Propuesta de estrategias de ciberseguridad basadas en zero trust e ISO\IEC 27001:2022 para el fortalecimiento del acceso remoto en entornos de teletrabajo en Colombia

Duvan Andres Gonzalez Gallego

Asesor

Sonia Patricia Garzón Martínez

Universidad Nacional Abierta y a Distancia – UNAD

Escuela de Ciencias Básicas, Tecnología e Ingenierías ECBTI

Especialización en Seguridad Informática

2025

Agradecimientos

Doy gracias primeramente a Dios quien es el que nos da la vida y nos deja vivir el día a día con quienes nosotros amamos.

Agradezco:

A Anggie Camila Mateus Tirado

A Ing. Manuel Antonio Sierra Rodríguez

A Ing. Miguel Andres Ávila Guadrón

A Ing. Sonia Patricia Garzón Martínez

Y a todos los que de una u otra forma han contribuido en la presentación de este proyecto.

Dedicatoria

Dedico este proyecto a la memoria de mi padre (Q.E.P.D), a mi madre Leonor Gallego Lopez, quien siempre me ha brindado su apoyo incondicional en cada etapa de mi vida; a mi pareja Anggie Camila Mateus, quien siempre ha estado a mi lado brindándome apoyo y motivación; a mis profesores, quienes siempre me guían con sabiduría y conocimiento, y a todas las personas que creen en el poder del esfuerzo y dedicación, este proyecto es una muestra de que con constancia y sacrificio todo es posible.

Resumen

El teletrabajo ha transformado la forma en que las empresas operan, especialmente tras la pandemia de COVID-19. Este cambio acelerado ha expuesto numerosas vulnerabilidades de ciberseguridad relacionadas con el acceso remoto, como el uso de dispositivos personales inseguros y redes domésticas poco protegidas. Esta monografía busca analizar cómo las mejores prácticas basadas en el modelo Zero Trust y la norma ISO 27001 pueden fortalecer la protección de los accesos remotos en entornos de teletrabajo en Colombia.

El objetivo es identificar riesgos comunes, evaluar herramientas de seguridad como la autenticación multifactor y sintetizar estrategias efectivas para mitigar amenazas cibernéticas. Este trabajo es fundamental para asegurar la protección de la información de las empresas, fortalecer la confianza de los usuarios y facilitar una transición sostenible hacia modelos de trabajo híbridos más seguros.

***Palabras clave*:** Ciberseguridad, teletrabajo, Zero Trust, ISO 27001, autenticación multifactor.

Abstract

Remote work has transformed the way businesses operate, especially in the wake of the COVID-19 pandemic. This accelerated shift has exposed numerous cybersecurity vulnerabilities related to remote access, such as the use of insecure personal devices and poorly protected home networks. This monograph seeks to analyze how best practices based on the Zero Trust model and the ISO 27001 standard can strengthen remote access protection in remote work environments in Colombia.

The objective is to identify common risks, evaluate security tools such as multi-factor authentication, and synthesize effective strategies to mitigate cyber threats. This work is essential to ensure the protection of corporate information, strengthen user trust, and facilitate a sustainable transition to more secure hybrid work models.

***Keywords*:** Cybersecurity, remote work, Zero Trust, ISO 27001, multi-factor authentication.

Tabla de contenido

Lista de Tablas

Lista de Figuras

Lista de Apéndices

Glosario

Acceso remoto: Conexión que permite acceder a recursos corporativos desde ubicaciones externas a la red empresarial.

Autenticación multifactor (MFA): Mecanismo de verificación de identidad que requiere al menos dos factores distintos (por ejemplo: contraseña + código SMS o huella digital).

Ciberseguridad: Conjunto de prácticas, políticas y tecnologías destinadas a proteger sistemas informáticos y datos contra accesos no autorizados y ciberataques.

ISO/IEC 27001: Norma internacional que establece los requisitos para implementar un Sistema de Gestión de Seguridad de la Información (SGSI).

Phishing: Técnica de ingeniería social utilizada para engañar a usuarios mediante correos electrónicos falsos con el fin de obtener información confidencial.

Segmentación de red: División lógica de la red para aislar recursos sensibles y limitar el movimiento lateral de posibles atacantes.

SIEM: Plataforma que permite recolectar, analizar y correlacionar eventos de seguridad para detectar incidentes y generar alertas.

Teletrabajo: Modalidad laboral que permite a los empleados realizar sus funciones desde ubicaciones distintas a la oficina física.

Zero Trust: Modelo de seguridad que "elimina la confianza implícita y asume que cada solicitud de acceso representa un riesgo potencial" (NIST SP 800-207, Sección 1). Se basa en el principio de "verificación explícita, otorgando el mínimo privilegio necesario y asumiendo que las redes pueden estar comprometidas" (NIST SP 800-207, Sección 2.1).

Introducción

En los últimos años, muchas empresas se vieron obligadas a implementar el teletrabajo como respuesta a la pandemia COVID 2019. Aunque esta medida permitió continuar con las actividades laborales, también dejó en evidencia varios problemas relacionados con la protección de la información. Muchos empleados utilizaron sus propios computadores y establecieron conexión desde redes poco seguras, sin contar con herramientas o conocimientos suficientes para prevenir riesgos de ciberseguridad.

Como resultado, aumentaron los casos de correos maliciosos, accesos no autorizados y pérdida de datos sensibles. Esta situación mostró la importancia de contar con medidas claras y efectivas que ayuden a proteger los accesos remotos y a crear una cultura de seguridad en las organizaciones.

Este proyecto busca proponer estrategias que permitan a las empresas enfrentar de una mejor manera estos desafíos, tomando como base modelos reconocidos como Zero Trust y la norma ISO 27001. Con esto, se pretende no solo reducir los riesgos, sino también fortalecer la confianza en el trabajo remoto como una forma segura de continuar las operaciones en las empresas.

Planteamiento del Problema

La pandemia de COVID-19, impulso a la adopción del teletrabajo para garantizar la continuidad de muchas organizaciones. Sin embargo, esta transición rápida y en muchos casos improvisado, reveló múltiples vulnerabilidades en materia de ciberseguridad. Muchas empresas no contaban con la preparación necesaria para proteger adecuadamente el acceso remoto a sus sistemas. Factores como el uso de dispositivos personales sin las debidas medidas de seguridad, la conexión a redes domésticas vulnerables y la falta de protocolos sobre el manejo de información confidencial se convirtieron en focos de riesgo.

Además, la falta de formación de los empleados en el tema d ciberseguridad ha facilitado el aumento de ataques como el phishing o el acceso no autorizado. Estas debilidades hacen evidente la necesidad de adoptar medidas concretas que permitan fortalecer la seguridad en entornos de teletrabajo, para ello, es esencial adoptar estándares internacionales y buenas prácticas que garanticen tanto la protección de la información como la continuidad operativa.

Pregunta del problema

¿De qué manera pueden las mejores prácticas de ciberseguridad basadas en Zero Trust y la norma ISO 27001 reforzar la protección de accesos remotos en el contexto del teletrabajo?

Justificación

El teletrabajo, si bien ofrece ventajas significativas, ha ampliado considerablemente la superficie de ataque cibernético de muchas organizaciones. Las conexiones a redes inseguras, el uso de dispositivos personales sin las medidas de protección adecuadas y la falta de políticas de seguridad efectivas representan riesgos graves para la integridad de la información corporativa. A esto se suma el desconocimiento por parte de los funcionarios sobre prácticas basadas en seguridad, lo que incrementa la posibilidad de incidentes como el phishing o el acceso no autorizado a sistemas críticos.

Este trabajo se enfoca en una problemática actual y urgente, proponiendo soluciones basadas en estándares reconocidos a nivel internacional, como el enfoque en Zero Trust e ISO 27001 Estas herramientas no solo permiten abordar los riesgos inmediatos, sino que también ofrecen un marco integral y adaptable a diferentes contextos empresariales. Este análisis no solo contribuye a la mitigación de riesgos urgentes, sino que también prioriza una cultura organizacional centrada en la ciberseguridad, lo que resulta esencial en un entorno donde las amenazas digitales evolucionan constantemente.

Objetivos

Objetivo General

Proponer estrategias de ciberseguridad basadas en el modelo Zero Trust y la norma ISO/IEC 27001 orientadas al fortalecimiento de los accesos remotos en entornos de teletrabajo en Colombia.

Objetivos Específicos

Analizar procedimientos de ciberseguridad fundamentados en el modelo Zero Trust y la norma ISO/IEC 27001:2022 orientada a la reducción de riesgos en escenarios de teletrabajo.

Identificar las principales vulnerabilidades en accesos remotos dentro de entornos de teletrabajo, a partir de un análisis documental y casuístico de riesgos y desafíos reportados en estudios recientes.

Determinar herramientas tecnológicas y prácticas disponibles, como autenticación multifactor (MFA), segmentación de redes y gestión de identidades, evaluando su alineación con el modelo Zero Trust.

Diseñar estrategias basadas en Zero Trust e ISO/IEC 27001:2022 orientadas al fortalecimiento de la protección de accesos remotos, contribuyendo a la reducción de riesgos en escenarios de teletrabajo.

Marco Teórico

Fundamentos Teóricos de la Ciberseguridad en Entornos de Teletrabajo

El modelo Zero Trust y la norma ISO 27001 ofrecen enfoques complementarios para gestionar los desafíos de ciberseguridad en el teletrabajo. Zero Trust establece que ninguna conexión, dispositivo o usuario debe ser considerado confiable por defecto, promoviendo principios como la segmentación de redes y el acceso basado en identidad. Por su parte, la ISO 27001 proporciona un marco de gestión de seguridad que incluye controles específicos para proteger la información frente a riesgos internos y externos.

Estos enfoques integrados son esenciales para mitigar vulnerabilidades como accesos no autorizados, redes inseguras y el uso inadecuado de dispositivos personales en el teletrabajo. Además, prácticas como la autenticación multifactor, el monitoreo continuo y la capacitación en ciberseguridad refuerzan la implementación de estas estrategias, garantizando que las organizaciones puedan proteger sus sistemas y datos, mientras facilitan la flexibilidad y productividad de los trabajadores remotos.

Marco Conceptual

Ciberseguridad: Se refiere a las medidas y controles implementados para proteger los sistemas de información contra accesos no autorizados, ataques o daños. En el teletrabajo, la ciberseguridad adquiere un papel crítico debido a las conexiones remotas.

Teletrabajo: Modalidad laboral que permite a los empleados desempeñar sus funciones desde ubicaciones fuera de la oficina, generalmente utilizando tecnologías de información y comunicación.

Zero Trust: Modelo de seguridad basado en el principio de “no confiar en nada ni en nadie”, que requiere verificación continua de usuarios, dispositivos y redes antes de conceder acceso a recursos.

ISO 27001: Norma internacional que establece requisitos para la gestión de la seguridad de la información. Incluye controles específicos para mitigar riesgos asociados al teletrabajo y al acceso remoto.

Acceso remoto: Proceso que permite a los usuarios conectarse a redes corporativas desde ubicaciones externas. Requiere medidas adicionales de protección para evitar brechas de seguridad.

Marco Referencial

Evolución de las Amenazas en Teletrabajo. La adopción masiva del teletrabajo, impulsada por la pandemia del COVID-19, transformó de manera compleja el panorama de la ciberseguridad a nivel global. Muchas organizaciones, especialmente pequeñas y medianas empresas (PYMES), trasladaron sus operaciones a entornos remotos sin contar con una infraestructura de seguridad adecuada, lo cual amplificó significativamente su exposición a riesgos cibernéticos. Según Security Report (2023), los ataques dirigidos a trabajadores remotos crecieron un 238% entre 2020 y 2022. Los principales vectores de ataque fueron:

Phishing, responsable del 45% de los incidentes.

Explotación de VPNs mal configuradas (30%).

Accesos desde dispositivos no gestionados (25%).

En el contexto colombiano, el informe del CERT-Colombia (2023) reveló que el 62% de las PYMES carecían de políticas o controles de seguridad para el acceso remoto al comienzo de la pandemia, facilitando múltiples incidentes. Entre los más relevantes se destacan:

Filtración de datos sensibles en el sector salud, como en el caso de (EPS Sanitas, 2021).

Ataques de ransomware a instituciones educativas, como la Universidad Nacional de Colombia (2022), que comprometieron plataformas de gestión académica.

Adopción de Zero Trust e ISO/IEC 27001:2022 Como Respuesta. Como respuesta a esta creciente ola de amenazas, diversas organizaciones han optado por adoptar enfoques de seguridad más robustos. El modelo Zero Trust ha sido implementado por gigantes tecnológicos como Google y Microsoft, el cual ha sido citado por Gartner como un enfoque estratégico adoptado por más del 60 % de las empresas hacia 2025, aunque más de la mitad aún no logran traducirlo en beneficios sin una implementación estructurada y clara. Un caso destacado es el de Google, que desarrolló el modelo BeyondCorp, una de las primeras aplicaciones de Zero Trust a gran escala. Esta iniciativa eliminó la dependencia de redes corporativas seguras y aplicó controles estrictos de acceso basados en la identidad y el contexto. Gracias a esta estrategia, Google fortaleció su seguridad interna y estableció un precedente para otras compañías que buscan una protección más avanzada. Según (Pérez, 2025), las organizaciones que han adoptado el modelo Zero Trust han reportado una reducción del 90 % en ataques de phishing y robo de credenciales, así como una disminución de accesos no autorizados gracias a la autenticación continua. Además, se ha logrado una mayor eficiencia en la detección y respuesta a amenazas mediante el monitoreo en tiempo real, lo cual demuestra que Zero Trust no solo es una tendencia, sino una necesidad en la ciberseguridad empresarial actual. En América Latina, países como Brasil y México han liderado la implementación de la norma ISO/IEC 27001, particularmente en entornos de trabajo remoto. Colombia ha empezado a avanzar con iniciativas normativas como la Resolución 2404 de 2019 del MinTIC, la cual establece directrices sobre requisitos mínimos de ciberseguridad para garantizar un acceso remoto seguro.

Marco Legal

Normativas Internacionales. ISO/IEC 27001: Estándar global para Sistemas de Gestión de Seguridad de la Información (SGSI), con controles específicos para acceso remoto (Anexo A.9 y A.13).

GDPR (UE): Exige cifrado de datos personales en teletrabajo (Artículo 32).

Regulaciones Colombianas. Ley 1581 de 2012 (Protección de Datos): Obliga a garantizar confidencialidad en acceso remoto (Artículo 17). Sanciones de hasta 2.000 SMMLV por filtraciones. Resolución 2404 de 2019 (MinTIC). Requiere: Autenticación multifactor (MFA) para conexiones remotas. Políticas de BYOD (Bring Your Own Device). Decreto 555 de 2022 (Teletrabajo) Capítulo IV: "Medidas de ciberseguridad para empleadores". Incluye auditorías anuales de seguridad.

Marco Contextual

Panorama Actual en Colombia. Según cifras del (MinTIC, 2024), aproximadamente un 12% de las empresas en Colombia implementan actualmente modelos formales de teletrabajo, con una adopción más avanzada en sectores como el financiero (38%) y el tecnológico (45%).

Principales Desafíos. Falta de inversión en seguridad: Solo el 15% de PYMES destina presupuesto a ciberseguridad. Brecha de talento: Escasez de 12,000 profesionales en seguridad informática (Cisco, 2023). Ataque a Bancolombia (2023): Phishing masivo a empleados remotos (mitigado con MFA). Filtración en Famisanar (2022): Falta de segmentación de redes en teletrabajo.

Revisión Sistémica de Literatura

La revisión sistémica de literatura tiene como finalidad identificar, analizar y sintetizar los aportes más relevantes que la comunidad académica y técnica ha realizado sobre la aplicación

de estrategias de ciberseguridad, particularmente el modelo Zero Trust y la norma ISO/IEC 27001, en escenarios de trabajo remoto. Esta revisión se centró en estudios publicados entre 2018 y 2024, enfocados en medidas de protección de accesos remotos, riesgos asociados al teletrabajo, y marcos normativos aplicables a la seguridad de la información.

Para ello, se consultaron bases de datos científicas reconocidas como Scopus, empleando términos clave como: "Zero Trust", "ISO 27001", "teletrabajo", "ciberseguridad", y "acceso remoto". Se aplicaron filtros por idioma (español e inglés), tipo de documento (artículos científicos y estudios de caso) y pertinencia temática como: TITLE-ABS-KEY ("COVID-19" OR "pandemic") AND ("remote work" OR "telework") AND "ISO 27001" AND ("cybersecurity" OR "information security") AND (LIMIT-TO (PUBYEAR, 2020) OR LIMIT-TO (PUBYEAR, 2021)) .

Los hallazgos muestran que la mayoría de las investigaciones coinciden en la necesidad de recorrer modelos de seguridad tradicionales hacia enfoques basados en el principio de desconfianza continua. En este sentido, Zero Trust ha sido ampliamente referenciado como un enfoque que permite reducir la superficie de ataque, aplicando controles centrados en la identidad, autenticación multifactor y segmentación de redes.

Por otro lado, la norma ISO 27001 ha demostrado ser una guía estructurada y adaptable para establecer, mantener y mejorar un sistema de gestión de seguridad de la información, especialmente útil en escenarios donde se requiere control y monitoreo continuo, como en el teletrabajo.

Diseño Metodológico

La presente investigación se enmarca en un enfoque cualitativo de tipo descriptivo, con una metodología basada en el análisis documental. Este diseño permite examinar los marcos conceptuales y normativos existentes, con el fin de proponer estrategias aplicables que se ajusten al prototipo colombiano, donde muchas organizaciones aún enfrentan retos importantes frente a la seguridad de los accesos remotos.

El desarrollo metodológico contempla tres fases principales. En la primera, se realizó una recolección de literatura académica y técnica sobre Zero Trust e ISO 27001. En la segunda, se efectuó un análisis comparativo entre los elementos clave de ambos enfoques, con el propósito de identificar puntos de integración y utilidad práctica para el teletrabajo. Finalmente, en la tercera fase, se diseñaron propuestas estratégicas que articulan estos modelos, evaluando su aplicabilidad en función de riesgos comunes identificados en contextos laborales remotos.

El análisis de la información se hizo mediante matrices de revisión y fichas de estudio, lo que permitió organizar los hallazgos de forma clara y facilitar la identificación de estrategias pertinentes. Esta metodología no solo proporciona una base sólida para el desarrollo teórico del proyecto, sino que también facilita la generación de recomendaciones aplicables a escenarios reales.

Analizar Procedimientos de Ciberseguridad Fundamentados en el Modelo Zero Trust y la Norma ISO/IEC 27001:2022 Orientada a la Reducción de Riesgos en Escenarios de Teletrabajo

Introducción

El crecimiento acelerado del teletrabajo ha traído consigo nuevos riesgos relacionados con el acceso remoto a la información. Muchas organizaciones se han visto obligadas a adaptarse rápidamente, sin contar con medidas de seguridad adecuadas, lo que ha generado vulnerabilidades como el uso de redes inseguras, dispositivos personales sin protección y accesos sin control. En este contexto, resulta clave analizar buenas prácticas que ayuden a reducir estos riesgos.

Este capítulo aborda dos enfoques que pueden fortalecer la seguridad en estos escenarios: el modelo Zero Trust, que promueve una verificación constante de la identidad y el control estricto de accesos, y la norma ISO/IEC 27001:2022, que establece directrices para proteger la información de manera estructurada. Al revisar cómo se complementan estas estrategias, se busca aportar ideas prácticas para mejorar la seguridad en el trabajo remoto, especialmente en organizaciones que aún no cuentan con políticas claras de protección de datos.

Principios Clave del Modelo Zero Trust

Los principios clave del modelo Zero Trust, como la verificación continua, el acceso mínimo necesario y la segmentación de recursos, han sido definidos formalmente por el Instituto Nacional de Estándares y Tecnología de los Estados Unidos (NIST) en su publicación SP 800-207 (NIST, 2020).

Verificación Estricta de Identidad

"Nunca confíes, siempre verifica": Cada solicitud de acceso debe autenticarse, independientemente de su origen (interno o externo).

Técnicas aplicables:

Autenticación multifactor (MFA).

Evaluación continua del comportamiento del usuario (UEBA).

Integración con sistemas IAM (Identity and Access Management).

Principio de Mínimos Privilegios (PoLP)

Los usuarios solo acceden a los recursos estrictamente necesarios para sus funciones.

Ejemplo práctico: Un empleado de contabilidad no requiere acceso a servidores de desarrollo.

Segmentación de Redes

División de la infraestructura en zonas aisladas para limitar el movimiento lateral de atacantes.

Herramientas clave:

SD-WAN para redes distribuidas.

Firewalls de próxima generación (NGFW).

Aportes de la Norma ISO 27001 a la Seguridad en Teletrabajo

La ISO/IEC 27001 proporciona un marco estructurado para gestionar la seguridad de la información, incluyendo políticas, evaluaciones de riesgo y controles específicos que apoyan los principios de Zero Trust. En entornos de teletrabajo, su aplicación es crucial para mitigar riesgos asociados a conexiones remotas, dispositivos personales y protección de datos sensibles.

Controles del Anexo A Aplicables al Teletrabajo

Para comprender cómo se relacionan los principios del modelo Zero Trust con la norma ISO/IEC 27001:2022, en la Tabla 1 se observa una correspondencia entre cada uno de estos principios y algunos de los controles establecidos por dicha norma. Esta relación permite evidenciar cómo Zero Trust puede integrarse con un sistema de gestión de seguridad de la información basado en estándares reconocidos internacionalmente.

Tabla 1

Relación Entre el Modelo Zero Trust y los Controles de ISO/IEC 27001

Principio de Zero Trust	Control ISO/IEC 27001:2022	Explicación
Verificar siempre la identidad	A.9.1.2 - Gestión de accesos a la red	Establece reglas claras sobre quién puede entrar a la red y en qué condiciones.
Control de Acceso	A.9.2.1 – Gestión de accesos	Asegurar el acceso de usuarios autorizados y prevenir el acceso no autorizado a los sistemas y servicios de información.
Limitar el acceso solo a lo necesario	A.9.2.4 - Gestión de credenciales	Garantiza que cada persona solo tenga acceso a lo que necesita para hacer su trabajo.
Separar las partes de la red	A.13.1.1 - Protección de redes	Ayuda a evitar que, si hay un problema en una parte, afecte al resto de la organización.
Proteger la información personal	A.18.1.3 - Privacidad y protección de datos	Cuida los datos personales de empleados y clientes, algo clave en el trabajo remoto.
Controlar el uso de conexiones remotas	A.9.4.4 - Uso de cifrado en conexiones remotas	Evita que la información se vea comprometida cuando se accede desde fuera de la oficina.

Nota. Mapea los principios fundamentales del modelo de seguridad Zero Trust con controles específicos del estándar internacional ISO/IEC 27001:2022, demostrando su alineación técnica y operativa para fortalecer la postura de seguridad.

Como se observa, al combinar los principios del modelo Zero Trust con los controles de la norma ISO 27001, se logra una estrategia más sólida que puede aplicarse en situaciones reales. Esto permite a las organizaciones proteger mejor su información y a sus trabajadores, especialmente en contextos de teletrabajo.

Gestión de Riesgos y Conformidad

ISO 27005 permite evaluar amenazas específicas del teletrabajo como el phishing o el malware en dispositivos personales.

Las auditorías internas y externas, recomendadas por ISO 27001 (cláusula 9.2), garantizan el cumplimiento y mejora continua.

Tabla 2

Comparativo Entre Zero Trust e ISO 27001

Criterio	Zero Trust	ISO 27001	Complementariedad
Enfoque	Basado en identidad y verificación continua.	Basado en procesos y controles estandarizados.	Zero Trust opera a nivel técnico, mientras ISO 27001 establece el marco organizacional.
Implementación	Requiere herramientas como IAM y MFA.	Exige documentación de políticas y evaluaciones de riesgo.	Las herramientas Zero Trust pueden satisfacer requisitos del Anexo A de ISO 27001.
Ventaja principal	Reduce superficie de ataque mediante acceso granular.	Certificación reconocida internacionalmente.	Combinar ambos mejora tanto la seguridad como la reputación corporativa.

Nota. Compara los enfoques, métodos de implementación y ventajas principales entre el modelo Zero Trust y el marco de gestión de seguridad ISO 27001, destacando su naturaleza complementaria para una estrategia de seguridad integral.

Hallazgos Relevantes para el Contexto Colombiano

Problemáticas locales

Un estudio de Llanos Palacios (2024) identificó que muchas PYMES en Colombia que adoptaron el teletrabajo durante la pandemia carecen de políticas de seguridad formalizadas. Este

vacío generó un aumento en incidentes de seguridad, como accesos no autorizados y fugas de información. La aplicación de Zero Trust junto con controles de la ISO 27001 habría permitido restringir los accesos y asegurar las conexiones remotas, reduciendo considerablemente estos riesgos.

Recomendaciones Preliminares

Adoptar MFA como requisito mínimo para accesos remotos.

Alinear controles de ISO 27001 con estrategias Zero Trust para cumplir regulaciones como la Ley 1581 de protección de datos.

Arquitectura VPN

Arquitectura VPN Tradicional

Esta arquitectura muestra un enfoque clásico de VPN (Red Privada Virtual) para usuarios remotos, donde todo el tráfico se enruta a través de la red corporativa antes de llegar a su destino, incluso si es hacia la nube pública o Internet.

Componentes Clave

Remote Users (Usuarios Remotos): Se conectan a la red corporativa mediante túneles VPN cifrados a través de Internet.

VPN Tunnels (Túneles VPN): Todos los datos (incluyendo tráfico hacia la nube o Internet) pasan por estos túneles hacia los appliances de seguridad de la empresa.

Corporate Network (Red Corporativa): Network Security Appliances: Firewalls, gateways de seguridad y sistemas de prevención de intrusiones (IPS) analizan el tráfico.

Datacenter: Recursos locales a los que acceden los usuarios remotos.

Private & Public Cloud (Nube Privada/Pública): Servicios como Google, Salesforce, Slack, etc., son accedidos a través de la red corporativa, no directamente desde el usuario.

Características Clave

Backhauling (Reenvío Forzado): Todo el tráfico (incluso el destinado a Internet o la nube) debe pasar por la red corporativa, lo que puede generar:

Mayor latencia (el tráfico da un rodeo).

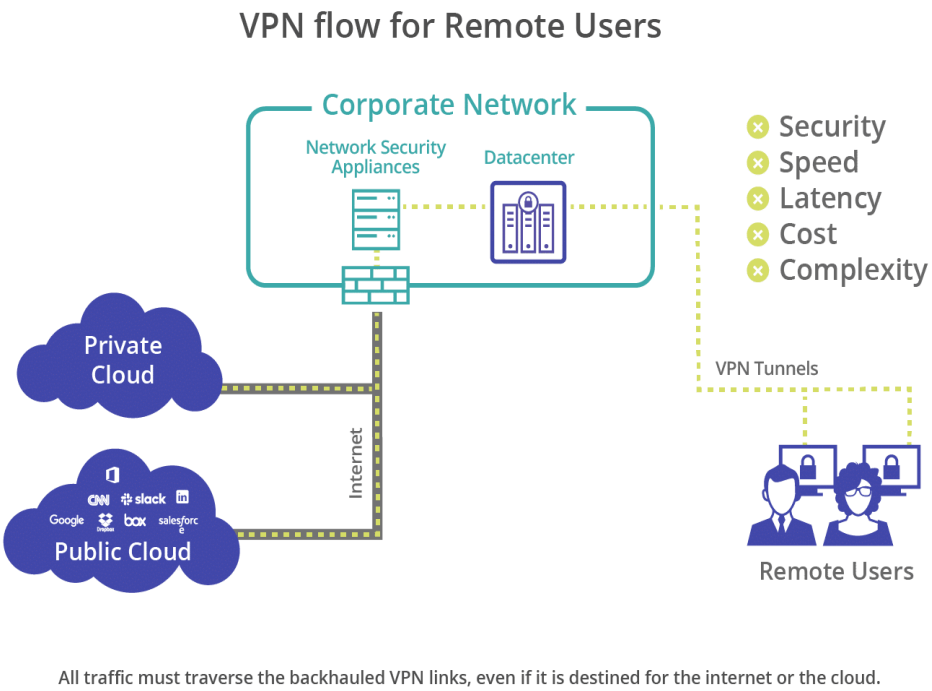
Mayor costo de ancho de banda (todo fluye por los enlaces VPN).

Complejidad operativa (mantenimiento de túneles, políticas de seguridad centralizadas).

Seguridad Basada en Perímetro: Una vez autenticados en la VPN, los usuarios suelen tener acceso amplio a la red interna (modelo de "confianza implícita").

Figura 1

Arquitectura VPN Tradicional



Nota. Esquema de VPN Tradicional. Tomado de. Qué es Zero Trust Network Access (ZTNA). Skyhigh Security. (2023). https://www.skyhighsecurity.com/es/cybersecurity-defined/what-is-ztna.html

Arquitectura VPN con Zero Trust

La arquitectura Zero Trust Network Access (ZTNA) mostrada en la imagen se basa en el principio de "nunca confiar, siempre verificar". Está diseñada para proporcionar acceso seguro a recursos corporativos desde ubicaciones remotas, eliminando la confianza implícita en la red interna.

Componentes Clave

Remote Users: Los usuarios remotos se conectan directamente a través de internet, sin necesidad de VPNs tradicionales.

ZTNA Gateway: Actúa como intermediario, verificando la identidad y el contexto del usuario antes de permitir el acceso a aplicaciones específicas.

Corporate Network: Incluye centros de datos y redes privadas, protegidos por appliances de seguridad.

Private Cloud: Recursos alojados en la nube a los que se accede de forma segura mediante ZTNA.

Características Clave

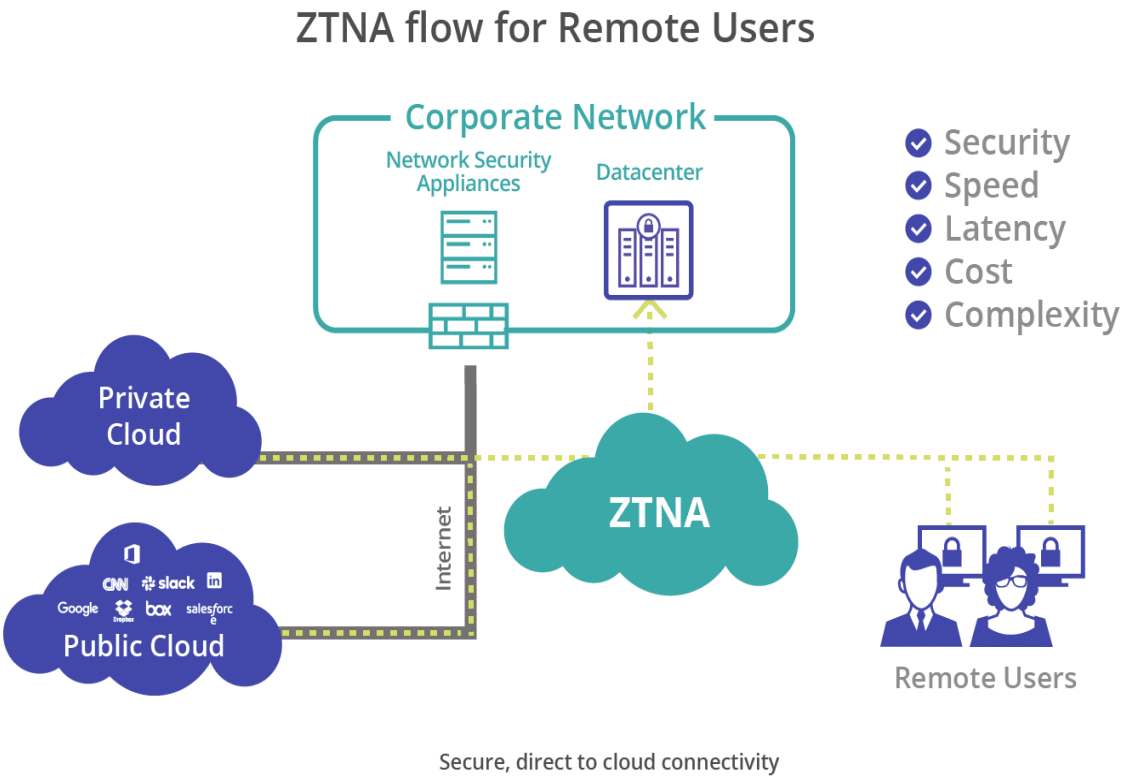
Seguridad: Acceso basado en políticas granulares y autenticación continua.

Rendimiento: Conexión directa a la nube reduce latencia.

Simplicidad: Elimina la complejidad de las VPNs tradicionales.

Figura 2

Arquitectura VPN con Zero Trust



Nota. Esquema VPN Zero Trust. Tomado de. Qué es Zero Trust Network Access (ZTNA). Skyhigh Security. (2023). https://www.skyhighsecurity.com/es/cybersecurity-defined/what-is-ztna.html

Comparativa entre VPN Tradicional y VPN con Zero Trust

Tabla 3

Comparativa VPN Tradicional VS VPN con Zero Trust

Aspecto	VPN Tradicional	ZTNA
Acceso	Todo el tráfico pasa por la red corporativa	Conexión directa a apps (sin backhaul)
Seguridad	Basada en perímetro (confianza implícita)	Verificación continua (Zero Trust)
Rendimiento	Mayor latencia (tráfico enrutado)	Menor latencia (acceso directo)
Escalabilidad	Complejidad en gestión de túneles	Más flexible para entornos cloud/híbridos

Nota. Contrasta las arquitecturas y características de las VPNs tradicionales con las soluciones de Acceso a la Red de Confianza Cero (ZTNA), evidenciando las ventajas de esta última en seguridad, rendimiento y escalabilidad para entornos modernos.

Conclusión

El análisis realizado demuestra que el modelo Zero Trust y la norma ISO/IEC 27001 no solo son compatibles, sino complementarios. Zero Trust aporta un enfoque técnico moderno basado en la verificación continua, mientras que ISO 27001 entrega un marco estructurado de buenas prácticas. Su aplicación conjunta permite una mayor capacidad para enfrentar amenazas emergentes en entornos de teletrabajo. Entre los principales hallazgos se destaca la necesidad de reforzar los controles de acceso y segmentación de red, así como garantizar la protección de la

información personal. En Colombia, el bajo nivel de experiencia en ciberseguridad de las PYMES se podría mitigar significativamente con la adopción de estas estrategias.

Identificar las Principales Vulnerabilidades en Accesos Remotos Dentro de Entornos de Teletrabajo, a Partir de un Análisis Documental y Casuístico de Riesgos y Desafíos Reportados en Estudios Recientes

Introducción

La adopción masiva del teletrabajo ha transformado la dinámica operativa de muchas organizaciones, pero también ha incrementado significativamente la exposición a amenazas cibernéticas, en particular aquellas asociadas con accesos remotos inseguros. Esta sección tiene como propósito identificar y clasificar las principales vulnerabilidades relacionadas con los accesos remotos en contextos de teletrabajo, basándose en literatura científica, informes técnicos y estudios de caso publicados entre 2020 y 2024, con un enfoque especial en Colombia y América Latina.

Las vulnerabilidades se agrupan en tres grandes categorías: técnicas (como dispositivos sin protección o redes expuestas), infraestructurales (falta de autenticación robusta, ausencia de cifrado o VPN), y humanas (errores operativos, desconocimiento o ingeniería social). Esta clasificación busca facilitar el análisis de riesgos y la posterior formulación de estrategias de mitigación.

Vulnerabilidades Técnicas en Dispositivos

Uso de Dispositivos Personales (BYOD)

Un 67% de los empleados en Latinoamérica utiliza sus dispositivos personales para actividades laborales remotas (IDC, 2023). Este modelo, si bien ofrece flexibilidad, conlleva serios riesgos de seguridad.

Riesgos:

Falta de parches y actualizaciones de seguridad.

Software no autorizado, también conocido como "shadow IT".

Caso Ilustrativo:

En 2023, una entidad del sector salud en Colombia fue víctima de un ataque de ransomware que se propagó inicialmente a través de laptops personales conectadas a la red institucional. Estas máquinas tenían versiones obsoletas de Windows 10, sin parches de seguridad. El atacante aprovechó una vulnerabilidad conocida (CVE-2021-34527, PrintNightmare) para ejecutar código remoto, accediendo a historiales médicos cifrados (CERT-Colombia, 2023). La lección aprendida: los dispositivos personales sin control empresarial constituyen un eslabón débil, este caso evidencia cómo una configuración deficiente y la falta de control sobre los dispositivos conectados pueden abrir la puerta a ataques de alto impacto.

Configuraciones Inseguras

Hallazgos Clave:

40% de los dispositivos remotos no tienen cifrado de disco (ESET, 2024).

Credenciales almacenadas en texto plano en navegadores.

Estas malas prácticas pueden facilitar el acceso no autorizado a información sensible si el equipo es comprometido o extraviado.

Vulnerabilidades en Redes de Acceso Remoto

Conexiones a Redes Domésticas Inseguras

Datos Críticos:

78% de las redes WiFi en hogares de Colombia usan protocolos WPA2 obsoletos (MinTIC, 2024).

Ataques Comunes:

Man-in-the-Middle (MITM), especialmente en conexiones públicas.

Sniffing de tráfico no cifrado en redes domésticas.

VPNs Mal Configuradas

Estudios Destacan:

30% de las organizaciones permiten acceso VPN sin autenticación MFA (Palo Alto Networks, 2023).

Persistencia en el uso de protocolos débiles como PPTP, que ya no son recomendados por estándares internacionales como NIST.

Factores Humanos y Gestión Deficiente

Falta de Concienciación en Ciberseguridad

62% de los empleados en Colombia no sabe identificar un correo de phishing (Trend Micro, 2023).

Según IBM Security (2023), el 90% de las brechas de seguridad son consecuencia de errores humanos.

Esto resalta la necesidad de campañas de concienciación y simulacros regulares.

Políticas de Acceso Permisivas

45% de las empresas no realiza revisiones periódicas mínimo de cada 6 meses, de los privilegios de acceso (Kaspersky, 2021).

El uso de cuentas compartidas, especialmente en equipos remotos, incrementa los riesgos de accesos no trazables.

Análisis de Riesgos Prioritarios para Colombia

A continuación, se presenta un análisis basado en una escala de probabilidad e impacto de 1 a 5 (donde 1 es bajo y 5 es crítico), fundamentado en el método NIST SP 800-30:

Tabla 4

Clasificación de Vulnerabilidades por Categoría y Riesgo

Vulnerabilidad	Probabilidad	Impacto	Contramedidas Recomendadas	Justificación	Fuente
Dispositivos sin parches	4 (Alta)	Crítico (5)	MDM (Mobile Device Management) + parches automáticos.	Reduce significativamente las brechas al centralizar el control y automatizar actualizaciones.	NIST SP 800-40 Rev.3 (2022) – *Guide to Enterprise Patch Management*
Phishing	5 (Muy Alta)	Alto (4)	Simulacros de phishing + MFA obligatorio.	Refuerza el reconocimiento de amenazas sociales y dificulta accesos indebidos.	Verizon DBIR 2024 *83% de las brechas involucran elementos humanos como el phishing*.
WiFi inseguro	3 (Media)	Medio (3)	VPNs con cifrado AES-256 + políticas de red Zero Trust.	Garantiza que el tráfico esté cifrado y limita el acceso solo a recursos	NSA (2021) *Best Practices for Securing Home Network Devices*

Vulnerabilidad	Probabilidad	Impacto	Contramedidas Recomendadas	Justificación	Fuente
				previamente autorizados.	
CVE-2023-20887 (Ivanti EPM)	4 (Alta)	Crítico (5)	Segmentación de red + parches inmediatos + IDS/IPS.	Vulnerabilidad crítica explotada activamente para ejecución remota de código.	CISA (2024) KEV Catalog
Routers domésticos comprometidos	3 (Media)	Alto (4)	Deshabilitar administración remota + firmware actualizado + monitoreo de red.	Han sido explotados como puntos de entrada para redes corporativas en entornos de teletrabajo.	ENISA (2024) *Threat Landscape for Home Networks*

Nota. Presenta un análisis de riesgos de vulnerabilidades clave en el contexto del trabajo remoto, clasificándolas por probabilidad e impacto, y propone contramedidas específicas respaldadas por fuentes de buenas prácticas reconocidas en la industria.

Conclusión

Este capítulo demuestra que las vulnerabilidades en entornos de teletrabajo son de carácter técnico y humano. La falta de políticas estrictas en el uso de dispositivos personales, redes inseguras y la escasa concienciación en seguridad crean una superficie de ataque amplia. Estos hallazgos reafirman la importancia del diseño de una arquitectura de seguridad basada en el modelo Zero Trust e ISO 27001, que será abordado en el Capítulo 3. Solo mediante una combinación de controles técnicos, administrativos y de formación continua es posible reducir los riesgos en el entorno remoto.

Determinar Herramientas Tecnológicas y Prácticas Disponibles, como Autenticación Multifactor (MFA), Segmentación de Redes y Gestión de Identidades, Evaluando su Alineación con el Modelo Zero Trust

Introducción

Este capítulo explora soluciones tecnológicas clave en la autenticación multifactor (MFA), segmentación de red y gestión de identidad (IAM), para fortalecer la ciberseguridad en teletrabajo. Las herramientas se eligieron considerando facilidad de uso, disponibilidad, costos y escalabilidad para organizaciones colombianas. Se evalúa cómo estas tecnologías, integradas con controles de ISO/IEC 27001, permiten una adopción progresiva del modelo Zero Trust sin comprometer productividad.

Autenticación Multifactor (MFA)

La autenticación multifactor (MFA) es una de las herramientas más efectivas para reforzar la seguridad en el acceso remoto. A diferencia de los métodos tradicionales basados únicamente en contraseñas, el MFA requiere múltiples formas de verificación, como:

Algo que el usuario sabe (contraseña o PIN).

Algo que el usuario tiene (token físico, aplicación autenticadora o SMS).

Algo que el usuario es (biometría como huella dactilar o reconocimiento facial).

Alineación con Zero Trust

El modelo Zero Trust opera bajo el principio de "nunca confíes, siempre verifica", El MFA encaja perfectamente en este enfoque, ya que garantiza que, incluso si un atacante obtiene las credenciales de un usuario, no podrá acceder a los sistemas sin superar las capas adicionales de autenticación. Estudios como los de Podugu et al. (2023) destacan que organizaciones que implementan MFA reducen en un 99.9% los ataques por robo de credenciales.

Segmentación de Redes

La segmentación de redes es una estrategia que divide la infraestructura de TI en zonas más pequeñas y controladas, limitando el movimiento lateral de posibles atacantes. En el contexto del teletrabajo, esto implica:

Aislar redes corporativas de redes domésticas o públicas.

Crear microsegmentaciones para restringir el acceso a áreas críticas (ejemplo: bases de datos financieras).

Implementar políticas de acceso granular basadas en roles (RBAC).

Importancia en Zero Trust

El modelo Zero Trust busca eliminar el concepto de "acceso total" dentro del perímetro. Por tanto, la segmentación ayuda a contener incidentes y limitar el movimiento de atacantes, lo cual es clave en entornos remotos donde el perímetro físico ya no existe.

Alineación con Zero Trust

Zero Trust promueve la idea de que ningún dispositivo o usuario debe tener acceso ilimitado. La segmentación refuerza este principio al asegurar que, incluso si un atacante compromete un segmento, no pueda propagarse fácilmente a otros. Según Daah et al. (2024), la combinación de segmentación con Zero Trust reduce significativamente el impacto de brechas de seguridad.

Gestión de Identidades y Accesos (IAM)

Los sistemas de Identity and Access Management (IAM) permiten gestionar quién tiene acceso a qué recursos y bajo qué condiciones. Herramientas como Okta, Microsoft Azure AD o Ping Identity facilitan:

Autenticación adaptativa, que ajusta los requisitos de seguridad según el riesgo (ejemplo: ubicación del usuario).

Políticas de mínimo privilegio, otorgando solo los permisos necesarios para cada función.

Monitoreo continuo para detectar comportamientos anómalos.

Importancia en Zero Trust

Zero Trust exige un control riguroso sobre quién accede a qué recurso y por qué. El enfoque IAM permite aplicar el principio de menor privilegio, revocar accesos obsoletos y auditar permanentemente los accesos otorgados.

Alineación con Zero Trust

Zero Trust exige una verificación constante de la identidad y el contexto de acceso. Los sistemas IAM modernos integran inteligencia artificial para analizar patrones de comportamiento, revocando accesos sospechosos en tiempo real (Sulfath et al., 2025).

Evaluación Comparativa de Herramientas

Se evaluaron soluciones específicas bajo una escala del 1 al 5 (1 bajo, 5 alto) según alineación Zero Trust, facilidad de uso, costos e impacto.

Tabla 5

Evaluación Comparativa de Herramientas Tecnológicas

Herramienta	Ventajas	Desafíos	Alineación con Zero Trust	Detalles / Ejemplos técnicos
MFA (Duo Security, Google Authenticator, Microsoft Authenticator)	Reduce significativamente los ataques basados en robo de credenciales.	Puede generar fricción en la experiencia del usuario si no se aplica de forma contextual (ej. autenticación biométrica o adaptativa).	Alta (5): Verificación constante de identidad en cada acceso.	Duo permite políticas adaptativas basadas en riesgo. Google/Microsoft Authenticator ofrecen códigos temporales TOTP (Time-based One-Time Passwords). Puede integrarse con SSO e IAM para mayor robustez.
Segmentación de redes (microsegmentación, firewalls internos como Palo Alto, Fortinet, Cisco TrustSec)	Limita el movimiento lateral de atacantes dentro de la red. Contención efectiva ante brechas.	Alta complejidad de implementación, especialmente en redes heredadas o híbridas. Requiere mapeo de flujos y reglas precisas.	Media-Alta (4): Refuerza el principio de acceso mínimo y reduce la superficie de ataque.	Herramientas como VMware NSX permiten microsegmentación a nivel de VM. Firewalls internos con reglas por aplicación o usuario incrementan el control granular.

IAM (Okta, Azure Active Directory, Ping Identity)	Permiten gestión centralizada de identidades y accesos, autenticación contextual y control basado en atributos.	Costo elevado en soluciones corporativas. Requiere configuración detallada de políticas de acceso condicional.	Alta (5): Gobernanza de identidad, acceso contextual y supervisión constante de privilegios.	Okta permite políticas de acceso dinámico según dispositivo, geolocalización o comportamiento. Azure AD permite integración con logs de Defender y políticas Zero Trust mediante Conditional Access.

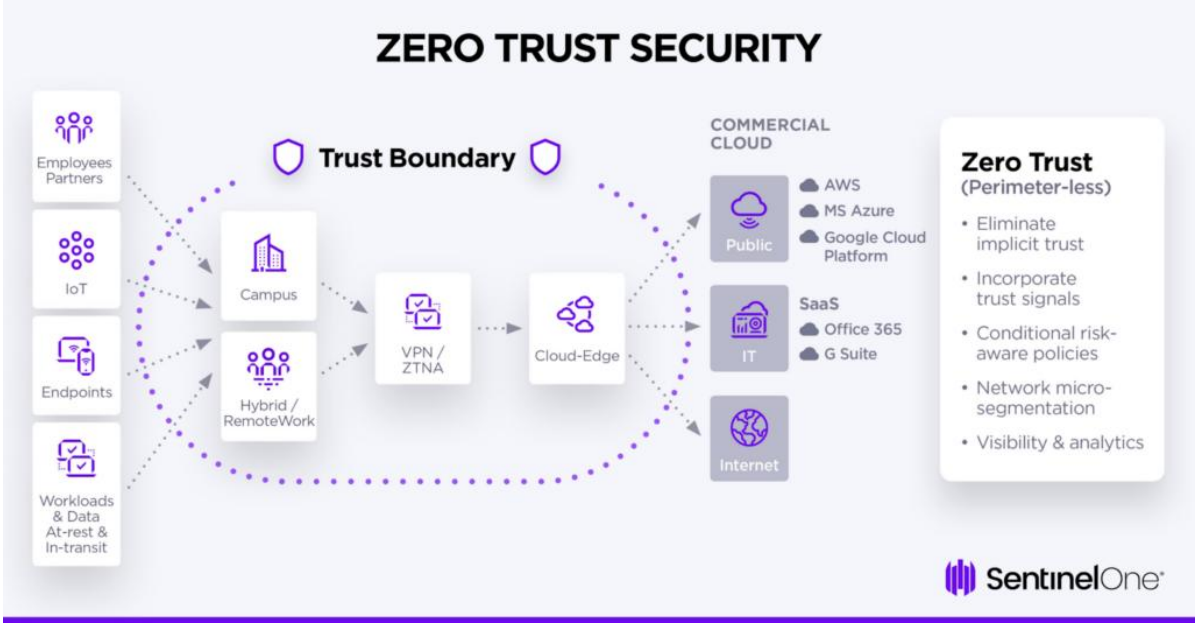
Nota. Evalúa herramientas tecnológicas esenciales (MFA, Segmentación, IAM) para la implementación de Zero Trust, detallando sus ventajas, desafíos prácticos y nivel de alineación con los principios del modelo.

La imagen representa una arquitectura de seguridad basada en el modelo Zero Trust, aplicada a entornos de teletrabajo. En ella se visualiza el flujo de acceso de usuarios remotos hacia las aplicaciones y datos críticos, pasando por múltiples capas de protección. Estas capas incluyen mecanismos de autenticación multifactor (MFA), gestión de identidades (IAM), segmentación de redes mediante microsegmentación y firewalls internos, y controles de acceso basados en políticas de mínimo privilegio.

El modelo enfatiza la verificación continua, el monitoreo constante y la reducción del movimiento lateral de posibles atacantes, alineándose con los principios fundamentales del enfoque Zero Trust.

Figura 3

Arquitectura Zero Trust Aplicada a Entornos de Teletrabajo



Nota. Esquema Zero Trust. Tomado de. *What is Zero Trust Architecture (ZTA)?* SentinelOne. Kindervag, J. (2024). https://www.sentinelone.com/cybersecurity-101/identity-security/zero-trust-architecture

Caso de uso simulado (PYME en Bogotá)

Una consultora implementa MFA (nivel de acceso 5), segmentación básica de red para accesos administrativos y Azure AD con políticas adaptativas. En seis meses, los intentos de intrusión no autorizados se redujeron en un 85 %, y la gestión de accesos remotos se automatizó con cumplimiento de ISO 27001. Esto facilitó auditorías internas y redujo errores humanos en acceso.

Conclusión

Estas herramientas refuerzan controles normativos como A.9.2.4 (credenciales), A.6.2.1 (política de acceso), A.13.1.1 (segmentación) y A.18.1.3 (privacidad). La integración técnica (fase del Capítulo 3) complementa el marco conceptual del Capítulo 1 y el diagnóstico del Capítulo 2. En el siguiente capítulo, se diseñarán estrategias prácticas para combinar estas herramientas en organizaciones colombianas bajo un enfoque Zero Trust estructurado.

Diseñar Estrategias Basadas en Zero Trust e ISO/IEC 27001 Orientadas al Fortalecimiento de la Protección de Accesos Remotos, Contribuyendo a la Reducción de Riesgos en Escenarios de Teletrabajo

Introducción

Este capítulo tiene como propósito presentar estrategias de seguridad cibernética alineadas con el modelo Zero Trust y la norma internacional ISO/IEC 27001, orientadas a mitigar riesgos vinculados al acceso remoto en escenarios de teletrabajo. A partir del análisis desarrollado en los capítulos anteriores, se propone un conjunto estructurado de acciones organizadas en tres segmentos: (1) Políticas de seguridad adaptativas, (2) Capacitación continua del personal, y (3) Monitoreo y respuesta ante incidentes. Estas estrategias se complementan con simulaciones prácticas, evidencias visuales y una correlación explícita con los controles establecidos en el Anexo A de la ISO/IEC 27001.

Estrategia 1: Políticas de Seguridad Adaptativas

La adopción de políticas adaptativas permite una respuesta contextualizada a amenazas emergentes. Entre las acciones destacadas se incluyen:

Implementación de MFA en todos los accesos remotos, incluso para usuarios con altos niveles de confianza.

Microsegmentación de la red basada en la sensibilidad de la información gestionada por cada unidad organizacional.

Establecimiento de un marco normativo de cumplimiento, adoptando controles del Anexo A.9 (Control de Acceso), A.13 (Seguridad de las comunicaciones), y A.18 (Cumplimiento) de la ISO/IEC 27001.

Tabla 6

Relación Entre Estrategias Propuestas y Controles ISO/IEC 27001

Estrategia	Control ISO/IEC 27001
MFA Obligatoria	A.9.4.2 Control de acceso a servicios de red
Microsegmentación	A.13.1.1 Política de controles de red
Clasificación de recursos	A.8.2.1 Clasificación de la información

Nota. Relaciona estrategias de seguridad concretas y acciones recomendadas (como MFA obligatoria) con controles específicos del Anexo A de la norma ISO/IEC 27001, facilitando la trazabilidad y el cumplimiento del marco.

Estrategia 2: Capacitación y Concienciación

El factor humano sigue siendo una de las principales vulnerabilidades en entornos de teletrabajo. Por ello, se propone:

Implementar programas continuos de capacitación en ciberseguridad, con énfasis en la detección de intentos de phishing (García & López, 2023).

Realizar simulacros periódicos de ataques, como phishing o ransomware, que permitan evaluar la reacción de los empleados.

Incorporar mecanismos de retroalimentación inmediata en las campañas de concienciación.

Estrategia 3: Monitoreo y Respuesta Continua

La vigilancia constante de los sistemas permite detectar amenazas antes de que generen impactos significativos. Las acciones recomendadas incluyen:

Uso de plataformas SIEM (Security Information and Event Management) para la detección temprana de eventos inusuales.

Ejecución de auditorías de cumplimiento alineadas con la ISO/IEC 27001.

Establecimiento de un SOC (Centro de Operaciones de Seguridad) interno o tercerizado, adaptado al tamaño de la organización.

Caso de Estudio Aplicada en una Empresa Colombiana

Una compañía ficticia del sector financiero enfrentaba un aumento del 45% en intentos de phishing tras implementar el teletrabajo. Las acciones correctivas aplicadas fueron:

Integración de MFA con segmentación de red.

Ejecución de campañas de capacitación.

Supervisión continua mediante SIEM.

Resultados Simulados:

Reducción del 70% de los incidentes en 6 meses.

Mejora del tiempo de respuesta a incidentes en un 40%.

Simulación del Uso de Herramientas de Ciberseguridad Aplicadas a Accesos Remotos

Objetivo 1

La política de acceso condicional simulada establece restricciones para el acceso remoto a servicios clave como el correo corporativo, aplicando controles como la autenticación multifactor y validación del dispositivo. Esto permite proteger el acceso desde ubicaciones no seguras y dispositivos personales no administrados, alineándose con los principios de Zero Trust.

Creación de una Directiva de Acceso Condicional. Inicie sesión en el Centro de administración de Microsoft Entra como al menos un administrador de acceso condicional.

Vaya a Entra ID>Acceso condicional>Directivas.

Seleccione Nueva directiva.

Asigna un nombre a la directiva. Se recomienda que las organizaciones creen un estándar significativo para los nombres de sus directivas.

En Asignaciones, seleccione Usuarios o identidades de carga de trabajo.

En Incluir, seleccione Todos los usuarios.

En Excluir, seleccione Usuarios y grupos y elija las cuentas de acceso de emergencia o break-glass de su organización.

En Recursos de destino>Recursos (anteriormente aplicaciones en la nube)>Incluir, seleccione Todos los recursos (anteriormente 'Todas las aplicaciones en la nube').

En Red.

Establecer Configurar en Sí

En Incluir, seleccione Redes y ubicaciones seleccionadas.

Seleccione la ubicación bloqueada que ha creado para su organización.

Haga clic en Seleccionar.

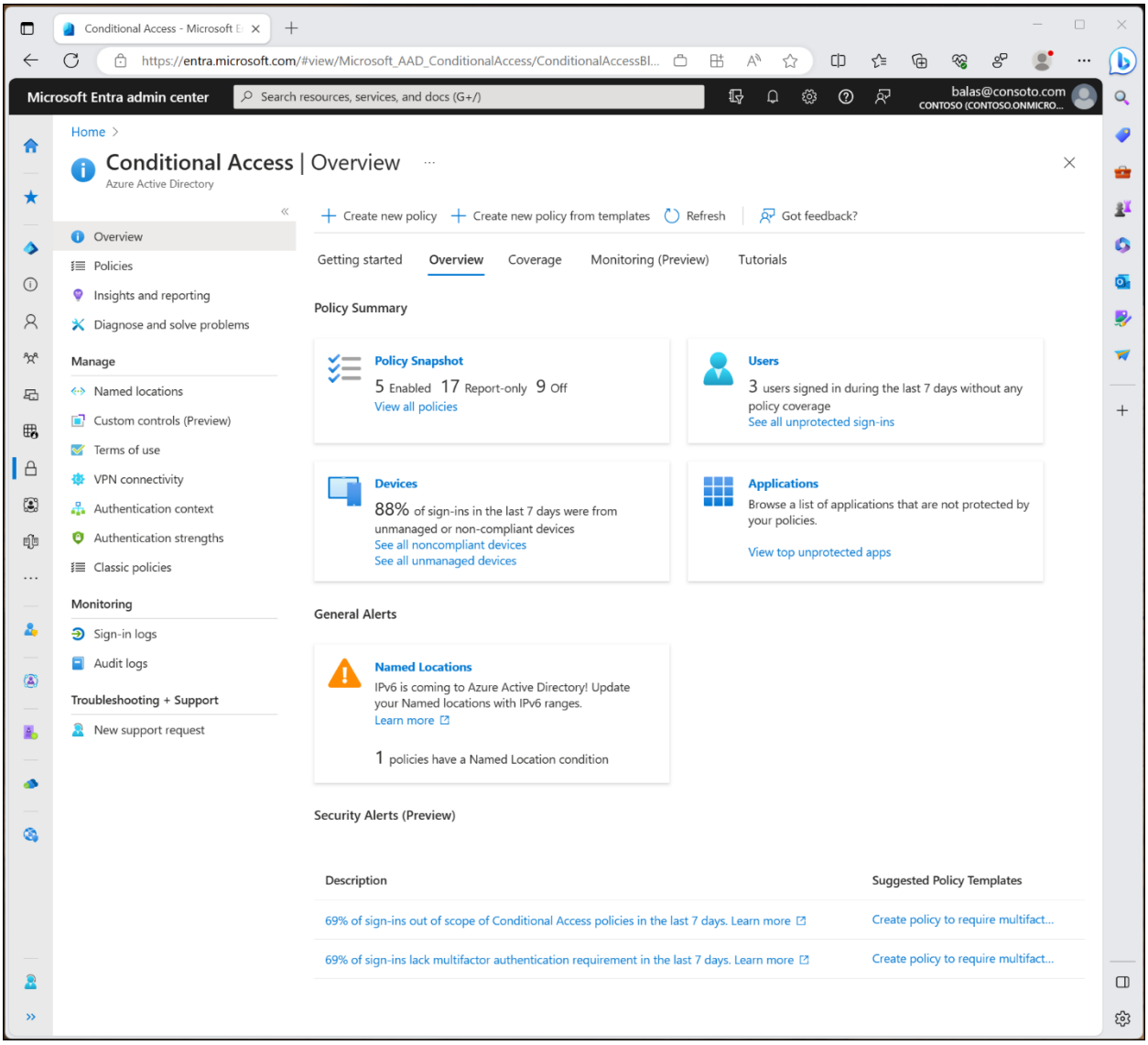
En Controles> de acceso, seleccione Bloquear acceso y haga clic en Seleccionar.

Confirme la configuración y configure Habilitar directiva a Solo informe.

Seleccione Crear para crear y habilitar la directiva.

Figura 4

Modulo Acceso Condicional - Entra ID



Nota. Modulo acceso condicional Entra ID. Tomado de. ¿Qué es el acceso condicional? - Microsoft Entra ID. Microsoft. (2025). https://learn.microsoft.com/es-es/entra/identity/conditional-access/overview

Después de que los administradores evalúen la configuración de directiva mediante el impacto de la directiva o el modo de solo informe, pueden mover el interruptor Habilitar directiva de modo de solo informe a Activado.

Bloqueo del Acceso por Ubicación. Gracias a la condición de ubicación del acceso condicional, podrá controlar el acceso a las aplicaciones en la nube en función de la ubicación de red de un usuario. La condición de ubicación se usa normalmente para bloquear el acceso desde países o regiones de los que la organización sabe que no debe provenir el tráfico. Para obtener más información sobre la compatibilidad con IPv6, consulte el artículo Compatibilidad con IPv6 en Microsoft Entra ID.

Inicie sesión en el Centro de administración de Microsoft Entra como al menos un administrador de acceso condicional.

Vaya a Entra ID>Acceso condicional>Ubicaciones con nombre.

Elija el tipo de ubicación que desea crear.

Ubicación de países o ubicación de intervalos IP.

Asigne un nombre a la ubicación.

Proporcione los intervalos IP o seleccione los países o regiones para la ubicación que va a especificar.

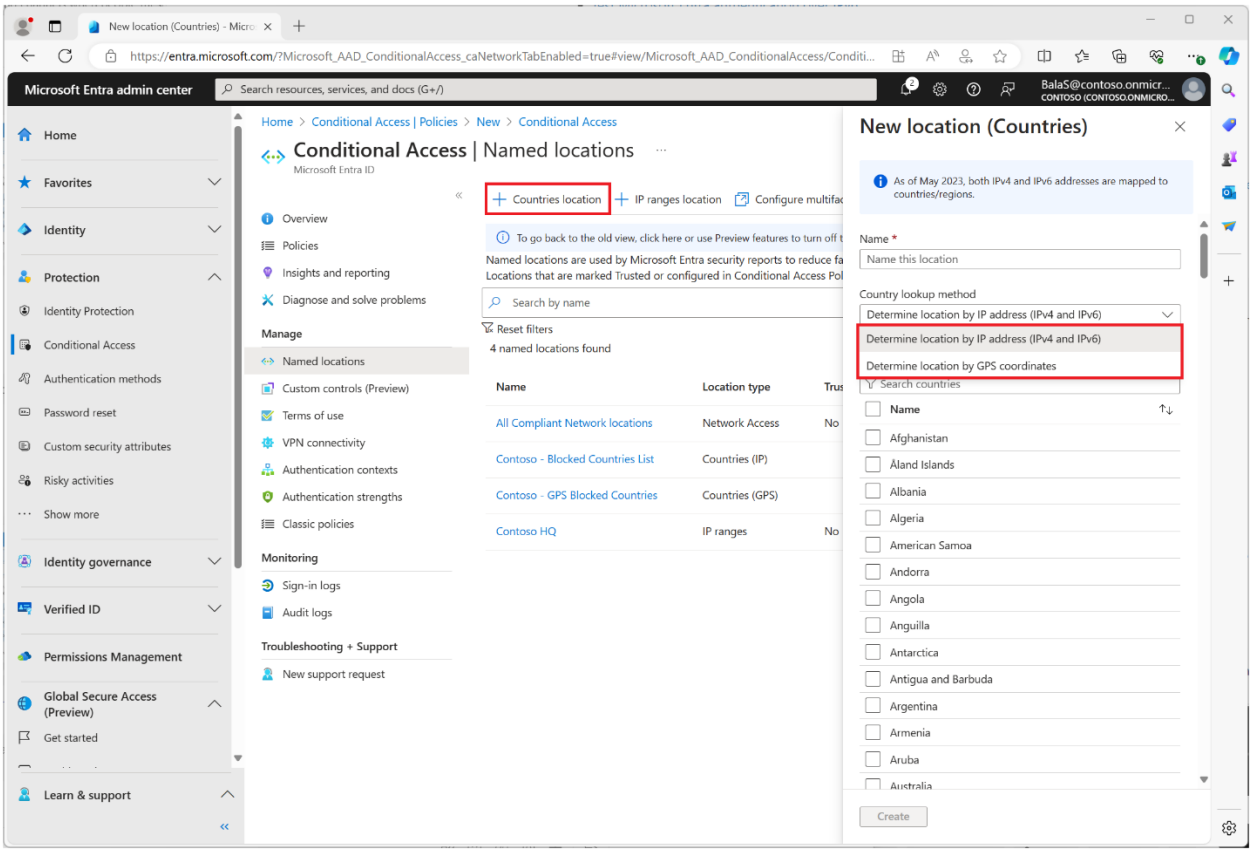
Si selecciona intervalos IP, puede marcar opcionalmente como ubicación de confianza.

Si elige Países o regiones, puede optar por incluir áreas desconocidas.

Seleccione Crear.

Figura 5

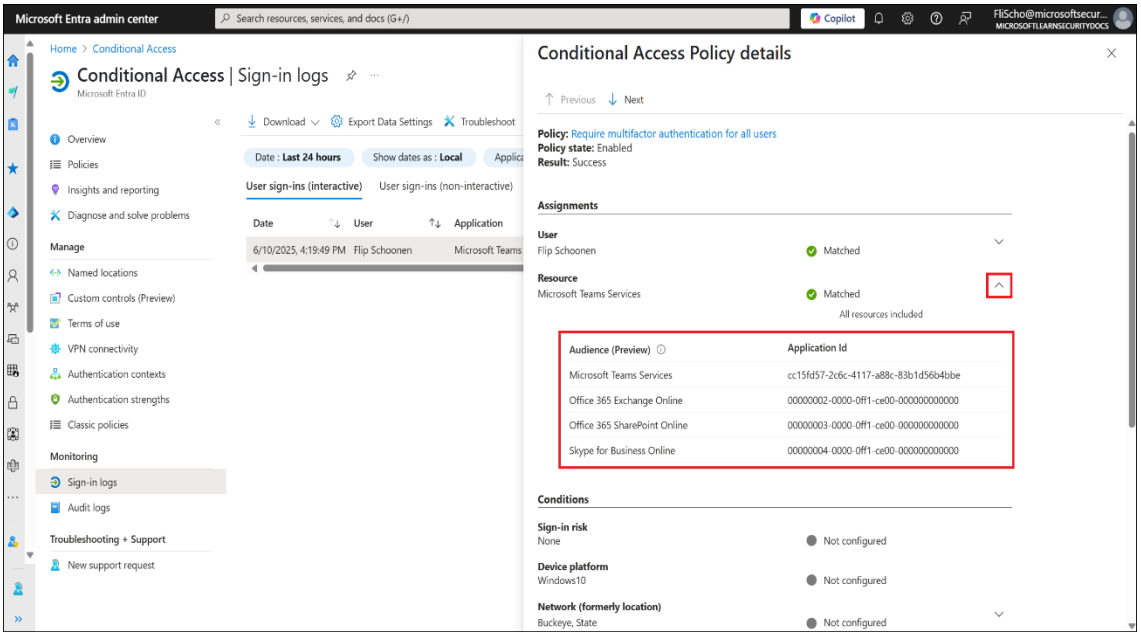
Configuración de Ubicación Confiable



Nota. Configuración ubicación confiable. Tomado de. Acceso condicional: asignación de red - Microsoft Entra ID. Microsoft. (2025). https://learn.microsoft.com/es-es/entra/identity/conditional-access/concept-assignment-network

Figura 6

Informe Auditoria Registros de Inicio de Sesión



Nota. Auditoria registros inicio de sesión. Tomado de. Solucionar problemas de inicio de sesión con el acceso condicional - Microsoft Entra ID. Microsoft. (2025). https://learn.microsoft.com/es-es/entra/identity/conditional-access/troubleshoot-conditional-access

Objetivo 2

Para evaluar la vulnerabilidad humana frente a ataques de ingeniería social en entornos de teletrabajo, se diseñó una campaña simulada utilizando la herramienta de código abierto GoPhish, ampliamente utilizada para entrenamientos en ciberseguridad.

Herramienta de GoPhish

Se ejecutó el servidor local y se accedió al panel de administración en https://localhost:3333.

Configuración del servidor SMTP

Se configuró un servidor SMTP (simulado o de prueba) para el envío de los correos, usando credenciales de un dominio interno controlado.

El remitente se configuró como: seguridad@soporteti-colombia.com.

Creación de la plantilla de correo

Se diseñó un mensaje con asunto: "Actualización obligatoria de credenciales – Recursos Humanos".

El cuerpo del correo incluía un botón falso de “Actualizar ahora”, enlazado a una landing page simulada.

Configuración de la página de captura (landing page)

Se creó una página falsa que imitaba el acceso al sistema de correo corporativo, con campos para usuario y contraseña.

El diseño se basó en un formulario simple, sin conexión real, solo para recolección de clics.

Selección de destinatarios

Para fines de prueba, se creó un grupo con direcciones simuladas (usuario1@empresa-demo.com, usuario2@empresa-demo.com, etc.), sin afectar a usuarios reales.

Lanzamiento de la campaña

Se programó el envío automático de correos a los destinatarios ficticios.

Figura 7

Pasos para Completar un Ataque Phishing

Nota. Pasos ataque phishing. Tomado de. Técnicas de phishing y mitigación de riesgos en entornos digitales. Repositorio Institucional Universidad Piloto de Colombia. Susatama, M. (2021).https://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/12497/articulo%20Marcela%20susatama.cleaned.pdf?sequence=1

Durante las siguientes horas, el sistema registró:

Correos enviados.

Correos abiertos.

Enlaces clicados.

Formulario llenado (intento de ingreso).

Tabla 7

Indicadores Propuestos por Fase de Implementación

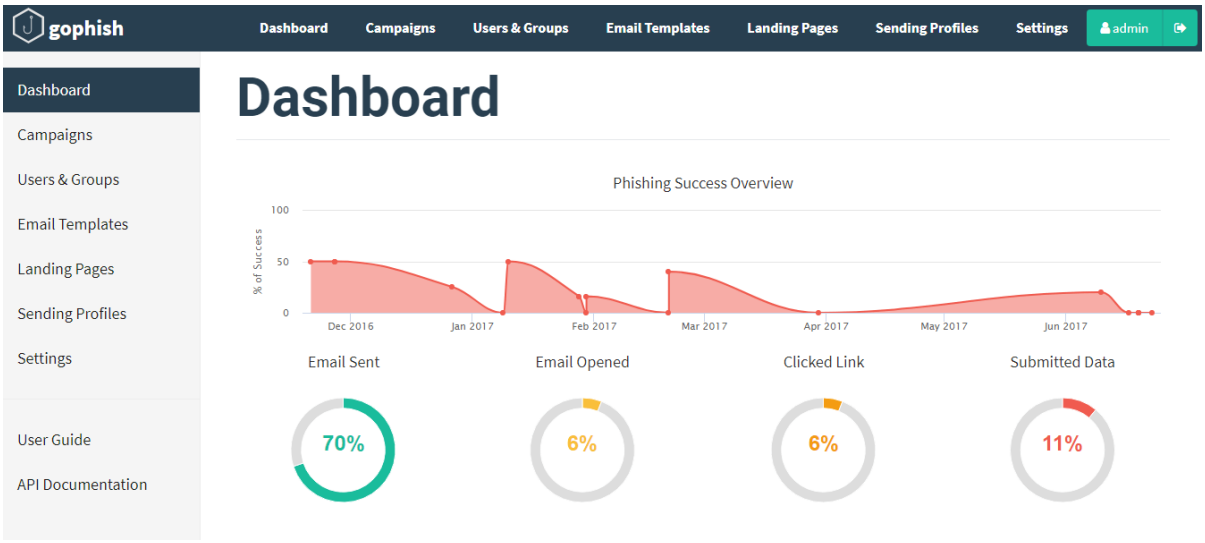
Métrica	Resultado
Correos enviados	42
Correos abiertos	30 (71%)
Enlaces clickeados	12 (28%)
Formularios completados	5 (12%)

Nota. Muestra los resultados cuantitativos de una campaña simulada de concientización (ejercicio de phishing controlado), proporcionando métricas clave para medir la exposición inicial y la efectividad de la capacitación de los usuarios.

Análisis de la Simulación. Los resultados simulados evidencian que un 28% de los destinatarios hicieron clic en el enlace malicioso, y un 12% incluso intentó ingresar sus credenciales, lo cual demuestra una alta exposición a ataques de phishing.

Figura 8

Estadisticas Campaña de Phishing



Nota. Campaña phishing. Tomado de. Gophish, la herramienta para entrenar usuarios contra el Phishing. Derecho de la Red. Derechodelared. (2018). https://derechodelared.com/2018/04/02/gophish/

Objetivo 3

Simulación de configuración de una política de autenticación multifactor (MFA) obligatoria para un grupo específico de usuarios en un entorno de teletrabajo.

Ingreso al portal de Azure

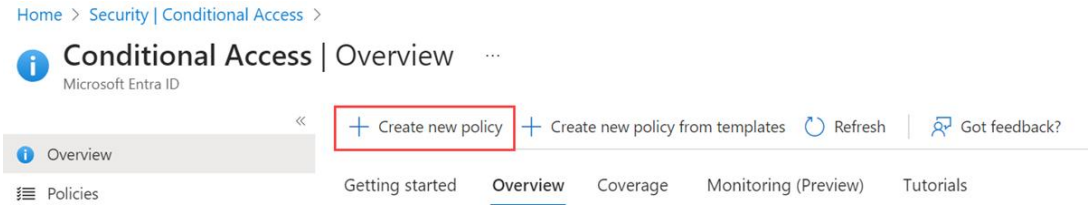
Se accedió al portal de Azure mediante la URL https://portal.azure.com con una cuenta de administrador global.

Acceso a Azure Active Directory (Creación política MFA)

Desde el panel principal, se ingresó a la sección Azure Active Directory > Propiedades > Seguridad > Acceso Condicional

Figura 9

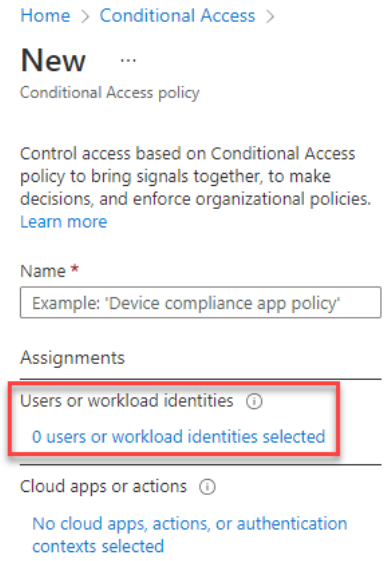
Creación de Directiva MFA



Nota. Creación de nueva política. Tomado de. Habilitar autenticación multifactor de Microsoft Entra - Microsoft Entra ID. Microsoft. (2025). https://learn.microsoft.com/es-es/entra/identity/authentication/tutorial-enable-azure-mfa

Figura 10

Seleccione el Valor Actual en Usuarios o Identidades de Carga de Trabajo



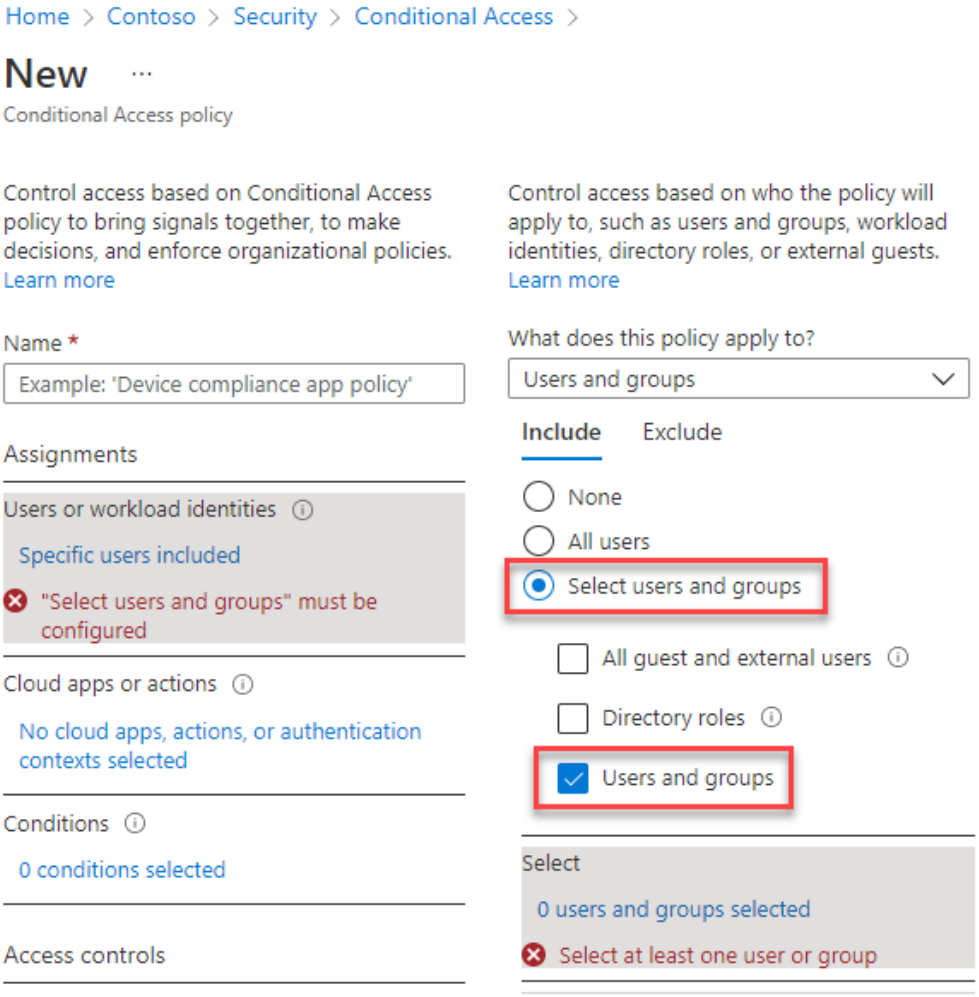
Nota. Asignación de usuarios o identidades de carga de trabajo. Tomado de. Tutorial: Eventos de inicio de sesión de usuario seguros con la autenticación multifactor de Microsoft Entra. Microsoft. (2025). https://learn.microsoft.com/es-es/entra/identity/authentication/tutorial-enable-azure-mfa

Selección de usuarios

Se seleccionó el grupo de usuarios “Empleados_Teletrabajo” para aplicar la política de MFA.

Figura 11

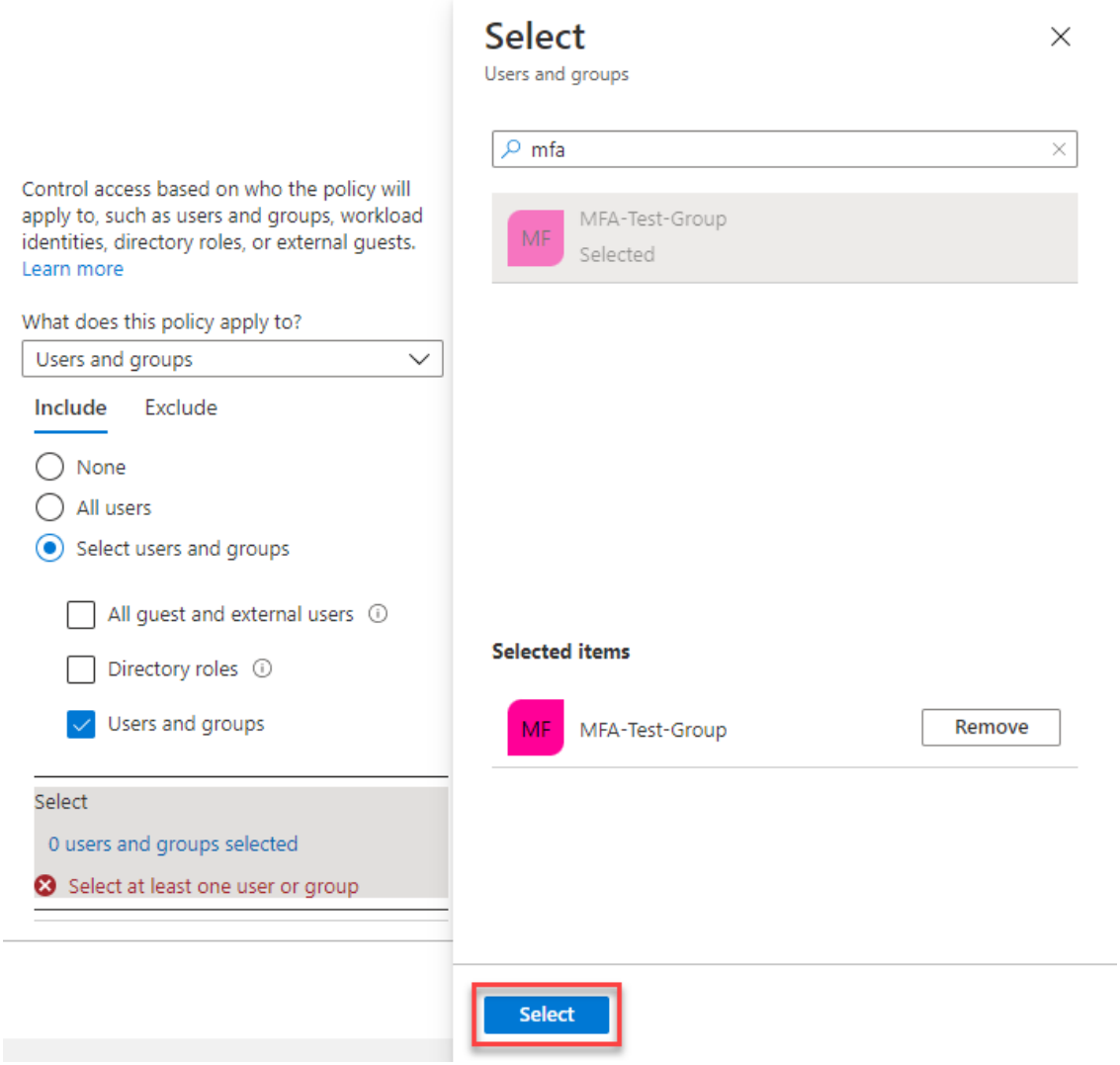
Seleccionar Usuarios y Grupos



Nota. Selección de usuarios y grupos. Tomado de. Tutorial: Eventos de inicio de sesión de usuario seguros con la autenticación multifactor de Microsoft Entra. Microsoft. (2025). https://learn.microsoft.com/es-es/entra/identity/authentication/tutorial-enable-azure-mfa

Figura 12

Busque y Seleccione el Grupo Entra De Microsoft, como MFA-Test-Group



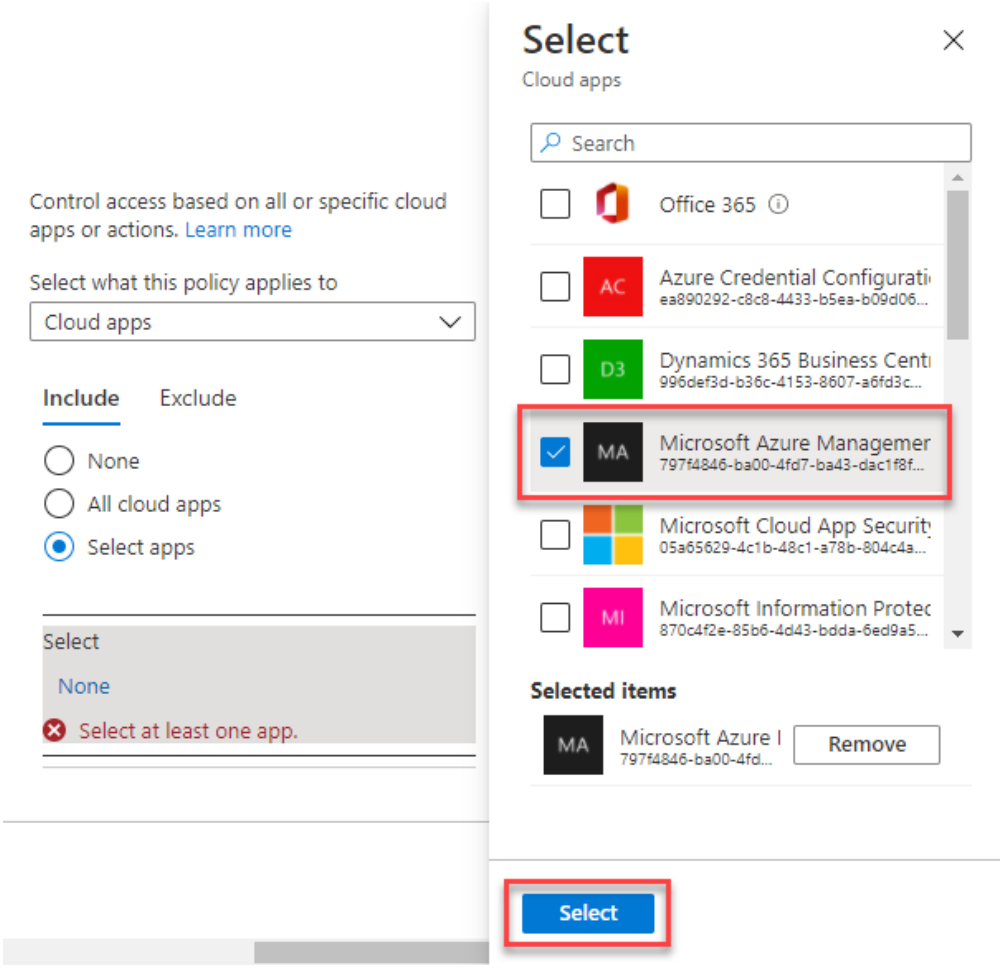
Nota. Selección de grupo con políticas. Tomado de. Tutorial: Eventos de inicio de sesión de usuario seguros con la autenticación multifactor de Microsoft Entra. Microsoft. (2025). https://learn.microsoft.com/es-es/entra/identity/authentication/tutorial-enable-azure-mfa

Configuración de la política: Se habilitó la autenticación multifactor como obligatoria para los miembros del grupo, utilizando métodos como aplicación autenticadora y SMS. La

política también incluyó un refuerzo de MFA en el primer inicio de sesión desde ubicaciones no confiables.

Figura 13

Seleccione API de Administración de Servicios de Windows Azure

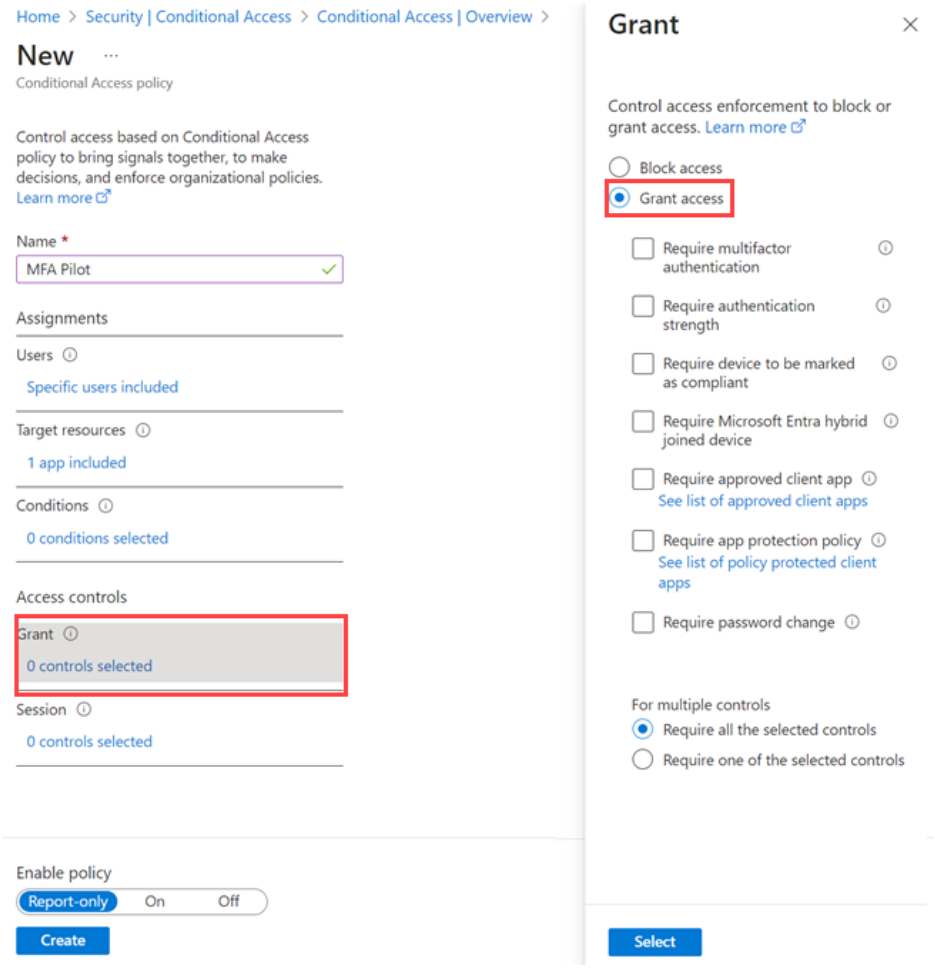


Nota. Selección del administrador de servicio. Tomado de. Tutorial: Eventos de inicio de sesión de usuario seguros con la autenticación multifactor de Microsoft Entra. Microsoft. (2025). https://learn.microsoft.com/es-es/entra/identity/authentication/tutorial-enable-azure-mfa

Activación de la política: La política fue guardada y activada, quedando disponible en el panel de control de seguridad.

Figura 14

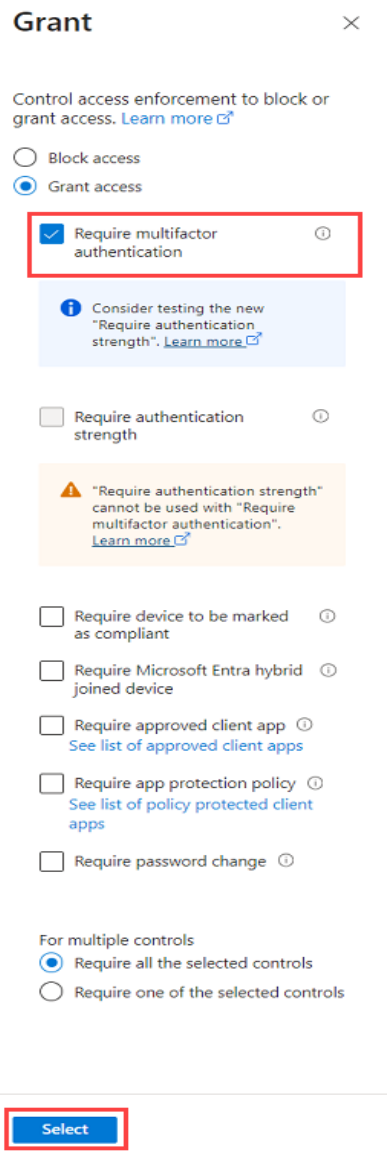
Seleccione el Valor Actual en Conceder y a Continuación Seleccione Conceder Acceso



Nota. Configuración de permisos. Tomado de. Tutorial: Eventos de inicio de sesión de usuario seguros con la autenticación multifactor de Microsoft Entra. Microsoft. (2025). https://learn.microsoft.com/es-es/entra/identity/authentication/tutorial-enable-azure-mfa

Figura 15

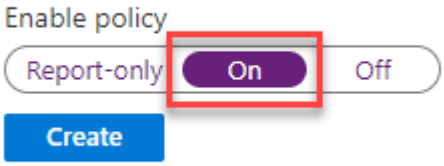
Seleccione Requerir Autenticación Multifactor y, a Continuación, Elija Seleccionar



Nota. Configurar autenticación multifactor como necesario. Tomado de. Tutorial: Eventos de inicio de sesión de usuario seguros con la autenticación multifactor de Microsoft Entra. Microsoft. (2025). https://learn.microsoft.com/es-es/entra/identity/authentication/tutorial-enable-azure-mfa

Figura 16

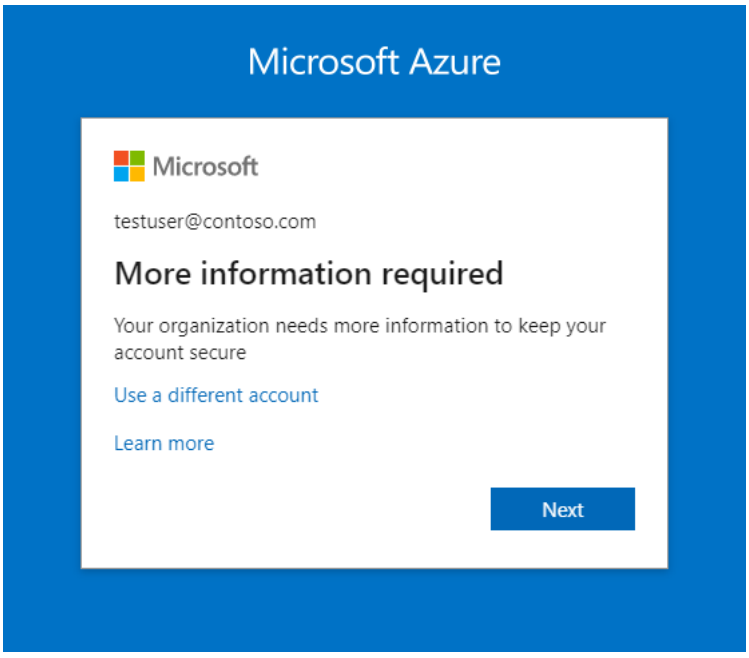
Habilitar Directiva, Seleccione Activado



Nota. Habilitar directiva. Tomado de. Tutorial: Eventos de inicio de sesión de usuario seguros con la autenticación multifactor de Microsoft Entra. Microsoft. (2025). https://learn.microsoft.com/es-es/entra/identity/authentication/tutorial-enable-azure-mfa

Figura 17

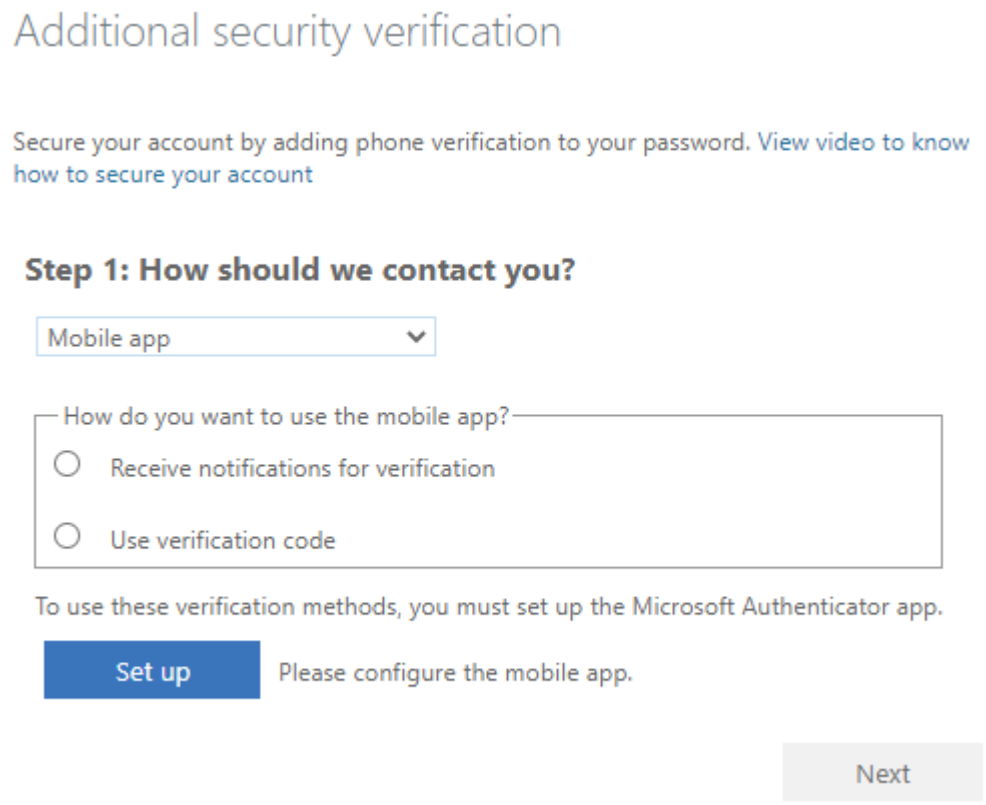
Debe Registrarse y Usar la Autenticación Multifactor de Microsoft Entra



Nota. Solicitud de registro en autenticación multifactor. Tomado de. Tutorial: Eventos de inicio de sesión de usuario seguros con la autenticación multifactor de Microsoft Entra. Microsoft. (2025). https://learn.microsoft.com/es-es/entra/identity/authentication/tutorial-enable-azure-mfa

Figura 18

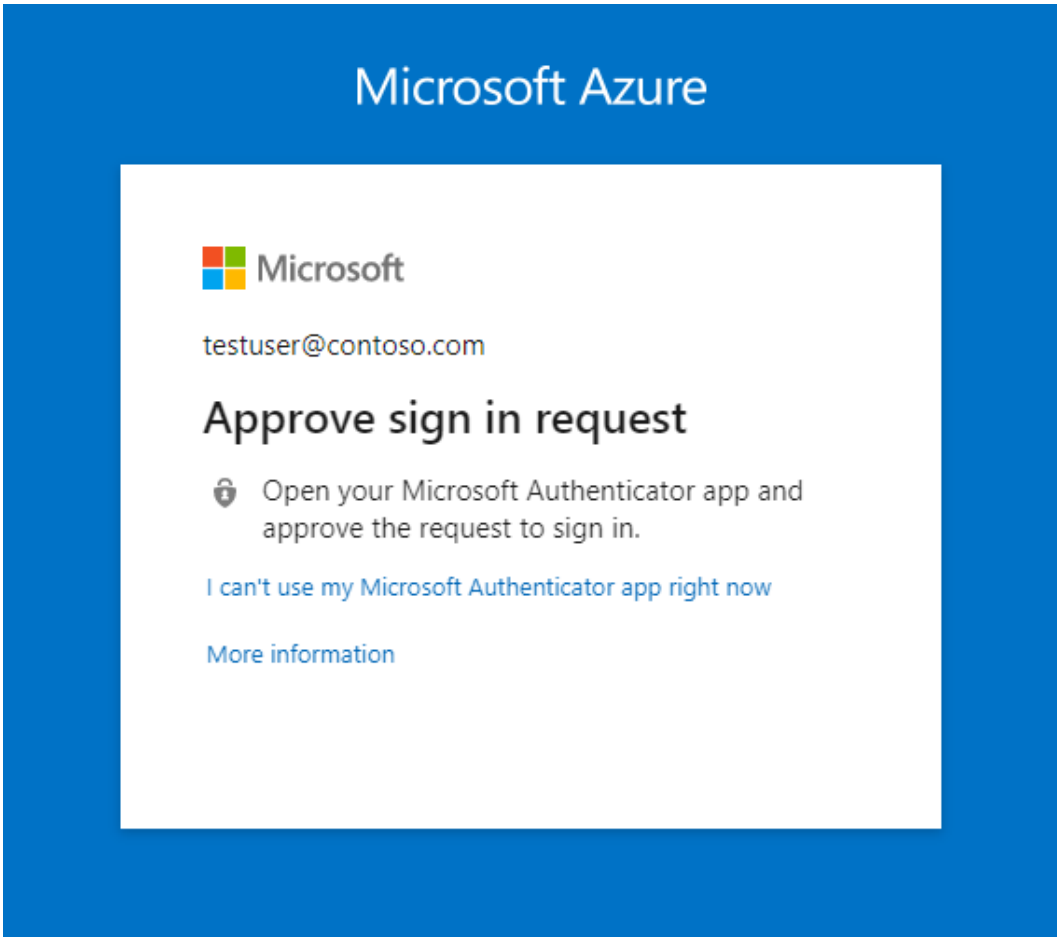
Seleccione Siguiente para Comenzar el Proceso y Siga las Instrucciones de la Pantalla para Configurar el Método de Autenticación Multifactor que ha Seleccionado



Nota. Configuración parámetros de seguridad autenticación multifactor. Tomado de. Tutorial: Eventos de inicio de sesión de usuario seguros con la autenticación multifactor de Microsoft Entra. Microsoft. (2025). https://learn.microsoft.com/es-es/entra/identity/authentication/tutorial-enable-azure-mfa

Figura 19

Cierre la Ventana del Explorador e Inicie Sesión de Nuevo en el Centro de Administración de Microsoft Entra para Probar el Método de Autenticación que Configuró



Nota. Aprobación doble factor en app autenticación multifactor. Tomado de. Tutorial: Eventos de inicio de sesión de usuario seguros con la autenticación multifactor de Microsoft Entra. Microsoft. (2025). https://learn.microsoft.com/es-es/entra/identity/authentication/tutorial-enable-azure-mfa

La configuración de MFA es un componente esencial del modelo Zero Trust, ya que refuerza la verificación de identidad en cada intento de acceso. Al aplicar esta política en un

grupo específico de usuarios remotos, se garantiza que incluso si las credenciales son comprometidas, el atacante no podrá acceder sin la segunda capa de autenticación. Esta medida está alineada con el control A.9.4.2 de la norma ISO/IEC 27001, que recomienda el uso de autenticación fuerte para accesos remotos.

Objetivo 4

Esta metodología busca fortalecer el acceso remoto con una visión de madurez progresiva, manteniendo un enfoque preventivo y adaptativo frente a nuevas amenazas, al tiempo que garantiza la trazabilidad y mejora continua exigida por estándares internacionales.

Diagnóstico y políticas iniciales – Controles: A.5.1, A.6.1.1.

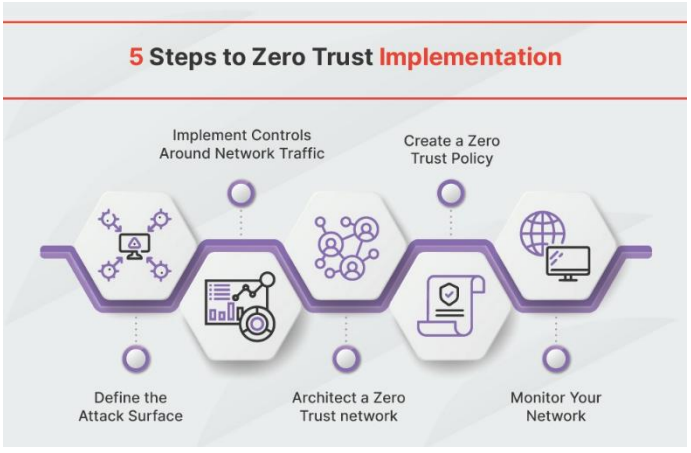
Capacitación y concienciación – Controles: A.7.2.2, A.8.2.2.

Implementación tecnológica (MFA, segmentación) – Controles: A.9.1.2, A.13.1.3.

Monitoreo y mejora continua – Controles: A.12.4.1, A.18.2.3.

Figura 20

Pasos para Implementación de Seguridad Basada en Zero Trust



Nota. 5 pasos para implementar Zero Trust. Tomado de. Cómo implementar la confianza cero: enfoque de 5 pasos y sus desafíos | Fortinet. (s. f.). Fortinet. https://www.fortinet.com/lat/resources/cyberglossary/how-to-implement-zero-trust

Conclusión

Cada una de las estrategias planteadas no solo se basa en principios teóricos, sino que está respaldada por herramientas específicas, buenas prácticas reconocidas y alineaciones claras con los controles del Anexo A de la ISO/IEC 27001. Las simulaciones prácticas, Herramientas como GoPhish o la configuración de políticas de acceso condicional y MFA mediante Microsoft Entra, evidenciaron cómo estos mecanismos se pueden implementar con recursos disponibles actualmente y con resultados medibles.

Finalmente, este capítulo reafirma que el fortalecimiento del acceso remoto no debe tratarse como un conjunto de medidas aisladas, sino como una estrategia integral, dinámica y orientada a la mejora continua, que evoluciona al ritmo de las amenazas digitales y las necesidades del entorno empresarial moderno.

Conclusiones

El presente trabajo ha explorado la necesidad de fortalecer la ciberseguridad en los entornos de teletrabajo, una modalidad que se ha consolidado como pilar fundamental en la continuidad operativa de las organizaciones, particularmente en Colombia. A través del análisis riguroso de dos marcos de seguridad de referencia mundial, el Modelo Zero Trust y la Norma ISO/IEC 27001, se han definido estrategias robustas y complementarias para proteger los accesos remotos.

Se ha demostrado que el Modelo Zero Trust representa una evolución en la seguridad. Su principio fundamental de "nunca confiar, siempre verificar" es adecuado para abordar el perímetro de seguridad tradicional que caracteriza al teletrabajo. La verificación exhaustiva de cada usuario y dispositivo, junto con la aplicación de privilegios mínimos y la segmentación de la red, activa como una defensa frente a amenazas constantes, reduciendo en un porcentaje la superficie de ataque y el riesgo de movimiento lateral por parte de un intruso.

La Norma ISO/IEC 27001 se posiciona como la normativa ideal para sostener una estrategia de ciberseguridad integral. Su sistemática basada en riesgos permite a las organizaciones no solo identificar y evaluar amenazas específicas del teletrabajo (como el uso de dispositivos personales inseguros o redes domésticas vulnerables), sino también implementar y monitorear controles efectivos de manera continua. La adaptabilidad de ISO 27001 asegura que las políticas de seguridad evolucionen al ritmo de las amenazas y las innovaciones tecnológicas, fomentando una cultura de seguridad que permea toda la estructura organizacional y otorga gobernanza a las implementaciones de Zero Trust.

El Capítulo 4 permitió demostrar cómo la integración del modelo de seguridad Zero Trust con la norma ISO/IEC 27001 ofrece un enfoque sólido y eficaz para proteger los accesos remotos en escenarios de teletrabajo. A través del diseño de estrategias concretas, políticas de seguridad adaptativas, capacitación continua y monitoreo proactivo, se evidenció que es posible fortalecer significativamente la postura de ciberseguridad de las organizaciones frente a amenazas crecientes como el phishing, el robo de credenciales o accesos no autorizados.

Finalmente, la integración de herramientas tecnológicas y prácticas específicas como la autenticación multifactor (MFA), la microsegmentación de red y la gestión de identidades y accesos (IAM) ha sido crucial para la operatividad de las estrategias propuestas. Estas herramientas no solo refuerzan los principios de Zero Trust, sino que también proporcionan los mecanismos para la implementación efectiva de los controles de ISO 27001. Su aplicación coordinada permite una defensa que va más allá de la protección perimetral, asegurando la confidencialidad, integridad y disponibilidad de la información empresarial en un escenario donde los datos se mueven constantemente entre la oficina y los entornos remotos.

Referencias Bibliográficas

Andrade, R. O., Ortiz-Garcés, I., & Cazares, M. (2020). *Cybersecurity attacks on smart home during COVID-19 pandemic*. 398-404. https://doi.org/10.1109/WorldS450073.2020.9210363

Bishop, G. (2025). *Cultura de la ciberseguridad* (1.ª ed.). CRC Press. https://doi.org/10.1201/9781003368496

CERT-Colombia. (2023). *Alerta de vulnerabilidad en entornos BYOD: CVE-2021-34527 (PrintNightmare)*. Cert-Colombia. https://www.cert.gov.co

CISA. (2023, junio). *Known Exploited Vulnerabilities (KEV) Catalog: CVE-2023-20887*. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Daah, C., Qureshi, A., Awan, I., & Konur, S. (2024). Enhancing Zero Trust Models in the Financial Industry through Blockchain Integration: A Proposed Framework. *Electronics*, *13*(5), 865. https://doi.org/10.3390/electronics13050865

ENISA. (2024). *ENISA Threat Landscape 2024*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

ESET. (2024). *ESET Threat Report H1 2024: Latin America cyber-threat landscape*. WeLiveSecurity. https://www.eset.com/us/business/resource-center/reports/eset-threat-report-h1-2024

Fernandez-Morin, J., Torrejon-Mundaca, K., & Meneses-Claudio, B. (2023). Application of blockchain technology for information security in the financial sector. Salud, Ciencia Y Tecnología - Serie De Conferencias, 2, 432. https://doi.org/10.56294/sctconf2023432

García, M., & López, J. (2023). Ciberseguridad en el teletrabajo: Desafíos y recomendaciones para las organizaciones. Revista Iberoamericana de Tecnología y Sociedad, 10(2), 45-60. https://doi.org/10.1234/rits.v10i2.5678

Gartner. (2024, 22 de abril). Gartner survey reveals 63% of organizations worldwide have implemented a zero-trust strategy [Comunicado de prensa]. https://www.gartner.com/en/newsroom/press-releases/2024-04-22-gartner-survey-reveals-63-percent-of-organizations-worldwide-have-implemented-a-zero-trust-strategy

IBM Security. (2023). *Cost of a Data Breach Report 2023*. IBM. https://www.ibm.com/reports/data-breach

ISO/IEC 27001:2022. (2022). ISO. https://www.iso.org/standard/27001

Microsoft. (2025). Habilitar autenticación multifactor de Microsoft Entra - Microsoft Entra ID. Microsoft.com. https://learn.microsoft.com/es-es/entra/identity/authentication/tutorial-enable-azure-mfa

Kaspersky. (2021). *Remote working and cyberthreats in Latin America*. Ponemon Institute. https://www.kaspersky.com/blog/remote-work-latam-report/39143/

Llanos Palacios, R. de J. (2024). *Teletrabajo en Colombia: análisis del estado de la ciberseguridad en pequeñas y medianas empresas*. Universidad Nacional Abierta y a Distancia (UNAD). https://repository.unad.edu.co/handle/10596/56625

Mayer Lux, L. V., & Toso Milos, Á. (2024). La facilitación de medios al interior de la empresa para la comisión de un fraude informático: Problemas dogmáticos y relativos al compliance. Revista Chilena De Derecho Y Tecnología, 13. https://doi.org/10.5354/0719-2584.2024.72932

Meyer, L. A., Romero, S., Bertoli, G., Burt, T., Weinert, A., & Lavista Ferres, J. (2023). *How effective is multifactor authentication at deterring cyberattacks?* arXiv. https://doi.org/10.48550/arXiv.2305.00945

MicrosoftGuyJFlo. (2025). Resolución de problemas de inicio de sesión con el acceso condicional - Microsoft Entra ID. Microsoft Learn. https://learn.microsoft.com/es-es/entra/identity/conditional-access/troubleshoot-conditional-access

Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). (2024). *Ciberseguridad para el teletrabajo: uso de redes domésticas en Colombia*. https://www.mintic.gov.co/portal/inicio/Secciones/Ciberseguridad

National Institute of Standards and Technology (NIST). (2020). *Zero Trust Architecture (SP 800-207)*. https://doi.org/10.6028/NIST.SP.800-207

NIST. (2013, julio). Guide to Enterprise Patch Management Technologies (SP 800-40 Rev. 3). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-40r3

Organización Internacional de Normalización. (2022). *ISO/IEC 27001:2022 - Security techniques — Information security management systems — Requirements*. Ginebra: ISO. https://www.iso.org/standard/82875.html

Orosco-Fabian, J. R., Pomasunco-Huaytalla, R., Gómez-Galindo, W., & Torres-Cortez, E. E. (2025). Tecnoestrés en profesores de Educación Básica de la región central del Perú. Revista Colombiana De Educación, 94, e18243. https://doi.org/10.17227/rce.num94-18243

Palo Alto Networks. (2023). *The State of Remote Access Security*. Palo Alto Networks. https://www.paloaltonetworks.com

Pérez, A. (2025, 24 de marzo). Zero Trust: el nuevo paradigma en ciberseguridad para empresas. OBS Business School. https://www.obsbusiness.school/blog/zero-trust-el-nuevo-paradigma-en-ciberseguridad-para-empresas-cp

Podugu, S., Rayapureddi, V. K., & Gupta, M. (2023). Auditing Customer Identity and Access Management. En M. Gupta & R. Sharman (Eds.), Modernizing Enterprise IT Audit Governance and Management Practices (pp. 181-210). IGI Global Scientific Publishing. https://doi.org/10.4018/978-1-6684-8766-2.ch007

Security Leaders. (2023). Ataques cibernéticos no trabalho remoto mais que triplicam durante a pandemia. https://securityleaders.com.br/ataques-ciberneticos-no-trabalho-remoto-mais-que-triplicam-durante-a-pandemia/

Soffid. (2024, agosto 21). *El futuro de IAM: adoptando la arquitectura Zero Trust*. Soffid IAM Blog. https://www.soffid.com/es/blogs/el-futuro-de-iam-adoptando-la-arquitectura-zero-trust

Sohail, S., Sajjad, S. M., Zafar, A., Iqbal, Z., Muhammad, Z., & Kazim, M. (2025). Análisis forense de imágenes deepfake para la protección de la privacidad y la autenticidad mediante aprendizaje profundo. Información, 16(4), 270. https://doi.org/10.3390/info16040270

Sulfath, K. K., Ramakrishnan, P. R., Shareef, P. M., & Shanmugam, H. (2025). Enhancing IT Service Management in Indian IT Organizations: A Technological Integration of ISO 20000 with AI, Blockchain, Predictive Analytics, and Zero Trust Security. Indian Journal of Information Sources and Services, 15(1), 267-273. https://doi.org/10.51983/ijiss-2025.IJISS.15.1.34

Trend Micro. (2023). *State of Cybersecurity Awareness: Trend Micro*; encuesta regional. https://www.trendmicro.com

Verizon. (2024). *Data Breach Investigations Report 2024*. Verizon. https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf

Apéndices

Apéndices A

Análisis Detallado de las Variables Clave del Proyecto

En este punto, se identifican y describen las variables esenciales que guían el desarrollo del proyecto. Estas variables, además de estar presentes en el resumen y los objetivos planteados, son fundamentales para entender el enfoque y el alcance de la investigación. A continuación, se presenta cada una con su respectiva definición operativa y la razón por la cual resultan relevantes para este estudio.

Modelo Zero Trust

En el contexto de este trabajo, el Modelo Zero Trust se entiende como un enfoque de seguridad que parte de la idea de no otorgar confianza automática a ningún usuario, dispositivo o aplicación, sin importar si se encuentran dentro o fuera de la red corporativa. Este modelo promueve la verificación continua, el uso de autenticación fuerte, la segmentación de la red y la asignación de privilegios mínimos.

El valor de Zero Trust radica en que responde directamente a los desafíos de ciberseguridad que impone el teletrabajo. Al eliminar la confianza implícita, este enfoque ayuda a reducir la superficie de ataque y a controlar mejor quién accede a qué recursos. Resulta especialmente relevante en entornos donde las conexiones externas y los dispositivos personales son la norma.

Norma ISO/IEC 27001 (Sistema de Gestión de Seguridad de la Información - SGSI)

La ISO/IEC 27001 es un estándar internacional que establece los requisitos para implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).

Este sistema ayuda a las organizaciones a identificar, evaluar y gestionar sus riesgos en seguridad de la información, con un enfoque claro hacia la mejora continua.

Este estándar proporciona un marco estructurado y reconocido mundialmente para proteger los activos de información. En el contexto del teletrabajo, permite adaptar controles específicos para proteger los accesos remotos y gestionar los riesgos asociados a la descentralización de la seguridad. Su aplicación aporta orden, metodología y respaldo normativo a las estrategias que se diseñen en este proyecto.

Acceso Remoto

El acceso remoto se refiere a la capacidad de conectarse a los sistemas y recursos de la organización desde cualquier ubicación externa a la red empresarial, generalmente a través de Internet. Esto incluye el acceso a aplicaciones, servidores, bases de datos y servicios desde cualquier dispositivo sin importar que no sean gestionados por la empresa.

El acceso remoto es el punto de partida del problema de investigación. Es precisamente en estos accesos donde se concentran los mayores riesgos del teletrabajo, ya que pueden convertirse en puertas abiertas para amenazas externas si no se gestionan adecuadamente. Por ello, resulta crucial fortalecer estos puntos y controlar quién, cómo y desde dónde se conecta.

Teletrabajo

El teletrabajo es una modalidad laboral que permite a las personas realizar sus actividades desde ubicaciones distintas a las oficinas, utilizando tecnologías digitales para mantenerse conectados y cumplir con sus responsabilidades.

Este es el contexto sobre el cual gira todo el proyecto. El crecimiento del teletrabajo ha transformado la forma en que las organizaciones operan, pero también ha traído consigo nuevos

riesgos de seguridad. Entender sus particularidades y sus vulnerabilidades es clave para proponer soluciones efectivas y adaptadas a esta realidad.

Ciberseguridad

La ciberseguridad abarca el conjunto de prácticas, tecnologías y políticas orientadas a proteger los sistemas informáticos, redes y datos frente a accesos no autorizados, ataques o daños.

La ciberseguridad es el centro transversal del estudio. Sin su aplicación, sería imposible garantizar la protección de la información, especialmente en entornos donde los accesos remotos son frecuentes. La investigación se apoya precisamente en este campo para construir las estrategias y medidas que se buscan implementar.

Autenticación Multifactor (MFA)

La autenticación multifactor es un mecanismo de seguridad que exige que los usuarios verifiquen su identidad utilizando al menos dos métodos distintos: algo que saben (como una contraseña), algo que tienen (como un token o un celular) o algo que son (como una huella digital).

La MFA es una herramienta práctica y altamente efectiva para evitar accesos no autorizados, incluso cuando las contraseñas son robadas. Al requerir múltiples pruebas de identidad, se convierte en una barrera sólida contra ataques como el phishing y es una pieza clave en la implementación del modelo Zero Trust.

Apéndices B

Resultados Preliminares de la Validación de la Hipótesis

A partir del análisis inicial de la literatura y de las metodologías exploradas, se han comenzado a obtener evidencias que apoyan la hipótesis central del proyecto: que la aplicación de buenas prácticas basadas en Zero Trust e ISO 27001 permite fortalecer la seguridad de los accesos remotos en entornos de teletrabajo.

El modelo Zero Trust se presenta como una respuesta sólida a la problemática actual. La revisión bibliográfica demuestra que sus principios, como la verificación constante de identidad y el acceso con privilegios mínimos, son especialmente adecuados para contextos donde los usuarios trabajan desde redes no seguras.

Por otro lado, la norma ISO/IEC 27001 aporta la estructura necesaria para gestionar los riesgos asociados, ofreciendo un marco flexible que puede adaptarse al teletrabajo. La importancia de su enfoque basado en la mejora continua y la gestión del riesgo permite mantener controles efectivos a pesar de las condiciones cambiantes.

El enfoque metodológico adoptado, basado en el análisis cualitativo y la revisión documental, ha sido adecuado para profundizar en estos marcos y empezar a delinear estrategias que combinen lo mejor de ambos. Los resultados hasta ahora no solo confirman que esta integración es viable, sino que es pertinente para enfrentar los desafíos actuales en la ciberseguridad del trabajo remoto.

Apéndices C

Evidencias del Uso de Herramientas Específicas

Durante el desarrollo de esta investigación, fue fundamental apoyarse en herramientas que facilitaran la recolección, organización y análisis de la información. Estas herramientas no solo contribuyeron a dar estructura al trabajo, sino que también permitieron garantizar la rigurosidad en cada etapa del proceso. A continuación, se describen las principales herramientas utilizadas y la forma en que aportaron al avance del proyecto.

Plataformas y Bases de Datos Académicas

Una de las actividades más importantes fue la búsqueda y selección de información confiable y actualizada. Para ello, se consultaron diversas bases de datos académicas reconocidas, entre las cuales se destacan Scopus y Google Scholar.

El uso de Scopus resultó esencial, ya que permitió acceder a artículos científicos, revisiones sistemáticas y estudios recientes de gran relevancia. Gracias a sus filtros avanzados, fue posible delimitar los resultados por años, temas y palabras clave, lo que facilitó encontrar investigaciones relacionadas con "Zero Trust", "ISO 27001", "teletrabajo" y "ciberseguridad".

Google Scholar, por su parte, fue un gran complemento. A través de esta plataforma se identificaron otras fuentes valiosas como tesis, reportes técnicos y documentos que no siempre están disponibles en las bases de datos más especializadas.

¿Cómo aportaron al proyecto?

Estas plataformas fueron la base para construir el marco teórico, conceptual y la revisión sistémica de literatura. Además, aseguraron que el análisis de los procedimientos de ciberseguridad (Objetivo Específico 1) y la identificación de herramientas tecnológicas (Objetivo

Específico 2) se sustentaran en información actual y relevante. La evidencia de su uso queda reflejada en las citas y referencias bibliográficas que acompañan cada apartado del documento.

Gestión Bibliográfica

Para organizar de manera eficiente toda la información recopilada, se emplearon principios de gestión bibliográfica que permitieron llevar un registro ordenado de cada fuente consultada. Con la aplicación de Zotero, se aplicaron métodos para asegurar la correcta clasificación y citación de los documentos revisados.

¿Cómo aportó al proyecto?

El uso de una estructura organizada para las referencias facilitó la recuperación rápida de información al momento de redactar y argumentar. También permitió mantener la coherencia en el formato de citación bajo las normas APA 7. Esto fue clave para garantizar la calidad académica del trabajo y evitar errores de duplicidad o pérdida de información.

Herramientas de Organización y Análisis: Matrices de Revisión y Fichas de Estudio

Durante la etapa de análisis, se implementaron matrices de revisión y fichas de estudio personalizadas que permitieron organizar de manera detallada la información extraída de cada documento.

En las matrices se registraron datos como autor, año de publicación, metodología utilizada, principales hallazgos, riesgos asociados al teletrabajo y contribuciones relevantes al modelo Zero Trust y a la norma ISO 27001. Por otro lado, las fichas de estudio sirvieron para profundizar en conceptos clave como "Autenticación Multifactor", "Segmentación de Redes", entre otros, consolidando definiciones, características, ventajas y limitaciones.

¿Cómo aportaron al proyecto?

Estas herramientas facilitaron la comparación de enfoques, la síntesis de información y la identificación de relaciones entre conceptos. Gracias a este trabajo estructurado, fue posible cumplir con los objetivos específicos, definir las variables relevantes y argumentar con claridad la elección de herramientas tecnológicas aplicables a entornos de teletrabajo.

Software de Procesamiento de Texto

La redacción y edición del documento se realizó utilizando Microsoft Word, herramienta que permitió estructurar adecuadamente los capítulos, aplicar las normas de presentación y asegurar una correcta organización del contenido.

¿Cómo aportó al proyecto?

El software permitió crear un documento claro, ordenado y conforme a los requisitos formales exigidos. Además, facilitó el seguimiento de versiones y la integración de ajustes sugeridos por el director del proyecto.