REVISTA CIENTÍFICA
Ciencia y Método
ISSN 3103-1072

EDITORIAL GRUPO AEA

Artículo Científico

Estrategias de ciberseguridad en entornos de trabajo híbridos y remoto

Cybersecurity strategies in hybrid and remote work environments

Boné-Andrade, Miguel Fabricio [1]
https://orcid.org/0000-0002-8635-1869
mbone6598@pucesm.edu.ec
Pontificia Universidad Católica del Ecuador, Ecuador, Riobamba.

Pinargote-Bravo, Victor Joel [2]
https://orcid.org/0000-0003-0599-1651
vpinargote@espam.edu.ec
Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, Ecuador, Jipijapa.

Bonilla-Fierro, Luis Fernando [3]
https://orcid.org/0000-0003-0599-1651
ferchobonilla1996@hotmail.com
Universidad Estatal de Bolívar, Ecuador, Bolivar.

Autor de correspondencia [1]

DOI / URL: https://doi.org/10.55813/gaea/rcym/v1/n4/21

Resumen: La presente investigación analiza críticamente las estrategias de ciberseguridad implementadas en entornos laborales híbridos y remotos, motivada por la transformación digital acelerada tras la pandemia de COVID-19, que ha incrementado las superficies de ataque y debilitado los modelos de seguridad tradicionales. Mediante un enfoque exploratorio de revisión bibliográfica, se recopilaron y clasificaron artículos científicos y documentos técnicos publicados entre 2018 y 2023, especialmente aquellos posteriores a 2020, seleccionados en bases como Scopus y Web of Science. Entre los hallazgos principales se destaca la efectividad de la arquitectura Zero Trust, basada en la verificación continua y el control contextual, y de herramientas de seguridad en la nube como SASE, EDR y CASB, que permiten una protección flexible y escalable. Además, se identifican factores organizacionales decisivos como la capacitación continua del personal y una cultura de seguridad sólida, así como marcos de gobernanza adaptativos alineados con estándares internacionales. La investigación concluye que la eficacia de las estrategias de ciberseguridad no depende exclusivamente de la tecnología, sino de su integración con procesos organizacionales robustos, liderazgo comprometido y políticas dinámicas, lo que permite a las organizaciones afrontar con éxito los desafíos del ecosistema digital descentralizado.

Palabras clave: ciberseguridad; trabajo remoto; Zero Trust; seguridad en la nube; cultura organizacional.

Check for updates

Received: 02/Oct/2023
Accepted: 31/Oct/2023
Published: 25/Nov/2023

Cita: Boné-Andrade, M. F., Pinargote-Bravo, V. J., & Bonilla-Fierro, L. F. (2023). Estrategias de ciberseguridad en entornos de trabajo híbridos y remoto. *Revista Científica Ciencia Y Método*, *1*(4), 31-43. https://doi.org/10.55813/gaea/rcym/v1/n4/21

Revista de Ciencia y Método (RCyM)
https://revistacym.com
revistacym@editorialgrupo-aea.com
info@editoriagrupo-aea.com

Abstract:

The present research critically analyzes cybersecurity strategies implemented in hybrid and remote work environments, motivated by the accelerated digital transformation following the COVID-19 pandemic, which has increased attack surfaces and weakened traditional security models. Using an exploratory literature review approach, scientific articles and technical papers published between 2018 and 2024, especially those after 2020, selected from databases such as Scopus and Web of Science, were collected and classified. Among the main findings, the effectiveness of Zero Trust architecture, based on continuous verification and contextual control, and cloud security tools such as SASE, EDR and CASB, which allow flexible and scalable protection, are highlighted. In addition, decisive organizational factors such as continuous staff training and a strong security culture as well as adaptive governance frameworks aligned with international standards are identified. The research concludes that the effectiveness of cybersecurity strategies does not depend solely on technology, but on their integration with robust organizational processes, committed leadership and dynamic policies, enabling organizations to successfully meet the challenges of the decentralized digital ecosystem.

Keywords: cybersecurity; remote work; Zero Trust; cloud security; organizational culture.

1. Introducción

En los últimos años, la transformación digital ha propiciado cambios estructurales en la forma en que las organizaciones llevan a cabo sus operaciones. Uno de los fenómenos más relevantes en este contexto ha sido la adopción acelerada de modalidades de trabajo híbrido y remoto, impulsadas principalmente por la pandemia de COVID-19. Este cambio ha permitido una mayor flexibilidad laboral y optimización de recursos, pero al mismo tiempo ha expuesto a las organizaciones a nuevas amenazas cibernéticas. La descentralización del trabajo ha ampliado la superficie de ataque para los actores maliciosos, dificultando la gestión integral de la seguridad informática. De acuerdo con el informe de IBM (2023), el 45 % de las brechas de seguridad en 2022 estuvieron vinculadas a usuarios que trabajaban fuera de la infraestructura de red corporativa, lo que pone en evidencia la urgencia de revisar las estrategias de ciberseguridad adaptadas a estos nuevos entornos laborales.

La problemática radica en que muchos esquemas tradicionales de seguridad no están diseñados para proteger infraestructuras distribuidas ni dispositivos personales utilizados en el trabajo remoto. En este sentido, las organizaciones enfrentan desafíos como la autenticación insegura, redes domésticas vulnerables, dispositivos no administrados y falta de formación del personal en prácticas de ciberseguridad. Además, la protección de la información sensible y la continuidad operativa están

constantemente amenazadas por vectores de ataque como el phishing, el ransomware y la suplantación de identidad, que han experimentado un incremento significativo desde 2020 (Verizon, 2023).

Uno de los principales factores que agravan esta problemática es la dependencia de tecnologías de comunicación en la nube, aplicaciones colaborativas y sistemas de acceso remoto. Si bien estas herramientas facilitan la continuidad del trabajo, también representan vectores potenciales de vulnerabilidad si no se implementan políticas de seguridad adecuadas. Estudios recientes señalan que el 60 % de las organizaciones que adoptaron el trabajo híbrido no actualizaron sus políticas de seguridad digital, lo que las expone a amenazas internas y externas (PwC, 2022). Asimismo, el bajo nivel de conciencia cibernética en los empleados constituye un riesgo crítico. De acuerdo con el informe de ENISA (2022), más del 80 % de los ciberincidentes registrados en entornos de trabajo remoto se originaron por errores humanos o malas prácticas en el manejo de credenciales y datos sensibles.

La revisión de estrategias efectivas de ciberseguridad en entornos híbridos y remotos se vuelve crucial para garantizar la resiliencia digital de las organizaciones. Esta investigación resulta especialmente relevante considerando el crecimiento continuo de esta modalidad laboral a nivel global. De hecho, Gartner (2023) estima que para 2025, el 70 % de los empleados en empresas tecnológicas trabajarán en esquemas híbridos o completamente remotos. En este sentido, es imperativo identificar, analizar y comparar las mejores prácticas de ciberseguridad que se están implementando actualmente y que han demostrado ser eficaces en contextos de trabajo distribuido.

La justificación de esta revisión bibliográfica se sustenta en la necesidad de aportar un análisis crítico y actualizado de las estrategias de ciberseguridad en el contexto laboral contemporáneo. A través del examen sistemático de literatura académica indexada y documentos técnicos relevantes, se busca ofrecer una síntesis comprensiva que sirva de guía tanto para responsables de seguridad informática como para tomadores de decisiones en organizaciones públicas y privadas. Asimismo, este estudio aspira a identificar vacíos en la literatura científica que podrían orientar futuras investigaciones en el campo. La viabilidad de esta revisión radica en la disponibilidad creciente de investigaciones empíricas y teóricas sobre la temática, muchas de las cuales se han producido a raíz del auge del teletrabajo desde 2020.

El objetivo principal de este artículo es analizar las estrategias de ciberseguridad adoptadas en entornos de trabajo híbridos y remotos, evaluando su eficacia, limitaciones y niveles de implementación en diferentes sectores organizacionales. Para ello, se recopilarán y examinarán estudios recientes, informes técnicos y revisiones académicas publicadas en revistas indexadas en Scopus y Web of Science. La finalidad es establecer un marco comparativo que permita reconocer enfoques exitosos, tecnologías emergentes, y modelos de gobernanza que respondan a los desafíos específicos de la ciberseguridad en estos entornos laborales.

En suma, la seguridad de la información en el trabajo híbrido y remoto se presenta como un campo de estudio prioritario ante la creciente dependencia de modelos laborales digitalizados. La presente revisión bibliográfica busca contribuir al debate académico y profesional sobre la adaptación de las estrategias de ciberseguridad al nuevo paradigma del trabajo, destacando la importancia de un enfoque holístico que considere tanto la dimensión tecnológica como la humana de la seguridad digital.

2. Materiales y métodos

La presente investigación adopta un enfoque exploratorio de revisión bibliográfica con el propósito de analizar y sintetizar estrategias de ciberseguridad aplicadas a entornos de trabajo híbridos y remotos. Este tipo de estudio se fundamenta en la recopilación, evaluación crítica e integración de investigaciones previas, informes técnicos y literatura científica pertinente, con el fin de construir una visión comprensiva del estado actual del conocimiento en la materia. La metodología empleada no pretende validar hipótesis, sino explorar el campo temático desde una perspectiva sistemática, interpretativa y analítica.

Para la recolección del material bibliográfico, se realizó una búsqueda exhaustiva de fuentes académicas en bases de datos científicas reconocidas, principalmente Scopus y Web of Science, a fin de garantizar la calidad, validez y relevancia de los documentos seleccionados. Se consideraron artículos publicados entre los años 2018 y 2024, con énfasis en aquellos posteriores a 2020 debido al impacto significativo de la pandemia en los modelos de trabajo y la consecuente evolución de las amenazas cibernéticas. Se utilizaron como criterios de inclusión trabajos en inglés y español que abordaran temáticas relacionadas con la ciberseguridad, el trabajo remoto o híbrido, las amenazas digitales contemporáneas y las estrategias de mitigación aplicadas en entornos corporativos.

La selección de los documentos se realizó mediante el uso de operadores booleanos y términos clave combinados, tales como: "cybersecurity", "remote work", "hybrid work", "information security strategies", "digital threats", y "cyber risk management". Posteriormente, se aplicó un proceso de filtrado en tres etapas: primero, la revisión de títulos y resúmenes para asegurar la pertinencia temática; segundo, la lectura detallada de los textos completos para valorar su profundidad analítica y metodológica; y tercero, la organización de los contenidos seleccionados de acuerdo con categorías emergentes relevantes para el análisis.

Los estudios fueron clasificados en función de su enfoque (conceptual, empírico o técnico), el tipo de organización analizada (privada, pública, tecnológica, educativa, entre otras) y el tipo de estrategia de ciberseguridad descrita (preventiva, correctiva, proactiva, adaptativa, etc.). Esta clasificación permitió identificar patrones, vacíos y tendencias en la implementación de medidas de seguridad digital en contextos laborales distribuidos. Asimismo, se llevó a cabo una comparación crítica entre las

diferentes estrategias documentadas, considerando su aplicabilidad, efectividad y sostenibilidad en el tiempo.

El análisis se desarrolló de forma cualitativa, permitiendo una interpretación contextualizada de los hallazgos, sin la utilización de herramientas estadísticas ni de meta-análisis cuantitativo. Esta aproximación fue seleccionada debido al carácter exploratorio del estudio y a la diversidad de los enfoques metodológicos presentes en los documentos revisados. El proceso de síntesis integradora permitió establecer relaciones conceptuales entre las estrategias identificadas, las amenazas enfrentadas y los factores organizacionales que influyen en la adopción de medidas de ciberseguridad.

Finalmente, para garantizar la transparencia y reproducibilidad del estudio, se llevó a cabo un registro detallado de las fuentes utilizadas, asegurando la trazabilidad de la información. La revisión bibliográfica fue guiada por principios de rigor académico, relevancia temática y actualidad, con el propósito de ofrecer una contribución válida y útil al conocimiento existente sobre la ciberseguridad en los entornos laborales emergentes.

3. Resultados

3.1. Estrategias tecnológicas de ciberseguridad en entornos híbridos y remotos

La consolidación del trabajo híbrido y remoto como modelo dominante en muchas organizaciones ha transformado el paradigma de la seguridad informática. En estos nuevos entornos, las redes corporativas ya no son estructuras contenidas, sino sistemas dinámicos, distribuidos y vulnerables a múltiples vectores de ataque. Esta descentralización ha obligado a las organizaciones a adoptar estrategias tecnológicas que permitan una protección integral de los datos, los dispositivos y las conexiones, sin depender exclusivamente de un perímetro físico. Entre estas estrategias, la implementación de arquitecturas Zero Trust y la integración de soluciones de seguridad basadas en la nube se perfilan como ejes fundamentales para la protección eficiente de los activos digitales.

3.1.1 Implementación de arquitecturas Zero Trust

La arquitectura Zero Trust ha emergido como una respuesta transformadora frente a las limitaciones de los modelos de seguridad tradicionales, que operaban bajo el supuesto de confianza dentro del perímetro de red. En un entorno híbrido o remoto, donde los usuarios acceden desde redes externas, dispositivos personales y ubicaciones diversas, este enfoque resulta obsoleto. Zero Trust plantea, en su núcleo, que no se debe asumir confianza implícita en ningún nodo de la red, usuario o sistema; todo acceso debe estar sujeto a verificación continua, políticas de mínima privilegiación y monitoreo contextualizado.

Este modelo de seguridad requiere la integración de múltiples tecnologías para su funcionamiento, tales como autenticación multifactor (MFA), gestión de identidades y accesos (IAM), segmentación de red, monitoreo en tiempo real, y análisis de comportamiento basado en inteligencia artificial. Su implementación, según Rose et al. (2020), debe ser holística, incluyendo tanto infraestructura tecnológica como procesos organizacionales y formación de usuarios.

En términos operativos, Zero Trust no sólo protege el acceso a los recursos, sino que también previene el movimiento lateral dentro de la red, es decir, el avance progresivo de una amenaza una vez que ha penetrado un nodo. Este tipo de ataques ha sido ampliamente documentado en los informes de ciberseguridad post-pandemia, donde se destaca un incremento de intrusiones sofisticadas en entornos remotos (Shen et al., 2023). Además, la integración de Zero Trust con tecnologías de análisis de comportamiento permite identificar patrones inusuales de acceso, como intentos de inicio de sesión desde ubicaciones atípicas o cambios drásticos en el uso de recursos, facilitando una respuesta proactiva frente a amenazas emergentes.

Diversos estudios de caso confirman la eficacia de este enfoque. Por ejemplo, una investigación desarrollada por Tang, Wu y Li (2022) señala que la implementación de Zero Trust en empresas del sector financiero logró reducir en un 48 % los incidentes de acceso indebido en los primeros doce meses de operación. Este tipo de evidencia subraya no sólo la capacidad de respuesta del modelo, sino también su potencial preventivo.

Sin embargo, la transición hacia Zero Trust no está exenta de desafíos. Uno de los principales obstáculos es la complejidad técnica que implica su implementación, especialmente en organizaciones que aún conservan infraestructuras heredadas. También se requiere una inversión significativa en capacitación, adaptación de sistemas y rediseño de políticas de acceso. A pesar de ello, las ventajas en términos de resiliencia cibernética y reducción de superficies de ataque justifican su adopción progresiva como estándar en ciberseguridad organizacional.

3.1.2 Uso de herramientas de seguridad basadas en la nube

La creciente adopción de tecnologías cloud ha acompañado la expansión del trabajo remoto, convirtiendo la nube no solo en un habilitador de productividad, sino también en una plataforma clave para la seguridad de los sistemas de información. Las soluciones de seguridad basadas en la nube ofrecen ventajas esenciales en entornos distribuidos: escalabilidad, visibilidad centralizada, respuesta automatizada y reducción de la dependencia del hardware local.

En este sentido, arquitecturas como Secure Access Service Edge (SASE) están revolucionando el modelo de protección perimetral. SASE integra funciones de seguridad y conectividad en una única plataforma gestionada desde la nube, que combina firewall como servicio (FWaaS), acceso a redes de confianza cero (ZTNA), seguridad web en la nube (SWG), y protección contra amenazas en tiempo real.

Según un análisis realizado por Gartner (2023), las organizaciones que adoptan SASE experimentan mejoras sustanciales en la agilidad operativa y una reducción promedio del 30 % en los costos de gestión de seguridad.

De igual forma, las herramientas Endpoint Detection and Response (EDR) han demostrado gran eficacia para proteger los dispositivos finales (endpoints), especialmente en contextos donde los empleados utilizan equipos personales o poco controlados. EDR combina capacidades de monitoreo continuo, análisis forense y respuesta automatizada, lo que permite identificar comportamientos sospechosos y contener ataques en sus fases iniciales. Esta capacidad es particularmente útil ante amenazas como el ransomware, que ha aumentado considerablemente desde el inicio del trabajo remoto (Pal & Pandey, 2021).

Por otra parte, los Cloud Access Security Brokers (CASB) desempeñan un papel fundamental al proporcionar visibilidad y control sobre las aplicaciones SaaS utilizadas por los empleados. Estas herramientas permiten establecer políticas de uso seguro, identificar accesos no autorizados, y garantizar el cumplimiento normativo mediante cifrado y control de fugas de datos. En un entorno donde las aplicaciones en la nube se han convertido en herramientas esenciales de colaboración —como Microsoft 365, Google Workspace o Slack—, el papel de los CASB es vital para mitigar riesgos de exposición accidental o deliberada de información confidencial.

La efectividad de estas soluciones está intrínsecamente vinculada a su integración dentro de una estrategia de ciberseguridad más amplia, que contemple tanto los aspectos técnicos como organizativos. Las investigaciones recientes sugieren que las organizaciones que combinan tecnologías de seguridad cloud con políticas claras de gobernanza, entrenamiento continuo del personal y monitoreo activo de amenazas, logran una reducción significativa en los incidentes de seguridad (Tang et al., 2022).

En síntesis, las herramientas de seguridad basadas en la nube representan una respuesta flexible, escalable y eficaz ante los desafíos del trabajo híbrido y remoto. Junto con el modelo Zero Trust, configuran un ecosistema de protección robusto, adaptable y alineado con las necesidades de la transformación digital contemporánea.

3.2. Factores organizacionales en la efectividad de las estrategias de ciberseguridad

El fortalecimiento de la ciberseguridad en entornos híbridos y remotos exige no sólo avances tecnológicos, sino una profunda reestructuración de los elementos organizacionales que configuran la respuesta institucional frente a los riesgos digitales. Aunque la inversión en infraestructura tecnológica —como firewalls, autenticación multifactor o soluciones de protección en la nube— es esencial, la literatura científica coincide en que su efectividad se ve significativamente condicionada por factores humanos, estructurales y normativos (Ahmad et al., 2014; Alavi et al., 2020). En este marco, la capacitación continua del personal y la promoción de una cultura organizacional centrada en la seguridad, junto con políticas de

gobernanza adaptativas, representan componentes críticos de una estrategia de defensa integral. La omisión de estos factores limita la sostenibilidad de las medidas tecnológicas, incrementa la exposición a amenazas internas y socava la capacidad de reacción ante incidentes cibernéticos complejos.

3.2.1 Capacitación continua del personal y cultura de seguridad

El factor humano sigue siendo uno de los eslabones más vulnerables en la cadena de ciberseguridad. En contextos de trabajo remoto e híbrido, esta vulnerabilidad se amplifica debido al uso de redes inseguras, dispositivos personales no gestionados (BYOD), y la frecuente carencia de supervisión directa. A pesar de las mejoras tecnológicas, el error humano, la negligencia y la ingeniería social continúan siendo las causas más comunes de incidentes de seguridad, tal como lo demuestra el informe de Verizon (2023), que atribuye más del 80 % de las brechas de seguridad a fallas humanas.

Ante este escenario, la capacitación continua del personal no debe considerarse una medida opcional o secundaria, sino un eje estructural de la estrategia de ciberseguridad. La formación debe ir más allá de la transmisión de conocimientos básicos, y enfocarse en modificar comportamientos y promover prácticas seguras mediante programas sistemáticos, personalizados y sostenibles en el tiempo. Las investigaciones de Parsons et al. (2017) evidencian que los programas de formación diseñados con base en el comportamiento del usuario y reforzados regularmente, son significativamente más eficaces que los entrenamientos únicos o genéricos.

Además, la capacitación efectiva debe incluir simulaciones de amenazas reales, ejercicios de respuesta a incidentes, talleres interactivos y módulos adaptativos basados en niveles de riesgo. La integración de tecnologías de aprendizaje automático para adaptar los contenidos de formación a los perfiles de riesgo de los empleados también ha mostrado resultados prometedores en la prevención de incidentes (Alavi et al., 2020). Estos programas deben ser diseñados con la participación activa del personal de tecnología, recursos humanos y liderazgo organizacional, garantizando así una alineación estratégica entre seguridad y cultura organizacional.

Por otro lado, la promoción de una cultura de seguridad organizacional es esencial para internalizar comportamientos seguros. Una cultura de seguridad robusta se caracteriza por la conciencia colectiva de las amenazas, la asunción de responsabilidades individuales y el respaldo institucional a las buenas prácticas. Esta cultura debe permear todos los niveles jerárquicos, desde los ejecutivos hasta los operativos, generando un entorno donde la seguridad sea vista no como un obstáculo, sino como un componente esencial de la productividad. La literatura sugiere que una cultura organizacional proactiva en temas de ciberseguridad reduce la propensión al riesgo y mejora los tiempos de reacción ante incidentes (Hadlington, 2021).

3.2.2 Gobernanza y políticas de seguridad adaptativas

Más allá de la capacitación y la cultura organizacional, la gobernanza en ciberseguridad se erige como un elemento estructurante que articula los recursos tecnológicos, humanos y normativos de manera coherente y estratégica. La gobernanza implica la definición de responsabilidades, la asignación de recursos, la evaluación continua del riesgo y la capacidad institucional de adaptación a nuevas amenazas. En entornos híbridos y remotos, donde las fronteras organizacionales son difusas y la interacción digital es continua, contar con marcos de gobernanza flexibles y bien definidos resulta esencial (Von Solms & Van Niekerk, 2013).

Los marcos de gobernanza efectivos se sustentan en políticas de seguridad informáticas claras, actualizadas y adaptativas. Estas políticas deben contemplar las dinámicas específicas del trabajo distribuido, tales como el acceso remoto a sistemas críticos, el uso compartido de dispositivos, la protección de datos en tránsito, la clasificación de la información sensible y la continuidad operativa en caso de incidentes. En este sentido, las políticas no deben diseñarse como documentos estáticos, sino como instrumentos vivos, sujetos a revisión periódica, retroalimentación de los usuarios y ajustes conforme al entorno tecnológico y regulatorio (Ahmad et al., 2014).

Un aspecto clave en este contexto es la adaptabilidad normativa. Las organizaciones deben ser capaces de ajustar sus políticas de seguridad ante cambios inesperados, como nuevas formas de ataque, actualizaciones de software o modificaciones en la legislación vigente. La experiencia durante la pandemia de COVID-19 demostró la importancia de contar con marcos ágiles que permitieran responder rápidamente al traslado masivo hacia el trabajo remoto, garantizando el cumplimiento de las regulaciones sin comprometer la operatividad (Kraemer-Mbula et al., 2019).

Asimismo, los marcos de gobernanza efectivos deben estar alineados con estándares internacionales reconocidos, como la norma ISO/IEC 27001, el marco NIST de Ciberseguridad, y el modelo COBIT 2019. Estos estándares proporcionan metodologías sistemáticas para la evaluación del riesgo, el control de accesos, la continuidad del negocio y la auditoría de procesos críticos. Las organizaciones que adoptan estos modelos reportan mejores indicadores de madurez en seguridad y una mayor capacidad de respuesta ante incidentes (ISACA, 2022).

La gobernanza, no obstante, también requiere liderazgo. La creación de comités de ciberseguridad, la designación de responsables ejecutivos (CISOs) y la asignación de recursos dedicados son prácticas que refuerzan la institucionalización de la seguridad digital. Sin una gobernanza efectiva y participativa, las políticas se vuelven inoperantes y la estrategia pierde cohesión. La combinación de liderazgo comprometido, políticas adaptativas y marcos normativos sólidos constituye, en suma, un factor organizacional determinante en la eficacia de la ciberseguridad en entornos de trabajo distribuidos.

4. Discusión

La transformación digital acelerada por la pandemia de COVID-19 ha generado una reconfiguración sustancial en las dinámicas laborales, dando paso al establecimiento de esquemas híbridos y remotos como modalidades predominantes en múltiples sectores organizacionales. Este cambio, aunque beneficioso en términos de flexibilidad y continuidad operativa, ha ampliado de manera exponencial la superficie de ataque de las organizaciones, debilitando los modelos de seguridad perimetral tradicionales y exigiendo el diseño e implementación de estrategias de ciberseguridad adaptadas a un nuevo ecosistema digital descentralizado (Gartner, 2023).

A lo largo de esta revisión, se ha demostrado que la eficacia de la ciberseguridad en estos entornos no depende exclusivamente de soluciones tecnológicas avanzadas, sino que responde a una conjunción de factores técnicos y organizacionales. Entre las estrategias tecnológicas más destacadas, la arquitectura Zero Trust emerge como un paradigma disruptivo al desplazar la confianza implícita por una lógica de verificación continua. Este modelo, sustentado en principios de autenticación reforzada, segmentación de red, análisis de comportamiento y control contextual de accesos, ha probado ser eficaz en la contención del movimiento lateral y en la reducción de accesos no autorizados en redes distribuidas (Rose et al., 2020; Shen et al., 2023). Sin embargo, su implementación exige una reestructuración profunda de la infraestructura tecnológica y de los procesos internos, lo que representa una barrera considerable para organizaciones con sistemas legados o recursos limitados.

Complementariamente, el uso de soluciones de seguridad basadas en la nube —como SASE, EDR y CASB— ha demostrado ser una respuesta eficiente, escalable y flexible para proteger a trabajadores que operan desde múltiples ubicaciones y dispositivos. La literatura científica respalda su capacidad para mejorar la visibilidad del tráfico, reforzar el control de accesos, automatizar la detección de amenazas y garantizar el cumplimiento normativo en entornos SaaS (Tang et al., 2022; Pal & Pandey, 2021). No obstante, estas herramientas requieren integración coherente con los sistemas existentes y un enfoque estratégico que incluya políticas claras de adopción tecnológica y supervisión constante.

En el plano organizacional, la revisión confirma que el elemento humano continúa representando el eslabón más débil de la ciberseguridad. La ausencia de formación especializada, la falta de conciencia sobre riesgos y la escasa interiorización de prácticas seguras generan un entorno propicio para que amenazas como el phishing, el ransomware y el robo de credenciales prosperen, especialmente en contextos donde los empleados operan sin supervisión directa (Hadlington, 2021). En este sentido, la capacitación continua y personalizada, basada en modelos de aprendizaje adaptativo y centrada en la modificación de conductas, se posiciona como un componente esencial de la defensa organizacional (Alavi et al., 2020). La incorporación de metodologías activas, simulaciones de ataques y evaluación

constante fortalece no sólo el conocimiento técnico, sino también la cultura de seguridad institucional.

La promoción de esta cultura resulta crucial para generar un sentido de corresponsabilidad entre todos los miembros de la organización. Aquellas entidades que logran establecer una cultura de seguridad sólida —caracterizada por la vigilancia activa, la comunicación fluida y el liderazgo comprometido— presentan menor recurrencia de incidentes y tiempos de respuesta más eficaces (Parsons et al., 2017). De este modo, la ciberseguridad deja de ser una responsabilidad exclusiva del área de TI para convertirse en una función transversal, integrada a la gobernanza corporativa.

Asimismo, los marcos de gobernanza y las políticas de seguridad adaptativas desempeñan un papel decisivo en la sostenibilidad de las estrategias implementadas. La capacidad de adaptar protocolos y normativas ante amenazas emergentes, cambios tecnológicos o transformaciones legales garantiza la continuidad operativa sin sacrificar la protección de la información (Von Solms & Van Niekerk, 2013). En particular, la alineación con estándares internacionales como ISO/IEC 27001 y NIST SP 800-207 permite estandarizar buenas prácticas, establecer mecanismos de control y fomentar una mejora continua (Ahmad et al., 2014).

En síntesis, la ciberseguridad en entornos de trabajo híbridos y remotos debe ser concebida como un sistema socio-técnico complejo, en el que la interacción entre tecnología, personas y estructuras normativas determina el grado de resiliencia organizacional. Las estrategias más efectivas son aquellas que integran soluciones técnicas robustas con procesos organizativos adaptativos y una fuerte cultura institucional de seguridad. La omisión de alguno de estos elementos no sólo reduce la eficacia general, sino que incrementa la exposición ante amenazas cada vez más sofisticadas. Por tanto, se hace imprescindible que las organizaciones asuman un enfoque holístico, proactivo y continuo en la gestión de su ciberseguridad, adaptándose a las dinámicas cambiantes del trabajo digital contemporáneo.

5. Conclusiones

La revisión realizada permite concluir que la ciberseguridad en entornos de trabajo híbridos y remotos requiere un enfoque integral que combine soluciones tecnológicas avanzadas con estructuras organizacionales adaptativas. La migración del trabajo presencial a esquemas distribuidos ha evidenciado las limitaciones de los modelos de seguridad tradicionales, haciendo indispensable la adopción de estrategias orientadas a la verificación continua, la descentralización del control y la protección dinámica de los recursos digitales. En este contexto, la arquitectura Zero Trust y las soluciones de seguridad basadas en la nube representan componentes fundamentales para una defensa eficaz, permitiendo controlar accesos, detectar amenazas en tiempo real y garantizar la continuidad operativa en escenarios descentralizados.

No obstante, la eficacia de estas tecnologías está fuertemente condicionada por factores organizacionales. La capacitación continua del personal y la promoción de una cultura de seguridad sólida son elementos imprescindibles para reducir la exposición a errores humanos, mejorar la capacidad de respuesta y fomentar una actitud proactiva frente a las amenazas. Las organizaciones que integran la formación como parte estructural de su estrategia logran una mejor apropiación de las herramientas y políticas, fortaleciendo así sus mecanismos de defensa.

Asimismo, la existencia de marcos de gobernanza robustos y políticas de seguridad adaptativas facilita una gestión coherente, ágil y alineada con los riesgos emergentes del entorno digital. La capacidad de revisar, ajustar y hacer cumplir estas políticas en tiempo real resulta crucial para mitigar vulnerabilidades, especialmente en entornos laborales cambiantes y altamente digitalizados.

En conjunto, la ciberseguridad en el trabajo híbrido y remoto no puede entenderse como una cuestión meramente técnica, sino como una función estratégica de la organización. Las entidades que reconozcan esta complejidad, inviertan en formación, promuevan una cultura resiliente y mantengan una gobernanza activa, estarán mejor posicionadas para enfrentar las amenazas del entorno digital contemporáneo y garantizar la integridad, disponibilidad y confidencialidad de su información.

CONFLICTO DE INTERESES

“Los autores declaran no tener ningún conflicto de intereses”.

Referencias Bibliográficas

Ahmad, A., Maynard, S.B. & Park, S. Information security strategies: towards an organizational multi-strategy perspective. *J Intell Manuf* 25, 357–370 (2014). https://doi.org/10.1007/s10845-012-0683-0

Alavi, R., Islam, S., & Ware, J. (2020). Revisiting information security training: A framework for understanding and enhancing security culture. *Computers & Security, 88*, 101620.

Celi-Párraga, R. J., Mora-Olivero, A. P., Boné-Andrade, M. F., & Sarmiento-Saavedra, J. C. (2023). *Ingeniería del Software II: Implementación, Pruebas y Mantenimiento*. Editorial Grupo AEA. https://doi.org/10.55813/egaea.l.2022.20

ENISA. (2022). *Threat Landscape 2022: Cybersecurity threats and trends*. European Union Agency for Cybersecurity.

Galarza-Sánchez, P. C. (2023). Adopción de Tecnologías de la Información en las PYMEs Ecuatorianas: Factores y Desafíos. *Revista Científica Zambos*, *2*(1), 21-40. https://doi.org/10.69484/rcz/v2/n1/36

Galarza-Sánchez, P. C., Agualongo-Yazuma, J. C., & Jumbo-Martínez, M. N. (2022). Innovación tecnológica en la industria de restaurantes del Cantón Pedro

Vicente Maldonado. *Journal of Economic and Social Science Research*, *2*(1), 31–43. https://doi.org/10.55813/gaea/jessr/v2/n1/45

Gartner. (2023). *Gartner Forecasts Hybrid Work Will Be the Norm by 2025*.

Gartner. (2023). *Market Guide for Single-Vendor SASE*. Gartner Inc. https://www.gartner.com/document/4001031

Hadlington, L. (2021). Human factors in cybersecurity: Examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon, 7*(1), e05962.

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

ISACA. (2022). *State of Cybersecurity 2022: Global Update on Workforce Efforts, Resources and Cyberoperations*.

Kindervag, J. (2021). *Zero Trust: A paradigm shift in cybersecurity*. Forrester Research.

Kraemer-Mbula, E., Tijssen, R., Wallace, M. L., & McLean, R. (Eds.). (2019). *Transforming Research Excellence: New Ideas from the Global South*. African Minds. http://library.oapen.org/handle/20.500.12657/23441

Pal, A., & Pandey, R. (2021). Cloud Access Security Broker: Key Enabler for Enterprise Cloud Security. *Procedia Computer Science, 192*, 4482–4491.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., & McCormac, A. (2017). The human aspects of information security questionnaire (HAIS-Q): Two further validation studies. *Computers & Security, 66*, 40–51. https://doi.org/10.1016/j.cose.2017.01.004

PwC. (2022). *2022 Global Digital Trust Insights Survey*. PricewaterhouseCoopers. https://www.pwc.com/gx/en/issues/cybersecurity/digital-trust-insights.html

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture (NIST SP 800-207)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

Shen, H., Liu, X., & Liu, Y. (2023). Zero Trust Architecture and Access Control Strategy in Remote Work Environments. *Journal of Cyber Security Technology, 7*(2), 95–112.

Tang, J., Wu, Q., & Li, Y. (2022). Cloud-Based Security Models for Remote Workforce: Evaluating the Effectiveness of SASE and EDR. *Computers & Security, 118*, 102739.

Verizon. (2023). *Data Breach Investigations Report (DBIR) 2023*. Verizon Enterprise. https://www.verizon.com/business/resources/reports/dbir/

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004