que reduce la necesidad de una capacitación exhaustiva sobre políticas y prácticas de contraseñas.

SSO

Para las empresas emergentes que buscan la certificación ISO 27001, el SSO puede ser fundamental de las siguientes maneras:

Gestión de acceso: ISO 27001 otorga gran importancia a la gestión y el control de acceso. SSO simplifica los procesos de gestión de acceso y aplica estrictos controles de acceso.

Reducción de riesgos: al implementar SSO y aplicar una autenticación sólida, las empresas emergentes pueden reducir el riesgo de acceso no autorizado y violaciones de datos, respaldando los requisitos de gestión de riesgos de ISO 27001.

Capacitación de usuarios: SSO simplifica la autenticación de usuarios, lo que reduce la necesidad de una capacitación exhaustiva de los usuarios sobre administración de contraseñas y prácticas de seguridad.

Puntos de control

El siguiente es un listado de puntos de control dentro de la auditoria los cuales fueron cubiertos por las herramientas implementadas:

A.6.1.2 - Segregación de funciones: **Tailscale**
A.9.1.2 - Acceso a Redes y Servicios de Red: **Tailscale**
A.9.2.1 - Alta y Baja de Usuario: **Autenticación sin contraseña, SSO, Tailscale**
A.9.2.2 - Provisión de acceso de usuarios: **Autenticación sin contraseña, SSO, Tailscale**
A.9.2.3 - Gestión de derechos de acceso privilegiado: **Tailscale**
A.9.2.4 - Gestión de la información secreta de autenticación de los usuarios: **Tailscale**
A.9.2.5 - Revisión de los derechos de acceso de los usuarios: **Autenticación sin contraseña, Tailscale**
A.9.2.6 - Eliminación o ajuste de derechos de acceso **Autenticación sin contraseña, Tailscale**
A.9.4.3 - Sistema de Gestión de Contraseñas: **Autenticación sin contraseña**
A.12.4.3 - Registros de administrador y operador: **Autenticación sin contraseña, SSO, Tailscale**
A.13.1.1 - Controles de red: **Tailscale**
A.13.1.3 - Segregación en Redes: **Tailscale**

Google A2LA

Tailscale

Para las empresas que buscan la certificación Google A2LA, Tailscale puede mejorar la seguridad y el cumplimiento de varias maneras:

Seguridad de red: Tailscale agrega una capa adicional de seguridad de red, complementando las funciones de seguridad de Google Cloud.

Gestión de identidad y acceso (IAM): Tailscale puede integrarse con el sistema IAM de Google Cloud, proporcionando controles de acceso unificados y mejorando la seguridad dentro del entorno de la nube.

Protección de datos: el cifrado de Tailscale y el modelo de confianza cero contribuyen a la protección de datos y se alinean con los estrictos requisitos de seguridad de Google para la certificación Google A2LA.

Autenticación sin contraseña

Para las empresas emergentes que operan en el entorno de Google Cloud y buscan la certificación Google A2LA, la autenticación sin contraseña puede mejorar la seguridad y el cumplimiento de varias maneras:

Seguridad mejorada de acceso a la nube: la autenticación sin contraseña proporciona una capa adicional de seguridad para acceder a los recursos de Google Cloud, complementando las funciones de seguridad existentes de Google.

Integración con Entra ID: la autenticación sin contraseña se puede integrar perfectamente con el sistema de gestión de identidad y acceso Entra ID, ofreciendo controles de acceso unificados y mejorando la seguridad dentro del entorno de la nube.

Protección de datos: al fortalecer los controles de acceso, la autenticación sin contraseña contribuye a la protección de datos y se alinea con los requisitos de seguridad de Google para la certificación Google A2LA.

SSO

En el contexto de la certificación Google A2LA, SSO puede mejorar la seguridad y el cumplimiento dentro del entorno de Google Cloud:

Controles de acceso unificados: SSO puede integrarse perfectamente con el sistema de gestión de acceso e identidad (IAM) de Google Cloud, proporcionando controles de acceso unificados y fortaleciendo la seguridad de los recursos de Google Cloud.

Autenticación multifactorial (MFA): muchas soluciones SSO admiten MFA, lo que agrega una capa adicional de seguridad en línea con los estrictos requisitos de seguridad de Google para la certificación Google A2LA.

Registro y monitoreo: los sistemas SSO suelen ofrecer amplias capacidades de registro y monitoreo, valiosas para mantener la visibilidad y demostrar el cumplimiento en Google Cloud.

Puntos de control

El siguiente es un listado de puntos de control dentro de la auditoria los cuales fueron cubiertos por las herramientas implementadas:

- El personal, incluidos los miembros del comité, contratistas, personal de organismos externos o personas que actúen en nombre del laboratorio, deberá mantener confidencial toda la información obtenida o creada durante la realización de las actividades del laboratorio, excepto según lo exija la ley: **Tailscale**
- El laboratorio deberá tener disponible el personal, instalaciones, equipos, sistemas y servicios de apoyo necesarios para gestionar y realizar sus actividades de laboratorio: **Tailscale**
- Todo el personal involucrado en las actividades del laboratorio deberá tener acceso a las partes de la documentación del sistema de gestión y a la información relacionada que sean aplicables a sus responsabilidades: **Tailscale, SSO**
- El laboratorio deberá implementar los controles necesarios para la identificación, almacenamiento, protección, respaldo, archivo, recuperación, tiempo de retención y disposición de sus registros: **Tailscale**
- El acceso a estos registros será consistente con los compromisos de confidencialidad y los registros deberán estar fácilmente disponibles: **Tailscale, SSO**

CAPITULO 4

Desarrollo del proyecto

Tailscale: mejora de la seguridad y el cumplimiento

Tailscale es una herramienta de conectividad de red moderna que ha ganado popularidad por su capacidad para proporcionar conexiones de red seguras y eficientes, particularmente en el contexto de fuerzas laborales remotas y distribuidas. Esta sección explora cómo Tailscale puede mejorar la seguridad y el cumplimiento para las empresas tecnológicas emergentes de tamaño mediano, con un enfoque en su aplicación en el contexto de las certificaciones SOC 2 TYPE II, ISO 27001 y Google A2LA.

Seguridad mejorada con Tailscale

Tailscale ofrece varias características y capacidades que pueden mejorar significativamente la postura de seguridad de las empresas de tecnología emergentes:

Conectividad de red segura: Tailscale crea conexiones cifradas entre dispositivos, lo que permite una comunicación segura a través de redes no confiables. Este cifrado ayuda a prevenir escuchas ilegales y ataques de intermediarios, lo que mejora la seguridad de los datos.

Modelo de confianza cero: Tailscale opera con un modelo de seguridad de confianza cero, lo que significa que ningún dispositivo o usuario es inherentemente confiable, incluso si se encuentra dentro de la red de la organización. Este enfoque garantiza que los controles de acceso se apliquen rigurosamente, lo que reduce el riesgo de acceso no autorizado.

Políticas de control de acceso: los administradores pueden definir políticas de control de acceso granulares, especificando qué usuarios o dispositivos pueden acceder a recursos específicos. Este control detallado ayuda a las nuevas empresas a hacer cumplir el principio de privilegio mínimo, limitando el acceso solo a lo necesario.

Autenticación multifactorial (MFA): Tailscale admite MFA, lo que agrega una capa adicional de seguridad al requerir que los usuarios proporcionen múltiples formas de autenticación antes de obtener acceso. MFA es un componente crítico de muchos marcos y certificaciones de seguridad.

Desafíos y consideraciones

Si bien Tailscale ofrece importantes beneficios de seguridad, es esencial considerar los siguientes desafíos:

Integración y configuración: la integración y configuración adecuadas de Tailscale dentro de la infraestructura existente pueden ser complejas y requerir experiencia técnica.

Complejidad operativa: gestionar políticas y controles de acceso en un entorno dinámico puede ser un desafío operativo y requiere un monitoreo continuo.

Capacitación de usuarios: Es posible que los usuarios necesiten capacitación para comprender y cumplir las nuevas políticas de control de acceso y prácticas de seguridad.

Implementación

La migración a Tailscale fue un paso fundamental para mejorar la seguridad de nuestra red, optimizar el acceso remoto para nuestros 500 usuarios y posicionarnos para un crecimiento escalable. En esta sección, se proporciona una descripción detallada de los pasos tomados durante la implementación, incluidos los plazos estimados para cada etapa, así como los resultados y beneficios logrados.

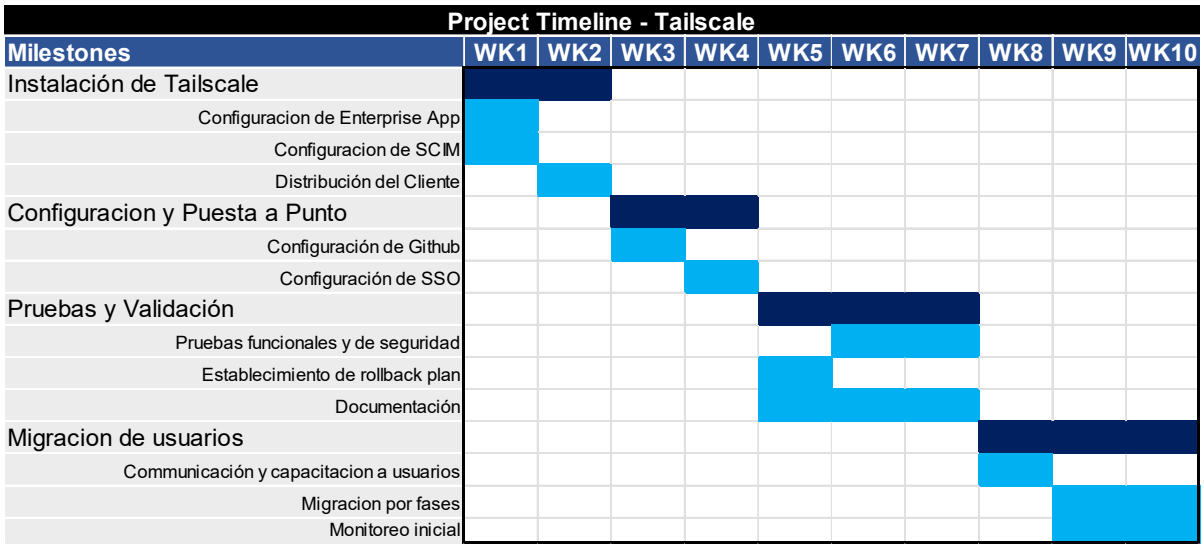

Ilustración 7. Diagrama de Gantt para implementación de Tailscale

Instalación de Tailscale (Tiempo: 10 días)

a) Configuración de Enterprise App con SCIM: Para sentar las bases para una integración optima con Entra ID, se implementó "*System for Cross-domain Identity Management (SCIM)*", este permite el aprovisionamiento automático de usuarios, lo que simplifica la administración alta y baja de usuarios. Se completó en un día

b) Distribución del cliente con PatchMyPC: El cliente Tailscale se distribuyó a las computadoras de los usuarios utilizando el software de distribución PatchMyPC. Este software se monitoreó continuamente para garantizar que los usuarios siempre tuvieran acceso a la última versión. La distribución se completó en un día.

Configuración y Puesta a punto (Tiempo: 10 Días)

a) Configuración del repositorio de GitHub para reglas de validación: Se configuró específicamente un repositorio de GitHub para aplicar reglas de validación estrictas antes de que cualquier código se envíe al entorno de producción. Estas reglas incluían validación de sintaxis, aprobación obligatoria de al menos un administrador de Tailscale y la prohibición de compartir recursos con "todos" para evitar el acceso no deseado. Esta configuración duró dos días.

b) Integración de Entra ID: Se integró Entra ID con Tailscale, lo que permitió la autenticación de usuario a través de las credenciales existentes. Esta fase se completó en un día

Pruebas y Validación (Tiempo: 15 Días)

a) Pruebas funcionales y de seguridad: Se ejecutaron pruebas funcionales y de seguridad para evaluar la implementación de Tailscale. Estas pruebas se realizaron durante 10 días.

A continuación, se muestra de manera general las fases de pruebas y validación que se llevaron a cabo:

Fases de prueba
Fase 1: Implementación piloto para aplicaciones corporativas
Objetivo: Validar Tailscale para aplicaciones corporativas con un grupo reducido de usuarios.

Grupo piloto:
Selección de entre 5 y 10 usuarios de diferentes departamentos.
Garantizando una combinación de usuarios técnicos y no técnicos.

Pasos:

Instalación y configuración:
Instalación de Tailscale en aplicaciones y dispositivos corporativos seleccionados.
Configurar políticas de acceso y permisos.

Pruebas:
Verificar la conectividad y el rendimiento de las aplicaciones corporativas.
Pruebas a la funcionalidad de acceso remoto.
Supervisión cualquier problema de conectividad o errores de aplicación.

Colección de comentarios:
Realizar encuestas y entrevistas a los usuarios piloto.
Recopilación de comentarios sobre usabilidad, rendimiento y cualquier problema encontrado.

Resolución de problemas:
Identificar y resolver cualquier problema reportado por los usuarios piloto.
Actualización de la configuración y los ajustes según sea necesario.

Fase 2: Implementación piloto para aplicaciones de ingeniería
Objetivo: Validar Tailscale para aplicaciones de ingeniería con un grupo pequeño de usuarios.

Grupo piloto:
Selección de entre 5 y 10 ingenieros de diferentes equipos.
Usuarios con diferentes conocimientos técnicos.

Pasos:

Instalación y configuración:
Instalación de Tailscale en aplicaciones y dispositivos de ingeniería seleccionados.
Configurar políticas de acceso y permisos.

Pruebas:
Verificar la conectividad y el rendimiento de las aplicaciones de ingeniería.
Prueba de la funcionalidad de acceso remoto.
Supervisión de cualquier problema de conectividad o errores de aplicación.

Colección de comentarios:
Realizar encuestas y entrevistas a los usuarios piloto.
Recopilación de comentarios sobre usabilidad, rendimiento y cualquier problema encontrado.

Resolución de problemas:
Identificar y resolver cualquier problema reportado por los usuarios piloto.
Actualice la configuración y los ajustes según sea necesario.

b) Establecimiento del Plan de Retroceso: Se estableció un plan de retroceso como medida de precaución. Este plan no fue necesario debido al éxito de la migración. La fase se llevó a cabo simultáneamente con otros esfuerzos de prueba.

c) Documentación integral y recursos de soporte: Se proporcionó a los usuarios un conjunto completo de documentación y recursos de soporte para ayudarles durante el proceso de migración. Estos recursos se mantienen disponibles.

Migración de usuarios (Tiempo: 15 días)

a) Comunicación y orientación para el usuario: Los usuarios fueron informados sobre la migración inminente. Se les proporcionaron instrucciones claras y concisas sobre cómo acceder a la guía de la red Tailscale. Este paso importante requirió 15 días de preparación. Se enviaron correos electrónicos con la información necesaria, cada tercer día durante los 15 días para concientizar y que el usuario se sienta familiarizado con el inminente cambio de herramienta.

b) Enfoque de migración por fases: Para minimizar la interrupción de las operaciones diarias, se adoptó un enfoque de migración por fases. Este enfoque se completó en tres días. Se realizo en principalmente dos fases, herramientas corporativas donde se migraron todas las herramientas de *back office* y herramientas de ingeniería donde se migraron todas las herramientas *core* de la organización, es decir todos aquellos que forman parte de la oferta hacia los clientes externos.

c) Monitoreo del acceso de los usuarios: El monitoreo y análisis continuo del acceso de los usuarios garantizaron una transición fluida de OpenVPN a Tailscale. Este proceso se completó en 15 días.

La migración a Tailscale fue un proceso planificado y ejecutado de manera eficiente que se completó en 45 días. Esta inversión de tiempo y esfuerzo ha dado como resultado un entorno de red que mejora la seguridad y simplifica el acceso remoto para nuestros usuarios. Con esta base sólida establecida, nuestra organización está preparada para aceptar el crecimiento futuro y los avances tecnológicos.

Resultados y beneficios

La migración a Tailscale ha mejorado significativamente nuestra infraestructura de red, generando una serie de resultados y beneficios tangibles que se han visto reflejados en varios aspectos de nuestra organización.

I. Seguridad mejorada

Las sólidas funciones de seguridad de Tailscale han fortalecido nuestra infraestructura de red, reduciendo significativamente las vulnerabilidades y mejorando la protección de datos.

a) Conectividad de red segura: La implementación de las conexiones cifradas de Tailscale ha mejorado la seguridad de los datos dentro de nuestra organización. Al cifrar los datos en tránsito, se ha reducido el riesgo de acceso no autorizado y violaciones de datos, esto gracias a la utilización de la tecnología wireguard. (Tailscale, 2022) Este compromiso con la seguridad es un activo importante para salvaguardar nuestra información confidencial y la de nuestros clientes.

b) Modelo de confianza cero: La adopción de un modelo de seguridad de confianza cero es un paso importante para garantizar que todo el acceso de usuarios y dispositivos esté autenticado y autorizado. Este enfoque proactivo de la seguridad reduce la superficie de ataque y refuerza nuestros mecanismos de defensa, lo que ayuda a proteger contra amenazas emergentes.

II. Experiencia de usuario simplificada

Tailscale no solo ha aumentado nuestra seguridad, sino que también ha simplificado la experiencia del usuario, promoviendo la facilidad de uso y la satisfacción del usuario.

a) Comentarios de los usuarios: Los comentarios iniciales de los usuarios indican que Tailscale ofrece una experiencia de uso más intuitiva y fácil que OpenVPN. Esta simplicidad ha sido bien recibida por los usuarios, lo que ha contribuido a un ambiente de trabajo positivo y productivo. Esta recopilación se llevo a cabo a través de encuestas enviadas a todos los usuarios a través de correo electrónico utilizando *Microsoft Forms*.

b) Integración de inicio de sesión único: Los usuarios ahora pueden acceder a Tailscale con un solo conjunto de credenciales, lo que reduce la necesidad de recordar y administrar múltiples contraseñas. Esto ha reducido el tiempo que los usuarios pasan lidiando con problemas de contraseñas, lo que les permite concentrarse en sus tareas principales.

III. Escalabilidad

En preparación para el crecimiento futuro, la escalabilidad inherente de Tailscale garantiza que nuestra red pueda adaptarse sin problemas para adaptarse a nuevos usuarios y dispositivos.

a) Soporte de crecimiento: la escalabilidad de Tailscale nos ha brindado la flexibilidad necesaria para incorporar sin esfuerzo nuevos usuarios y dispositivos, alineándose perfectamente con nuestra estrategia de crecimiento prospectiva.

IV. Satisfacción del usuario

Los comentarios de nuestros usuarios dicen mucho sobre el impacto positivo de Tailscale en su experiencia dentro de nuestra red.

a) Satisfacción del usuario: Se realizo una encuesta teniendo la participación del 75% donde el 90% de nuestros usuarios han informado de una experiencia positiva con Tailscale. Sus relatos sobre mayor confiabilidad y velocidad de acceso confirman que Tailscale cumplió con sus expectativas, contribuyendo a una mayor satisfacción.

Autenticación sin contraseña: fortalecimiento de los controles de acceso

La autenticación sin contraseña es un enfoque moderno para la verificación de identidad que elimina la necesidad de inicios de sesión tradicionales basados en contraseñas. Se basa en factores alternativos para la verificación del usuario, como datos biométricos, códigos de acceso de un solo uso o autenticación basada en dispositivos. En el contexto de las empresas tecnológicas emergentes de tamaño mediano, la autenticación sin contraseña puede desempeñar un papel crucial para fortalecer los controles de acceso y mejorar la seguridad. Esta sección explora los beneficios, la aplicación y la relevancia de la autenticación sin contraseña en el contexto de la gobernanza y las certificaciones (SOC 2 TYPE II, ISO 27001 y Google A2LA).

Beneficios de la autenticación sin contraseña

La implementación de la autenticación sin contraseña ofrece varias ventajas que contribuyen directamente a mejorar los controles de acceso y la seguridad:

Eliminación de riesgos relacionados con las contraseñas: las contraseñas son un objetivo común para los ciberataques. La autenticación sin contraseña elimina los riesgos asociados con contraseñas débiles, la reutilización de contraseñas y los ataques basados en credenciales, lo que mejora la seguridad general.

Autenticación más sólida: los métodos sin contraseña a menudo incorporan múltiples factores de autenticación, como la biometría o la posesión de un dispositivo físico, lo que dificulta el acceso de personas no autorizadas.

Experiencia de usuario mejorada: la autenticación sin contraseña simplifica el proceso de inicio de sesión para los usuarios, lo que reduce la fricción y mejora la experiencia general del usuario.

Reducción de gastos generales de soporte: las contraseñas olvidadas y los restablecimientos de contraseñas pueden sobrecargar los recursos de soporte de TI. La autenticación sin contraseña reduce la necesidad de solicitudes de soporte relacionadas con contraseñas.

Consideraciones y desafíos de implementación

Si bien la autenticación sin contraseña ofrece importantes beneficios, es importante considerar los desafíos de implementación:

Compatibilidad: la compatibilidad con sistemas y aplicaciones existentes puede requerir ajustes o integraciones.

Adopción de usuarios: los usuarios necesitaran capacitación y educación sobre los nuevos métodos de autenticación, y algunos pueden resistirse al cambio.

Mecanismos de respaldo: las organizaciones deben contar con mecanismos de respaldo en caso de problemas con los métodos de autenticación sin contraseña.

En conclusión, la autenticación sin contraseña es una herramienta poderosa para fortalecer los controles de acceso y mejorar la seguridad en empresas. Al eliminar los riesgos relacionados con las contraseñas, aplicar una autenticación sólida y alinearse con los requisitos de certificación, la autenticación sin contraseña contribuye a un marco de gobernanza sólido esencial para lograr las certificaciones SOC 2 TYPE II, ISO 27001 y Google A2LA. Una implementación exitosa requiere una planificación cuidadosa, educación de los usuarios y consideración de las necesidades y objetivos específicos de la organización.

Implementación

Nuestra implementación de autenticación sin contraseña representa un cambio fundamental en nuestra estrategia de autenticación, destinada a reforzar la seguridad, optimizar el acceso de los usuarios y reducir nuestra dependencia de las contraseñas convencionales. Esta sección proporciona una descripción detallada de los pasos tomados durante esta implementación transformadora.

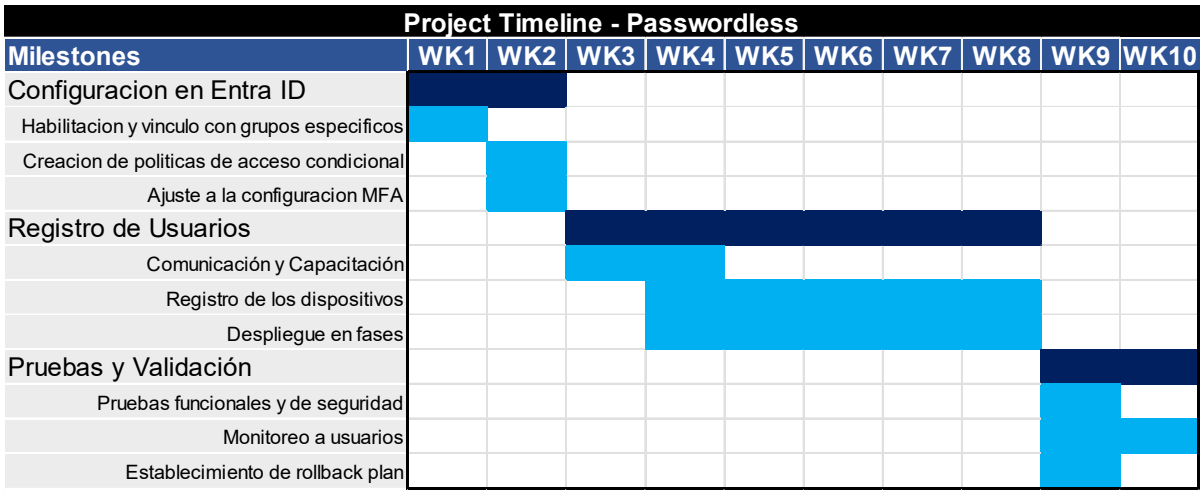

Ilustración 8. Diagrama de Gantt para implementación de Passwordless

Configuración de autenticación sin contraseña en Entra ID (Tiempo: 10 días)

a) Configuración de Entra ID: Entra ID se ha configurado para admitir métodos de autenticación sin contraseña, incluidos datos biométricos y llaves de seguridad. La configuración se completó en 5 días.

b) Políticas de Acceso Condicional en Entra ID: Se definieron políticas de acceso condicional en Entra ID para exigir la autenticación sin contraseña para aplicaciones y grupos de usuarios específicos. Esta alineación de las políticas de control de acceso se completó en 2 días.

c) Ajuste de la configuración de MFA: La configuración de MFA en nuestro entorno Entra ID se ajustó para armonizar con la introducción de la autenticación sin contraseña. Este proceso se completó en 2 días.

Registro de Usuarios (Tiempo: 30 Días)

a) Comunicación y Orientación al Usuario: Se informó a los usuarios sobre la implementación de la autenticación sin contraseña. Se les proporcionaron instrucciones claras y concisas sobre cómo registrar sus dispositivos para este enfoque de autenticación. La comunicación con el usuario requirió de 15 días. Se enviaron correos electrónicos con la información necesaria, cada tercer día durante los 15 días para concientizar y que el usuario se sienta familiarizado con el inminente cambio de forma de autenticación.

b) Registro del Dispositivo: Los usuarios registraron sus dispositivos para autenticación biométrica (Smartphones) o llaves de seguridad. Este proceso, esencial para la inscripción de usuarios, duró aproximadamente 15 días.

c) Enfoque de inscripción por etapas: Para minimizar la interrupción de las operaciones diarias, se adoptó un enfoque de inscripción por fases. Este enfoque permitió una implementación escalonada de la autenticación sin contraseña, lo que facilitó la transición para los usuarios. Los esfuerzos de inscripción por fases continúan a medida que se incorporan nuevos usuarios y dispositivos.

Pruebas y Validación (Tiempo: 10 Días)

a) Pruebas funcionales y de seguridad: Se ejecutaron distintos escenarios de prueba para verificar la funcionalidad y seguridad del sistema de autenticación sin contraseña. Esta fase de prueba duró 5 días.

b) Monitoreo de acceso de usuarios: El acceso de los usuarios se monitoreó y analizó continuamente para garantizar una transición perfecta a la autenticación sin contraseña. Este proceso continúa como parte de nuestro compromiso de proporcionar una experiencia de usuario fluida.

c) Establecimiento del Plan de Reversión: Se estableció un plan de reversión como medida de precaución. Este plan no fue necesario, ya que la implementación sin contraseña fue un éxito. El plan se preparó y mantuvo al mismo tiempo que otros esfuerzos de prueba.

Resultados y Beneficios

La implementación de la autenticación sin contraseña utilizando Entra ID como nuestro proveedor de identidad ha supuesto un cambio significativo en nuestro panorama de autenticación. Este cambio ha generado una serie de resultados y beneficios tangibles que han tenido un impacto positivo en varias facetas de nuestra organización

I. Seguridad mejorada

Los métodos de autenticación sin contraseña ofrecen una mayor seguridad que las contraseñas convencionales.

a) Autenticación sólida. La adopción de métodos de autenticación sin contraseña, como la biometría y las llaves de seguridad, ha generado una mejora notable en nuestra postura de seguridad. Ya que comparado a como anteriormente se hacía con solo usuario y contraseña, esta nueva formo de hacerlo, presenta un desafío numérico al usuario el cual tiene que ser introducido a su teléfono inteligente y validar su identidad a través de sus datos biométricos. Estos métodos eliminan los riesgos inherentes asociados con las contraseñas tradicionales y ofrecen una defensa mejorada contra el acceso no autorizado. Este compromiso con una autenticación sólida fortalece continuamente nuestra seguridad.

b) Acceso condicional. Las políticas de acceso condicional dentro de Entra ID sirven como centinela, garantizando que solo los usuarios autorizados con dispositivos inscritos obtengan acceso a aplicaciones críticas y datos confidenciales. Este mecanismo de control dinámico representa una salvaguardia contra intentos de acceso no autorizados y evoluciona en tiempo real para enfrentar las amenazas de seguridad emergentes.

II. Experiencia de usuario mejorada

La introducción de la autenticación sin contraseña ha aumentado la seguridad y ha mejorado mucho la experiencia del usuario.

a) Comentarios de los usuarios: Los comentarios iniciales de los usuarios indican que la autenticación sin contraseña ha sido una experiencia positiva. Los usuarios han valorado la conveniencia de no tener que recordar contraseñas. Este sentimiento ha continuado, lo que ha generado una sensación de tranquilidad y control.

b) Acceso simplificado: Los usuarios ahora disfrutan de un proceso de inicio de sesión simplificado y acelerado, con menos obstáculos de autenticación para navegar. El ahorro de tiempo resultante se traduce en una mayor productividad y satisfacción del usuario.

III. Eficiencia administrativa

Nuestra transición a la autenticación sin contraseña también ha generado notables eficiencias administrativas.

a) Restablecimientos de contraseñas reducidos: la implementación ha producido una marcada reducción en la necesidad de restablecimientos de contraseñas y solicitudes de soporte asociadas. La reducción agiliza los procesos administrativos y minimiza la frustración del usuario, lo que lleva a una relación usuario-administrador armoniosa. Esto debido a la ausencia de constantes interacciones para solucionar un procedimiento si bien fácil de realizar, genera un tedio de ambas partes.

b) Control centralizado: los administradores ahora ejercen un control centralizado sobre el acceso de los usuarios y las políticas de autenticación desde Entra ID. Este centro de comando centralizado simplifica las tareas de administración, lo que permite a los administradores adaptarse rápidamente a las necesidades cambiantes de la organización mientras mantienen una postura de seguridad sólida.

IV. Satisfacción del Usuario

a) Satisfacción del usuario: Se realizo una encuesta contando con la participación del 87% donde el 91% de los usuarios están satisfechos con la autenticación sin contraseña. Sus comentarios destacan los beneficios de una mayor seguridad y una experiencia de usuario más sencilla, lo que está en línea con nuestro compromiso con la seguridad y la usabilidad.

Inicio de sesión único (SSO): optimización de la gestión de acceso

El inicio de sesión único (SSO) es un proceso de autenticación centralizado que permite a los usuarios acceder a múltiples aplicaciones y servicios con un único conjunto de credenciales de inicio de sesión (Okta, 2021). En las empresas tecnológicas de tamaño mediano, el SSO puede desempeñar un papel fundamental a la hora de agilizar la gestión del acceso, mejorar la seguridad y facilitar el cumplimiento de los requisitos de gobernanza y certificación. Esta sección profundiza en los beneficios, la aplicación y la relevancia del SSO en el contexto de la gobernanza y las certificaciones (SOC 2 TYPE II, ISO 27001 y Google A2LA).

Beneficios del inicio de sesión único (SSO)

La implementación de SSO ofrece numerosas ventajas, todas las cuales contribuyen a mejorar la seguridad y la gestión del acceso:

Acceso simplificado: los usuarios obtienen acceso a varios sistemas y aplicaciones con un único inicio de sesión, lo que reduce la necesidad de recordar varias contraseñas. Esta simplificación mejora la experiencia del usuario y aumenta la productividad.

Seguridad mejorada: los sistemas SSO a menudo incorporan métodos de autenticación sólidos, como la autenticación multifactorial (MFA), lo que refuerza la seguridad al garantizar que solo los usuarios autorizados puedan acceder a los recursos.

Control centralizado: los administradores pueden gestionar de forma centralizada el acceso de los usuarios, los permisos y las políticas de autenticación desde un único panel, lo que proporciona un mayor nivel de control y supervisión.

Pistas de auditoría: las soluciones SSO suelen ofrecer capacidades sólidas de auditoría y registro, lo que genera pistas de auditoría valiosas que son esenciales para los informes de cumplimiento y gobernanza.

Consideraciones de implementación

Si bien el SSO ofrece beneficios sustanciales, es importante considerar las siguientes consideraciones de implementación:

Complejidad de la integración: la integración adecuada de SSO con sistemas y aplicaciones existentes puede requerir experiencia técnica y una planificación exhaustiva.

Capacitación de usuarios: los usuarios pueden necesitar educación y capacitación para adaptarse al nuevo método de autenticación y comprender las políticas de control de acceso.

Mecanismos de respaldo: la implementación de mecanismos de autenticación de respaldo es esencial en caso de fallas del sistema SSO.

Implementación

Si bien durante este proyecto se implementó SSO a las aplicaciones compatibles existentes en esta sección se generó pasos generalizados para en un futuro poder integrar más aplicaciones cuando sea necesario.

Recopilación de documentación de la aplicación a integrar

a) Recopilar toda la información existente sobre la integración con SSO generada por la aplicación tercera a integrar.

Configuración de Entra ID

a) Crear la *Enterprise App* en Azure.
b) En la sección de *Single sign-on* seleccionar SAML
c) En base a la información de la aplicación ingresar al menos la siguiente información:

- Identifier (Entity ID)
- Reply URL

d) En Attributes & claims, hacer las modificaciones necesarias de acuerdo con la documentación de la aplicación tercera.
e) Tomar nota de la siguiente información que será necesaria para la configuración en la aplicación tercera:

- Tenant ID
- Application ID
- App Federation Metadata URL

f) En caso de que la aplicación soporte aprovisionamiento de usuarios automática, en la sección de *Provisioning* ingresar los siguientes datos generados en la aplicación tercera:

- Tenant URL
- Secret Token

g) En la sección de *Users and Groups*, agregar todos los usuarios y/o grupos que tendrán acceso a esta aplicación tercera.

Configuración de aplicación tercera

a) Crear un proveedor de identidad.
b) Ingresar la información recopilada en Azure:

- Tenant ID
- Application ID
- App Federation Metadata URL

c) Habilitar el SSO
d) En caso de que soporte el aprovisionamiento automático de usuarios, generar el secret token necesario en Azure.
e) Realizar pruebas con usuarios piloto.

Capacitación y comunicación al usuario

a) Se informó a los usuarios sobre la próxima implementación de SSO a través de sesiones de capacitación y correos electrónicos informativos.
b) Se proporcionaron guías y materiales de capacitación para educar a los usuarios sobre el nuevo proceso SSO.
c) Se creó un servicio de asistencia técnica para ayudar a los usuarios durante el período de transición inicial del SSO.

Resultados y beneficios

Se genero el proceso estándar para la implementación de SSO para aplicaciones terceras utilizando Entra ID como proveedor de identidad. Si bien en este caso solo es una referencia ya que los pasos exactos pueden variar dependiendo la aplicación tercera, se considera una guía suficientemente detallada para poder replicarlo exitosamente en futuras implementaciones.

I. Gestión de acceso mejorada

a. Control centralizado: la implementación de SSO centraliza el control de acceso de los usuarios, lo que permite a los administradores gestionar los permisos y las políticas de autenticación de manera eficiente.
b. Acceso granular: el acceso a cada aplicación ahora se administra con precisión, lo que garantiza que los usuarios tengan acceso solo a los recursos que necesitan.

II. Productividad del usuario mejorada

a. Acceso optimizado: los usuarios ahora pueden acceder a todas las aplicaciones integradas con un único inicio de sesión, lo que reduce significativamente el tiempo dedicado a iniciar sesión y mejora la productividad.
b. Gestión de contraseñas: la menor dependencia de recordar múltiples contraseñas ha llevado a una disminución de los problemas y restablecimientos de contraseñas.

III. Eficiencia Administrativa

a. Carga de trabajo reducida: la cantidad reducida de solicitudes de soporte relacionadas con contraseñas ha permitido que el equipo de TI se centre en iniciativas más estratégicas.
b. Seguimientos de auditoría: los registros de auditoría detallados generados por Azure AD brindan información valiosa para fines de cumplimiento y seguridad.

IV. Comentarios del usuario

Recepción positiva: Se aplico una encuesta contando con la participación de un 83% los comentarios de los usuarios han sido abrumadoramente positivos, donde el 98% expresaron satisfacción con el proceso de inicio de sesión simplificado y el aumento de la productividad.

Menos solicitudes de soporte: el servicio de asistencia técnica informó una reducción significativa en los tickets de soporte relacionados con problemas de inicio de sesión, lo que indica una experiencia de usuario más fluida.

Costos de implementación

La implementación de herramientas avanzadas de seguridad y autenticación, como Tailscale y Microsoft 365 E5, es crucial para fortalecer la infraestructura de TI de una empresa en crecimiento. Este capítulo se centrará en los costos asociados con la implementación de Tailscale en su versión premium con SCIM y los costos de Microsoft 365 E5, que ya se estaba pagando, pero sin utilizar todas sus capacidades avanzadas de seguridad, como el inicio de sesión único (SSO) y la autenticación sin contraseña (passwordless).

Costo de Implementación de Tailscale Premium con SCIM

Tailscale es una solución de red privada virtual (VPN) que simplifica la creación de redes privadas seguras mediante la autenticación y la conectividad de dispositivos de manera intuitiva y robusta. La versión premium de Tailscale, que incluye el Sistema de Gestión de Identidades y Accesos Basado en Seguridad (SCIM), ofrece características adicionales de seguridad y administración.

Para 500 usuarios, el costo mensual de Tailscale Premium con SCIM es de 23 dólares por usuario. A continuación, se desglosa el costo anual:

Costo mensual por usuario: $23
Número de usuarios: 500
Costo mensual total: $23 * 500 = $11,500
Costo anual total: $11,500 * 12 = $138,000

Por lo tanto, el costo de implementar Tailscale Premium con SCIM para 500 usuarios durante un año es de $138,000. Este gasto cubre la suscripción a una herramienta que proporciona una robusta seguridad de red y una gestión eficiente de identidades y accesos, crucial para mantener la integridad y la protección de los datos en una empresa en expansión.

Costo de la Licencia Microsoft 365 E5

Microsoft 365 E5 es una suite de productividad empresarial que incluye herramientas como Office 365, funciones avanzadas de seguridad, y capacidades de gestión y cumplimiento normativo. Además, ofrece características avanzadas de autenticación como el inicio de sesión único (*SSO*) y la autenticación sin contraseña *(passwordless*), las cuales no estaban siendo aprovechadas por la empresa.

Para 500 usuarios, el costo mensual de Microsoft 365 E5 es de 55 dólares por usuario. A continuación, se desglosa el costo anual:

Costo mensual por usuario: $55
Número de usuarios: 500
Costo mensual total: $55 * 500 = $27,500
Costo anual total: $27,500 * 12 = $330,000

Este costo ya era asumido por la empresa, pero sin implementar las funciones avanzadas de seguridad que ofrece Microsoft 365 E5, como SSO y la autenticación *passwordless.* La falta de utilización de estas funciones significaba que la empresa no estaba maximizando el valor de su inversión en esta plataforma.

Evaluación del Retorno de Inversión (ROI)

La integración de Tailscale Premium con SCIM y la plena utilización de Microsoft 365 E5, incluyendo SSO y la autenticación *passwordless*, representan una inversión significativa, pero con beneficios claros en términos de seguridad, eficiencia y cumplimiento normativo.

Seguridad Mejorada:

Tailscale: Asegura una red privada robusta, protege contra amenazas internas y externas, y simplifica la gestión de acceso.
Microsoft 365 E5: Fortalece la seguridad mediante SSO y autenticación *passwordless,* reduciendo el riesgo de ataques basados en credenciales.

Eficiencia Operativa:

Reducción de la carga de trabajo del personal de TI: Al centralizar y simplificar la gestión de acceso y autenticación.
Productividad del usuario: Al reducir el número de credenciales que deben recordar y gestionar.

Cumplimiento Normativo:

La implementación de estas herramientas ayuda a la empresa a cumplir con estándares y regulaciones de seguridad de la información, como SOC 2, ISO 27001, y otros requisitos específicos de la industria.

El costo total de implementar Tailscale Premium con SCIM para 500 usuarios durante un año asciende a $138,000, mientras que el costo de la licencia de Microsoft 365 E5 para el mismo número de usuarios es de $330,000 anuales, un gasto que la empresa ya estaba asumiendo. Sin embargo, la plena utilización de las funciones avanzadas de seguridad de

Microsoft 365 E5, junto con la implementación de Tailscale, proporciona una capa adicional de seguridad y eficiencia que justifica la inversión.

Al adoptar estas soluciones, la empresa no solo mejora su postura de seguridad y su capacidad de cumplimiento normativo, sino que también optimiza sus operaciones de TI, lo cual es crucial para apoyar su continuo crecimiento y éxito en un entorno empresarial cada vez más complejo y exigente.

Conclusiones

La implementación de la arquitectura Zero Trust representa un paso fundamental hacia la mejora de la seguridad y la protección de los activos digitales de la empresa. Al adoptar este enfoque, se alcanzaron diversos beneficios, tales como una mayor protección contra amenazas tanto internas como externas, una reducción significativa de la superficie de ataque y una mayor capacidad de recuperación frente a posibles violaciones de seguridad. Además, la implementación de herramientas Zero Trust tuvo un impacto positivo en las operaciones de TI, al optimizar la gestión de acceso y fortalecer los controles de seguridad.

Es importante destacar que el éxito de este proyecto dependió en gran medida de una cuidadosa selección e implementación de las herramientas adecuadas, así como de la definición de políticas de seguridad de la información claras y efectivas. Además, la gestión de la resistencia cultural dentro de la organización es un aspecto crítico que no debe pasarse por alto. Superar las posibles reticencias y garantizar la adopción efectiva de los principios de Zero Trust en todos los niveles de la empresa requirió un enfoque estratégico y una comunicación clara y continua.

En resumen, la implementación exitosa de herramientas Zero Trust no solo implico la adquisición de tecnología avanzada, sino también un cambio cultural y organizativo que promueve una mentalidad de seguridad en todos los aspectos de las operaciones de la empresa. Con un enfoque cuidadoso y una ejecución diligente, la adopción de Zero Trust se convirtió en un pilar fundamental de la estrategia de seguridad de la empresa, fortaleciendo su posición frente a las amenazas actuales y futuras.

A continuación, las conclusiones específicas para cada una de las implementaciones:

Tailscale. La adopción de Tailscale representa un importante paso adelante para nuestra organización. Más allá de sus méritos técnicos, Tailscale se ha convertido en una herramienta valiosa para mejorar la seguridad, promover el cumplimiento y mejorar la experiencia general del usuario dentro de nuestra empresa. Sus contribuciones a la conectividad de red segura, la aplicación del control de acceso y la alineación con los requisitos de certificación son fundamentales para fortalecer nuestro marco de gobernanza, un componente fundamental en nuestro camino hacia las certificaciones SOC 2 TYPE II, ISO 27001 y Google A2LA.

La implementación de tailscale significo una reducción de 76 *tickets* de soporte mensuales con un tiempo de atención promedio de 35 min. Lo que equivale a 44.3 horas que los analistas de soporte pueden enfocarse a otras actividades.

SSO. La implementación del inicio de sesión único (SSO) con Entra ID ha optimizado con éxito la administración de acceso, mejorado la productividad del usuario y mejorado la seguridad general de nuestra organización. La implementación cuidadosamente planificada y los comentarios positivos de los usuarios validan el éxito de esta iniciativa, alineando nuestra organización con las prácticas modernas de gestión de acceso.

Esta transición ha producido tres resultados positivos: seguridad mejorada, una experiencia de usuario mejorada y mayor eficiencia administrativa. La autenticación sin contraseña es un testimonio de nuestro compromiso de combinar la seguridad con la usabilidad, garantizando que nuestro futuro digital siga siendo seguro y accesible.

Esto significó una disminución de un promedio de 184 *tickets* mensuales con un tiempo de atención de 10 min por lo que equivale a 30.6 horas liberadas.

El inicio de sesión único (SSO) sirve como una herramienta valiosa para que las empresas tecnológicas emergentes de tamaño mediano agilicen la gestión del acceso, mejoren la seguridad y faciliten el cumplimiento de los requisitos de gobernanza y certificación. Al simplificar el acceso, aplicar una autenticación sólida y proporcionar control centralizado, SSO contribuye a un marco de gobernanza sólido esencial para lograr las certificaciones SOC 2 TYPE II, ISO 27001 y Google A2LA. Sin embargo, una implementación exitosa requiere una planificación cuidadosa, educación del usuario y consideración de las necesidades y objetivos específicos de la organización.

Esto significó una disminución de 122 *tickets* mensuales con un promedio de atención de 5 minutos lo que significó una liberación de 10.1 horas

Autenticación sin contraseña. La implementación de la autenticación sin contraseña representa un avance significativo para la seguridad y la experiencia del usuario de nuestra organización. No se trata solo de un cambio técnico, sino de un cambio estratégico hacia métodos de autenticación más seguros. Los plazos estimados para cada fase de esta implementación reflejan nuestro compromiso con una planificación y ejecución cuidadosas.

Con esta implementación nuestra organización está a la vanguardia de la seguridad de la autenticación. La transición exitosa a la autenticación sin contraseña demuestra nuestro compromiso con la seguridad, la eficiencia y las experiencias centradas en el usuario.

Esta transición está alineada con nuestra visión de un futuro digital seguro y accesible.

En el rubro mas personal, la implementación de Tailscale, *Single Sign-On (SSO)* y tecnologías de autenticación sin contraseña ha sido una experiencia transformadora en mi rol como ingeniero de infraestructura. Cada una de estas tecnologías ha aportado un valor significativo a mi desarrollo profesional y ha mejorado de manera notable la seguridad y eficiencia de las infraestructuras que gestiono.

No solo ha mejorado la seguridad y eficiencia de las infraestructuras que administro, sino que también ha enriquecido mi experiencia profesional y mi comprensión de las tecnologías modernas de seguridad. Estas experiencias me han enseñado la importancia de adoptar soluciones innovadoras y de mantenerse actualizado con las tendencias emergentes para continuar siendo un profesional efectivo y relevante en el campo de la ingeniería de infraestructura.

Lecciones aprendidas

La planificación minuciosa es clave: planificar adecuadamente la implementación. Comprenda la estructura de su red, los requisitos del usuario y las necesidades de seguridad antes de implementar Tailscale. Un plan integral puede evitar muchos problemas de implementación.

Comunicación y Capacitación Efectiva: Invertir en capacitación de usuarios y comunicación clara. Proporcione guías completas y sesiones de capacitación para ayudar a los usuarios a adaptarse al nuevo sistema sin problemas.

Pruebas exhaustivas: las pruebas rigurosas en un entorno controlado son cruciales. Pruebe diferentes escenarios, aplicaciones y dispositivos para garantizar la compatibilidad y la funcionalidad antes de implementar Tailscale en toda la organización.

Configuraciones de seguridad sólidas: implemente medidas de seguridad sólidas. Aplique políticas estrictas de control de acceso, configure firewalls correctamente y audite periódicamente las configuraciones para garantizar que se ajusten a las mejores prácticas de seguridad.

Cumplimiento del cumplimiento: manténgase actualizado con los estándares y regulaciones de la industria. Asegúrese de que la implementación de Tailscale cumpla con estos estándares para evitar complicaciones legales y regulatorias.

Consideración de la escalabilidad: diseñe la implementación teniendo en cuenta la escalabilidad. Tailscale debería poder manejar un número cada vez mayor de usuarios y dispositivos sin comprometer el rendimiento y la seguridad.

Monitoreo y actualizaciones periódicas: Establecer prácticas de monitoreo continuo. Revise periódicamente los registros, realice auditorías de seguridad y mantenga actualizado el software Tailscale para abordar las vulnerabilidades de seguridad con prontitud.

Flexibilidad y adaptabilidad: Esté preparado para adaptarse. El panorama de TI y las amenazas a la seguridad están en constante evolución. Ser flexible y estar preparado para ajustar configuraciones y políticas es esencial para mantener una red segura.

Bibliografía

American Institute of CPAs (AICPA). (2018). *SOC 2 privacy criteria and control objectives*. Retrieved from AICPA: https://www.aicpa.org/professional-insights/video/soc-2-privacy-criteria-and-control-objectives

American Institute of CPAs (AICPA). (n.d.). *SOC for Service Organizations*. Retrieved from https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report.html

Ant, A. (2021, October 19). *Take 3 Steps Toward Passwordless Authentication.* Retrieved from Gartner: https://www.gartner.com/doc/reprints?id=1-2ABVDPV8&ct=220616&st=sb

App Defence Alliance. (n.d.). *App Defence Alliance*. Retrieved from https://appdefensealliance.dev/

Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2013). *Internal Control-Integrated Framework*. Retrieved from https://www.coso.org/Shared%20Documents/CROWE-COSO-Internal-Control-Integrated-Framework.pdf

Cybersecurity & Infrastructure Security Agency. (2020, January). *MULTI-FACTOR AUTHENTICATION (MFA) .* Retrieved from Cybersecurity & Infrastructure Security Agency: https://www.cisa.gov/publication/multi-factor-authentication-mfa

DUO. (2021). *The Road to a Passwordless Future.* Cisco Secure.

Information Security Media Group. (2020). *Zero trust strategies for 2022.* ISMG.

International Organization for Standardization (ISO). (2013). *ISO/IEC 27001:2013 - Information technology - Security techniques - Information security management systems - Requirements*. Retrieved from https://www.iso.org/standard/54534.html

International Organization for Standardization (ISO). (2018). *Risk management*. Retrieved from https://www.iso.org/standard/65694.html

Kotadia, M. (2004, February 25). *Gates predicts death of the password.* Retrieved from CNET: https://www.cnet.com/news/privacy/gates-predicts-death-of-the-password/

Lewis, K. D., & Lewis, J. E. (2009). Web Single Sign-On Authentication using SAML. *IJCSI International Journal of Computer Science Issues, Vol. 2, 2009*, pp. 41-48.

Microsoft. (2022). *Implement a Zero Trust security model.* Retrieved from https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-overview

Microsoft. (2023, September 21). *App sign-in flow with the Microsoft identity platform*. Retrieved from Microsoft Learn: https://learn.microsoft.com/en-us/azure/active-directory/develop/app-sign-in-flow

Microsoft. (2023, September 19). *Passwordless authentication options for Microsoft Entra ID*. Retrieved from Microsoft Learn: https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-passwordless

My1Login. (2022). *What is Single Sign-On?* Retrieved from my1Login: https://content.my1login.com/hubfs/Whitepapers/What%20is%20SSO/What%20is%20SSO%20-%20My1Login.pdf

NIST Special Publication 800-63B. (2017). *Digital Identity Guidelines: Authentication and Lifecycle Management*. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf

Okta. (2019). *The passwordless Future Report.* Okta.

Okta. (2021). *What is Single Sign-On (SSO)?* Retrieved from https://www.okta.com/identity-101/what-is-single-sign-on/

Paloalto. (2020, January). *What is a Zero Trust Architecture*. Retrieved from PaloAlto: https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture

Pennarun, A. (2020, March 20). *How Tailscale works.* Retrieved from Tailscale: https://tailscale.com/blog/how-tailscale-works/

Rose, S., Borchert, O., Michell, S., & Connelly, S. (2020). *NIST Special Publication 800-207 - Zero Trust Architecture.* National Institute of Standars and Technology.

Saltzer, J. H., & Schroeder, M. D. (1975). *The Protection of Information in Computer Systems.*

Tailscale. (2022). *Why Tailscale?* Retrieved from https://tailscale.com/why-tailscale/

Terdiman, D. (2013, September 10). *Google security exec: 'Passwords are dead'.* Retrieved from CNET: https://www.cnet.com/news/privacy/google-security-exec-passwords-are-dead/

The National Institute of Standards and Technology. (2020). *Zero Trust Architecture*. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

Verizon. (2021). *Data Breach Investigations Report.*

Yubico. (2022). *USB Security Key*. Retrieved from https://www.yubico.com/products/yubikey-hardware/compare-yubikeys/

Glosario

A

Autenticación sin contraseña
La autenticación sin contraseña es un método de autenticación en el que un usuario puede iniciar sesión en un sistema informático sin ingresar una contraseña o cualquier otro secreto basado en el conocimiento. · 4, 6, 8, 26, 41, 42, 43

I

ISO 27001
Es un estándar internacional que establece los requisitos para la implementación, mantenimiento y mejora continua de un Sistema de Gestión de la Seguridad de la Información (SGSI). Este sistema se utiliza para proteger la confidencialidad, integridad y disponibilidad de la información. · 5, 6, 7, 8, 9, 11, 12, 13, 14, 24, 25, 36, 37, 41, 42, 43, 44, 47, 48, 51

M

MFA
La autenticación de múltiples factores, más comúnmente conocida por sus siglas en inglés MFA, es un método de control de acceso informático en el que a un usuario se le concede acceso al sistema solo después de que presente dos o más pruebas diferentes de que es quien dice ser. · 10, 17, 21, 36, 44, 47, 49, 53

O

OpenVPN
OpenVPN es una herramienta de conectividad basada en software libre
SSL, VPN Virtual Private Network. OpenVPN ofrece conectividad punto-a-punto con validación jerárquica de usuarios y host conectados remotamente. · 5, 39, 40

P

Project Manager
Un gestor de proyecto, es la persona que tiene la responsabilidad total del planeamiento y la ejecución acertada de cualquier proyecto. · 15, 16

S

SOC 2 Type II
Es un marco utilizado para ayudar a las empresas a demostrar los controles de seguridad que existen para proteger los datos de los clientes en la nube. Estos controles pasaron a conocerse como los Principios de los Servicios de Confianza
Seguridad, Disponibilidad, Integridad del Proceso, Confidencialidad y, por último, Privacidad. · 5, 11

SSO
El inicio de sesión único o inicio de sesión unificado es un procedimiento de autenticación que habilita a un usuario determinado para acceder a varios sistemas con una sola instancia de identificación. · 4, 6, 8, 10, 11, 12, 13, 14, 16, 17, 18, 20, 26, 27, 31, 32, 33, 34, 35, 47, 48, 49, 50, 51, 53

stakeholders

El participante, parte interesada o interesado es una persona, organización o empresa que tiene algún tipo de participación interna o externa en una empresa u organización dada. · 15, 16

T

Tailscale

Tailscale es un servicio VPN que hace que sus dispositivos y aplicaciones sean accesibles en cualquier parte del mundo, de forma segura y sin esfuerzo. Permite conexiones cifradas punto a punto utilizando el protocolo WireGuard de código abierto, lo que significa que sólo los dispositivos de su red privada pueden comunicarse entre sí. · 4, 6, 8, 11, 12, 13, 14, 16, 17, 18, 20, 22, 26, 27, 28, 29, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 51, 52, 53

V

VPN

Una red privada virtual es una tecnología de red de ordenadores que permite una extensión segura de la red de área local sobre una red pública o no controlada como Internet · 5, 6, 8, 9, 10, 15, 17, 20, 21, 22

Z

Zero-Trust

Redes de confianza cero, en el marco de la Tecnología de la Información describe un enfoque de diseño e implementación de redes TI. · 1, 4, 15