CyberTrack 360
Una Guía de autodiagnóstico para pymes basada en ISO/IEC 27001

Flor Alba Tovar Perea

Jhon Fredy Aguirre Cañón

Universidad EAN

Facultad de Ingeniería

Ingeniería de Sistemas

Bogotá, Colombia

25/05/2026

Título del Artículo

Flor Alba Tovar Perea

Jhon Fredy Aguirre Cañón

Trabajo de grado presentado como requisito para optar al título de:

Ingeniero de Sistemas

Director

William López Castrillón

Universidad EAN

Facultad de Ingeniería

Ingeniería de Sistemas

Bogotá, Colombia

25/05/2026

Nota de aceptación:

Firma del jurado

Firma del jurado

Firma del director del trabajo de grado

Ciudad, día/mes/año

El mejor momento para reparar el techo es cuando está brillando el sol.

John F. Kennedy.

Agradecimientos

Agradecemos a la Universidad EAN y a los docentes del programa de Ingeniería de Sistemas por los conocimientos compartidos y el acompañamiento en cada una de sus materias y finalmente a las microempresas colombianas, cuya realidad sirvió de inspiración para este proyecto.

Resumen

La creciente dependencia de los sistemas digitales ha incrementado la exposición de las microempresas a riesgos relacionados con la seguridad de la información. Aunque existen marcos reconocidos internacionalmente como ISO/IEC 27001, ISO/IEC 27002 y NIST Cybersecurity Framework, su complejidad dificulta su adopción en organizaciones con recursos limitados. En este contexto, el objetivo de la investigación fue diseñar y evaluar un producto mínimo viable (MVP) denominado CyberTrack 360, orientado a facilitar el diagnóstico inicial de madurez en seguridad de la información y la adopción progresiva de controles esenciales en microempresas colombianas.

La investigación se desarrolló bajo un enfoque mixto, alcance descriptivo y diseño no experimental transversal, apoyado en la metodología Design Science Research Methodology (DSRM). Se aplicó una encuesta a 50 propietarios y cargos gerenciales de microempresas para identificar necesidades, barreras y percepciones relacionadas con la ciberseguridad. Los resultados evidenciaron que el 82% de los participantes considera que la pérdida de acceso a la información tendría un impacto alto o muy alto en sus operaciones, mientras que solo el 28% percibe una alta probabilidad de sufrir incidentes. Asimismo, se identificaron bajos niveles de adopción de controles básicos, predominando barreras asociadas a la falta de conocimiento técnico (72%), desconocimiento sobre cómo iniciar (68%) y percepción de altos costos (54%).

A partir de estos hallazgos se desarrolló CyberTrack 360, una plataforma web basada en cuestionarios por roles, evaluación de madurez, generación de recomendaciones priorizadas, gestión de evidencias y políticas básicas de seguridad. Los resultados obtenidos respaldan la hipótesis de que las microempresas requieren herramientas prácticas, comprensibles y accesibles para facilitar la adopción de controles de seguridad. Se concluye que CyberTrack 360 constituye una alternativa viable para reducir la brecha entre el conocimiento de buenas prácticas y su implementación efectiva, promoviendo una cultura de mejora continua en organizaciones con recursos limitados.

Palabras clave: ciberseguridad, microempresas, ISO/IEC 27001, autodiagnóstico, madurez en seguridad, gestión de evidencias, mejora continua.

Abstract

The increasing reliance on digital systems has heightened microenterprises' exposure to risks related to information security. Although internationally recognized frameworks such as ISO/IEC 27001, ISO/IEC 27002, and the NIST Cybersecurity Framework exist, their complexity makes them difficult to adopt in organizations with limited resources. In this context, the objective of this research was to design and evaluate a minimum viable product (MVP) called CyberTrack 360, aimed at facilitating the initial assessment of information security maturity and the progressive adoption of essential security controls in Colombian microenterprises.

The research was conducted using a mixed-method approach with a descriptive scope and a non-experimental cross-sectional design, supported by the Design Science Research Methodology (DSRM). A survey was administered to 50 owners and managerial personnel of microenterprises to identify cybersecurity needs, barriers, and perceptions. The results revealed that 82% of participants considered the loss of access to information to have a high or very high operational impact, while only 28% perceived a high probability of experiencing a cybersecurity incident. Additionally, low levels of adoption of basic security controls were identified, with the main barriers being lack of technical knowledge (72%), uncertainty about how to begin (68%), and perceived implementation costs (54%).

Based on these findings, CyberTrack 360 was developed as a web-based platform incorporating role-based questionnaires, maturity assessment, prioritized recommendations, evidence management, and basic security policies. The results support the hypothesis that microenterprises require practical, understandable, and affordable tools to facilitate the adoption of information security controls. It is concluded that CyberTrack 360 represents a viable alternative to reduce the gap between awareness of best practices and their effective implementation, promoting a culture of continuous improvement in organizations with limited resources.

Keywords: cybersecurity, microenterprises, ISO/IEC 27001, self-assessment, security maturity, evidence management, continuous improvement.

Introducción

En los últimos años, la transformación digital ha cambiado la forma en que las empresas operan, almacenan y utilizan la información. Hoy activos como el correo electrónico, los servicios en la nube y el acceso remoto son parte esencial del funcionamiento organizacional. Sin embargo, este avance también ha incrementado la exposición a riesgos asociados a la seguridad de la información digital. Informes recientes evidencian que una proporción significativa de los incidentes está relacionada a motivaciones económicas como el ransomware o la extorsión digital, aprovechando debilidades básicas como contraseñas inseguras o el desconocimiento del usuario (Microsoft., 2025; Verizon., 2025).

Este panorama afecta especialmente a las microempresas, que debido a limitaciones de recursos, conocimiento técnico y estructura organizacional, suelen carecer de controles básicos estandarizados. Estudios como el Data Breach Investigations Report, muestran que estas organizaciones son más vulnerables a interrupciones operativas y pérdida de información crítica, impactando directamente su sostenibilidad (Verizon., 2025).

En las primeras fases de una empresa se prioriza el crecimiento y la operación, relegando la seguridad de la información a un segundo plano. Según la European Union Agency for Cybersecurity (ENISA), las pequeñas y medianas empresas enfrentan barreras recurrentes en ciberseguridad por presupuesto, capacidades técnicas y soporte especializado para aplicar medidas sostenidas en el tiempo con ciclos de mejora continua (Sarri et al., 2021). Simultáneamente, El National Institute of Standards and Technology (NIST) señala que muchas organizaciones pequeñas carecen de planes estructurados y requieren guías prácticas para iniciar la gestión del riesgo (NIST, 2024a).

El problema de fondo no es la ausencia de estándares, sino la brecha entre conocer buenas prácticas y ejecutarlas de manera estructurada. Existen marcos robustos y altamente reconocidos como ISO/IEC 27001 e ISO/IEC 27002 orientados a la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI o ISMS) mediante gestión del riesgo y mejora continua (ISO/IEC, 2022a, 2022b). A su vez, el NIST Cybersecurity Framework (CSF) 2.0 propone una estructura flexible para identificar, proteger, detectar, responder y recuperarse ante incidentes (NIST, 2024b). No obstante, su aplicación en microempresas suele ser limitada debido a su complejidad, extensión y lenguaje técnico.

Diversos estudios coinciden en que persisten brechas de conocimiento, financiación, formación y acompañamiento, lo que dificulta la implementación sostenida de controles básicos (Rombaldo et al., 2023). Esto se traduce en fallas recurrentes como contraseñas débiles, ausencia de autenticación multifactor (MFA), copias de seguridad no verificadas, accesos sin supervisión y falta de evidencia comprobable. Por todo esto, la ciberseguridad deja de ser un tema exclusivamente técnico y se convierte en un factor clave para la continuidad del negocio y la gestión organizacional.

A partir de esta necesidad surge CyberTrack 360, un MVP concebido como una plataforma web de autodiagnóstico que traduce estándares internacionales en acciones comprensibles y aplicables, basada en ISO/IEC 27001 e ISO/IEC 27002. Su enfoque no está orientado a la certificación, sino a facilitar un punto de partida práctico para identificar brechas, priorizar mejoras y registrar evidencias de avance (CIS., 2024).

En este sentido, el objetivo general de esta investigación es diseñar y evaluar, durante 2026, un producto mínimo viable (MVP) de la plataforma web CyberTrack 360, basado en la norma ISO/IEC 27001:2022, que permita a microempresas colombianas diagnosticar su nivel inicial de madurez en seguridad de la información digital y obtener un plan de mejora priorizado con trazabilidad mediante evidencias.

En consecuencia, la pregunta de investigación que orienta el estudio es: ¿cómo diseñar, desarrollar y evaluar una herramienta práctica, basada en estándares internacionales, que permita a las microempresas colombianas diagnosticar su nivel inicial de madurez en seguridad de la información digital y avanzar en la implementación de controles esenciales de manera progresiva y verificable?

Se plantea como hipótesis principal que el uso de una herramienta de autodiagnóstico simplificada, basada en estándares internacionales y adaptada a un lenguaje comprensible, facilita la adopción inicial de controles de seguridad de la información digital en microempresas, mejorando su capacidad para gestionar riesgos básicos.

Adicionalmente se plantea como hipótesis secundaria que la incorporación de mecanismos de trazabilidad mediante evidencias incrementa la implementación efectiva de controles al permitir verificar y dar seguimiento a las acciones realizadas.

Finalmente, CyberTrack 360 se plantea no como una herramienta de certificación, sino como un punto de entrada práctico para reducir la complejidad normativa y facilitar su adopción progresiva, en organizaciones con recursos limitados. Para validar esta propuesta, el estudio adopta un enfoque de diseño y evaluación de un artefacto tecnológico, permitiendo analizar su utilidad, comprensión y viabilidad mediante la construcción y prueba del MVP.

Marco teórico

El presente marco teórico integra los principales referentes conceptuales, normativos y metodológicos que sustentan el diseño de CyberTrack 360, plataforma web orientada a evaluar el nivel inicial de madurez en ciberseguridad de microempresas en Colombia. Este marco evidencia que, aunque existen guías y estándares internacionales, persisten dificultades significativas para su adopción en organizaciones pequeñas.

En el contexto económico, las micro, pequeñas y medianas empresas (pymes) representan un componente crítico del tejido productivo. Según el Banco Mundial y la Organización para la Cooperación y el Desarrollo Económicos (OCDE), las pymes constituyen aproximadamente el 90% de las empresas a nivel global y generan más del 50% del empleo (World Bank Group, 2026; OCDE, 2026). En Colombia representan más del 99% del tejido empresarial y aportan cerca del 40% del PIB. Sin embargo, esta relevancia contrasta con su alta vulnerabilidad frente a riesgos de ciberseguridad, debido a limitaciones en recursos, conocimientos y adopción tecnológica.

Se define para este proyecto información, como los datos procesados por un sistema, susceptibles de alteración, robo o destrucción y ciberseguridad como las capacidades orientadas a prevenir, detectar, responder y recuperarse de incidentes que afectan la confidencialidad, integridad y disponibilidad de dicha información. Estudios evidencian que una proporción significativa de pymes carece de políticas formales y presenta bajos niveles de adopción de controles básicos como la autenticación MFA (Bada, M., Nurse J. R. C., 2019).

A través de encuestas realizadas a propietarios y gerentes de pequeños negocios se evidencia que las microempresas enfrentan barreras presupuestales, falta de conocimiento técnico y baja percepción de urgencia. Además, se identifica una brecha entre reconocer el impacto de un incidente y ejecutar medidas concretas de protección. Aunque algunos participantes consideran importante la ciberseguridad, la mayoría no la prioriza como inversión inmediata. En el Anexo A se encuentra el modelo de encuesta aplicada.

El desarrollo del sistema se apoya en la Investigación en Ciencias del Diseño (DSRM), propuesta por Hevner et al., (2004), la cual plantea crear soluciones tecnológicas para resolver problemas organizacionales con rigor científico. Desde una perspectiva normativa, se justifica con la gestión del riesgo definida por Humphreys (2025) para los sistemas de gestión de seguridad de la información (SGSI), evitando que el diagnóstico sea una lista de chequeo aislada.

A nivel normativo, la norma ISO/IEC 27001:2022 establece los requisitos para implementar, mantener y mejorar un SGSI, promoviendo un enfoque basado en la gestión del riesgo y mejora continua mediante el ciclo PHVA (planear-hacer-verificar-actuar) (ISO/IEC, 2022a). Este enfoque es clave para las microempresas al no depender únicamente de herramientas aisladas.

De manera complementaria, la norma ISO/IEC 27002:2022 proporciona controles organizacionales, humanos, físicos y tecnológicos (ISO/IEC, 2022b). Esta clasificación estructura los cuestionarios por roles en CyberTrack 360, reconociendo que la seguridad no depende sólo de herramientas técnicas, sino también de políticas, personas y procesos.

Por su parte, el NIST Cybersecurity Framework (CSF) 2.0 propone un enfoque basado en gestión del riesgo y advierte que el cumplimiento no equivale necesariamente a reducción efectiva del riesgo (NIST, 2024a). En línea con esto, CyberTrack 360 prioriza acciones según el impacto real en cada empresa.

Igualmente el Center for Internet Security (CIS) define el Implementation Group 1 (IG1) como controles esenciales para organizaciones con recursos limitados (CIS., 2024), respaldando prácticas como autenticación MFA, copias de seguridad (backups) y control de accesos.

El factor humano constituye un elemento crítico. Según Tan Jia Jun et al. (2025), existe una limitada compresión operativa de conceptos como ingeniería social, lo que evidencia que la capacitación por sí sola no garantiza cambios en el comportamiento. Por ello, CyberTrack 360 incorpora seguimiento y evidencia para convertir el conocimiento en acciones comprobables.

Dado que la solución propuesta es una plataforma web, se consideran los lineamientos del OWASP (Open Worldwide Application Security Project) Top 10 como referencia para mitigar vulnerabilidades. (OWASP Foundation, 2025). En Colombia la Ley 1581 de 2012 y el Decreto 1377 de 2013 establecen principios para el tratamiento de datos personales (Barreras et al., 2012; Santos, 2013). Además, el Registro Nacional de Bases de Datos (RNBD), define información mínima para su registro (Santos, 2014), lo que implica incorporar controles de privacidad y trazabilidad.

Finalmente, la viabilidad de CyberTrack 360 se expone desde los modelos de adopción tecnológica. Según la Teoría Unificada de Aceptación y Uso de Tecnología (UTAUT 3) propuesta por Venkatesh et al., (2016), el éxito del software depende de la expectativa de esfuerzo y la

utilidad percibida. Por ello, la plataforma prioriza una interfaz liviana y resultados operativos directos para facilitar su integración en la operación diaria de las microempresas.

Estado del Arte

El estado del arte del presente estudio se desarrolló siguiendo los lineamientos de la metodología PRISMA, buscando identificar enfoques, herramientas y tendencias relacionadas con la ciberseguridad en microempresas y la adopción de marcos normativos internacionales.

Para ello, se consultaron bases de datos académicas y fuentes especializadas, incluyendo literatura indexada en Scopus, Web of Science y repositorios técnicos. La ecuación de búsqueda utilizada incluyó combinaciones de términos como: “cybersecurity AND SMEs”, “ISO 27001 adoption small business”, “cyber higiene SMEs”, “information security maturity small companies”, empleando operadores boleanos. Se consideraron publicaciones en inglés y español de los últimos 10 años (2016-2026), aunque en mayor proporción entre 2022 y 2026. Como criterios de inclusión se seleccionaron estudios que abordaran implementación de ciberseguridad en pequeñas empresas, barreras de adopción, modelos de madurez o herramientas de apoyo. Se excluyeron estudios enfocados exclusivamente en grandes organizaciones o con enfoques altamente técnicos sin aplicabilidad práctica en microempresas.

El proceso de selección permitió identificar una tendencia clara: aunque existen múltiples marcos y estándares reconocidos como ISO/IEC 27001 e ISO/IEC 27002 (ISO/IEC, 2022b, 2022a), el NIST Cybersecurity Framework (CSF) 2.0 (NIST, 2024b) y la guía de arranque para pequeñas empresas basada en CSF 2.0 (NIST, 2024a), su adopción en microempresas sigue siendo limitada debido a factores como complejidad, costos y falta de acompañamiento (NIST, 2024b; Sarri et al., 2021). Esta situación coincide con lo planteado por Rombaldo et al. (2023), quienes evidencian que las pequeñas empresas suelen ser “no conscientes, no financiadas y no capacitadas” en materia de ciberseguridad.

Diversos estudios coinciden en que la principal barrera no es la ausencia de marcos normativos, sino la dificultad para traducirlos en acciones concretas. Azinheira et al., (2023), proponen metodologías para mapear estándares como ISO 27001 en guías comprensibles, mientras que Gundu y Mmango (2026) destacan la necesidad de simplificar prácticas como la gestión de contraseñas para asegurar su adopción en entornos con recursos limitados. En esta misma línea, Adriko y Nurse, (2026) identifican una brecha significativa entre la percepción del riesgo y la inversión real en controles, lo que limita la implementación efectiva de medidas preventivas.

Por otra parte, investigaciones recientes también resaltan el impacto del factor humano en la seguridad organizacional. Hao et al., (2026) evidencian que el estrés relacionado con la seguridad

de la información en los responsables de las empresas puede afectar negativamente el desempeño organizacional, lo que refuerza la necesidad de soluciones simples, guiadas y comprensibles.

En el ámbito aplicado, existen múltiples plataformas orientadas a la gestión de seguridad de la información y cumplimiento normativo, como ISOTools, ISMS.online, Thoropass, Secureframe, Drata, Scytale y Sprinto. Estas soluciones se caracterizan por ofrecer automatización, integración con múltiples sistemas y soporte a procesos de auditoría y certificación (ISO TOOLS, 2026a, 2026b; Edwards, 2026; Peters, 2025; Thoropass., 2026; Secureframe, 2026a, 2026b; Drata, 2026a, 2026b; Scytale, 2026; Sprinto, 2026a, 2026b). Su principal aporte radica en transformar el cumplimiento de flujos de trabajo estructurados y en facilitar la trazabilidad mediante evidencia automatizada.

Sin embargo, estas herramientas presentan limitaciones relevantes en el contexto de las microempresas. Aunque resultan valiosas para organizaciones con infraestructura conectable, mayor capacidad operativa u objetivos de certificación formal, su implementación suele implicar altos costos, dependencia de integraciones tecnológicas, curva de aprendizaje y una carga administrativa considerable. Estas condiciones reducen su viabilidad en organizaciones con baja madurez digital, por lo que persiste un vacío en el segmento de microempresas que requieren soluciones más accesibles, livianas y priorizadas, apoyadas en prácticas de higiene esencial como CIS Implementation Group 1 (IG1) (CIS, 2024).

Adicionalmente, reportes de la industria evidencian que las pequeñas organizaciones son especialmente vulnerables a amenazas como ransomware cuando presentan fallas en controles básicos como autenticación multifactor, copias de seguridad, gestión de accesos y protección del correo electrónico. Por ello, estas medidas deben asumirse como mínimos estratégicos obligatorios y no como acciones opcionales (Verizon, 2025; Microsoft, 2025). Así mismo IBM (2025). Señala que los costos de las brechas siguen siendo elevados y que detectar y contener incidentes con mayor rapidez reduce su impacto, reforzando la necesidad de prácticas de seguridad repetibles y verificables.

En síntesis, el análisis del estado del arte permite identificar tres hallazgos clave: primero, existe una amplia disponibilidad de marcos normativos robustos, pero con baja adopción en microempresas; segundo, las soluciones existentes están orientadas a automatización y

certificación, lo que limita su aplicabilidad en contextos de baja madurez; y tercero, persiste una brecha entre conocimiento y ejecución en ciberseguridad.

Estos hallazgos se alinean con la evidencia empírica obtenida en el presente estudio mediante encuestas, donde se identificó que, aunque los empresarios reconocen el impacto de un incidente, no cuentan con herramientas prácticas para gestionarlo. En este contexto, CyberTrack 360 se plantea como una alternativa que busca cerrar esta brecha, mediante un enfoque de diagnóstico simplificado, priorización de acciones y trazabilidad de evidencias adaptadas al contexto de las microempresas.

Tabla 1
Comparación simplificada de soluciones industriales y su ajuste a microempresas.

Autor(es) / Año	Título del estudio	Objetivo principal	Metodología empleada	Variables analizadas	Principales hallazgos	Limitaciones reportadas	Relación con el proyecto actual
ISO TOOLS (2026)	ISOTools	Soportar la implementación y mantenimiento de un SGSI basado en ISO 27001, con énfasis en control documental y auditoría.	Análisis documental comparativo de funcionalidades declaradas por el proveedor.	Registros de auditoría, control de acceso, cifrado, evidencia, trazabilidad, soporte a SGSI.	Centraliza procesos del SGSI y fortalece la trazabilidad mediante evidencia registrada en la herramienta.	Puede resultar pesado en documentación y administración para microempresas que no buscan certificación formal.	Sirve como referente de centralización y trazabilidad, pero CyberTrack 360 propone una entrada más liviana, con menor carga documental.
ISMS.online (2025–2026)	ISMS.online	Facilitar la gestión de riesgos, controles, activos y Statement of Applicability (SoA) dentro de un SGSI.	Análisis documental comparativo de capacidades funcionales y flujos de auditoría.	SoA, activos, riesgos, controles, paquetes de auditoría, trazabilidad entre tareas y evidencia.	Convierte el cumplimiento en flujo de trabajo estructurado y fortalece la preparación de auditoría.	La gestión continua puede ser exigente para microempresas con baja capacidad operativa o administrativa.	Aporta como referencia en estructura de auditoría y trazabilidad, pero CyberTrack 360 reduce complejidad y prioriza controles esenciales.
Thoropass (2026)	Thoropass	Automatizar el recorrido de cumplimiento y preparación para auditoría, incluyendo recolección de evidencia y acompañamiento experto.	Análisis documental comparativo de plataforma de automatización de cumplimiento.	Automatización, flujos de evidencia, políticas, tareas, acompañamiento experto, integraciones.	Ofrece guía y soporte experto para acelerar procesos de cumplimiento y certificación.	Requiere alta dependencia de integraciones y presenta un costo/stack más alineado con organizaciones de mayor madurez.	Contrasta con CyberTrack 360, que evita depender de automatización avanzada y busca adopción inicial en microempresas.
Secureframe (2026)	Secureframe	Automatizar la recolección de evidencia, la gestión de auditoría y el cumplimiento continuo mediante integraciones y repositorios.	Análisis documental comparativo basado en documentación del proveedor.	Integraciones, data room, carga manual, evidencia continua, soporte de auditoría.	Permite evidencia continua y soporte de auditoría en un esquema “todo en uno”.	Está pensado principalmente para entornos tecnológicos con infraestructura conectable; puede ser sobredimensionado para microempresas.	Aporta como benchmark en evidencia continua, pero CyberTrack 360 adopta una trazabilidad manual y simple, más realista para microempresas.
Drata (2026)	Drata	Centralizar controles, riesgos, políticas y evidencias con altos niveles de automatización para cumplimiento normativo.	Análisis documental comparativo de plataforma comercial orientada a certificación.	Automatización, controles, políticas, riesgos, evidencia, integraciones, cumplimiento continuo.	Escala bien en entornos multi-framework y con necesidades avanzadas de monitoreo de cumplimiento.	Puede sobredimensionarse para microempresas por costo, complejidad y dependencia de integraciones.	Funciona como contraste directo: CyberTrack 360 sacrifica automatización avanzada para ganar viabilidad de adopción inicial.
Scytale (2026)	Scytale	Automatizar la recolección de	Análisis documental	Automatización, integraciones,	Combina automatización	Alta dependencia de integraciones	Refuerza que el mercado premium

		evidencia y acompañar procesos de cumplimiento mediante integraciones y soporte experto.	comparativo de solución de cumplimiento.	evidencia, acompañamiento experto, auditoría.	y acompañamiento, lo que reduce carga operativa en organizaciones con cierto nivel de madurez digital.	y menor ajuste a contextos con infraestructura limitada.	asume conectividad e integración; CyberTrack 360 se diseña para contextos con menor madurez tecnológica.
Sprinto (2026)	Sprinto	Gestionar el ciclo de vida de la evidencia con captura automatizada, sello de tiempo y rastro de auditoría.	Análisis documental comparativo de plataforma enfocada en auditoría continua.	Evidencia, rastro de auditoría, sello de tiempo, automatización, integraciones, cumplimiento.	Reduce carga manual y fortalece la auditabilidad de la evidencia.	Se orienta más a auditoría/certificación y depende de integraciones para aprovechar todo su potencial.	Inspira la importancia de la trazabilidad, pero CyberTrack 360 traslada ese principio a una bitácora simple y evidencia manual.
CyberTrack 360 (propuesta actual)	CyberTrack 360	Permitir a microempresas colombianas diagnosticar su nivel inicial de madurez en seguridad digital y obtener un plan de mejora priorizado con trazabilidad simple.	Diseño de MVP basado en priorización de controles esenciales, evidencia manual y enfoque por roles.	Diagnóstico por roles, evidencia manual, bitácora, controles mínimos, plan de mejora, adopción inicial.	Se diferencia por ofrecer una entrada liviana, con menor costo, menor dependencia de integraciones y énfasis en hábitos de mejora continua.	Menor automatización, menor orientación a certificación formal y necesidad de disciplina operativa por parte del usuario.	Es el proyecto actual; sintetiza los aportes del estado del arte y se posiciona como alternativa especializada para microempresas.

La Tabla 1 indica que las opciones de las plataformas industriales están orientadas a maximizar automatización e integraciones para auditoría/certificación, mientras que la opción de CyberTrack 360 se orienta a entrar con un enfoque más sencillo en la ruta con evidencia manual y trazabilidad. Este enfoque responde a la realidad descrita para pequeñas empresas: capacidades limitadas y necesidad de guías prácticas para iniciar y sostener gestión del riesgo sin depender de infraestructura compleja (NIST, 2024b).

Metodología

El presente estudio adopta un enfoque mixto con alcance descriptivo y diseño no experimental transversal, porque busca comprender una problemática real y diseñar un artefacto tecnológico orientado a su solución. La combinación de técnicas cualitativas y cuantitativas permite integrar la comprensión del contexto organizacional con la evaluación de resultados obtenidos durante el desarrollo del MVP (Creswell & Creswell, 2018). El diseño no experimental se justifica porque las variables no son manipuladas y la información se recolecta en un único momento de observación (Hernández Sampieri et al., 2018) La investigación se fundamenta en la metodología de Investigación en Ciencias del Diseño (DSRM), propuesta por Hevner et al. (2004) y Peffers et al. (2007), enfocada en construir y validar soluciones tecnológicas para problemas organizacionales con criterios de utilidad y rigor científico.

El artefacto desarrollado corresponde al MVP de CyberTrack 360, una plataforma web de autodiagnóstico de madurez en ciberseguridad para microempresas colombianas, basada en ISO/IEC 27001:2022 e ISO/IEC 27002:2022, NIST CSF 2.0 y CIS IG1, buscando traducir estándares técnicos en acciones comprensibles para organizaciones con recursos limitados.

Como parte de la fase de relevancia, se realizaron entrevistas y encuestas exploratorias a propietarios y cargos gerenciales de microempresas. La población objetivo estuvo conformada por negocios entre 2 y 10 empleados. Se utilizó muestreo no probabilístico por conveniencia y se recopilaron cincuenta (50) respuestas para identificar patrones sobre percepción del riesgo, barreras de adopción y capacidad de respuesta ante incidentes. El instrumento aplicado se presenta en el Anexo A y los modelos desarrollados se presentan en el Anexo B.

Los hallazgos permitieron identificar una brecha entre reconocer el impacto potencial de un incidente y aplicar controles básicos de seguridad. Esta información orientó el diseño funcional del MVP y complementó la revisión bibliográfica y el estado del arte.

Desde la perspectiva de ingeniería, el MVP se desarrolló como SPA con React 18, TypeScript, Vite y Tailwind CSS. Para la gestión de datos y servicios backend se empleó Supabase, integrando PostgresSQL, autenticación y almacenamiento de evidencias. También se utilizaron React Hook Form y Zod para validación de formularios, TanStack React Query para sincronización de datos y Recharts para indicadores y reportes de madurez.

El sistema se estructuró mediante cuestionarios dinámicos por roles organizacionales, vinculando cada pregunta con controles, recomendaciones y evidencias verificables. Un modelo de puntuación dinámica calcula el nivel de madurez y clasifica los resultados en riesgo crítico, mejora necesaria y fortaleza. Adicionalmente, se elaboró un conjunto de políticas básicas de seguridad alineadas con los controles evaluados por la plataforma, con el propósito de proporcionar a las organizaciones documentos de apoyo para la implementación inicial de buenas prácticas. Los modelos desarrollados se presentan en el Anexo D.

La plataforma incorpora gestión de evidencias mediante documentos o capturas vinculados a una bitácora de auditoría, facilitando la verificación de acciones y el seguimiento de mejora continua.

La evaluación del MVP se realizó mediante pruebas funcionales controladas para validar su comprensión, utilidad, coherencia entre pregunta-recomendación-evidencia y viabilidad de adopción utilizando un análisis descriptivo cualitativo y cuantitativo, apoyado en estadística básica.

Resultados

Durante la investigación se aplicó un instrumento de recolección de información a cincuenta (50) propietarios y cargos gerenciales de pequeñas empresas pertenecientes a los sectores de servicios, comercio, industria y otros sectores económicos.

Los participantes representan organizaciones en promedio entre dos y diez empleados. La encuesta permitió identificar la percepción frente a los riesgos digitales, las prácticas actuales de seguridad, las barreras para la adopción de controles y la disposición para implementar herramientas de apoyo. La información recopilada sirvió como base para definir los requerimientos funcionales del MVP CyberTrack 360.

Una vez recopilada la información, las respuestas fueron consolidadas en una matriz de análisis y procesadas mediante estadística descriptiva. Se calcularon frecuencias y porcentajes para identificar tendencias relacionadas con percepción del riesgo, preparación organizacional, adopción de controles, barreras de implementación y preferencias de apoyo.

Las preguntas abiertas fueron agrupadas en categorías temáticas para identificar patrones recurrentes sobre riesgos digitales y necesidades de ciberseguridad. Los resultados se presentan mediante tablas y figuras para facilitar su interpretación.

Para comprender el contexto de las organizaciones participantes, la Tabla 2 presenta la caracterización general de las empresas incluidas en el estudio.

Tabla 2

Caracterización de las empresas participantes

Variable	Categoría	Frecuencia	Porcentaje
Número de empleados	1–2 empleados	12	24%
Número de empleados	3–5 empleados	18	36%
Número de empleados	6–10 empleados	15	30%
Número de empleados	Más de 10 empleados	5	10%
Sector económico	Servicios	18	36%
Sector económico	Comercio	16	32%
Sector económico	Industrial	10	20%
Sector económico	Otros	6	12%

Nota. Elaboración propia a partir de las encuestas aplicadas (2026).

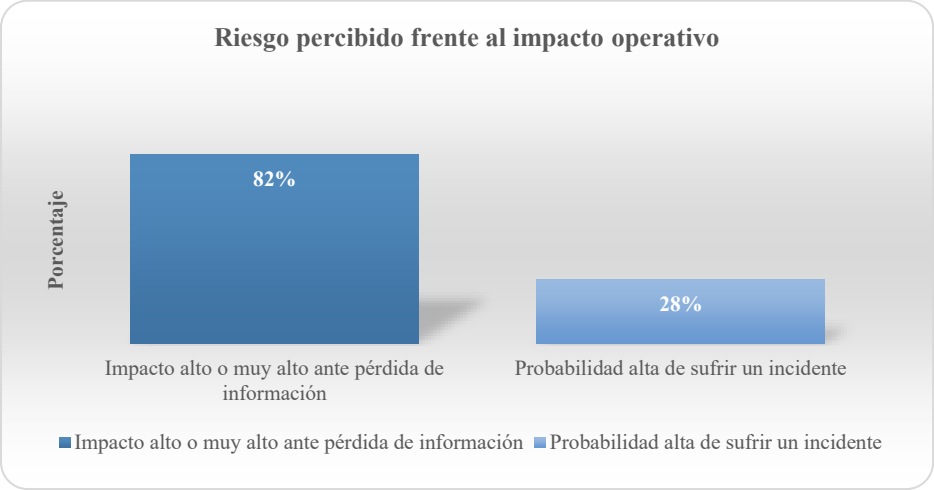
Los resultados muestran una participación predominante de empresas pertenecientes a los sectores de servicios y comercio.

Respecto a la percepción del riesgo, el 28% de los participantes consideró alta la probabilidad de sufrir un incidente de seguridad durante los siguientes doce meses. Sin embargo, el 82% indicó que la pérdida de acceso a la información durante 48 horas tendría un impacto alto o muy alto sobre la operación del negocio.

En la Figura 1 se presenta la relación entre la percepción del riesgo y el impacto operativo esperado.

Figura 1.

Percepción del riesgo frente al impacto operativo



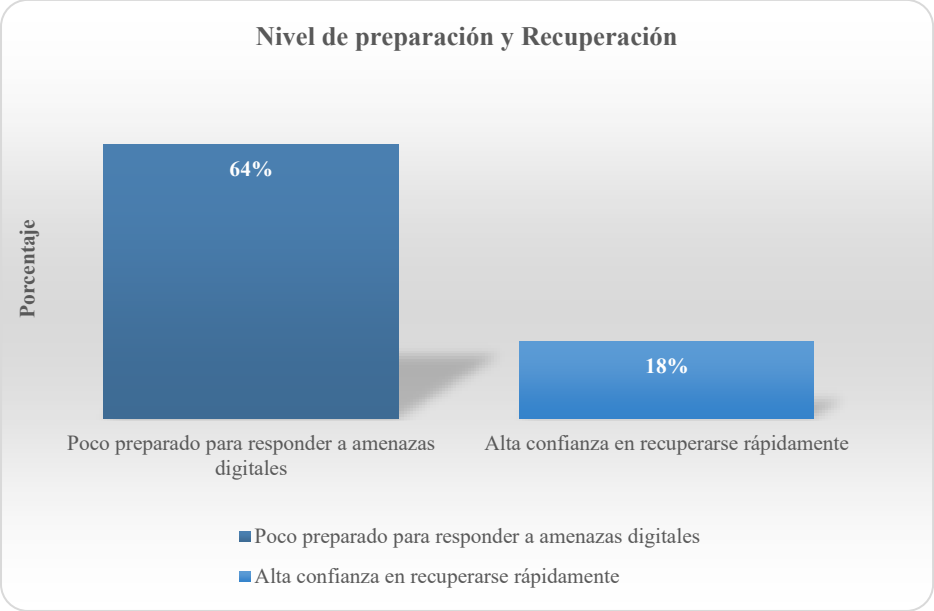
Nota. Elaboración propia a partir de las encuestas aplicadas (2026).

En cuanto al nivel de preparación organizacional, el 64% manifestó sentirse poco preparado para responder a amenazas digitales y únicamente el 18% afirmó tener confianza en su capacidad de recuperación frente a un incidente significativo.

La Figura 2 presenta los resultados relacionados con la preparación para responder a amenazas digitales y la capacidad de recuperación.

Figura 2.

Preparación para responder a amenazas digitales y recuperación ante incidentes.



Nota. Elaboración propia a partir de las encuestas aplicadas (2026).

La revisión de las prácticas actuales de seguridad mostró niveles limitados de adopción de controles básicos. El 58% indicó que las contraseñas son administradas individualmente por cada usuario, el 62% no utiliza autenticación multifactor y el 54% no cuenta con una persona claramente responsable de la seguridad de la información.

Para identificar el nivel actual de adopción de controles básicos, la Tabla 3 resume los resultados obtenidos.

Tabla 3

Implementación de controles básicos de seguridad.

Variable	Categoría	Frecuencia	Porcentaje
Control evaluado	Copias de seguridad periódicas	21	42%
Control evaluado	Responsable definido de seguridad	23	46%
Control evaluado	Autenticación multifactor	19	38%
Control evaluado	Reglas básicas de uso seguro	17	34%
Control evaluado	Capacitación sobre phishing	14	28%

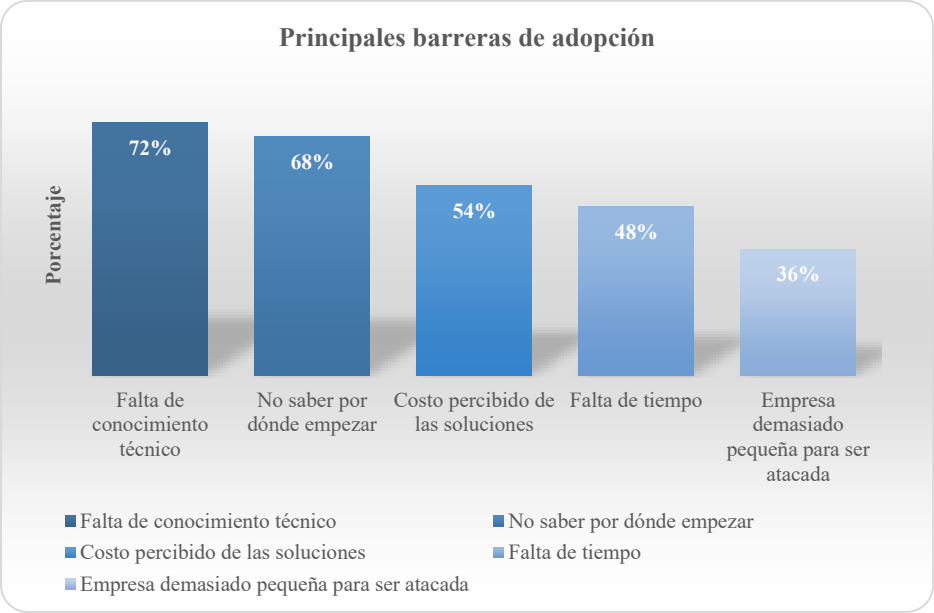
Nota. Elaboración propia a partir de las encuestas aplicadas (2026).

Las principales barreras identificadas para la adopción de medidas de seguridad fueron la falta de conocimiento técnico (72%), no saber por dónde empezar (68%), el costo percibido (54%) y la falta de tiempo (48%). Adicionalmente, el 36% consideró que su empresa era demasiado pequeña para convertirse en objetivo de un ataque.

La Figura 3 presenta las principales barreras reportadas por los participantes.

Figura 3

Principales barreras para la adopción de medidas de seguridad.



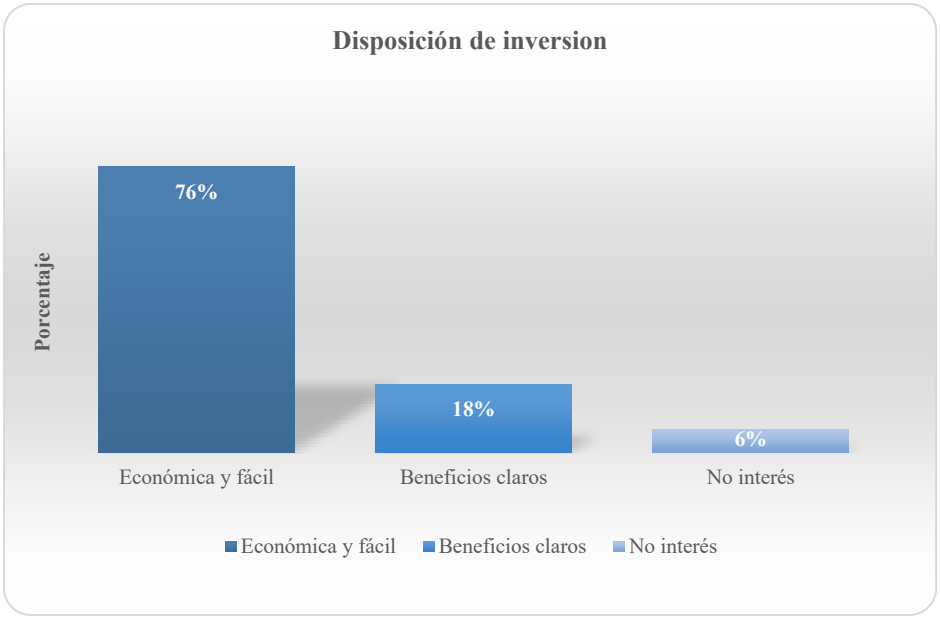
Nota. Elaboración propia a partir de las encuestas aplicadas (2026).

Los resultados también muestran que el 76% de los participantes invertiría en una herramienta de seguridad si esta fuera económica y fácil de utilizar. Un 18% manifestó interés condicionado a la obtención de beneficios claros para el negocio, mientras que el 6% indicó no tener interés en invertir actualmente.

La Figura 4 presenta la disposición de inversión reportada por los participantes.

Figura 4

Disposición de inversión en herramientas de seguridad.



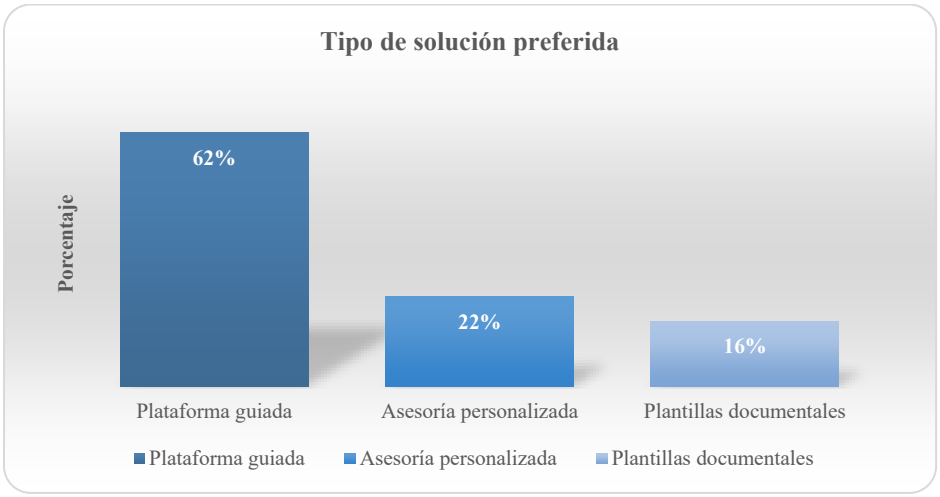
Nota. Elaboración propia a partir de las encuestas aplicadas (2026).

Respecto al tipo de solución preferida, el 62% seleccionó una plataforma guiada paso a paso, superando opciones como asesoría personalizada (22%) o plantillas documentales (16%).

La Figura 5 presenta las preferencias de los participantes respecto al tipo de solución.

Figura 5

Solución preferida para implementar controles de seguridad.



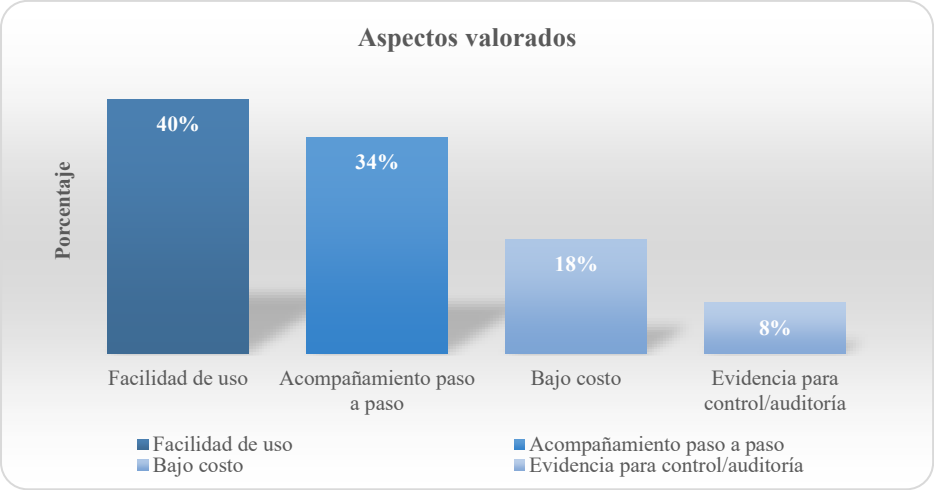
Nota. Elaboración propia a partir de las encuestas aplicadas (2026).

Asimismo, los aspectos más valorados en una herramienta de apoyo fueron la facilidad de uso (40%), el acompañamiento paso a paso (34%) y el bajo costo (18%).

La Figura 6 resume los factores considerados más importantes por los participantes.

Figura 6

Aspectos más valorados en una herramienta de apoyo.



Nota. Elaboración propia a partir de las encuestas aplicadas (2026).

Con el fin de complementar los resultados cuantitativos, se realizó un análisis cualitativo de las respuestas abiertas relacionadas con la percepción de riesgos digitales y las condiciones necesarias para implementar medidas de ciberseguridad.

La Tabla 4 presenta las categorías identificadas respecto a los principales riesgos percibidos.

Tabla 4

Principales riesgos digitales percibidos por los participantes.

Categoría identificada	Frecuencia	Porcentaje
Pérdida o indisponibilidad de información	16	32%
Fraude, phishing y suplantación de identidad	12	24%
Gestión inadecuada de accesos y contraseñas	9	18%
Error humano y falta de capacitación	7	14%
Interrupción de la operación y continuidad del negocio	6	12%

Nota. Elaboración propia a partir de las encuestas aplicadas (2026).

Por otra parte, las respuestas relacionadas con la adopción de medidas de ciberseguridad permitieron identificar las necesidades presentadas en la Tabla 5.

Tabla 5

Necesidades identificadas para adoptar medidas de ciberseguridad.

Categoría identificada	Frecuencia	Porcentaje
Guía sencilla y paso a paso	15	30%
Diagnóstico y priorización de acciones	11	22%
Capacitación y sensibilización	8	16%
Soluciones económicas y adaptadas a pequeñas empresas	9	18%
Políticas, procedimientos y seguimiento	7	14%

Nota. Elaboración propia a partir de las encuestas aplicadas (2026).

Los resultados permitieron identificar necesidades comunes relacionadas con orientación práctica, priorización de acciones, capacitación básica y acceso a herramientas asequibles. Estos hallazgos sirvieron como base para definir los requerimientos funcionales del MVP CyberTrack 360.

Las respuestas individuales de la encuesta y la matriz consolidada de resultados se incluyen en los anexos para garantizar la trazabilidad del proceso de investigación.

Análisis de resultados

El análisis de los resultados permitió identificar una brecha significativa entre la percepción del impacto de los incidentes de seguridad y la implementación efectiva de medidas de protección dentro de las microempresas participantes. Aunque la mayoría de los encuestados reconoce que la pérdida de acceso a la información podría afectar considerablemente la operación del negocio, la adopción de controles básicos continúa siendo limitada. Esta situación evidencia que la conciencia sobre las consecuencias de los riesgos digitales no necesariamente se traduce en acciones preventivas concretas.

Los hallazgos muestran niveles iniciales de madurez en seguridad de la información. La limitada implementación de controles como autenticación multifactor, capacitación frente a amenazas de ingeniería social y asignación formal de responsabilidades evidencia una gestión predominantemente reactiva. Esta situación se complementa con la percepción de insuficiente preparación para responder y recuperarse de incidentes.

Respecto a las barreras para la adopción de medidas de seguridad, los resultados indican que el principal desafío no se encuentra exclusivamente en la disponibilidad de recursos económicos. La falta de conocimiento técnico, la incertidumbre sobre cómo iniciar un proceso de fortalecimiento de la seguridad y la ausencia de orientación práctica aparecen como factores más determinantes. Este hallazgo coincide con las respuestas abiertas, en las cuales los participantes manifestaron la necesidad de contar con diagnósticos iniciales, recomendaciones priorizadas y guías sencillas que faciliten la toma de decisiones.

Por otra parte, la alta aceptación de herramientas guiadas y de bajo costo evidencia una oportunidad para desarrollar mecanismos de apoyo adaptados a las características de las microempresas. Los participantes manifestaron preferencia por soluciones que permitan comprender su situación actual, identificar prioridades y avanzar progresivamente en la implementación de controles sin requerir conocimientos especializados ni inversiones elevadas.

En relación con el objetivo general de la investigación, los resultados obtenidos permitieron identificar las principales necesidades, limitaciones y expectativas de las microempresas frente a la seguridad de la información. Los hallazgos evidencian la existencia de una brecha entre la preocupación por los riesgos digitales y la implementación efectiva de controles de protección, situación que justifica el desarrollo de un producto mínimo viable orientado al diagnóstico, priorización y seguimiento de acciones de mejora. En consecuencia, los resultados respaldan la pertinencia de CyberTrack 360 como una alternativa viable para facilitar la adopción progresiva de prácticas de seguridad de la información en organizaciones con recursos limitados.

Propuesta de solución a la problemática

Situación actual

Los resultados evidencian que las microempresas reconocen la importancia de proteger su información digital, pero la implementación de controles básicos continúa siendo limitada debido a la falta de conocimiento técnico, la dificultad para establecer prioridades, las restricciones de tiempo y la percepción de que los marcos de referencia existentes resultan complejos para organizaciones de pequeño tamaño.

Además, muchas empresas carecen de mecanismos formales para gestionar la seguridad de la información, lo que limita la adopción de prácticas preventivas y la capacidad de respuesta ante incidentes.

Oportunidades identificadas

El estudio identificó una oportunidad para desarrollar soluciones adaptadas a las necesidades de las microempresas. Los participantes manifestaron interés por herramientas que proporcionen orientación práctica, diagnósticos iniciales, recomendaciones priorizadas y mecanismos sencillos para evidenciar avances.

Asimismo, existe disposición para adoptar soluciones accesibles y fáciles de utilizar que permitan comprender claramente los beneficios para la organización.

Propuesta de solución

Como respuesta a la problemática identificada, se desarrolló CyberTrack 360, un producto mínimo viable (MVP) orientado a apoyar a las microempresas en la evaluación y fortalecimiento progresivo de sus prácticas de seguridad de la información. La solución toma como referencia controles derivados de la norma ISO/IEC 27001:2022 y los adapta a un contexto organizacional caracterizado por recursos limitados y bajos niveles de especialización técnica.

La plataforma incorpora cuestionarios organizados por roles organizacionales con el propósito de obtener una visión integral del estado de la seguridad dentro de la empresa. A partir de las respuestas registradas, el sistema aplica un modelo de puntuación dinámica que determina el nivel de madurez alcanzado y clasifica los resultados en categorías de riesgo comprensibles para los usuarios.

Como mecanismo de apoyo a la mejora continua, CyberTrack 360 genera recomendaciones priorizadas y planes de acción orientados a la implementación gradual de controles esenciales. Adicionalmente, integra un sistema de gestión de evidencias que permite adjuntar documentos o capturas para respaldar las prácticas implementadas y mantener trazabilidad sobre las acciones ejecutadas.

Como complemento al diagnóstico, se desarrolló un conjunto de políticas básicas de seguridad de la información adaptadas a microempresas, incluyendo lineamientos sobre gestión de contraseñas, copias de seguridad, control de accesos, uso aceptable de recursos tecnológicos, protección de la información y respuesta a incidentes. Los documentos completos se presentan en el Anexo D.

De esta manera, CyberTrack 360 busca reducir la brecha identificada entre la preocupación por los riesgos digitales y la adopción efectiva de controles de seguridad, proporcionando una herramienta práctica, accesible y orientada al fortalecimiento progresivo de la seguridad de la información en microempresas.

Discusión

Los resultados obtenidos permiten comprender con mayor claridad la situación de las microempresas frente a la seguridad de la información y responder a la pregunta de investigación. En términos generales, los hallazgos evidencian una brecha entre la preocupación por los riesgos digitales y la implementación efectiva de medidas de protección. Aunque los participantes reconocen que un incidente de seguridad puede afectar significativamente la operación del negocio, la adopción de controles básicos continúa siendo limitada. Esto sugiere que el principal problema no es la falta de interés por la seguridad, sino la ausencia de mecanismos prácticos que faciliten su implementación en organizaciones con recursos limitados.

Uno de los hallazgos más relevantes corresponde a la diferencia entre la percepción de probabilidad y la percepción de impacto. Mientras pocos participantes consideran probable sufrir un incidente de seguridad, la mayoría reconoce que la pérdida de acceso a la información tendría consecuencias graves para la continuidad del negocio. Esta situación coincide con estudios previos que señalan que las microempresas suelen percibir los ataques informáticos como una amenaza más asociada a grandes organizaciones que a sus propios entornos. Como resultado, se genera una sensación de baja exposición al riesgo que retrasa la adopción de medidas preventivas.

Los resultados también muestran niveles iniciales de madurez en seguridad de la información. La limitada implementación de controles como autenticación multifactor, capacitación frente a ataques de phishing y asignación formal de responsabilidades evidencia una gestión predominantemente reactiva. Además, la baja confianza de los participantes respecto a su capacidad para responder y recuperarse de incidentes sugiere que muchas organizaciones carecen de procesos estructurados para gestionar riesgos y garantizar la continuidad de sus operaciones.

Desde la perspectiva de la norma ISO/IEC 27001:2022, esta situación resulta especialmente relevante, ya que la protección de la información no depende únicamente de controles técnicos, sino también de procesos organizacionales orientados a la gestión de riesgos, la respuesta ante incidentes y la mejora continua. Los hallazgos indican que gran parte de las microempresas aún se encuentran lejos de alcanzar este nivel de formalización.

Las barreras identificadas durante la investigación permiten comprender mejor esta realidad. Aunque el costo suele considerarse uno de los principales obstáculos para adoptar medidas de seguridad, los resultados muestran que la falta de conocimiento técnico y la incertidumbre sobre cómo iniciar un proceso de mejora representan desafíos aún más importantes. Esto evidencia que muchas microempresas requieren orientación y acompañamiento antes que soluciones tecnológicas complejas.

Este resultado coincide con el estado del arte y con los planteamientos de marcos como ISO/IEC 27001, ISO/IEC 27002 y el NIST Cybersecurity Framework. Aunque estos estándares ofrecen lineamientos ampliamente reconocidos para gestionar riesgos, su implementación puede resultar compleja para organizaciones con recursos limitados. En consecuencia, la principal dificultad no parece ser la ausencia de buenas prácticas disponibles, sino la falta de mecanismos que permitan interpretarlas y aplicarlas de manera gradual dentro del contexto de las microempresas.

Los resultados cualitativos refuerzan esta interpretación. Las respuestas abiertas muestran que los participantes asocian los riesgos digitales principalmente con la pérdida de información, el fraude, la suplantación de identidad y la interrupción de las operaciones. Asimismo, expresan la necesidad de contar con diagnósticos iniciales, orientación práctica, recomendaciones priorizadas y soluciones accesibles económicamente. Estos hallazgos indican que las microempresas buscan herramientas que les permitan comprender su situación actual y avanzar progresivamente hacia mejores prácticas de seguridad.

La alta aceptación de herramientas guiadas representa otro hallazgo relevante. La mayoría de los participantes manifestó interés en utilizar soluciones fáciles de implementar y de bajo costo, siempre que aporten beneficios claros para la organización. Este resultado evidencia una oportunidad para desarrollar mecanismos que acerquen los estándares internacionales a las necesidades reales de las microempresas.

Desde esta perspectiva, los resultados respaldan la pertinencia de CyberTrack 360 como propuesta de solución. El MVP incorpora cuestionarios estructurados, recomendaciones priorizadas, clasificación de niveles de riesgo y gestión de evidencias, elementos que responden directamente a las necesidades identificadas durante la investigación. Más que sustituir marcos como ISO/IEC 27001 o NIST, la plataforma busca actuar como un mecanismo de aproximación que facilite su comprensión y aplicación progresiva en organizaciones con recursos limitados.

Los hallazgos también ponen de manifiesto la necesidad de desarrollar estrategias de ciberseguridad diferenciadas para microempresas. A diferencia de organizaciones con mayores recursos y niveles de madurez, este segmento requiere enfoques más flexibles, prácticos y orientados a la realidad operativa de sus procesos. En este sentido, la investigación aporta evidencia que respalda la importancia de adaptar las buenas prácticas internacionales a contextos organizacionales con limitaciones técnicas y presupuestarias.

Adicionalmente, los resultados sugieren que la seguridad de la información no debe abordarse únicamente como un problema tecnológico. Factores como la capacitación, la sensibilización, la definición de responsabilidades y la construcción de una cultura organizacional orientada a la

protección de la información desempeñan un papel fundamental en la adopción de medidas de seguridad. Por ello, las iniciativas dirigidas a microempresas deberían combinar herramientas tecnológicas con acciones de acompañamiento y formación.

Es importante reconocer algunas limitaciones del estudio. La investigación se desarrolló mediante una muestra no probabilística de cincuenta participantes, lo que limita la generalización de los resultados. Además, la información obtenida se basa en percepciones y respuestas declaradas por los participantes, sin incluir una auditoría técnica que permitiera verificar objetivamente el nivel de implementación de los controles reportados. No obstante, estas limitaciones no afectan el carácter exploratorio del estudio ni su utilidad para comprender las necesidades del sector analizado.

Finalmente, la investigación abre oportunidades para trabajos futuros orientados a evaluar la efectividad de CyberTrack 360 en escenarios reales de implementación. Estudios posteriores podrían analizar la aceptación de la plataforma, su facilidad de uso y su impacto sobre la adopción de controles de seguridad en microempresas.

En conclusión, los hallazgos obtenidos respaldan la premisa central de la investigación: las microempresas requieren herramientas que faciliten la adopción progresiva de prácticas de seguridad de la información mediante enfoques simples, comprensibles y alineados con sus capacidades. En este contexto, CyberTrack 360 se presenta como una alternativa viable para reducir las barreras identificadas y contribuir al fortalecimiento gradual de la seguridad de la información en organizaciones con recursos limitados

Plan de divulgación

La divulgación de los resultados de esta investigación se orientará principalmente hacia la publicación académica y la transferencia de conocimiento a organizaciones interesadas en fortalecer sus prácticas de seguridad de la información. Considerando la naturaleza del proyecto, el producto de divulgación seleccionado corresponde a un artículo científico derivado del trabajo de grado, complementado con la publicación del documento final en el repositorio Minerva de la Universidad EAN y la continuidad del desarrollo del producto mínimo viable (MVP) CyberTrack 360.

La elección del artículo científico como principal mecanismo de divulgación responde a que la investigación no se limita al desarrollo de una herramienta tecnológica, sino que aporta conocimiento sobre las necesidades, barreras y oportunidades asociadas a la adopción de prácticas de seguridad de la información en microempresas. Los hallazgos obtenidos permiten generar evidencia relevante para la comunidad académica y para organizaciones interesadas en la aplicación de enfoques simplificados de ciberseguridad basados en estándares reconocidos internacionalmente. Adicionalmente, la publicación facilita la visibilidad de los resultados, la validación por pares y la posibilidad de que futuras investigaciones utilicen los hallazgos como punto de referencia.

Como primera acción de divulgación, el documento final será incorporado al repositorio institucional de la Universidad EAN, permitiendo el acceso público a los resultados de la investigación y facilitando su consulta por estudiantes, investigadores y organizaciones interesadas en la gestión de la seguridad de la información en microempresas. Este mecanismo garantiza la preservación del conocimiento generado y contribuye a incrementar la visibilidad académica del proyecto.

Adicionalmente, se contempla la socialización de los resultados con algunas de las empresas que participaron en la etapa de levantamiento de información. Esta actividad tiene como propósito presentar los principales hallazgos obtenidos, compartir recomendaciones generales sobre seguridad de la información y recopilar retroalimentación que permita fortalecer futuras versiones de CyberTrack 360. La participación de estas organizaciones constituye una oportunidad para validar la utilidad práctica de la propuesta y generar posibles escenarios de implementación piloto.

Aunque actualmente no se tiene previsto realizar procesos de registro de propiedad intelectual o patente, se proyecta continuar el desarrollo de la plataforma una vez concluido el proyecto académico. En este sentido, CyberTrack 360 se concibe como una iniciativa con potencial de

crecimiento que podrá evolucionar mediante la incorporación de nuevas funcionalidades, mejoras en los mecanismos de evaluación y ampliación de los servicios ofrecidos a micro y pequeñas empresas. Esta continuidad permitirá avanzar desde un producto mínimo viable hacia una solución con mayor nivel de madurez tecnológica y comercial.

El cronograma de divulgación contempla durante los meses posteriores a la aprobación del trabajo de grado, se desarrollarán actividades de acercamiento con empresas interesadas en conocer la herramienta y participar en pruebas piloto del MVP.

Para la ejecución de este plan se requerirá la participación voluntaria de algunas empresas que colaboraron durante la investigación. Asimismo, será necesario disponer de la infraestructura tecnológica utilizada para alojar y mantener operativa la plataforma CyberTrack 360 durante las etapas iniciales de validación.

Como resultado esperado, se proyecta fortalecer la visibilidad de CyberTrack 360, obtener retroalimentación de potenciales usuarios y generar oportunidades para futuras implementaciones en microempresas. De esta manera, la divulgación no se limita a la comunicación de resultados, sino que se convierte en un mecanismo para promover la transferencia de conocimiento, apoyar la adopción de buenas prácticas de seguridad de la información y contribuir al desarrollo progresivo de una solución tecnológica orientada a las necesidades reales de las pequeñas organizaciones.

Conclusiones

La investigación permitió evidenciar que existe una brecha significativa entre la percepción del impacto de los riesgos digitales y la implementación efectiva de controles de seguridad en las microempresas participantes. Aunque el 82% de los encuestados considera que la pérdida de acceso a la información tendría consecuencias altas o muy altas para la continuidad del negocio, la adopción de prácticas básicas como autenticación multifactor, capacitación frente a phishing, respaldo de información y definición formal de responsabilidades continúa siendo limitada. Estos resultados confirman que la preocupación por los riesgos digitales no se traduce automáticamente en acciones preventivas dentro de las organizaciones.

En relación con el primer objetivo específico, orientado a identificar las necesidades y barreras de las microempresas frente a la seguridad de la información, se encontró que los principales obstáculos corresponden a la falta de conocimiento técnico, la incertidumbre sobre cómo iniciar un proceso de fortalecimiento de la seguridad y la percepción de altos costos. Los resultados muestran que el problema principal no radica exclusivamente en la disponibilidad de recursos económicos, sino en la ausencia de herramientas y metodologías que traduzcan los estándares internacionales en acciones comprensibles y aplicables para organizaciones de pequeño tamaño.

Respecto al diseño y desarrollo de la solución propuesta, se concluye que CyberTrack 360 responde directamente a las necesidades identificadas durante la investigación. La incorporación de cuestionarios estructurados por roles, modelos de evaluación de madurez, recomendaciones priorizadas, gestión de evidencias y políticas básicas de seguridad permite transformar conceptos técnicos derivados de ISO/IEC 27001, ISO/IEC 27002 y NIST CSF en actividades concretas y verificables. De esta manera, la plataforma se posiciona como un mecanismo de aproximación a las buenas prácticas de seguridad de la información, más que como una herramienta orientada a la certificación formal.

La evaluación del MVP y el análisis de aceptación muestran que las características más valoradas por los participantes son la facilidad de uso, el acompañamiento paso a paso y la accesibilidad económica. Adicionalmente, el 76% manifestó disposición a utilizar una herramienta de este tipo si resulta sencilla y asequible. Estos hallazgos respaldan la hipótesis principal de la investigación, al evidenciar que una herramienta simplificada y adaptada al contexto de las microempresas puede facilitar la adopción inicial de controles de seguridad y mejorar la capacidad organizacional para gestionar riesgos básicos.

Los resultados también respaldan parcialmente la hipótesis relacionada con la trazabilidad mediante evidencias. Las respuestas obtenidas muestran que los participantes valoran la posibilidad de registrar acciones realizadas, conservar documentación de respaldo y realizar seguimiento a los avances. Esto sugiere que la gestión de evidencias puede contribuir a fortalecer la disciplina organizacional y favorecer procesos de mejora continua, especialmente en entornos donde las responsabilidades suelen gestionarse de manera informal.

Los hallazgos obtenidos son consistentes con la literatura revisada, que señala que las microempresas enfrentan dificultades para adoptar marcos robustos de ciberseguridad debido a limitaciones de conocimiento, recursos y acompañamiento. En este sentido, la investigación aporta evidencia empírica que refuerza la necesidad de desarrollar enfoques simplificados y adaptados a las capacidades reales de este segmento empresarial, contribuyendo a cerrar la brecha existente entre los estándares internacionales y su aplicación práctica.

Como limitación principal, el estudio se desarrolló mediante una muestra no probabilística de cincuenta participantes y se apoyó en información declarada por los encuestados, sin realizar auditorías técnicas que permitieran verificar objetivamente la implementación de los controles reportados. Por esta razón, los resultados deben interpretarse desde una perspectiva exploratoria y contextualizada al grupo analizado.

Finalmente, se identifican oportunidades para futuras investigaciones orientadas a evaluar la efectividad de CyberTrack 360 en escenarios reales de implementación, medir su impacto sobre la adopción de controles de seguridad y analizar la evolución del nivel de madurez de las organizaciones a lo largo del tiempo. Asimismo, se proyecta continuar el desarrollo de la plataforma mediante la incorporación de nuevas funcionalidades, ampliación de cuestionarios, automatización de procesos y validación con una muestra más amplia de micro y pequeñas empresas. En consecuencia, CyberTrack 360 constituye una propuesta viable para promover la adopción progresiva de buenas prácticas de seguridad de la información y fortalecer la resiliencia digital de las microempresas colombianas.

Glosario

Activo: Elemento con valor para la organización (información, sistemas, personas, infraestructura).

Amenaza: Causa potencial de un incidente no deseado.

Auditoría interna: revisión sistemática de prácticas y evidencias para mejora.

CIS: Center for Internet Security; organización que publica los CIS Critical Security Controls.

CIS IG1: Implementation Group 1 del Center for Internet Security (CIS); conjunto de higiene esencial para controles de ciberseguridad en organizaciones con recursos limitados.

Control: Medida para modificar o mantener el riesgo.

CSF: Cybersecurity Framework; marco del NIST para gestionar riesgos de ciberseguridad.

Evidencia: prueba verificable de implementación.

IEC: International Electrotechnical Commission (Comisión Electrotécnica Internacional).

ISO: International Organization for Standardization.

Logs: registros de eventos del sistema para auditoría/detección.

MFA: Autenticación multifactor (más de un factor de verificación, por ejemplo contraseña + código).

NIST CSF 2.0: Cybersecurity Framework 2.0 del National Institute of Standards and Technology (NIST); marco voluntario para gestionar riesgos de ciberseguridad.

OWASP Top 10: lista de riesgos críticos de aplicaciones web.

Phishing: suplantación para engañar y obtener credenciales o ejecutar acciones.

Ransomware: malware que cifra datos y exige pago, puede incluir exfiltración.

Riesgo: efecto de la incertidumbre sobre objetivos; en seguridad, combinación de probabilidad e impacto.

RNBD: Registro Nacional de Bases de Datos administrado por la Superintendencia de Industria y Comercio (SIC) en Colombia.

SGSI/ISMS: Sistema de Gestión de Seguridad de la Información (SGSI) / Information Security Management System (ISMS).

SIC: Superintendencia de Industria y Comercio (Colombia); autoridad administrativa asociada al RNBD y protección de datos.

TI: Tecnologías de la Información; área responsable de administrar y soportar sistemas y servicios tecnológicos.

Trazabilidad: capacidad de rastrear quién hizo qué, cuándo y con qué evidencia.

Vulnerabilidad: debilidad explotable por una amenaza.

Referencias bibliográficas

Adriko, R., & Nurse, J. R. C. (2026). Cybersecurity and Cyber insurance for Small to Medium-sized Enterprises (SMEs): Perceptions, challenges and decision-making dynamics. *Computers & Security*, *163*, 104818. https://doi.org/10.1016/j.cose.2025.104818

Azinheira, B., Antunes, M., Maximiano, M., & Gomes, R. (2023). A methodology for mapping cybersecurity standards into governance guidelines for SME in Portugal. *Procedia Computer Science*, *219*, 121–128. https://doi.org/10.1016/j.procs.2023.01.272

Bada, M. & Nurse J. R. C. (2019). Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). *Emerald insight, 27, 3.* https://www.emerald.com/ics/article-abstract/27/3/393/105969/Developing-cybersecurity-education-and-awareness?redirectedFrom=fulltext

Barreras, R., Elja, G., Posada, A., y Daza, F. (2012). *Ley 1581 de 2012 (Régimen general de protección de datos personales).* https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

CIS. (2024). *CIS Critical Security Controls*. http://www.cisecurity.org/controls/

Creswell, J. & Creswell J. (2018). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches (5th edition).* Sage Publications, Inc.

Drata. (2026a). *Compliance automation platform (SOC 2, ISO 27001, HIPAA)*. https://drata.com/compliance

Drata. (2026b). *Expand global reach by accelerating ISO 27001:2022*. https://drata.com/product/iso-27001

Edwards, Max. (2026). *Best ISO 27001 Compliance Software*. https://www.isms.online/compliance-software/

Gundu, T., & Mmango, N. (2026). *Password Hygiene Guidelines for SMEs in South Africa: A Systematic Literature Review* (pp. 287–298). https://doi.org/10.1007/978-3-032-12999-4_26

Hao, C., Jiajia, F., & Tu, L. (2026). Manager information security-related stress and organizational information security performance. *Emerald Publishing*. https://doi.org/10.1108/MD-10-2024-2308

Hernández, R., Fernández, C., y Baptista, M. (2018). *Metodología de la Investigación* (Sexta edición.). McGraw-Hill Education.

Hevner, Alan., March, Salvatore., Park, Jinsoo., & Ram, Sudha. (2004). *Design Science in Information Systems Research*. https://misq.umn.edu/misq/article-abstract/28/1/75/261/Design-Science-in-Information-Systems-Research1?redirectedFrom=fulltext

Humphreys, Edward. (2025). *Implementing the ISO/IEC 27001 Information Security Management System Standard.* https://books.google.hn/books?hl=es&lr=&id=5s_BEQAAQBAJ&oi=fnd&pg=PR13&dq=Humphreys+2025+27001&ots=qAL3YYFYpU&sig=sbXWNLIJFLML3LUQyHPL_-VpDNw&redir_esc=y#v=onepage&q=Humphreys%202025%2027001&f=false

IBM. (2025). *Cost of a Data Breach Report 2025 The AI Oversight Gap think report*.

ISO TOOLS. (2026a). *Auditoria con casos reales a través de un software ISO*. https://isotools.org/2026/02/17/auditoria-con-casos-reales/

ISO TOOLS. (2026b). *Beneficios del software ISO 27001 La gestión de la Seguridad de la Información, más ágil que nunca*. https://isotools.org/software/riesgos-y-seguridad/iso-27001/

ISO/IEC. (2022a). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. https://www.iso.org/es/norma/27001

ISO/IEC. (2022b). *ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls*. https://www.iso.org/standard/75652.html

Microsoft. (2025). *Microsoft Digital Defense Report 2025*. https://www.microsoft.com/en-us/corporate-responsibility/cybersecurity/microsoft-digital-defense-report-2025/

NIST. (2024a). *NIST cybersecurity framework 2.0:* https://doi.org/10.6028/NIST.SP.1300.spa

NIST, G. M. (2024b). *Spanish Translation of the NIST Cybersecurity Framework 2.0*. https://doi.org/10.6028/NIST.CSWP.29.spa

OECD. (2026). *SMEs and entrepreneurship.* https://www.oecd.org/en/topics/smes-and-entrepreneurship.html

OWASP Foundation. (2025). *OWASP Top 10:2025*. https://owasp.org/Top10/2025/

Peffers, Ken., Tuunanen, Tuure., Rothenberger, Marcus., & Chatterjee, Samir. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems*, *24*(3), 45–77. https://doi.org/10.2753/MIS0742-1222240302

Peters, Sam. (2025). *Statement of Applicability (SoA): The Complete Guide*. https://www.isms.online/iso-27001/statement-of-applicability/

Rombaldo, Carlos., Becker, Ingolf., & Johnson, Shane. (2023). *Unaware, Unfunded and Uneducated: A Systematic Review of SME Cybersecurity*. https://arxiv.org/html/2309.17186v1#S1

Santos, Juan. (2013). *Decreto 1377 de 2013 (Reglamenta parcialmente la Ley 1581 de 2012)*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

Santos, Juan. (2014). *Decreto 886 de 2014 (Registro Nacional de Bases de Datos – RNBD)*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=57338

Sarri, Anna., Paggio, Viktor., & Bafoutsou, Georgia. (2021). *Cybersecurity for SMEs : challenges and recommendations*. [Publications Office of the European Union].

Scytale. (2026). *Where compliance happens.* https://scytale.ai/

Secureframe. (2026a). *ISO 27001 Automatice el cumplimiento de la norma ISO 27001.* https://secureframe.com/frameworks/iso-27001

Secureframe. (2026b). *ISO 27001 Evidence Collection List for Your Certification Audit*. https://secureframe.com/hub/iso-27001/evidence-list

Sprinto. (2026a). *Do a lot more with a lot less.* https://sprinto.com/automate-evidence-collection/

Sprinto. (2026b). *ISO 27001 Gaining your ISO 27001 Certification Evidence Collection*. https://sprinto.com/hub/iso-27001-evidence-collection/

Tan Jia Jun, Dennis., Rafsanjani, Ahmad., Aslam, Saad., & Behjati, Mehran. (2025). *Human Factors in Information Security: A Qantitative Study with Technical Solutions to Prevent Social Engineering Atacks*. https://dl.acm.org/doi/full/10.1145/3767320

Thoropass. (2026). *Global business starts here Unlock new markets and build trust with streamlined ISO 27001 software*. https://www.thoropass.com/frameworks/iso-27001

Venkatesh, V., Thong, J., & Xu, X. (2016). Unified Theory of Acceptance and Use of Technology: A Synthesis and the Road Ahead. *Journal of the Association for Information Systems*, *17*(5), 328–376. https://doi.org/10.17705/1jais.00428

Verizon. (2025). *2025 Data Breach Investigations Report*. https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf

World Bank Group. (2026). *SME Finance.* https://www.worldbank.org/ext/en/topic/competitiveness/small-and-medium-enterprises-smes-finance?utm

Anexos

Anexo A – Instrumento de encuesta aplicado.

Anexo B – Matriz anonimizada de respuestas.

Anexo C – Resultados consolidados de las encuestas.

Anexo D – Capturas del MVP CyberTrack 360.

Anexo E – Políticas de seguridad desarrolladas.

Anexo A – Instrumento de encuesta aplicado

Sección 1: Perfil de la empresa

1. ¿Qué tan dependiente es su empresa de sistemas digitales para operar?
- o Baja (uso básico: WhatsApp, correo)
- o Media (facturación, inventarios)
- o Alta (operación totalmente digital)

2. ¿Cuántos empleados laboran en su empresa? *(Selección única)*
- o 1–2 empleados
- o 3–5 empleados
- o 6–10 empleados
- o Más de 10 empleados

3. ¿En qué sector económico opera su empresa? *(Selección única)*
- o Servicios
- o Comercio
- o Industrial
- o Otros:_____

4. ¿Hace cuánto opera la empresa? *(Selección única)**
- o Menos de 1 año
- o 1–3 años
- o Más de 3 años

Sección 2: Percepción del riesgo

5. En una escala del 1 al 5 (donde 1 es muy bajo y 5 muy alto): ¿Qué tan probable considera que su empresa experimente un incidente de seguridad en los próximos 12 meses (pérdida de datos, hackeo, fraude digital)? *
- o 1
- o 2
- o 3
- o 4
- o 5

6. En una escala del 1 al 5 (donde 1 es muy bajo y 5 muy alto): Si su empresa perdiera acceso a su información por 48 horas, ¿qué impacto tendría en sus operaciones (clientes, ventas, proveedores)?
- o 1
- o 2
- o 3
- o 4
- o 5

7. En una escala del 1 al 5 (donde 1 es muy bajo y 5 muy alto): ¿Qué tan preparado considera que está su negocio frente a amenazas digitales?
- o 1

- 2
- 3
- 4
- 5

8. En una escala del 1 al 5 (donde 1 es muy bajo y 5 muy alto): ¿Qué tan confiado está en que su empresa podría recuperarse rápidamente ante un incidente?
- 1
- 2
- 3
- 4
- 5

Sección 3: Nivel actual de prácticas

9. ¿Cómo gestionan el manejo de contraseñas? *(Selección única)**
- No se gestionan formalmente
- Cada usuario decide
- Hay reglas básicas
- Se usa gestor de contraseñas

10. ¿Cuentan con copias de seguridad (backup) de la información? *(Selección única)**
- No existen
- Se hacen ocasionalmente
- Son periódicos pero no verificados
- Son automáticos y probados

11. ¿Tienen definido quién es responsable de la seguridad de la información? *(Selección única)**
- No hay responsable
- Es informal
- Está asignado pero sin funciones claras
- Está definido con responsabilidades

12. ¿Utilizan algún tipo de autenticación adicional / Autenticación en dos pasos (ej. código al celular)? *(Selección única)**
- Sí
- No

13. ¿Tienen reglas escritas o instructivos básicos (aunque sean sencillos) sobre el uso seguro de la tecnología en el negocio? *(Selección única)**
- Sí
- No

14. ¿Se les da pautas o recomendaciones a los empleados para identificar correos o mensajes sospechosos (Phishing)? *(Selección única)**
- Sí
- No
- Ocasionalmente

Sección 4: Barreras de adopción

15. Seleccione los principales motivos por los cuales su empresa NO ha implementado más medidas de seguridad (máx. 3): *(Selección de **Casillas de verificación**)**
- o No sabemos por dónde empezar
- o Falta de conocimiento técnico
- o Costo percibido alto
- o Falta de tiempo
- o No lo vemos urgente
- o No conocemos soluciones adecuadas
- o Considerar que el negocio es "muy pequeño" para ser atacado

Sección 5: Disposición y modelo de solución

16. ¿Cuál de las siguientes opciones se ajusta más a su empresa? *(Selección única)**
- o Prefiero no invertir en este momento
- o Invertiría si es económico y fácil de usar
- o Invertiría si veo beneficios claros
- o Ya estoy invirtiendo en ciberseguridad

17. ¿Qué tipo de solución le resultaría más útil? *(Selección única)**
- o Asesoría personalizada
- o Plataforma guiada paso a paso
- o Plantillas y documentos
- o No estoy interesado

18. ¿Qué valoraría más en una solución de seguridad? *(Selección única)**
- o Bajo costo
- o Facilidad de uso
- o Acompañamiento paso a paso
- o Evidencia para control/auditoría

19. ¿Cuál de las siguientes frases describe mejor su situación actual? *(Selección única)**
- o Sé que es importante, pero no hago nada
- o He implementado algunas medidas básicas
- o Tengo control parcial
- o Tengo una estrategia definida

Sección 6: Preguntas abiertas

20. ¿Cuál considera que es el mayor riesgo digital para su negocio? *(Texto de respuesta larga / Párrafo)*

21. ¿Qué necesitaría para tomar la decisión de implementar medidas de ciberseguridad? *(Texto de respuesta larga / Párrafo)*

Anexo B – Matriz anonimizada de respuestas

Este anexo presenta la consolidación de los resultados obtenidos mediante la encuesta aplicada a cincuenta (50) propietarios, socios y cargos directivos de micro y pequeñas empresas. La información se encuentra agrupada y tabulada con el propósito de facilitar el análisis de tendencias, percepciones y necesidades relacionadas con la seguridad de la información. Para proteger la privacidad de los participantes y la confidencialidad de las organizaciones consultadas, los resultados se presentan de forma anonimizada. Los hallazgos obtenidos sirvieron como insumo para identificar problemáticas comunes, validar la pertinencia de la propuesta CyberTrack 360 y fundamentar las decisiones tomadas durante el diseño del producto mínimo viable (MVP).

Tabla B.1.

Preguntas 1-8

ID	Cargo	P1	P2	P3	P4	P5	P6	P7	P8
1	Socio gerente	Alta	6–10 empleados	Servicios	1–3 años	4	4	1	2
2	Propietario	Alta	1–2 empleados	Industrial	1–3 años	4	4	2	3
3	Administrador	Alta	6–10 empleados	Comercio	1–3 años	4	5	1	2
4	Administrador	Alta	3–5 empleados	Servicios	Más de 3 años	5	4	1	2
5	Administrador	Alta	1–2 empleados	Otros	Más de 3 años	5	4	1	3
6	Propietario	Alta	1–2 empleados	Industrial	Más de 3 años	5	4	1	2
7	Socio gerente	Alta	3–5 empleados	Servicios	Más de 3 años	5	4	1	2
8	Director administrativo	Alta	Más de 10 empleados	Comercio	Más de 3 años	4	4	2	2
9	Propietario	Alta	3–5 empleados	Industrial	1–3 años	5	5	1	3
10	Director administrativo	Alta	3–5 empleados	Comercio	Menos de 1 año	3	4	2	2
11	Socio gerente	Alta	6–10 empleados	Industrial	Más de 3 años	3	4	2	3
12	Socio gerente	Alta	Más de 10 empleados	Servicios	Más de 3 años	3	4	2	3
13	Propietario	Alta	3–5 empleados	Servicios	1–3 años	2	4	2	1
14	Gerente general	Alta	3–5 empleados	Comercio	Más de 3 años	2	4	1	2
15	Director administrativo	Alta	3–5 empleados	Comercio	Más de 3 años	3	4	1	2
16	Administrador	Alta	6–10 empleados	Comercio	Menos de 1 año	3	4	2	1
17	Director administrativo	Alta	3–5 empleados	Industrial	Menos de 1 año	3	5	2	2
18	Socio gerente	Alta	6–10 empleados	Otros	1–3 años	3	4	1	1

19	Socio gerente	Alta	3–5 empleados	Servicios	1–3 años	2	5	2	2
20	Propietario	Alta	3–5 empleados	Servicios	Más de 3 años	3	5	2	2
21	Gerente general	Media	1–2 empleados	Industrial	1–3 años	5	4	1	1
22	Administrador	Media	6–10 empleados	Servicios	1–3 años	4	4	2	1
23	Director administrativo	Media	6–10 empleados	Comercio	1–3 años	5	4	1	1
24	Gerente general	Media	Más de 10 empleados	Otros	Más de 3 años	4	5	2	2
25	Administrador	Media	6–10 empleados	Comercio	Menos de 1 año	4	5	1	1
26	Socio gerente	Media	3–5 empleados	Servicios	Menos de 1 año	2	4	1	1
27	Socio gerente	Media	6–10 empleados	Servicios	Más de 3 años	3	4	2	2
28	Propietario	Media	1–2 empleados	Comercio	Menos de 1 año	2	5	1	1
29	Propietario	Media	6–10 empleados	Servicios	1–3 años	3	4	1	2
30	Director administrativo	Media	3–5 empleados	Comercio	1–3 años	2	4	2	2
31	Gerente general	Media	Más de 10 empleados	Comercio	Más de 3 años	3	4	1	3
32	Gerente general	Media	1–2 empleados	Industrial	Menos de 1 año	3	3	1	2
33	Administrador	Media	1–2 empleados	Servicios	Menos de 1 año	3	5	4	2
34	Director administrativo	Media	1–2 empleados	Comercio	Más de 3 años	3	5	3	3
35	Propietario	Media	6–10 empleados	Servicios	1–3 años	2	5	3	2
36	Director administrativo	Media	Más de 10 empleados	Industrial	1–3 años	2	3	3	3
37	Socio gerente	Media	6–10 empleados	Servicios	Más de 3 años	2	4	3	3
38	Propietario	Media	1–2 empleados	Servicios	1–3 años	3	3	3	2
39	Gerente general	Media	6–10 empleados	Servicios	Más de 3 años	3	4	3	1
40	Propietario	Media	3–5 empleados	Industrial	1–3 años	3	3	3	1
41	Socio gerente	Media	3–5 empleados	Otros	1–3 años	3	5	3	3
42	Propietario	Media	1–2 empleados	Servicios	Más de 3 años	3	5	3	5
43	Gerente general	Baja	3–5 empleados	Comercio	Más de 3 años	1	4	4	5
44	Socio gerente	Baja	1–2 empleados	Comercio	Más de 3 años	3	2	3	5
45	Administrador	Baja	3–5 empleados	Comercio	Más de 3 años	1	4	3	5
46	Director administrativo	Baja	6–10 empleados	Industrial	Más de 3 años	2	2	4	4
47	Administrador	Baja	6–10 empleados	Otros	Más de 3 años	1	2	3	4
48	Socio gerente	Baja	3–5 empleados	Servicios	Más de 3 años	2	4	3	4

49	Socio gerente	Baja	3–5 empleados	Comercio	Más de 3 años	3	2	4	5
50	Socio gerente	Baja	1–2 empleados	Otros	1–3 años	3	3	3	5

Tabla B.2.

Preguntas 9-14

ID	P9	P10	P11	P12	P13	P14
1	Cada usuario decide	Se hacen ocasionalmente	Es informal	No	No	Ocasionalmente
2	Cada usuario decide	Son automáticos y probados	Está definido con responsabilidades	Sí	Sí	Ocasionalmente
3	No formal	Se hacen ocasionalmente	No hay responsable	No	Sí	Ocasionalmente
4	Hay reglas básicas	Son periódicos pero no verificados	Es informal	Sí	No	Sí
5	Cada usuario decide	No existen	No hay responsable	No	Sí	Ocasionalmente
6	Cada usuario decide	Se hacen ocasionalmente	Está asignado pero sin funciones claras	No	No	Sí
7	Cada usuario decide	Se hacen ocasionalmente	No hay responsable	Sí	No	Ocasionalmente
8	Cada usuario decide	Son periódicos pero no verificados	Está definido con responsabilidades	No	No	No
9	No formal	Son periódicos pero no verificados	Está definido con responsabilidades	No	Sí	Sí
10	Se usa gestor de contraseñas	Son periódicos pero no verificados	Está definido con responsabilidades	Sí	No	Ocasionalmente
11	Cada usuario decide	Son periódicos pero no verificados	No hay responsable	Sí	Sí	No
12	Cada usuario decide	No existen	Está definido con responsabilidades	No	No	Ocasionalmente
13	Cada usuario decide	Se hacen ocasionalmente	Está definido con responsabilidades	No	No	Sí
14	No formal	Son automáticos y probados	Está definido con responsabilidades	No	Sí	Sí
15	Cada usuario decide	No existen	Es informal	No	Sí	Sí
16	Cada usuario decide	Son periódicos pero no verificados	Está definido con responsabilidades	No	No	Sí
17	Hay reglas básicas	Se hacen ocasionalmente	Está definido con responsabilidades	No	Sí	Ocasionalmente
18	Cada usuario decide	Se hacen ocasionalmente	Está definido con responsabilidades	Sí	No	Sí
19	Cada usuario decide	Se hacen ocasionalmente	Está definido con responsabilidades	No	No	Ocasionalmente
20	No formal	Son periódicos pero no verificados	Es informal	No	Sí	No
21	Cada usuario decide	Son periódicos pero no verificados	No hay responsable	Sí	No	No
22	No formal	Son automáticos y probados	Está definido con responsabilidades	Sí	Sí	No

23	Hay reglas básicas	Se hacen ocasionalmente	Está definido con responsabilidades	Sí	No	No
24	Cada usuario decide	No existen	No hay responsable	Sí	No	Sí
25	Cada usuario decide	No existen	Está definido con responsabilidades	Sí	Sí	No
26	Cada usuario decide	No existen	Es informal	No	Sí	Sí
27	Cada usuario decide	No existen	Es informal	No	No	No
28	Hay reglas básicas	Se hacen ocasionalmente	Está definido con responsabilidades	Sí	No	No
29	Cada usuario decide	Son periódicos pero no verificados	No hay responsable	No	Sí	No
30	No formal	Se hacen ocasionalmente	No hay responsable	No	No	No
31	Cada usuario decide	Son periódicos pero no verificados	Está asignado pero sin funciones claras	No	No	No
32	Hay reglas básicas	Son periódicos pero no verificados	No hay responsable	No	No	No
33	Cada usuario decide	Son periódicos pero no verificados	Está asignado pero sin funciones claras	No	No	No
34	Hay reglas básicas	Son periódicos pero no verificados	Está definido con responsabilidades	No	No	Sí
35	Cada usuario decide	No existen	Está definido con responsabilidades	No	No	No
36	Hay reglas básicas	Se hacen ocasionalmente	Es informal	No	No	No
37	Hay reglas básicas	Se hacen ocasionalmente	Está definido con responsabilidades	No	Sí	No
38	Hay reglas básicas	Se hacen ocasionalmente	No hay responsable	No	No	No
39	No formal	Son automáticos y probados	Está asignado pero sin funciones claras	No	No	Sí
40	Cada usuario decide	No existen	No hay responsable	Sí	No	No
41	Cada usuario decide	Son periódicos pero no verificados	Es informal	No	No	Sí
42	No formal	Son automáticos y probados	No hay responsable	No	No	Ocasionalmente
43	Cada usuario decide	Se hacen ocasionalmente	Está definido con responsabilidades	Sí	No	Ocasionalmente
44	Cada usuario decide	Se hacen ocasionalmente	Está definido con responsabilidades	Sí	No	Ocasionalmente
45	Cada usuario decide	Son periódicos pero no verificados	Está asignado pero sin funciones claras	Sí	Sí	Sí
46	Cada usuario decide	Se hacen ocasionalmente	Está definido con responsabilidades	Sí	Sí	No
47	Se usa gestor de contraseñas	Se hacen ocasionalmente	Es informal	Sí	No	Ocasionalmente
48	Cada usuario decide	Son periódicos pero no verificados	Está definido con responsabilidades	Sí	No	Ocasionalmente
49	Hay reglas básicas	No existen	Es informal	No	No	Ocasionalmente

50	No formal	Se hacen ocasionalmente	Está definido con responsabilidades	No	Sí	No

Tabla B.3

Preguntas 15-18

ID	P15	P16	P17	P18
1	No sabemos por dónde empezar; Falta de conocimiento técnico; Falta de tiempo	Invertiría si es económico y fácil de usar	Plataforma guiada paso a paso	Bajo costo
2	No sabemos por dónde empezar; Falta de tiempo; Falta de conocimiento técnico	Invertiría si es económico y fácil de usar	Plataforma guiada paso a paso	Facilidad de uso
3	Falta de tiempo; Falta de conocimiento técnico; No sabemos por dónde empezar	Invertiría si es económico y fácil de usar	Plataforma guiada paso a paso	Bajo costo
4	Costo percibido alto; Considerar que el negocio es “muy pequeño” para ser atacado; Falta de conocimiento técnico	Invertiría si es económico y fácil de usar	Plantillas y documentos	Facilidad de uso
5	Costo percibido alto; Considerar que el negocio es “muy pequeño” para ser atacado; Falta de conocimiento técnico	Invertiría si es económico y fácil de usar	Asesoría personalizada	Facilidad de uso
6	Costo percibido alto; Considerar que el negocio es “muy pequeño” para ser atacado; Falta de conocimiento técnico	Invertiría si veo beneficios claros	Plataforma guiada paso a paso	Facilidad de uso
7	No sabemos por dónde empezar; Costo percibido alto	Invertiría si es económico y fácil de usar	Plataforma guiada paso a paso	Acompañamiento paso a paso
8	No sabemos por dónde empezar; Falta de tiempo	Invertiría si es económico y fácil de usar	Plantillas y documentos	Evidencia para control/auditoría
9	Falta de conocimiento técnico; No sabemos por dónde empezar; Falta de tiempo	Invertiría si veo beneficios claros	Plataforma guiada paso a paso	Facilidad de uso
10	Falta de tiempo; Falta de conocimiento técnico; No sabemos por dónde empezar	Invertiría si veo beneficios claros	Plantillas y documentos	Acompañamiento paso a paso
11	Falta de tiempo; Costo percibido alto; Falta de conocimiento técnico	Invertiría si es económico y fácil de usar	Plataforma guiada paso a paso	Acompañamiento paso a paso
12	Falta de conocimiento técnico; Costo percibido alto; Considerar que el negocio es “muy pequeño” para ser atacado	Invertiría si es económico y fácil de usar	Plataforma guiada paso a paso	Facilidad de uso
13	Falta de conocimiento técnico; Costo percibido alto; Considerar que el negocio es “muy pequeño” para ser atacado	Invertiría si es económico y fácil de usar	Plataforma guiada paso a paso	Acompañamiento paso a paso
14	Costo percibido alto; No sabemos por dónde empezar	Invertiría si veo beneficios claros	Plataforma guiada paso a paso	Bajo costo

15	Falta de tiempo; No sabemos por dónde empezar	Invertiría si es económico y fácil de usar	Asesoría personalizada	Acompañamiento paso a paso
16	Falta de tiempo; Falta de conocimiento técnico; No sabemos por dónde empezar	Invertiría si es económico y fácil de usar	Plataforma guiada paso a paso	Evidencia para control/auditoría
17	Falta de tiempo; Falta de conocimiento técnico; No sabemos por dónde empezar	Invertiría si es económico y fácil de usar	Asesoría personalizada	Bajo costo
18	No sabemos por dónde empezar; Falta de conocimiento técnico; Falta de tiempo	Invertiría si veo beneficios claros	Asesoría personalizada	Acompañamiento paso a paso
19	Costo percibido alto; Falta de conocimiento técnico; Considerar que el negocio es “muy pequeño” para ser atacado	Invertiría si es económico y fácil de usar	Plataforma guiada paso a paso	Bajo costo
20	Considerar que el negocio es “muy pequeño” para ser atacado; Falta de conocimiento técnico; Costo percibido alto	Invertiría si es económico y fácil de usar	Plantillas y documentos	Facilidad de uso
21	Costo percibido alto; No sabemos por dónde empezar	Invertiría si es económico y fácil de usar	Plataforma guiada paso a paso	Facilidad de uso
22	Falta de tiempo; No sabemos por dónde empezar	Invertiría si es económico y fácil de usar	Plataforma guiada paso a paso	Facilidad de uso
23	Falta de tiempo; No sabemos por dónde empezar; Falta de conocimiento técnico	Invertiría si es económico y fácil de usar	Plataforma guiada paso a paso	Acompañamiento paso a paso
24	Falta de conocimiento técnico; No sabemos por dónde empezar; Falta de tiempo	Invertiría si es económico y fácil de usar	Plataforma guiada paso a paso	Facilidad de uso
25	Falta de tiempo; Falta de conocimiento técnico; No sabemos por dónde empezar	Invertiría si es económico y fácil de usar	Plataforma guiada paso a paso	Facilidad de uso
26	Falta de conocimiento técnico; Considerar que el negocio es “muy pequeño” para ser atacado; Costo percibido alto	Invertiría si es económico y fácil de usar	Plataforma guiada paso a paso	Bajo costo
27	Falta de conocimiento técnico; Costo percibido alto; Considerar que el negocio es “muy pequeño” para ser atacado	Invertiría si es económico y fácil de usar	Asesoría personalizada	Acompañamiento paso a paso
28	No sabemos por dónde empezar; Costo percibido alto	Invertiría si es económico y fácil de usar	Plataforma guiada paso a paso	Facilidad de uso
29	No sabemos por dónde empezar; Costo percibido alto	Invertiría si es económico y fácil de usar	Plataforma guiada paso a paso	Facilidad de uso
30	Falta de tiempo; Falta de conocimiento técnico; No sabemos por dónde empezar	Prefiero no invertir en este momento	Plataforma guiada paso a paso	Facilidad de uso
31	No sabemos por dónde empezar; Falta de conocimiento técnico; Falta de tiempo	Prefiero no invertir en este momento	Plataforma guiada paso a paso	Acompañamiento paso a paso

32	Falta de conocimiento técnico; Falta de tiempo; No sabemos por dónde empezar	Prefiero no invertir en este momento	Asesoría personalizada	Acompañamiento paso a paso
33	Falta de conocimiento técnico; Costo percibido alto; Considerar que el negocio es “muy pequeño” para ser atacado	Invertiría si es económico y fácil de usar	Plataforma guiada paso a paso	Acompañamiento paso a paso
34	Costo percibido alto; Considerar que el negocio es “muy pequeño” para ser atacado; Falta de conocimiento técnico	Invertiría si es económico y fácil de usar	Plataforma guiada paso a paso	Bajo costo
35	Costo percibido alto; Considerar que el negocio es “muy pequeño” para ser atacado; No sabemos por dónde empezar	Invertiría si veo beneficios claros	Plataforma guiada paso a paso	Acompañamiento paso a paso
36	No sabemos por dónde empezar; Costo percibido alto	Invertiría si veo beneficios claros	Plantillas y documentos	Facilidad de uso
37	No sabemos por dónde empezar; Falta de conocimiento técnico; Falta de tiempo	Invertiría si es económico y fácil de usar	Plantillas y documentos	Evidencia para control/auditoría
38	Falta de tiempo; No sabemos por dónde empezar; Falta de conocimiento técnico	Invertiría si es económico y fácil de usar	Plantillas y documentos	Acompañamiento paso a paso
39	Falta de conocimiento técnico; No sabemos por dónde empezar; Falta de tiempo	Invertiría si es económico y fácil de usar	Plataforma guiada paso a paso	Facilidad de uso
40	Considerar que el negocio es “muy pequeño” para ser atacado; Falta de conocimiento técnico; Costo percibido alto	Invertiría si es económico y fácil de usar	Asesoría personalizada	Facilidad de uso
41	Falta de conocimiento técnico; Costo percibido alto; Considerar que el negocio es “muy pequeño” para ser atacado	Invertiría si es económico y fácil de usar	Asesoría personalizada	Facilidad de uso
42	No sabemos por dónde empezar; Costo percibido alto; Considerar que el negocio es “muy pequeño” para ser atacado	Invertiría si es económico y fácil de usar	Plataforma guiada paso a paso	Facilidad de uso
43	Costo percibido alto; No sabemos por dónde empezar	Invertiría si es económico y fácil de usar	Asesoría personalizada	Acompañamiento paso a paso
44	Falta de conocimiento técnico; Falta de tiempo; No sabemos por dónde empezar	Invertiría si veo beneficios claros	Asesoría personalizada	Evidencia para control/auditoría
45	Falta de conocimiento técnico; Falta de tiempo; No sabemos por dónde empezar	Invertiría si es económico y fácil de usar	Plataforma guiada paso a paso	Bajo costo
46	Falta de tiempo; Falta de conocimiento técnico; No sabemos por dónde empezar	Invertiría si es económico y fácil de usar	Plataforma guiada paso a paso	Acompañamiento paso a paso
47	Considerar que el negocio es “muy pequeño” para ser atacado; Costo percibido alto; Falta de conocimiento técnico	Invertiría si es económico y fácil de usar	Plataforma guiada paso a paso	Bajo costo

48	Falta de conocimiento técnico; Considerar que el negocio es “muy pequeño” para ser atacado; Costo percibido alto	Invertiría si es económico y fácil de usar	Plantillas y documentos	Facilidad de uso
49	No sabemos por dónde empezar; Considerar que el negocio es “muy pequeño” para ser atacado; Costo percibido alto	Invertiría si veo beneficios claros	Plataforma guiada paso a paso	Acompañamiento paso a paso
50	Costo percibido alto; No sabemos por dónde empezar	Invertiría si es económico y fácil de usar	Asesoría personalizada	Acompañamiento paso a paso

Tabla B.4.

Preguntas 19-21

ID	P19	P20	P21
1	Tengo control parcial	Que alguien entre al correo de la empresa y use esa información para engañar a clientes.	Necesitaría una guía sencilla que me diga por dónde empezar sin lenguaje técnico complicado.
2	He implementado algunas medidas básicas	Perder los archivos de facturación y no poder atender pedidos pendientes.	Me ayudaría una herramienta económica que explique paso a paso qué debo corregir primero.
3	Sé que es importante, pero no hago nada	Un fraude por mensajes falsos, porque casi todo lo coordinamos por WhatsApp.	Primero tendría que entender qué riesgos son realmente urgentes para mi tipo de negocio.
4	He implementado algunas medidas básicas	Que se dañen los equipos y no tengamos una copia reciente de la información.	Requerimos capacitación corta para el personal, porque todos usamos los sistemas de alguna forma.
5	He implementado algunas medidas básicas	Robo de datos de clientes o proveedores, aunque sea un negocio pequeño.	Necesito plantillas listas para adaptar, no documentos largos que nadie termina leyendo.
6	Sé que es importante, pero no hago nada	Una estafa bancaria digital por descuido al revisar enlaces o correos.	Sería útil recibir recomendaciones priorizadas, porque no podemos hacerlo todo al mismo tiempo.
7	He implementado algunas medidas básicas	Quedarnos sin acceso al sistema de ventas durante días de alta demanda.	Me convencería más si pudiera ver beneficios concretos y no solo teoría de seguridad.
8	Sé que es importante, pero no hago nada	Que un empleado comparta contraseñas sin mala intención y eso genere un problema.	Necesitamos acompañamiento inicial para ordenar contraseñas, respaldos y accesos.
9	Sé que es importante, pero no hago nada	La pérdida de información contable, porque reconstruirla sería costoso.	Haría falta una solución que no requiera contratar un equipo técnico especializado.
10	Sé que es importante, pero no hago nada	Que nos suplanten en redes o WhatsApp y afecten la confianza de los clientes.	Me serviría un diagnóstico rápido que muestre el nivel actual y los pasos mínimos.
11	Sé que es importante, pero no hago nada	Un virus en los computadores donde guardamos cotizaciones e inventario.	Necesito saber cuánto costaría y qué acciones dan más valor en el corto plazo.
12	He implementado algunas medidas básicas	Que alguien borre información importante y no sepamos cómo recuperarla.	La empresa requiere algo práctico, con ejemplos parecidos a negocios pequeños.

13	He implementado algunas medidas básicas	El acceso no autorizado a cuentas de correo, bancos o plataformas de proveedores.	Me gustaría contar con recordatorios y seguimiento, porque empezamos procesos y luego se abandonan.
14	Tengo una estrategia definida	No detectar a tiempo un incidente y que el daño crezca sin darnos cuenta.	Necesitaría que el proceso sea claro para gerencia y también para empleados operativos.
15	He implementado algunas medidas básicas	Que los empleados caigan en phishing porque no han recibido orientación formal.	Hace falta organizar responsabilidades; ahora todos creen que otro se encarga.
16	He implementado algunas medidas básicas	La dependencia de una sola persona para manejar claves y accesos.	Implementaría medidas si vienen explicadas en tareas pequeñas y medibles.
17	Sé que es importante, pero no hago nada	Un bloqueo de información justo cuando necesitamos facturar o entregar pedidos.	Necesitamos evidencia de qué se hizo, para no depender solo de la palabra de cada persona.
18	Sé que es importante, pero no hago nada	Que se filtre información sensible y luego sea difícil explicar lo ocurrido.	Me ayudaría tener políticas básicas ya redactadas y ajustarlas al negocio.
19	Sé que es importante, pero no hago nada	El uso de contraseñas débiles en cuentas compartidas del negocio.	Requiero una solución que funcione con poco presupuesto y poco tiempo disponible.
20	He implementado algunas medidas básicas	Que los respaldos no funcionen cuando realmente se necesiten.	Primero debemos crear conciencia interna, porque varios todavía no ven el riesgo cercano.
21	Tengo control parcial	Una caída del computador principal donde se administra la operación diaria.	Necesitaría apoyo para configurar autenticación en dos pasos y copias de seguridad.
22	He implementado algunas medidas básicas	Que un proveedor externo tenga acceso y no sepamos qué permisos conserva.	Sería bueno tener una plataforma que indique qué documentos o capturas guardar como prueba.
23	He implementado algunas medidas básicas	La falta de control sobre quién entra a cada sistema o documento.	Necesito que alguien traduzca las normas a acciones simples para una empresa pequeña.
24	Sé que es importante, pero no hago nada	Que se pierda información de clientes por no tener procesos definidos.	Me motivaría ver un semáforo de riesgos y un plan de mejora realista.
25	Tengo control parcial	Un engaño por correo que termine en pago a una cuenta equivocada.	Haría falta definir políticas mínimas sin volver pesado el trabajo diario.
26	Tengo control parcial	Que un celular de trabajo se pierda con información de clientes y ventas.	Necesitamos aprender a reconocer correos sospechosos con ejemplos claros.
27	Sé que es importante, pero no hago nada	El exceso de confianza; pensamos que por ser pequeños nadie nos mira.	Me serviría una ruta de implementación por etapas, empezando por lo más crítico.
28	He implementado algunas medidas básicas	Que se mezclen cuentas personales y del negocio y eso abra riesgos innecesarios.	Para invertir, tendría que comprobar que no será una carga adicional para el equipo.
29	He implementado algunas medidas básicas	No tener un plan si un sistema deja de funcionar o si se bloquean los datos.	Necesitamos ordenar los respaldos y probar que se puedan recuperar los datos.
30	Sé que es importante, pero no hago nada	Que los archivos importantes estén en equipos sin mantenimiento ni respaldo.	Me gustaría una solución con lenguaje empresarial, no demasiado técnico.

31	Sé que es importante, pero no hago nada	La falta de reglas claras para manejar información interna.	Hace falta saber qué controles aplican a nosotros y cuáles pueden esperar.
32	He implementado algunas medidas básicas	Que una contraseña antigua siga activa después de que alguien deje de trabajar aquí.	Necesitaría reportes simples para revisar avances en reuniones de dirección.
33	He implementado algunas medidas básicas	Un ataque que interrumpa las ventas y dañe la relación con clientes habituales.	Nos ayudaría una asesoría inicial y luego una plataforma para continuar solos.
34	Tengo control parcial	Que por ahorrar tiempo usemos prácticas inseguras sin medir las consecuencias.	Requiero instrucciones claras para separar accesos personales de accesos del negocio.
35	He implementado algunas medidas básicas	La pérdida de acceso al correo, porque desde ahí coordinamos casi todo.	Sería importante que la herramienta permita documentar responsables y fechas.
36	He implementado algunas medidas básicas	Que una persona no autorizada vea información comercial o de pagos.	Necesito algo que nos ayude a convertir la preocupación en acciones concretas.
37	Tengo una estrategia definida	La suplantación del negocio para pedir dinero o datos a nuestros clientes.	Haría falta apoyo para que los empleados entiendan que seguridad no es solo tecnología.
38	Sé que es importante, pero no hago nada	No saber diferenciar un mensaje real de uno malicioso cuando llega con urgencia.	Necesitamos medir el avance, porque hoy no sabemos si estamos bien o mal.
39	He implementado algunas medidas básicas	Que se pierdan evidencias de pagos, entregas o acuerdos con proveedores.	Me serviría comenzar con controles básicos: claves, backups, permisos y capacitación.
40	Tengo control parcial	Un ransomware o bloqueo de archivos, aunque no conozco bien cómo funciona.	Para implementarlo necesitaría una versión sencilla, accesible y con resultados visibles.
41	Sé que es importante, pero no hago nada	Que los empleados usen redes públicas o dispositivos personales sin precaución.	Requiero recomendaciones adaptadas al tamaño de la empresa, no soluciones corporativas grandes.
42	He implementado algunas medidas básicas	La falta de seguimiento: hacemos algunas cosas, pero nadie verifica si sirven.	Necesitamos un plan que no interrumpa la operación diaria ni exija demasiado tiempo.
43	Sé que es importante, pero no hago nada	Que un error humano afecte información crítica más que un ataque sofisticado.	Me ayudaría que la plataforma priorice riesgos según nuestras respuestas.
44	Sé que es importante, pero no hago nada	Que la información esté dispersa y sea imposible recuperarla con rapidez.	Haría falta demostrar al dueño que esto reduce pérdidas, no que es solo un gasto.
45	Sé que es importante, pero no hago nada	Una brecha de datos que nos genere reclamos o pérdida de reputación.	Necesitamos procesos escritos, pero breves, para que la gente sí los use.
46	Sé que es importante, pero no hago nada	Que no tengamos trazabilidad de cambios, accesos o documentos eliminados.	Me gustaría recibir alertas sobre tareas pendientes y evidencias faltantes.
47	He implementado algunas medidas básicas	Quedar paralizados por 48 horas, especialmente si no podemos vender ni cobrar.	Requiero una guía que permita empezar aunque no tengamos personal de sistemas.
48	Tengo control parcial	Que la seguridad dependa de memoria y costumbre, no de reglas escritas.	Sería útil comparar nuestro resultado con un nivel básico esperado para empresas similares.

49	Sé que es importante, pero no hago nada	El manejo informal de usuarios y claves en aplicaciones de trabajo.	Necesitamos soporte en los primeros pasos y luego autonomía para mantenerlo.
50	Sé que es importante, pero no hago nada	Que por desconocimiento dejemos abierta una puerta fácil para un atacante.	Me convencería una herramienta que entregue diagnóstico, políticas y plan de mejora en un solo lugar.

Anexo C – Resultados consolidados de las encuestas.

Este anexo contiene el registro de las respuestas individuales obtenidas durante la aplicación de las encuestas. Su inclusión tiene como finalidad respaldar la trazabilidad del proceso de investigación, permitiendo verificar la información utilizada para el análisis de resultados y la construcción de las conclusiones del estudio.

Tabla C.1

Pregunta 1: Dependencia digital	Cantidad	Porcentaje
Respuesta	**Cantidad**	**Porcentaje**
Baja	8	16%
Media	22	44%
Alta	20	40%
	50	**100%**

Tabla C.2.

Pregunta 2: Empleados	Cantidad	Porcentaje
Respuesta	**Cantidad**	**Porcentaje**
1–2 empleados	12	24%
3–5 empleados	18	36%
6–10 empleados	15	30%
Más de 10 empleados	5	10%
	50	**100%**

Tabla C.3.

Pregunta 3: Sector	Cantidad	Porcentaje
Respuesta	**Cantidad**	**Porcentaje**
Servicios	18	36%
Comercio	16	32%
Industrial	10	20%
Otros	6	12%
	50	**100%**

Tabla C.4.

Pregunta 4: Antigüedad	Cantidad	Porcentaje
Respuesta	**Cantidad**	**Porcentaje**
Menos de 1 año	8	16%
1-3 años	18	36%
Más de 3 años	24	48%
	50	**100%**

Tabla C.5.

Pregunta 5: Probabilidad incidente	Cantidad	Porcentaje
Respuesta	**Cantidad**	**Porcentaje**
1	3	6%
2	11	22%
3	22	44%
4	7	14%
5	7	14%
	50	**100%**

Tabla C.6.

Pregunta 6: Impacto pérdida 48h	Cantidad	Porcentaje
Respuesta	**Cantidad**	**Porcentaje**
1	0	0%
2	4	8%
3	5	10%
4	28	56%
5	13	26%
	50	**100%**

Tabla C.7.

Pregunta 7: Preparación	Cantidad	Porcentaje
Respuesta	**Cantidad**	**Porcentaje**
1	18	36%
2	14	28%
3	14	28%
4	4	8%
5		0%
	50	**100%**

Tabla C.8.

Pregunta 8: Recuperación	Cantidad	Porcentaje
Respuesta	**Cantidad**	**Porcentaje**
1	11	22%
2	20	40%
3	10	20%
4	3	6%
5	6	12%
	50	**100%**

Tabla C.9.

Pregunta 9: Contraseñas	Cantidad	Porcentaje
Respuesta	**Cantidad**	**Porcentaje**
Cada usuario decide	29	58%
Hay reglas básicas	10	20%
No se gestionan formalmente	9	18%
Se usa gestor de contraseñas	2	4%
	50	**100%**

Tabla C.10.

Pregunta 10: Backups	Cantidad	Porcentaje
Respuesta	**Cantidad**	**Porcentaje**
No existen	10	20%
Se hacen ocasionalmente	19	38%
Son automáticos y probados	5	10%
Son periódicos pero no verificados	16	32%
	50	**100%**

Tabla C.11.

Pregunta 11: Responsable SI	Cantidad	Porcentaje
Respuesta	**Cantidad**	**Porcentaje**
Es informal	10	20%
Está asignado pero sin funciones claras	5	10%
Está definido con responsabilidades	23	46%
No hay responsable	12	24%
	50	**100%**

Tabla C.12.

Pregunta 12: 2FA	Cantidad	Porcentaje
Respuesta	**Cantidad**	**Porcentaje**
No	31	62%
Sí	19	38%
	50	**100%**

Tabla C.13.

Pregunta 13: Políticas	Cantidad	Porcentaje
Respuesta	**Cantidad**	**Porcentaje**
No	33	66%
Sí	17	34%
	50	**100%**

Tabla C.14.

Pregunta 14: Capacitación phishing	Cantidad	Porcentaje
Respuesta	**Cantidad**	**Porcentaje**
No	21	42%
Ocasionalmente	15	30%
Sí	14	28%
	50	**100%**

Tabla C.15.

Pregunta 15: Barreras	Cantidad	Porcentaje
Respuesta	**Cantidad**	**Porcentaje**
Considerar que el negocio es “muy pequeño” para ser atacado	18	36%
Costo percibido alto	27	54%
Falta de conocimiento técnico	36	72%
Falta de tiempo	24	48%
No sabemos por dónde empezar	34	68%
	139	**278%**

Tabla C.16.

Pregunta 16: Disposición inversión	Cantidad	Porcentaje
Respuesta	**Cantidad**	**Porcentaje**
Invertiría si es económico y fácil de usar	38	76%
Invertiría si veo beneficios claros	9	18%
Prefiero no invertir en este momento	3	6%
Ya estoy invirtiendo en ciberseguridad	0	0%
	50	**100%**

Tabla C.17.

Pregunta 17: Solución preferida	Cantidad	Porcentaje
Respuesta	**Cantidad**	**Porcentaje**
Asesoría personalizada	11	22%
No estoy interesado	0	0%
Plantillas y documentos	8	16%
Plataforma guiada paso a paso	31	62%
	50	**100%**

Tabla C.18.

Pregunta 18: Valor principal	Cantidad	Porcentaje
Respuesta	**Cantidad**	**Porcentaje**
Acompañamiento paso a paso	17	34%
Bajo costo	9	18%
Evidencia para control/auditoría	4	8%
Facilidad de uso	20	40%
	50	**100%**

Tabla C.19.

Pregunta 19: Situación actual	Cantidad	Porcentaje
Respuesta	**Cantidad**	**Porcentaje**
He implementado algunas medidas básicas	20	40%
Sé que es importante, pero no hago nada	21	42%
Tengo control parcial	7	14%
Tengo una estrategia definida	2	4%
	50	**100%**

Tabla C.20.

Pregunta 20: Mayor riesgo digital	Cantidad	Porcentaje
Respuesta	**Cantidad**	**Porcentaje**
Que alguien entre al correo de la empresa y use esa información para engañar a clientes.	**1**	2%
Perder los archivos de facturación y no poder atender pedidos pendientes.	**1**	2%
Un fraude por mensajes falsos, porque casi todo lo coordinamos por WhatsApp.	**1**	2%
Que se dañen los equipos y no tengamos una copia reciente de la información.	**1**	2%
Robo de datos de clientes o proveedores, aunque sea un negocio pequeño.	**1**	2%
Una estafa bancaria digital por descuido al revisar enlaces o correos.	**1**	2%
Quedarnos sin acceso al sistema de ventas durante días de alta demanda.	**1**	2%
Que un empleado comparta contraseñas sin mala intención y eso genere un problema.	**1**	2%
La pérdida de información contable, porque reconstruirla sería costoso.	**1**	2%
Que nos suplanten en redes o WhatsApp y afecten la confianza de los clientes.	**1**	2%
Un virus en los computadores donde guardamos cotizaciones e inventario.	**1**	2%
Que alguien borre información importante y no sepamos cómo recuperarla.	**1**	2%
El acceso no autorizado a cuentas de correo, bancos o plataformas de proveedores.	**1**	2%
No detectar a tiempo un incidente y que el daño crezca sin darnos cuenta.	**1**	2%
Que los empleados caigan en phishing porque no han recibido orientación formal.	**1**	2%
La dependencia de una sola persona para manejar claves y accesos.	**1**	2%
Un bloqueo de información justo cuando necesitamos facturar o entregar pedidos.	**1**	2%
Que se filtre información sensible y luego sea difícil explicar lo ocurrido.	**1**	2%
El uso de contraseñas débiles en cuentas compartidas del negocio.	**1**	2%
Que los respaldos no funcionen cuando realmente se necesiten.	**1**	2%

Una caída del computador principal donde se administra la operación diaria.	**1**	2%
Que un proveedor externo tenga acceso y no sepamos qué permisos conserva.	**1**	2%
La falta de control sobre quién entra a cada sistema o documento.	**1**	2%
Que se pierda información de clientes por no tener procesos definidos.	**1**	2%
Un engaño por correo que termine en pago a una cuenta equivocada.	**1**	2%
Que un celular de trabajo se pierda con información de clientes y ventas.	**1**	2%
El exceso de confianza; pensamos que por ser pequeños nadie nos mira.	**1**	2%
Que se mezclen cuentas personales y del negocio y eso abra riesgos innecesarios.	**1**	2%
No tener un plan si un sistema deja de funcionar o si se bloquean los datos.	**1**	2%
Que los archivos importantes estén en equipos sin mantenimiento ni respaldo.	**1**	2%
La falta de reglas claras para manejar información interna.	**1**	2%
Que una contraseña antigua siga activa después de que alguien deje de trabajar aquí.	**1**	2%
Un ataque que interrumpa las ventas y dañe la relación con clientes habituales.	**1**	2%
Que por ahorrar tiempo usemos prácticas inseguras sin medir las consecuencias.	**1**	2%
La pérdida de acceso al correo, porque desde ahí coordinamos casi todo.	**1**	2%
Que una persona no autorizada vea información comercial o de pagos.	**1**	2%
La suplantación del negocio para pedir dinero o datos a nuestros clientes.	**1**	2%
No saber diferenciar un mensaje real de uno malicioso cuando llega con urgencia.	**1**	2%
Que se pierdan evidencias de pagos, entregas o acuerdos con proveedores.	**1**	2%
Un ransomware o bloqueo de archivos, aunque no conozco bien cómo funciona.	**1**	2%
Que los empleados usen redes públicas o dispositivos personales sin precaución.	**1**	2%
La falta de seguimiento: hacemos algunas cosas, pero nadie verifica si sirven.	**1**	2%
Que un error humano afecte información crítica más que un ataque sofisticado.	**1**	2%
Que la información esté dispersa y sea imposible recuperarla con rapidez.	**1**	2%
Una brecha de datos que nos genere reclamos o pérdida de reputación.	**1**	2%
Que no tengamos trazabilidad de cambios, accesos o documentos eliminados.	**1**	2%
Quedar paralizados por 48 horas, especialmente si no podemos vender ni cobrar.	**1**	2%
Que la seguridad dependa de memoria y costumbre, no de reglas escritas.	**1**	2%
El manejo informal de usuarios y claves en aplicaciones de trabajo.	**1**	2%
Que por desconocimiento dejemos abierta una puerta fácil para un atacante.	**1**	2%
	50	**100%**

Tabla C.21.

Pregunta 21: Qué necesita para implementar	**Cantidad**	**Porcentaje**
Respuesta	**Cantidad**	**Porcentaje**
Necesitaría una guía sencilla que me diga por dónde empezar sin lenguaje técnico complicado.	**1**	2%
Me ayudaría una herramienta económica que explique paso a paso qué debo corregir primero.	**1**	2%
Primero tendría que entender qué riesgos son realmente urgentes para mi tipo de negocio.	**1**	2%
Requerimos capacitación corta para el personal, porque todos usamos los sistemas de alguna forma.	**1**	2%

Necesito plantillas listas para adaptar, no documentos largos que nadie termina leyendo.	**1**	2%
Sería útil recibir recomendaciones priorizadas, porque no podemos hacerlo todo al mismo tiempo.	**1**	2%
Me convencería más si pudiera ver beneficios concretos y no solo teoría de seguridad.	**1**	2%
Necesitamos acompañamiento inicial para ordenar contraseñas, respaldos y accesos.	**1**	2%
Haría falta una solución que no requiera contratar un equipo técnico especializado.	**1**	2%
Me serviría un diagnóstico rápido que muestre el nivel actual y los pasos mínimos.	**1**	2%
Necesito saber cuánto costaría y qué acciones dan más valor en el corto plazo.	**1**	2%
La empresa requiere algo práctico, con ejemplos parecidos a negocios pequeños.	**1**	2%
Me gustaría contar con recordatorios y seguimiento, porque empezamos procesos y luego se abandonan.	**1**	2%
Necesitaría que el proceso sea claro para gerencia y también para empleados operativos.	**1**	2%
Hace falta organizar responsabilidades; ahora todos creen que otro se encarga.	**1**	2%
Implementaría medidas si vienen explicadas en tareas pequeñas y medibles.	**1**	2%
Necesitamos evidencia de qué se hizo, para no depender solo de la palabra de cada persona.	**1**	2%
Me ayudaría tener políticas básicas ya redactadas y ajustarlas al negocio.	**1**	2%
Requiero una solución que funcione con poco presupuesto y poco tiempo disponible.	**1**	2%
Primero debemos crear conciencia interna, porque varios todavía no ven el riesgo cercano.	**1**	2%
Necesitaría apoyo para configurar autenticación en dos pasos y copias de seguridad.	**1**	2%
Sería bueno tener una plataforma que indique qué documentos o capturas guardar como prueba.	**1**	2%
Necesito que alguien traduzca las normas a acciones simples para una empresa pequeña.	**1**	2%
Me motivaría ver un semáforo de riesgos y un plan de mejora realista.	**1**	2%
Haría falta definir políticas mínimas sin volver pesado el trabajo diario.	**1**	2%
Necesitamos aprender a reconocer correos sospechosos con ejemplos claros.	**1**	2%
Me serviría una ruta de implementación por etapas, empezando por lo más crítico.	**1**	2%
Para invertir, tendría que comprobar que no será una carga adicional para el equipo.	**1**	2%
Necesitamos ordenar los respaldos y probar que se puedan recuperar los datos.	**1**	2%
Me gustaría una solución con lenguaje empresarial, no demasiado técnico.	**1**	2%
Hace falta saber qué controles aplican a nosotros y cuáles pueden esperar.	**1**	2%
Necesitaría reportes simples para revisar avances en reuniones de dirección.	**1**	2%
Nos ayudaría una asesoría inicial y luego una plataforma para continuar solos.	**1**	2%
Requiero instrucciones claras para separar accesos personales de accesos del negocio.	**1**	2%
Sería importante que la herramienta permita documentar responsables y fechas.	**1**	2%
Necesito algo que nos ayude a convertir la preocupación en acciones concretas.	**1**	2%

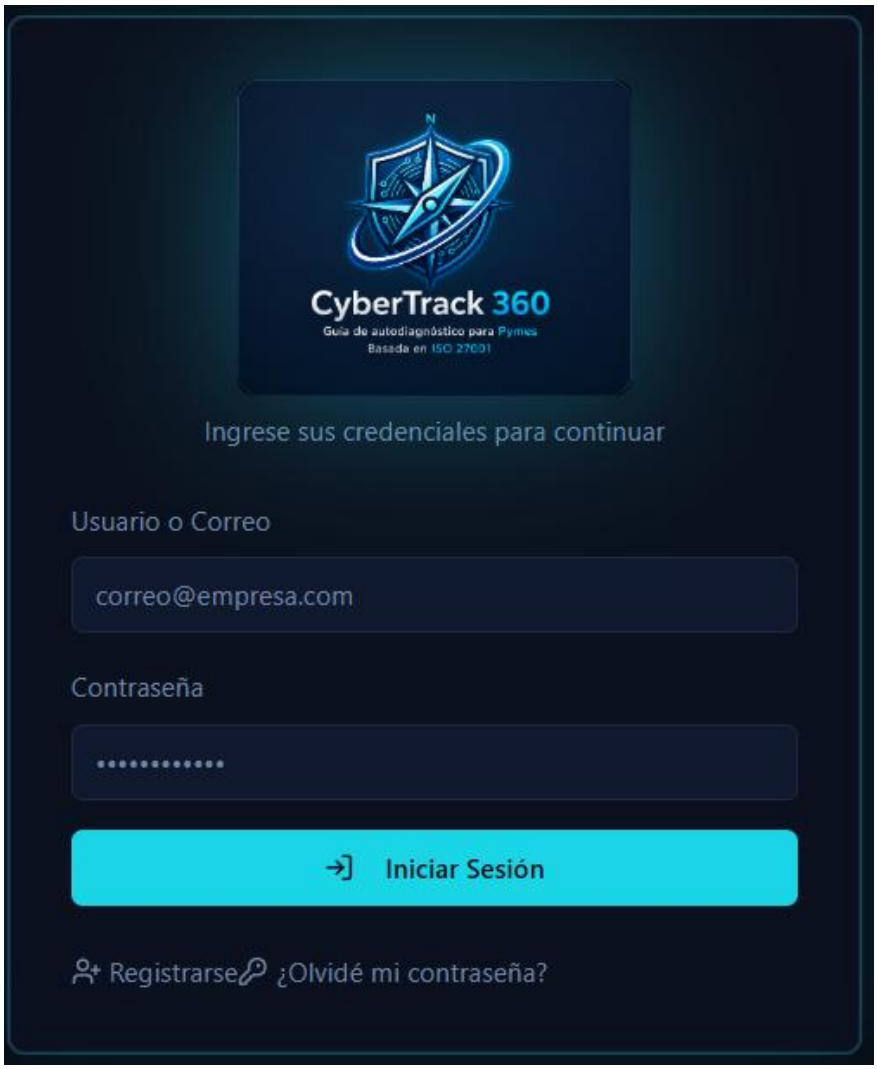
Haría falta apoyo para que los empleados entiendan que seguridad no es solo tecnología.	**1**	2%
Necesitamos medir el avance, porque hoy no sabemos si estamos bien o mal.	**1**	2%
Me serviría comenzar con controles básicos: claves, backups, permisos y capacitación.	**1**	2%
Para implementarlo necesitaría una versión sencilla, accesible y con resultados visibles.	**1**	2%
Requiero recomendaciones adaptadas al tamaño de la empresa, no soluciones corporativas grandes.	**1**	2%
Necesitamos un plan que no interrumpa la operación diaria ni exija demasiado tiempo.	**1**	2%
Me ayudaría que la plataforma priorice riesgos según nuestras respuestas.	**1**	2%
Haría falta demostrar al dueño que esto reduce pérdidas, no que es solo un gasto.	**1**	2%
Necesitamos procesos escritos, pero breves, para que la gente sí los use.	**1**	2%
Me gustaría recibir alertas sobre tareas pendientes y evidencias faltantes.	**1**	2%
Requiero una guía que permita empezar aunque no tengamos personal de sistemas.	**1**	2%
Sería útil comparar nuestro resultado con un nivel básico esperado para empresas similares.	**1**	2%
Necesitamos soporte en los primeros pasos y luego autonomía para mantenerlo.	**1**	2%
Me convencería una herramienta que entregue diagnóstico, políticas y plan de mejora en un solo lugar.	**1**	2%
	50	**100%**

Anexo D – Capturas del MVP CyberTrack 360.

Este anexo presenta una selección de capturas de pantalla del producto mínimo viable (MVP) CyberTrack 360. Las imágenes permiten evidenciar la implementación de las funcionalidades desarrolladas, incluyendo la autenticación de usuarios, la gestión de cuestionarios por roles, la evaluación de controles, el sistema de puntuación, la gestión de evidencias, la generación de recomendaciones y los paneles de resultados. Su propósito es respaldar visualmente la construcción y funcionamiento de la solución propuesta en el marco de esta investigación.

Figura D.1.

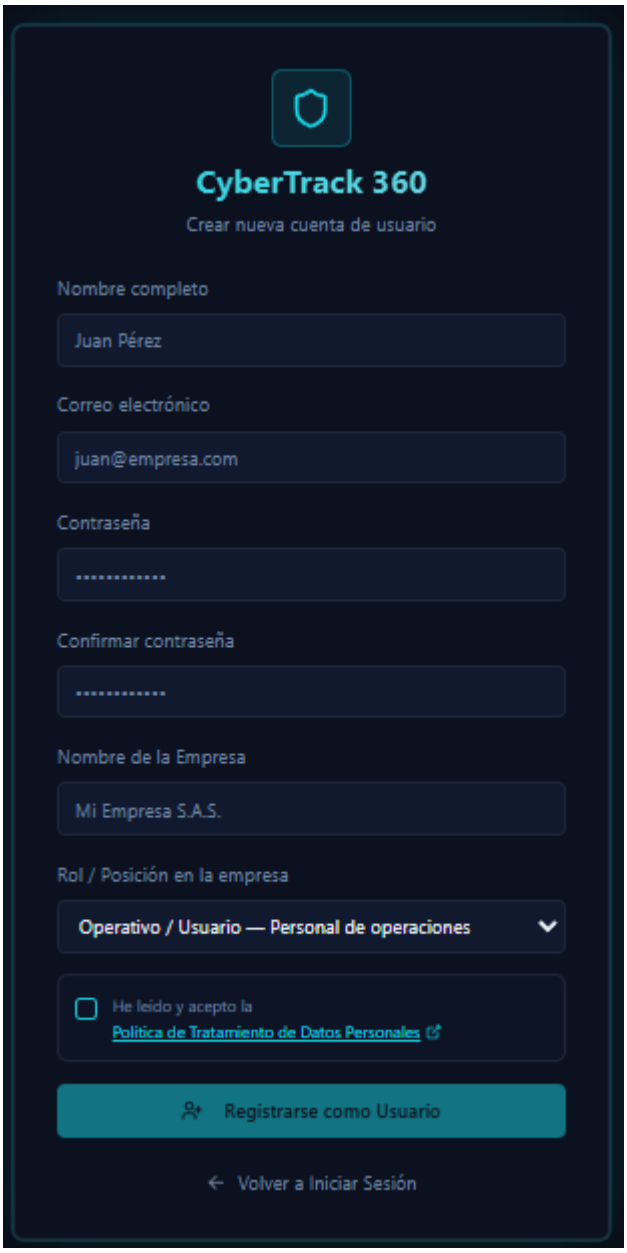
Pantalla inicio de sesión CyberTrack 360



Nota. Imagen tomada del MVP CyberTrack 360 (2026).

Figura D.2.

Pantalla Registrarse CyberTrack 360



Nota. Imagen tomada del MVP CyberTrack 360 (2026).

Figura D.3.

Pantalla Recuperar contraseña CyberTrack 360

Nota. Imagen tomada del MVP CyberTrack 360 (2026).

Figura D.4.

Pantalla Arquitectura del sistema CyberTrack 360

Nota. Imagen tomada del MVP CyberTrack 360 (2026).

Figura D.5.

Pantalla autodiagnóstico usuario Administrador CyberTrack 360

Nota. Imagen tomada del MVP CyberTrack 360 (2026).

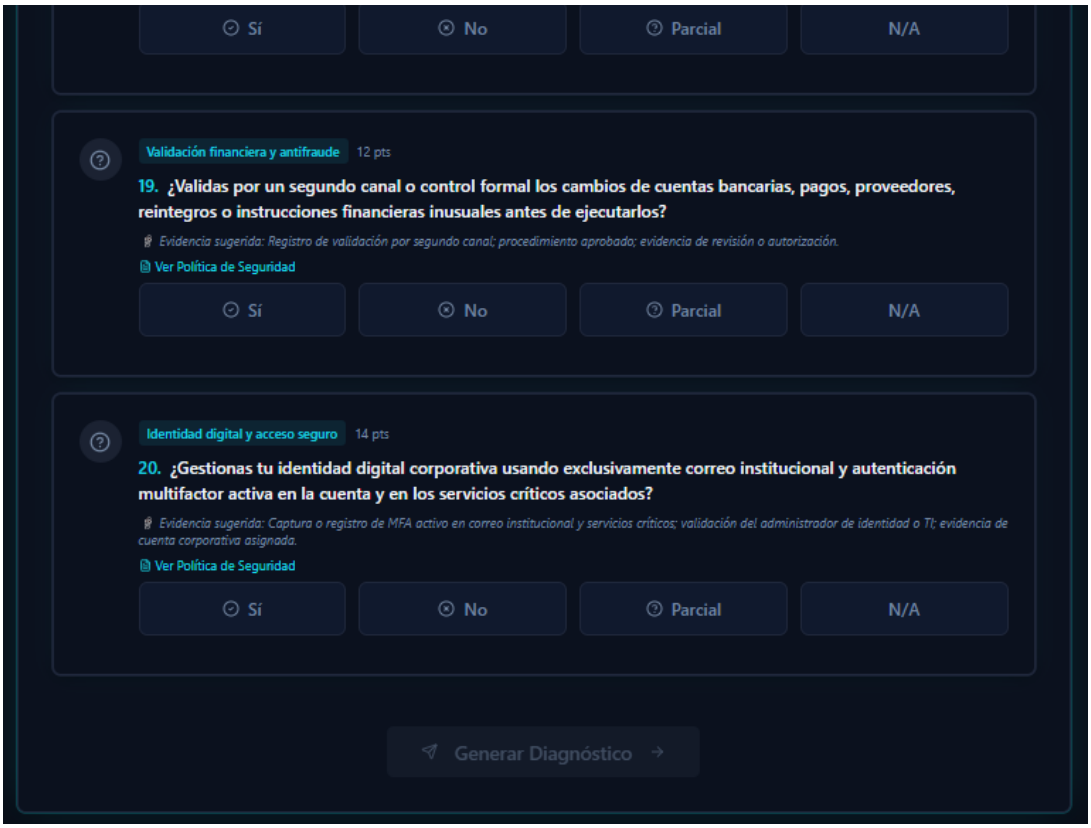
Figura D.6.

Pantalla autodiagnóstico despliegue por rol usuario Administrador CyberTrack 360

Nota. Imagen tomada del MVP CyberTrack 360 (2026).

Figura D.7.

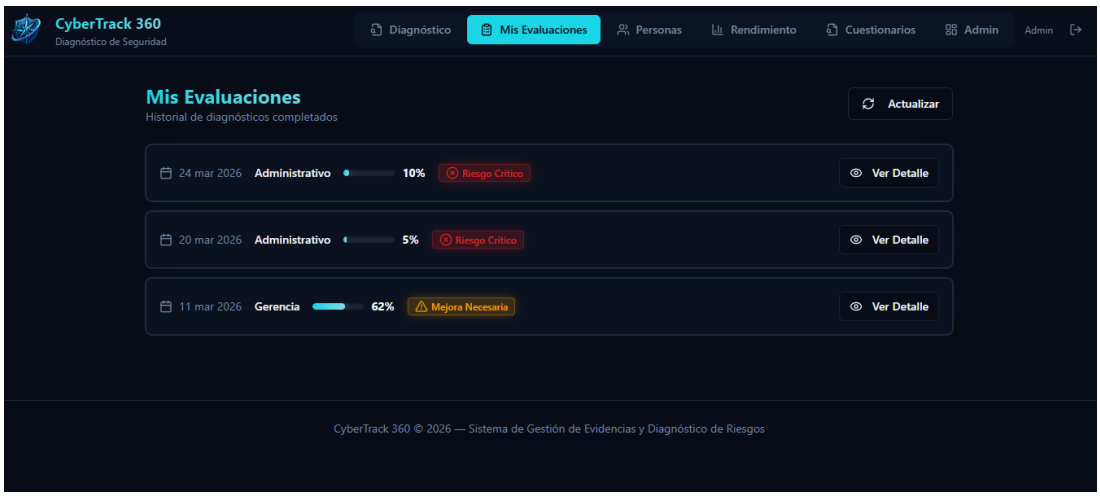
Pantalla generación autodiagnóstico usuario Administrador CyberTrack 360



Nota. Imagen tomada del MVP CyberTrack 360 (2026).

Figura D.8.

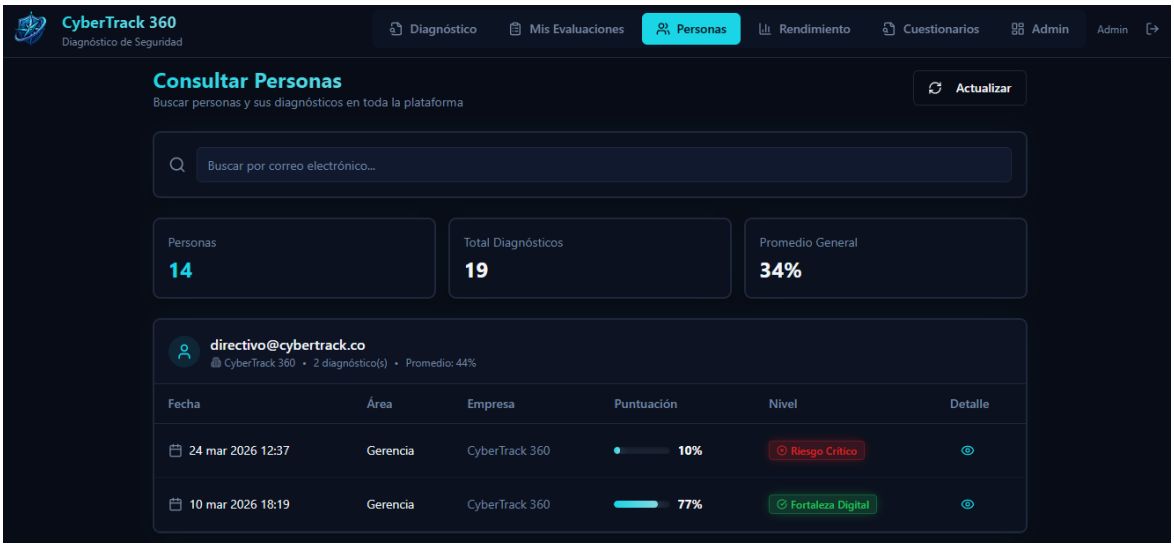
Pantalla panel mis evaluaciones usuario Administrador CyberTrack 360



Nota. Imagen tomada del MVP CyberTrack 360 (2026).

Figura D.9.

Pantalla panel de personas usuario Administrador CyberTrack 360



Nota. Imagen tomada del MVP CyberTrack 360 (2026).

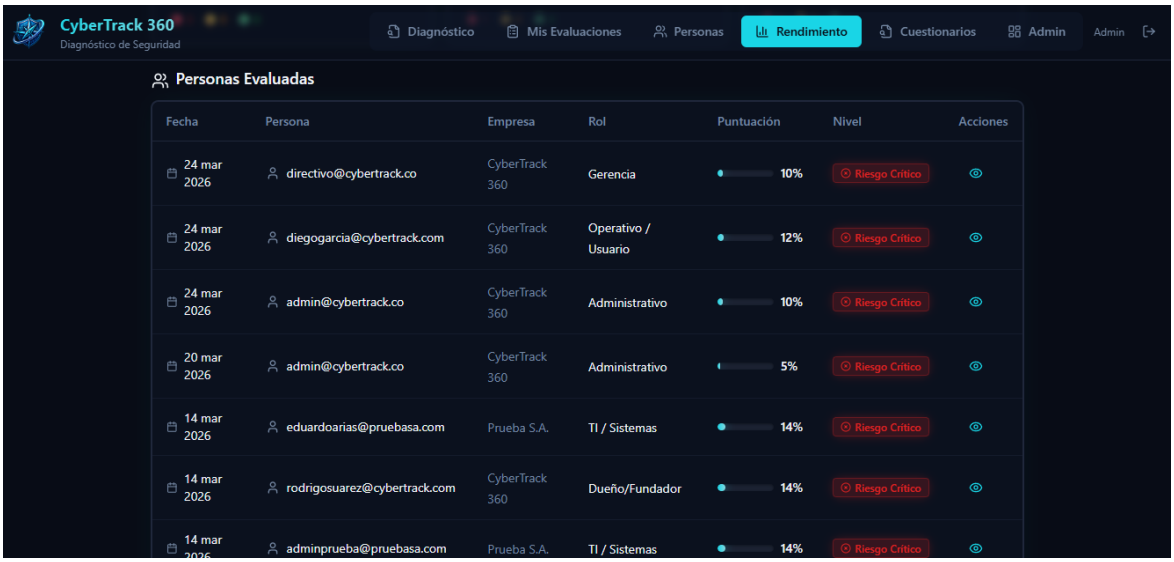
Figura D.10.

Pantalla panel de rendimiento usuario Administrador CyberTrack 360

Nota. Imagen tomada del MVP CyberTrack 360 (2026).

Figura D.11.

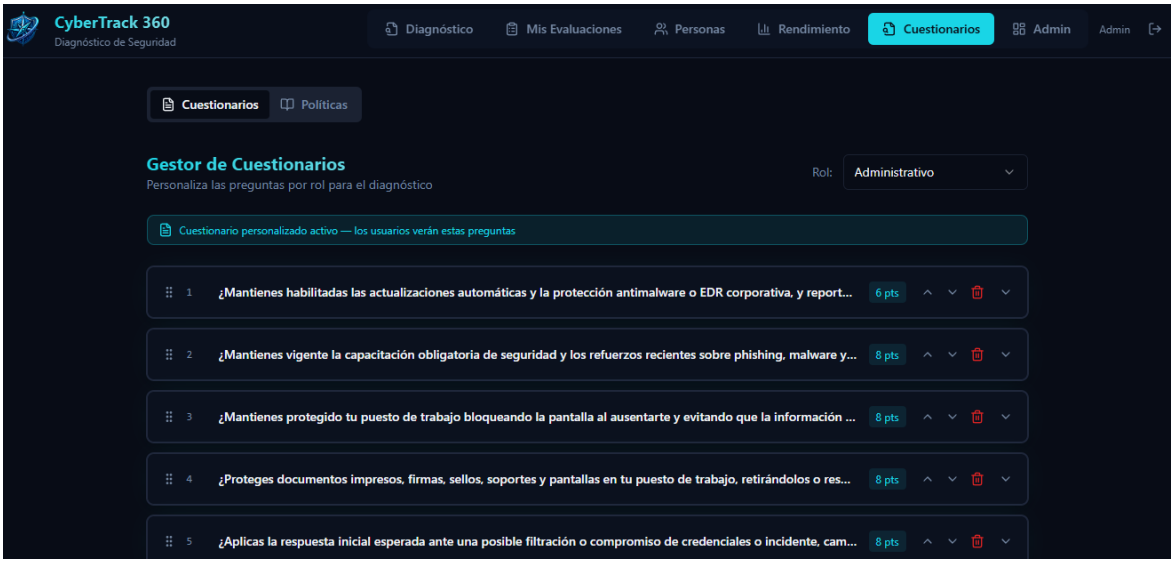
Pantalla panel de rendimiento personas usuario Administrador CyberTrack 360



Nota. Imagen tomada del MVP CyberTrack 360 (2026).

Figura D.12.

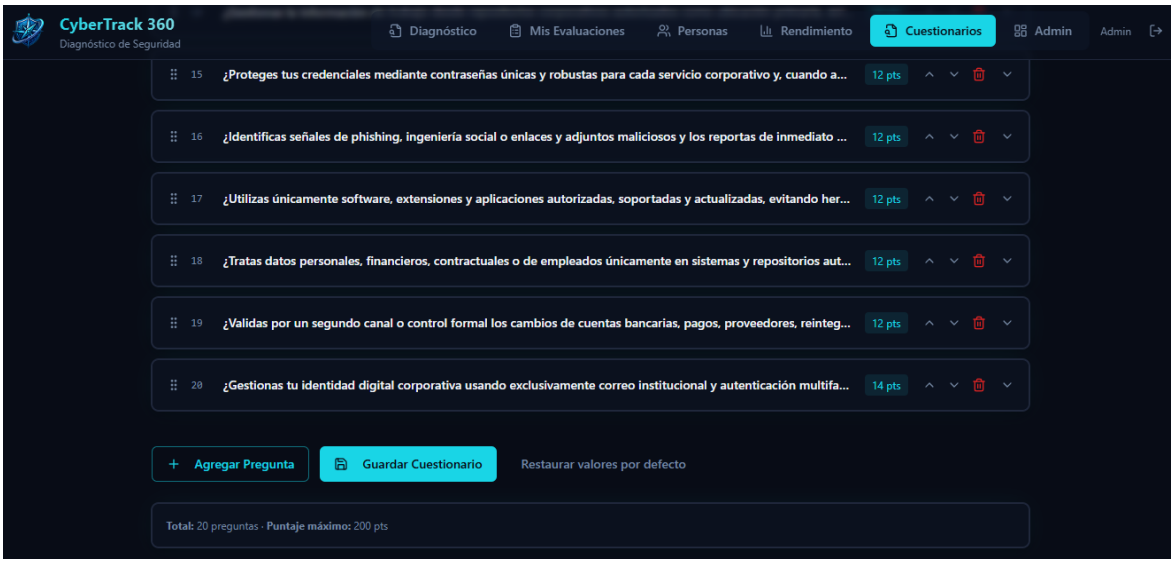
Pantalla panel gestor de cuestionarios usuario Administrador CyberTrack 360 1



Nota. Imagen tomada del MVP CyberTrack 360 (2026).

Figura D.13.

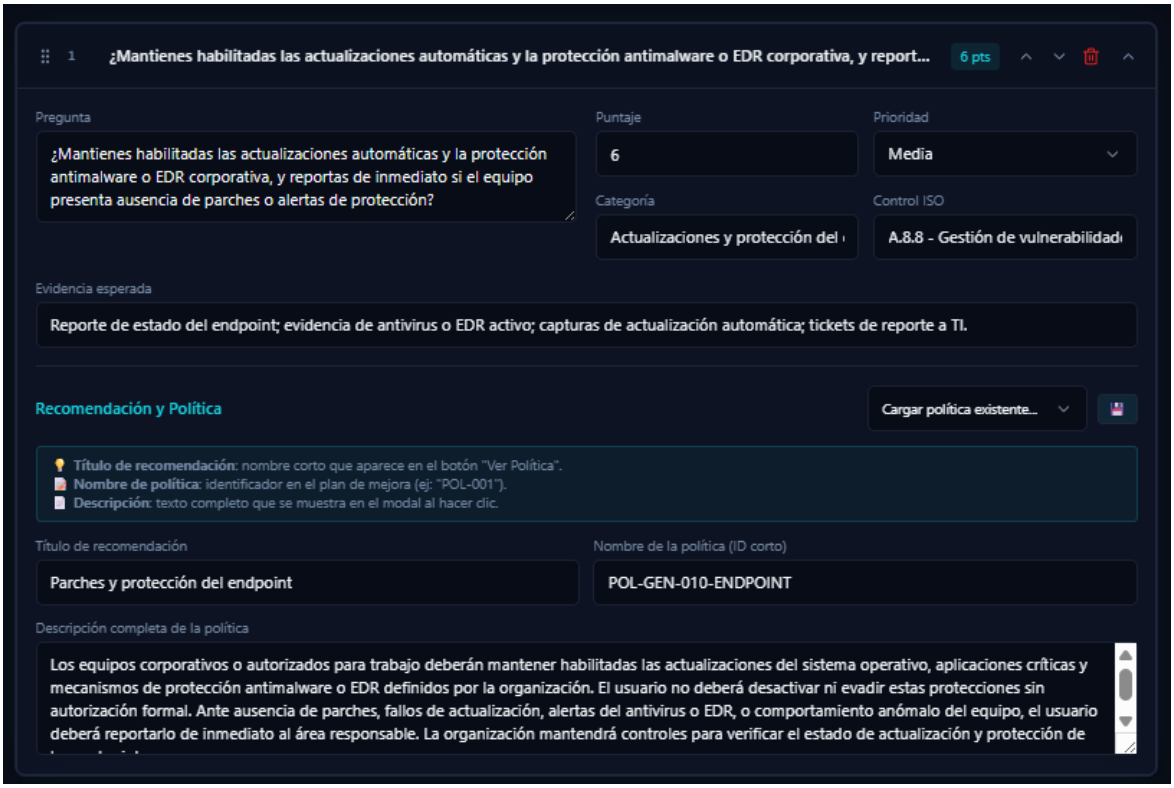
Pantalla panel gestor de cuestionarios usuario Administrador CyberTrack 360 2



Nota. Imagen tomada del MVP CyberTrack 360 (2026).

Figura D.14.

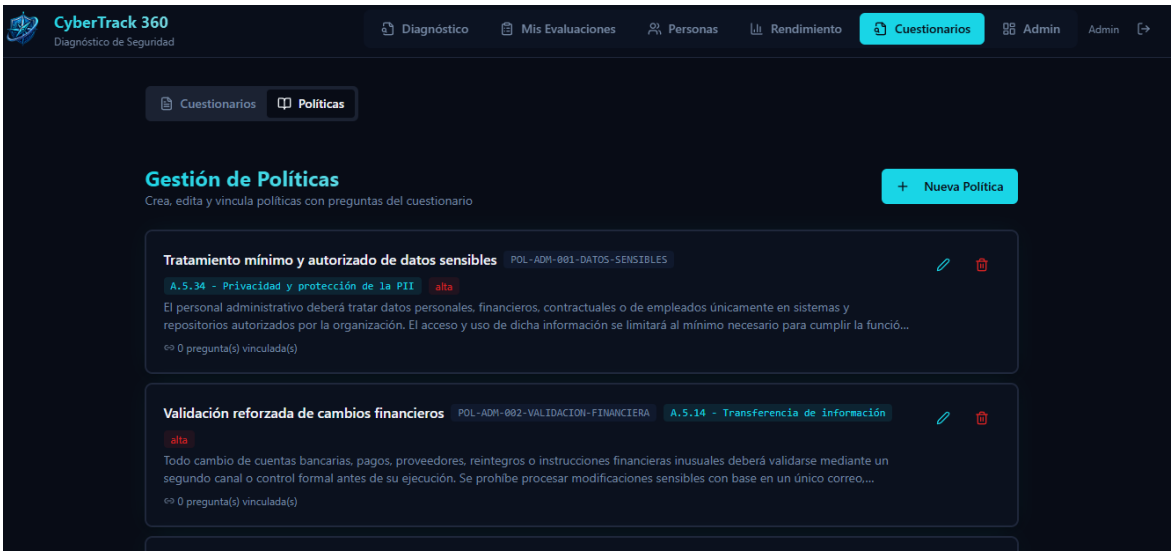
Pantalla panel adición de cuestionarios usuario Administrador CyberTrack 360



Nota. Imagen tomada del MVP CyberTrack 360 (2026).

Figura D.15.

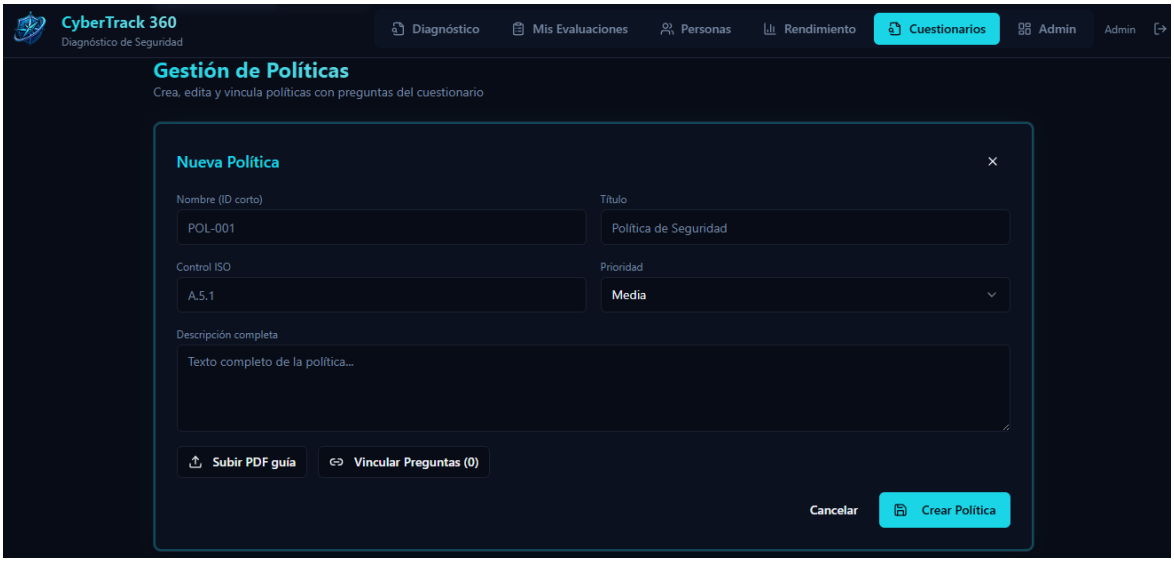
Pantalla panel gestión de políticas usuario Administrador CyberTrack 360



Nota. Imagen tomada del MVP CyberTrack 360 (2026).

Figura D.16.

Pantalla panel agregar política usuario Administrador CyberTrack 360



Nota. Imagen tomada del MVP CyberTrack 360 (2026).

Figura D.17.

Pantalla panel Admin usuario Administrador CyberTrack 360 1

Nota. Imagen tomada del MVP CyberTrack 360 (2026).

Figura D.18.

Pantalla panel Admin usuario Administrador CyberTrack 360 2

Nota. Imagen tomada del MVP CyberTrack 360 (2026).

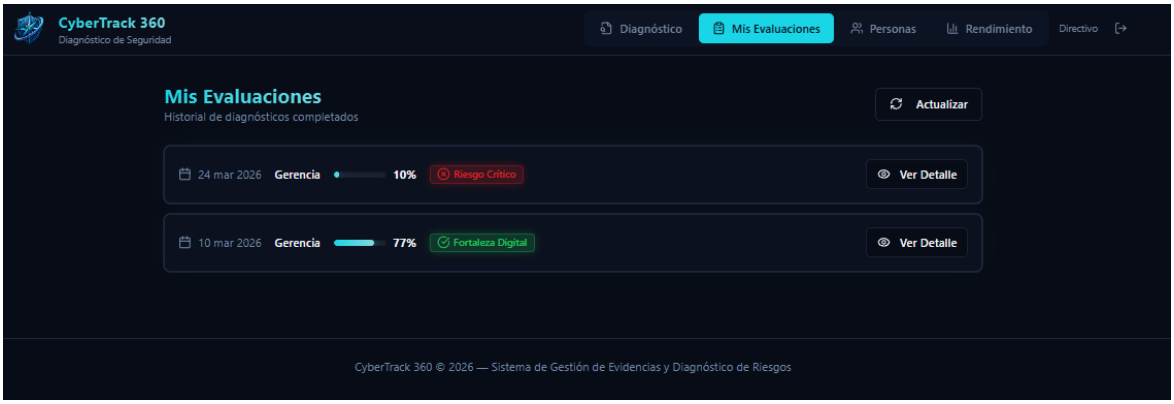
Figura D.19.

Pantalla panel de autodiagnóstico usuario Directivo CyberTrack 360

Nota. Imagen tomada del MVP CyberTrack 360 (2026).

Figura D.20.

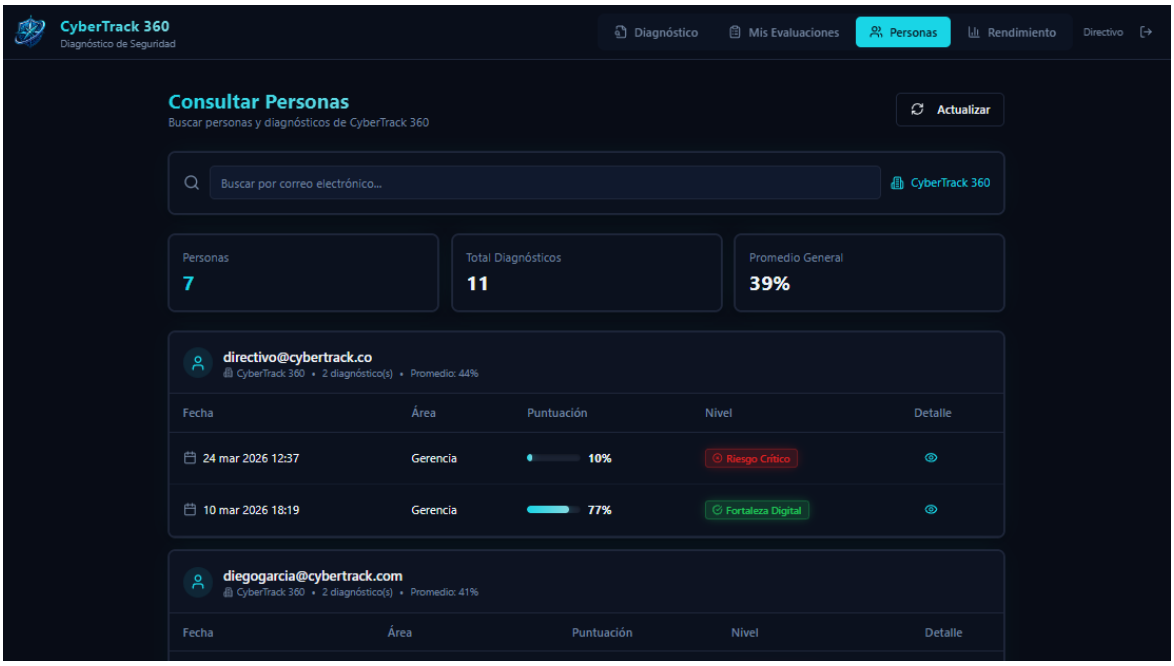
Pantalla panel mis evaluaciones usuario Director CyberTrack 360



Nota. Imagen tomada del MVP CyberTrack 360 (2026).

Figura D.21.

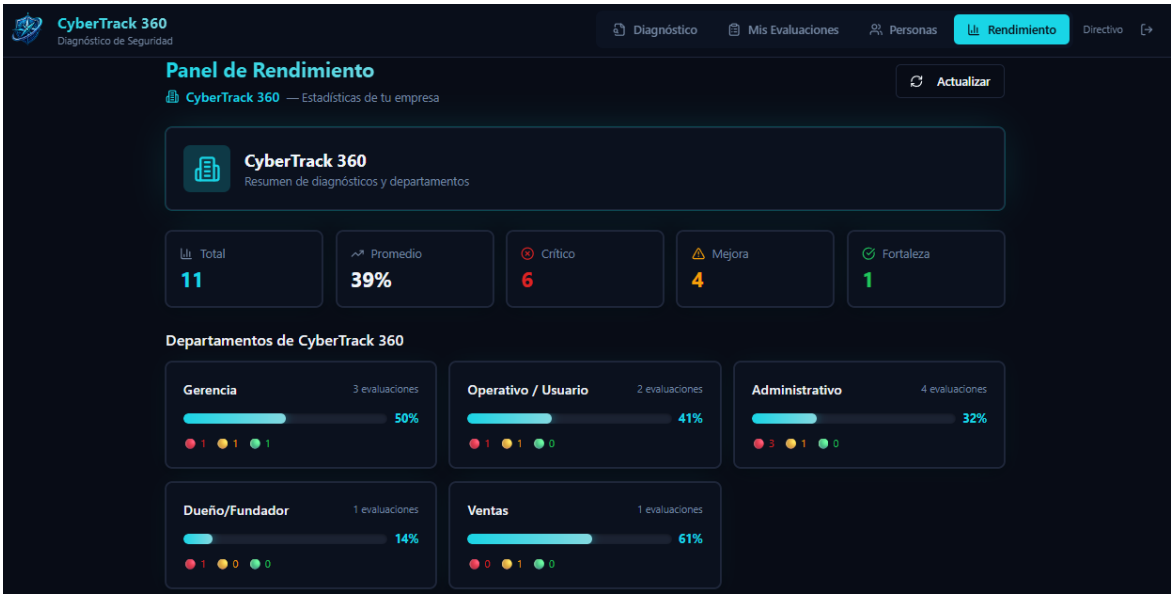
Pantalla panel personas usuario Director CyberTrack 360



Nota. Imagen tomada del MVP CyberTrack 360 (2026).

Figura D.22.

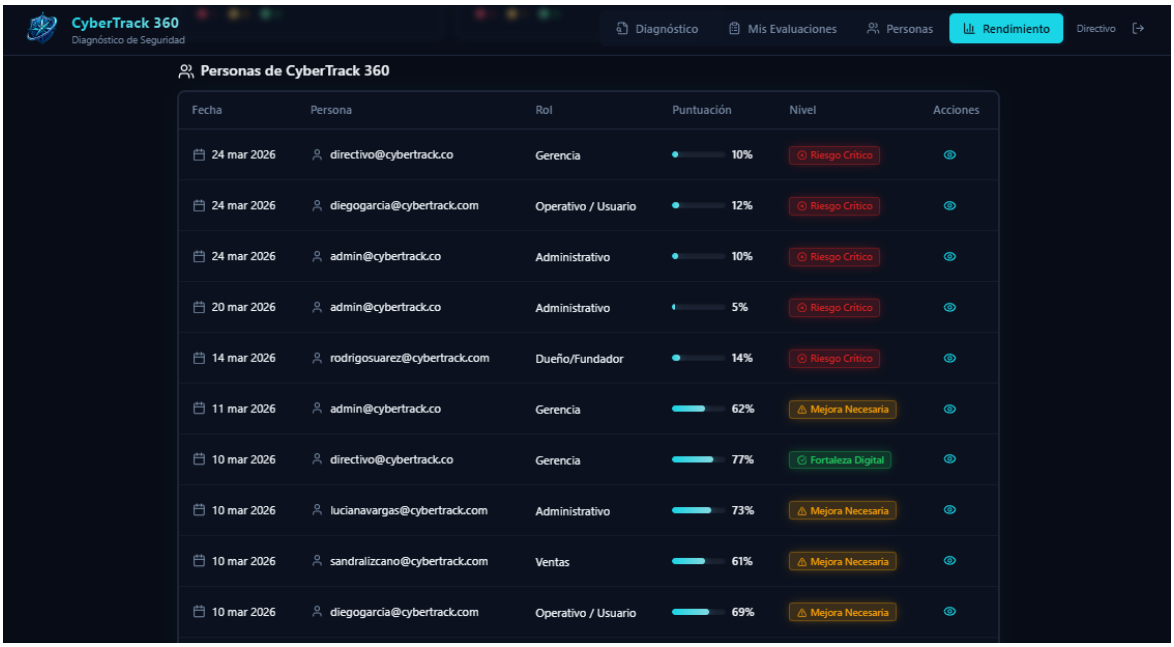
Pantalla panel rendimiento usuario Director CyberTrack 360 1



Nota. Imagen tomada del MVP CyberTrack 360 (2026).

Figura D.23.

Pantalla panel rendimiento usuario Director CyberTrack 360 2



Nota. Imagen tomada del MVP CyberTrack 360 (2026).

Figura D.24.

Pantalla panel autodiagnóstico usuario Operativo CyberTrack 360

Nota. Imagen tomada del MVP CyberTrack 360 (2026).

Figura D.25.

Pantalla panel mis evaluaciones usuario Operativo CyberTrack 360

Nota. Imagen tomada del MVP CyberTrack 360 (2026).

Anexo E – Políticas de seguridad desarrolladas.

Las siguientes tablas presentan las políticas de seguridad de la información desarrolladas para CyberTrack 360, elaboradas a partir de controles de las normas ISO/IEC 27001:2022 e ISO/IEC 27002:2022 y organizadas según los diferentes roles evaluados.

Tabla E.1.

Políticas Generales

Nombre	Objetivo	Control ISO	Lineamientos	Alcance	Evidencia
POL-GEN-001-IDENTIDAD-MFA	Establecer directrices para la implementación y mantenimiento del control A.5.17 - Información de autenticación, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.	A.5.17 - Información de autenticación	Toda comunicación laboral, acceso a plataformas corporativas, recuperación de credenciales e intercambio formal de información deberá realizarse exclusivamente mediante la cuenta institucional asignada por la organización. La autenticación multifactor será obligatoria en el correo institucional y en los servicios corporativos críticos o expuestos a Internet. Ningún usuario podrá desactivar, compartir, delegar o eludir los factores de autenticación sin autorización formal del área responsable.	Aplica a todos los colaboradores, contratistas, terceros, procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.	Captura o registro de MFA activo en correo institucional y servicios críticos; validación del administrador de identidad o TI; evidencia de cuenta corporativa asignada.
POL-GEN-002-CREDENCIALES	Establecer directrices para la implementación y mantenimiento del control A.5.17 - Información de autenticación, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.	A.5.17 - Información de autenticación	Todo usuario deberá utilizar contraseñas únicas, robustas y no reutilizadas entre servicios corporativos ni entre servicios corporativos y personales. Cuando la organización lo disponga, la generación, almacenamiento y uso de credenciales deberá realizarse mediante un gestor de contraseñas aprobado. Se prohíbe compartir credenciales por correo, chat, llamadas, notas físicas o cualquier otro medio no autorizado. Ante sospecha de exposición o compromiso, la contraseña deberá cambiarse de inmediato y reportarse por el canal oficial.	Aplica a todos los colaboradores, contratistas, terceros, procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.	Declaración de uso de gestor aprobado; evidencia de configuración cuando aplique; aceptación de política; validación de inducción o campaña de seguridad.
POL-GEN-003-ACCESO	Establecer directrices para la implementación y mantenimiento del control A.5.15 - Control de acceso, con el fin de proteger la confidencialidad, integridad y disponibilidad de	A.5.15 - Control de acceso	El acceso a sistemas, aplicaciones, carpetas, repositorios y demás recursos corporativos será personal, intransferible y otorgado conforme a la necesidad del rol. Se prohíbe el uso de cuentas compartidas para actividades ordinarias y el préstamo de credenciales entre usuarios. Todo acceso	Aplica a todos los colaboradores, contratistas, terceros, procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control	Registro de usuario individual; tickets o aprobaciones de acceso; evidencia de matriz de accesos o asignación por rol;

	la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.		nuevo, ampliación de privilegios o modificación de permisos deberá solicitarse y aprobarse mediante el proceso formal definido por la organización. Los accesos deberán retirarse o ajustarse cuando cambie la función del usuario o termine su relación con la organización.	establecido, dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.	revisión de privilegios.
POL-GEN-004-PANTALLA	Establecer directrices para la implementación y mantenimiento del control A.7.7 - Escritorio despejado y pantalla limpia, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.	A.7.7 - Escritorio despejado y pantalla limpia	Todo usuario deberá bloquear su sesión al ausentarse del puesto de trabajo, aunque sea por un periodo corto. Los equipos deberán contar con bloqueo automático por inactividad conforme al estándar definido por la organización. La información laboral, física o digital, no deberá quedar visible, accesible o expuesta a terceros no autorizados. Esta obligación aplica en oficina, teletrabajo, reuniones, espacios compartidos y desplazamientos.	Aplica a todos los colaboradores, contratistas, terceros, procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.	Captura de configuración de bloqueo automático; aceptación de política; validación por TI o verificación en auditoría interna/supervisión.
POL-GEN-005-SOFTWARE	Establecer directrices para la implementación y mantenimiento del control A.8.19 - Instalación de software en sistemas operacionales, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.	A.8.19 - Instalación de software en sistemas operacionales	Solo podrá instalarse, ejecutarse o utilizarse software, aplicaciones, extensiones, plugins y herramientas previamente autorizadas por la organización o por el área responsable. Se prohíbe expresamente el uso de software pirata, sin licencia, descontinuado, sin soporte o descargado desde fuentes no confiables. Todo software autorizado deberá mantenerse actualizado y dentro de su ciclo de soporte. El usuario deberá reportar cualquier necesidad de instalación o cualquier hallazgo de software no autorizado.	Aplica a todos los colaboradores, contratistas, terceros, procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.	Inventario de software; lista de software autorizado; evidencia de actualizaciones; validación de TI, MDM o EDR.
POL-GEN-006-DATOS	Establecer directrices para la implementación y mantenimiento del control A.5.14 - Transferencia de información, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la	A.5.14 - Transferencia de información	La documentación de trabajo deberá almacenarse y compartirse, como ubicación primaria, en repositorios corporativos autorizados por la organización. Se prohíbe el almacenamiento de información sensible o de trabajo en el Escritorio local, dispositivos USB no autorizados, correos personales o nubes personales. El acceso y la compartición de archivos deberán respetar la clasificación de la información y el principio de necesidad de	Aplica a todos los colaboradores, contratistas, terceros, procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la	Evidencia de uso de OneDrive, SharePoint, Google Drive o repositorio corporativo; permisos de acceso; muestra de documentos en entorno autorizado.

	información de la organización.		conocer. Toda transferencia deberá realizarse por medios autorizados y trazables.	Información de la organización.	
POL-GEN-007-PHISHING	Establecer directrices para la implementación y mantenimiento del control A.6.8 - Reporte de eventos de seguridad de la información, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.	A.6.8 - Reporte de eventos de seguridad de la información	Todo usuario deberá revisar con criterio de seguridad los correos, enlaces, archivos adjuntos, mensajes y solicitudes que reciba en el contexto laboral. Ante cualquier indicio de phishing, ingeniería social, suplantación o contenido sospechoso, el usuario deberá abstenerse de abrir enlaces o adjuntos, no responder al mensaje y reportarlo inmediatamente por el canal oficial definido por la organización. El reporte oportuno se considera una obligación de seguridad. La organización deberá mantener visible el mecanismo y el punto de contacto para este reporte.	Aplica a todos los colaboradores, contratistas, terceros, procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.	Resultado de capacitación o simulación; evidencia de reporte real o de prueba; constancia de conocimiento del canal oficial de reporte.
POL-GEN-008-INCIDENTE	Establecer directrices para la implementación y mantenimiento del control A.5.26 - Respuesta a incidentes de seguridad de la información, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.	A.5.26 - Respuesta a incidentes de seguridad de la información	Ante sospecha o confirmación de compromiso de contraseña, dispositivo, archivo, cuenta o sesión, el usuario deberá ejecutar las acciones inmediatas definidas por la organización: cambio de contraseña, cierre de sesiones, desconexión o aislamiento cuando aplique, y notificación inmediata al canal oficial. El usuario no deberá ocultar, borrar ni alterar evidencias básicas que puedan apoyar la investigación. La respuesta temprana tiene como objetivo contener el impacto y facilitar el tratamiento del incidente. La organización deberá comunicar claramente qué, cómo, cuándo y a quién reportar.	Aplica a todos los colaboradores, contratistas, terceros, procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.	Resultado de cuestionario o simulacro; constancia de inducción; procedimiento entregado; registro de participación en ejercicio o campaña.
POL-GEN-009-CAPACITACION	Establecer directrices para la implementación y mantenimiento del control A.6.3 - Concienciación, educación y formación en seguridad de la información, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.	A.6.3 - Concienciación, educación y formación en seguridad de la información	Toda persona con acceso a activos o información corporativa deberá completar la capacitación obligatoria de seguridad al ingreso y según la periodicidad definida por la organización. El plan deberá incluir, como mínimo, phishing, credenciales, malware, ransomware, manejo seguro de la información y reporte de incidentes. La organización podrá complementar esta formación con cápsulas, simulaciones, boletines o refuerzos periódicos. El cumplimiento de la capacitación será verificable y su omisión deberá gestionarse como incumplimiento del programa de seguridad.	Aplica a todos los colaboradores, contratistas, terceros, procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.	Registro de asistencia o LMS; certificado; acta o captura de finalización; reporte de campañas o refuerzos periódicos.

Tabla E.2.

Políticas orientadas a gobernanza, riesgo, recursos, terceros y continuidad (Gerencia)

Nombre	Objetivo	Control ISO	Lineamientos	Alcance	Evidencia
POL-GER-001-GOBERNANZA	Establecer directrices para la implementación y mantenimiento del control A.5.1 - Políticas de seguridad de la información, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.	A.5.1 - Políticas de seguridad de la información	La alta dirección deberá aprobar, comunicar y revisar periódicamente la política de seguridad de la información y las políticas temáticas relacionadas. Además, deberá asegurar que las responsabilidades de seguridad estén definidas, asignadas y entendidas, y que la estrategia de seguridad se alinee con la misión, los objetivos y el contexto de negocio.	Aplica a todos los colaboradores, contratistas, terceros, procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.	Política aprobada; acta o evidencia de revisión por dirección; organigrama o matriz de roles y responsabilidades.
POL-GER-002-ACTIVOS	Establecer directrices para la implementación y mantenimiento del control A.5.9 - Inventario de la información y otros activos asociados, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.	A.5.9 - Inventario de la información y otros activos asociados	La organización deberá mantener un inventario actualizado de activos, sistemas y datos críticos, con propietarios claramente asignados. La gerencia revisará periódicamente esta información para priorizar inversiones, tratamiento de riesgos, continuidad y controles de protección sobre los activos que soportan el negocio.	Aplica a todos los colaboradores, contratistas, terceros, procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.	Inventario de activos y datos; clasificación de criticidad; asignación de propietarios; reporte ejecutivo o dashboard.
POL-GER-003-IDENTIDAD-ACCESO	Establecer directrices para la implementación y mantenimiento del control A.5.15 - Control de acceso, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.	A.5.15 - Control de acceso	La organización deberá establecer y supervisar controles de identidad y acceso basados en funciones, necesidad de conocer y segregación de responsabilidades. La MFA será obligatoria en servicios críticos y accesos expuestos. La gerencia exigirá evidencia periódica de control sobre altas, cambios, bajas, cuentas privilegiadas y accesos de terceros.	Aplica a todos los colaboradores, contratistas, terceros, procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.	Matriz de accesos; evidencia de MFA; procedimiento de altas, cambios y bajas; revisión de cuentas privilegiadas y de terceros.
POL-GER-004-	Establecer directrices para la implementación y	A.8.8 - Gestión de	La alta dirección deberá asegurar recursos, responsables y seguimiento	Aplica a todos los colaboradores, contratistas,	Plan o presupuesto; responsables

HIGIENE-TEC	mantenimiento del control A.8.8 - Gestión de vulnerabilidades técnicas, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.	vulnerabilidades técnicas	para sostener la higiene tecnológica esencial de la organización. Esto incluye software autorizado, configuraciones seguras, parchado oportuno y mecanismos de protección antimalware o EDR sobre los activos críticos del negocio.	terceros, procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.	asignados; reportes de parchado, hardening, software autorizado y EDR/antimalware.
POL-GER-005-RIESGOS	Establecer directrices para la implementación y mantenimiento del control A.5.7 - Inteligencia sobre amenazas, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.	A.5.7 - Inteligencia sobre amenazas	La organización deberá gestionar los riesgos de seguridad mediante un registro actualizado, planes de tratamiento y seguimiento directivo. Toda excepción o aceptación de riesgo requerirá justificación documentada, responsable asignado, fecha objetivo y revisión periódica. No se aceptarán riesgos de forma tácita o sin trazabilidad.	Aplica a todos los colaboradores, contratistas, terceros, procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.	Registro de riesgos; registro de excepciones; aceptación formal de riesgos; planes de tratamiento con responsables y fechas.
POL-GER-006-PROVEEDORES	Establecer directrices para la implementación y mantenimiento del control A.5.19 - Seguridad de la información en las relaciones con proveedores, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.	A.5.19 - Seguridad de la información en las relaciones con proveedores	Todo proveedor, tercero o servicio crítico deberá ser evaluado antes de su contratación en aspectos de seguridad, confidencialidad, protección de datos y continuidad. La organización incorporará requisitos mínimos en contratos y realizará seguimiento durante la relación comercial para verificar el cumplimiento esperado.	Aplica a todos los colaboradores, contratistas, terceros, procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.	Evaluación de proveedores; cláusulas contractuales; NDA; checklist de seguridad; evidencias de revisión periódica.
POL-GER-007-INCIDENTES	Establecer directrices para la implementación y mantenimiento del control A.5.24 - Planificación y preparación para la gestión de incidentes de seguridad de la información, con el fin de proteger la	A.5.24 - Planificación y preparación para la gestión de incidentes de seguridad de la información	La organización deberá mantener canales formales para el reporte de eventos e incidentes de seguridad, con criterios de escalamiento, responsables y tiempos de respuesta definidos. La gerencia revisará periódicamente los incidentes relevantes, su causa, impacto, tratamiento y acciones correctivas derivadas.	Aplica a todos los colaboradores, contratistas, terceros, procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido,	Procedimiento de incidentes; canal de reporte; bitácora o tickets; métricas de tiempos de atención y escalamiento.

	confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.			dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.	
POL-GER-008-RECUPERACION	Establecer directrices para la implementación y mantenimiento del control A.5.30 - Preparación de las TIC para la continuidad del negocio, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.	A.5.30 - Preparación de las TIC para la continuidad del negocio	La organización deberá asegurar respaldos adecuados de la información y servicios críticos, así como capacidades de recuperación verificadas mediante pruebas periódicas. La gerencia deberá conocer y revisar los objetivos mínimos de recuperación y la evidencia de restauración para los activos de mayor impacto al negocio.	Aplica a todos los colaboradores, contratistas, terceros, procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.	Política o plan de respaldo; calendario de copias; evidencia de pruebas de restauración; RTO/RPO cuando aplique.
POL-GER-009-CULTURA	Establecer directrices para la implementación y mantenimiento del control A.6.3 - Concienciación, educación y formación en seguridad de la información, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.	A.6.3 - Concienciación, educación y formación en seguridad de la información	Toda persona con acceso a activos o información de la organización deberá participar en el programa de concienciación y capacitación en seguridad con la periodicidad definida. La gerencia supervisará cobertura, cumplimiento y refuerzos específicos para reducir exposición a phishing, malware, ransomware y manejo inadecuado de información.	Aplica a todos los colaboradores, contratistas, terceros, procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.	Plan anual de capacitación; registros de asistencia; campañas de concienciación; seguimiento de cumplimiento.

Tabla E.3.

Políticas orientadas a operación técnica, hardening, monitoreo, backups e incidentes (TI)

Nombre	Objetivo	Control ISO	Lineamientos	Alcance	Evidencia
POL-TI-001-INVENTARIO	Establecer directrices para la implementación y mantenimiento del control A.5.9 - Inventario de la información y otros activos asociados, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.	A.5.9 - Inventario de la información y otros activos asociados	El área de TI deberá mantener un inventario actualizado de activos y software autorizados, incluyendo propietarios, criticidad y estado. Asimismo, deberá ejecutar un proceso operativo para identificar, aislar, retirar o regularizar activos y software no autorizados detectados en el entorno.	Aplica a todos los colaboradores, contratistas, terceros, procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.	Inventario actualizado; hallazgos de activos no autorizados; evidencias de remediación; listado de software permitido/no permitido.
POL-TI-002-IAM	Establecer directrices para la implementación y mantenimiento del control A.5.18 - Derechos de acceso, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.	A.5.18 - Derechos de acceso	TI deberá administrar identidades y accesos mediante cuentas individuales, MFA en servicios críticos, privilegios mínimos y segregación adecuada. Las cuentas privilegiadas, de servicio y de terceros deberán revisarse periódicamente, justificarse documentalmente y retirarse o ajustarse cuando ya no sean necesarias.	Aplica a todos los colaboradores, contratistas, terceros, procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.	Matriz de accesos; evidencia de MFA; revisión de cuentas privilegiadas, de servicio y terceros; tickets de altas/bajas/cambios.
POL-TI-003-HARDENING	Establecer directrices para la implementación y mantenimiento del control A.8.9 - Gestión de la configuración, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.	A.8.9 - Gestión de la configuración	TI deberá establecer y mantener configuraciones seguras de referencia para sistemas, endpoints y dispositivos de red. Toda desviación o cambio de configuración deberá gestionarse mediante proceso formal. Deberán eliminarse o deshabilitarse cuentas predeterminadas, servicios, puertos y componentes innecesarios que aumenten la superficie de ataque.	Aplica a todos los colaboradores, contratistas, terceros, procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.	Baselines de hardening; evidencia de cambios aprobados; listas de puertos/servicios; deshabilitación de cuentas predeterminadas.
POL-TI-004-VULNE	Establecer directrices para la implementación y mantenimiento del	A.8.8 - Gestión de vulnerabilidades técnicas	TI deberá ejecutar gestión continua de vulnerabilidades y parchado con periodicidad definida y trazabilidad de	Aplica a todos los colaboradores, contratistas, terceros,	Escaneos; plan de parchado; SLA internos;

RABILIDADES	control A.8.8 - Gestión de vulnerabilidades técnicas, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.		resultados. Los activos críticos y las vulnerabilidades de mayor severidad deberán priorizarse en su tratamiento. Toda excepción deberá justificarse, aprobarse y mantenerse bajo seguimiento hasta su cierre o sustitución por controles compensatorios.	procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.	evidencia de remediación; reporte de excepciones justificadas.
POL-TI-005-ENDPOINT	Establecer directrices para la implementación y mantenimiento del control A.8.7 - Protección contra malware, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.	A.8.7 - Protección contra malware	TI deberá mantener mecanismos de protección antimalware o EDR activos y administrados sobre los activos dentro del alcance definido. Las alertas deberán ser monitoreadas, clasificadas, contenidas y cerradas con trazabilidad. No se permitirá la desactivación no autorizada de estas protecciones.	Aplica a todos los colaboradores, contratistas, terceros, procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.	Consola de EDR/antimalware; cobertura por activo; alertas atendidas; acciones de contención y cierre.
POL-TI-006-LOGS	Establecer directrices para la implementación y mantenimiento del control A.8.15 - Registro, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.	A.8.15 - Registro	TI deberá recopilar, centralizar y revisar registros relevantes de autenticación, cambios administrativos, malware, acceso y eventos críticos de seguridad. La retención de registros deberá ser suficiente para investigación y trazabilidad. Todo hallazgo sospechoso deberá escalarse conforme al procedimiento de incidentes.	Aplica a todos los colaboradores, contratistas, terceros, procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.	Consola de logs o SIEM; política de retención; muestras de revisión; tickets o casos escalados.
POL-TI-007-BACKUP	Establecer directrices para la implementación y mantenimiento del control A.8.13 - Copia de seguridad de la información, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de	A.8.13 - Copia de seguridad de la información	TI deberá gestionar respaldos de información y sistemas críticos con periodicidad definida, evidencia de ejecución, protección adecuada del repositorio y pruebas periódicas de restauración. Los resultados de las pruebas deberán documentarse y utilizarse para corregir fallas de recuperación.	Aplica a todos los colaboradores, contratistas, terceros, procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la	Calendario de respaldos; evidencias de ejecución; cifrado o protección de repositorios; pruebas de restauración.

	seguridad de la información de la organización.			Información de la organización.	
POL-TI-008-CORREO-WEB	Establecer directrices para la implementación y mantenimiento del control A.8.23 - Filtrado web, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.	A.8.23 - Filtrado web	TI deberá mantener controles técnicos de correo y navegación para reducir exposición a phishing, malware, dominios maliciosos y descargas riesgosas. Asimismo, deberá habilitar mecanismos sencillos para que los usuarios reporten eventos sospechosos y para que estos se atiendan oportunamente.	Aplica a todos los colaboradores, contratistas, terceros, procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.	Configuración de filtrado; bloqueo de dominios o adjuntos; canal de reporte; evidencias de campañas o simulaciones.
POL-TI-009-IR	Establecer directrices para la implementación y mantenimiento del control A.5.26 - Respuesta a incidentes de seguridad de la información, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.	A.5.26 - Respuesta a incidentes de seguridad de la información	TI deberá operar un procedimiento técnico de respuesta a incidentes que cubra detección, análisis, contención, erradicación, recuperación y preservación de evidencias básicas. Todo incidente relevante deberá documentarse, escalarse cuando corresponda y dejar acciones correctivas y preventivas trazables.	Aplica a todos los colaboradores, contratistas, terceros, procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.	Procedimiento técnico; runbooks; tickets o casos; evidencias preservadas; pruebas o simulacros.

Tabla E.4.

Políticas orientadas a uso seguro de activos, operación diaria, movilidad y escalamiento temprano (Operativo/usuario)

Nombre	Objetivo	Control ISO	Lineamientos	Alcance	Evidencia
POL-OPR-001-ACTIVOS-ASIGNADOS	Establecer directrices para la implementación y mantenimiento del control A.5.10 - Uso aceptable de la información y de otros activos asociados, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.	A.5.10 - Uso aceptable de la información y de otros activos asociados	Toda actividad operativa deberá realizarse únicamente desde el equipo, usuario o terminal asignado por la organización. Se prohíbe operar con cuentas ajenas, equipos no autorizados o dejar sesiones abiertas al finalizar la labor. Cuando el trabajo implique relevo, uso compartido controlado o cambio de turno, el usuario deberá cerrar sesión o entregar formalmente el control conforme al procedimiento definido.	Aplica a todos los colaboradores, contratistas, terceros, procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.	Validación del activo asignado; registro de usuario individual; evidencia de cierre de sesión o relevo conforme al procedimiento.
POL-OPR-002-MEDIOS	Establecer directrices para la implementación y mantenimiento del control A.8.1 - Dispositivos terminales de usuario, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.	A.8.1 - Dispositivos terminales de usuario	Se prohíbe conectar medios removibles, dispositivos móviles, accesorios o periféricos no autorizados a equipos de trabajo. Todo dispositivo desconocido, encontrado o requerido para la operación deberá reportarse y validarse antes de su uso. Cuando exista una necesidad operativa justificada, el uso deberá realizarse bajo autorización previa y con las medidas de verificación definidas por la organización.	Aplica a todos los colaboradores, contratistas, terceros, procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.	Inspección o declaración de cumplimiento; política firmada; registro de reporte o autorización previa cuando aplique.
POL-OPR-003-INFO-FISICA	Establecer directrices para la implementación y mantenimiento del control A.7.7 - Escritorio despejado y pantalla limpia, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.	A.7.7 - Escritorio despejado y pantalla limpia	La información operativa impresa o visible en pantallas deberá mantenerse bajo control del usuario responsable y fuera del acceso de terceros no autorizados. Se prohíbe dejar formatos, órdenes, etiquetas, evidencias o pantallas expuestas cuando no estén en uso. La organización definirá medidas de resguardo, archivo temporal, retiro y destrucción segura según el nivel de sensibilidad y el proceso involucrado.	Aplica a todos los colaboradores, contratistas, terceros, procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.	Observación en sitio; cumplimiento del procedimiento de escritorio limpio; evidencia de resguardo de formatos o pantallas.

POL-OPR-004-CANALES	Establecer directrices para la implementación y mantenimiento del control A.5.10 - Uso aceptable de la información y de otros activos asociados, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.	A.5.10 - Uso aceptable de la información y de otros activos asociados	El registro y transmisión de evidencias, fotografías, mensajes o datos de la operación deberá realizarse únicamente mediante aplicaciones, canales y equipos aprobados por la organización. Se prohíbe el uso de herramientas personales, informales o no autorizadas para capturar, almacenar o enviar información operativa. Toda excepción deberá estar formalmente autorizada y controlada.	Aplica a todos los colaboradores, contratistas, terceros, procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.	Evidencia de uso de aplicación o canal aprobado; validación del supervisor; revisión de registros o flujo de trabajo.
POL-OPR-005-VALIDACION	Establecer directrices para la implementación y mantenimiento del control A.6.3 - Concienciación, educación y formación en seguridad de la información, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.	A.6.3 - Concienciación, educación y formación en seguridad de la información	Antes de ejecutar una instrucción, solicitud o cambio que afecte información, equipos, pedidos o procesos, el usuario deberá validar que provenga de una fuente autorizada y por el canal definido. Las solicitudes inusuales, urgentes, ambiguas o fuera del procedimiento deberán escalarse antes de su ejecución. La organización deberá comunicar criterios claros de validación y canales oficiales de autorización.	Aplica a todos los colaboradores, contratistas, terceros, procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.	Constancia de capacitación; evidencia de procedimiento; validación del supervisor o resultado de simulacro.
POL-OPR-006-REPORTE	Establecer directrices para la implementación y mantenimiento del control A.6.8 - Reporte de eventos de seguridad de la información, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.	A.6.8 - Reporte de eventos de seguridad de la información	Toda pérdida, robo, daño, anomalía o comportamiento sospechoso relacionado con equipos, credenciales, cuentas o terminales de trabajo deberá reportarse de inmediato por el canal oficial definido por la organización. El usuario no deberá ocultar, retrasar ni minimizar el evento. El reporte temprano permite contener impactos operativos, preservar evidencias y activar el tratamiento oportuno del incidente.	Aplica a todos los colaboradores, contratistas, terceros, procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.	Ticket, reporte o bitácora; evidencia de conocimiento del canal oficial; simulacro o constancia de inducción.
POL-OPR-007-EQUIPO	Establecer directrices para la implementación y mantenimiento del control A.8.1 - Dispositivos	A.8.1 - Dispositivos terminales de usuario	Los equipos utilizados en la operación deberán mantener habilitados los controles de seguridad definidos por la organización, incluyendo antivirus, bloqueo, rastreo,	Aplica a todos los colaboradores, contratistas, terceros, procesos, activos de información,	Estado del equipo; validación de antivirus o control activo; revisión de

	terminales de usuario, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.		perfiles administrados u otros mecanismos de protección. Se prohíbe desactivar, evadir o alterar estos controles sin autorización formal. Cualquier fallo o incompatibilidad deberá reportarse al área responsable.	sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.	configuración o herramienta de gestión.
POL-OPR-008-CONECTIVIDAD	Establecer directrices para la implementación y mantenimiento del control A.6.7 - Trabajo remoto, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.	A.6.7 - Trabajo remoto	Cuando el trabajo se realice fuera de las instalaciones, el usuario deberá utilizar únicamente mecanismos de conectividad autorizados y seguros para acceder a recursos corporativos. Se prohíbe el uso de redes Wi-Fi públicas, estaciones de carga desconocidas o conexiones informales para actividades de trabajo, salvo que exista un mecanismo de protección definido y aprobado por la organización.	Aplica a todos los colaboradores, contratistas, terceros, procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.	Declaración de cumplimiento; capacitación; evidencia de uso de VPN o mecanismo aprobado cuando aplique.
POL-OPR-009-INGENIERIA-SOCIAL	Establecer directrices para la implementación y mantenimiento del control A.6.8 - Reporte de eventos de seguridad de la información, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.	A.6.8 - Reporte de eventos de seguridad de la información	Ante correos, llamadas, mensajes o visitas inusuales que soliciten información, accesos, códigos, credenciales o acciones urgentes, el usuario deberá suspender la interacción y reportar por el canal oficial antes de continuar. Se prohíbe entregar información o ejecutar acciones fuera del procedimiento sin validación previa. La organización mantendrá campañas de concienciación y canales visibles de escalamiento.	Aplica a todos los colaboradores, contratistas, terceros, procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.	Registro de capacitación o simulación; evidencia de reporte; conocimiento del canal oficial.

Tabla E.5.

Políticas orientadas a datos sensibles, documentos, validación antifraude y trazabilidad administrativa (Administrativo)

Nombre	Objetivo	Control ISO	Lineamientos	Alcance	Evidencia
POL-ADM-001-DATOS-SENSIBLES	Establecer directrices para la implementación y mantenimiento del control A.5.34 - Privacidad y protección de la PII, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.	A.5.34 - Privacidad y protección de la PII	El personal administrativo deberá tratar datos personales, financieros, contractuales o de empleados únicamente en sistemas y repositorios autorizados por la organización. El acceso y uso de dicha información se limitará al mínimo necesario para cumplir la función asignada. Se prohíbe copiar, descargar, reenviar o conservar información sensible fuera de los entornos y finalidades autorizadas.	Aplica a todos los colaboradores, contratistas, terceros, procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.	Evidencia de uso de sistema autorizado; matriz o perfil de acceso; validación del supervisor o TI.
POL-ADM-002-VALIDACION-FINANCIERA	Establecer directrices para la implementación y mantenimiento del control A.5.14 - Transferencia de información, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.	A.5.14 - Transferencia de información	Todo cambio de cuentas bancarias, pagos, proveedores, reintegros o instrucciones financieras inusuales deberá validarse mediante un segundo canal o control formal antes de su ejecución. Se prohíbe procesar modificaciones sensibles con base en un único correo, mensaje o llamada no verificada. La organización deberá definir responsables, umbrales y mecanismos de validación reforzada para prevenir fraude y suplantación.	Aplica a todos los colaboradores, contratistas, terceros, procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.	Registro de validación por segundo canal; procedimiento aprobado; evidencia de revisión o autorización.
POL-ADM-003-TRANSFERENCIA	Establecer directrices para la implementación y mantenimiento del control A.5.14 - Transferencia de información, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.	A.5.14 - Transferencia de información	La documentación administrativa deberá compartirse únicamente con destinatarios autorizados y mediante medios aprobados por la organización. Antes del envío, el usuario deberá verificar identidad, correo, permisos y necesidad de acceso del receptor. Se prohíbe compartir información sensible por canales no autorizados o sin validación previa de destinatarios.	Aplica a todos los colaboradores, contratistas, terceros, procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.	Evidencia de revisión de destinatarios; permisos del repositorio; muestras de envío o flujo aprobado.
POL-ADM-004-	Establecer directrices para la implementación y mantenimiento del	A.5.15 - Control de acceso	Los contratos, expedientes, soportes de pago, facturación y demás documentos administrativos deberán	Aplica a todos los colaboradores, contratistas, terceros,	Ubicación de archivos en repositorio designado;

REPOSITORIO	control A.5.15 - Control de acceso, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.		mantenerse en los repositorios designados por la organización, con permisos y trazabilidad definidos. Se prohíbe almacenar documentación sensible en ubicaciones informales, cuentas personales o carpetas compartidas sin control. El acceso deberá ajustarse al principio de necesidad de conocer.	procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.	permisos configurados; evidencia de trazabilidad o control de versiones.
POL-ADM-005-CLASIFICACION	Establecer directrices para la implementación y mantenimiento del control A.5.13 - Etiquetado de la información, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.	A.5.13 - Etiquetado de la información	La documentación administrativa deberá clasificarse o etiquetarse cuando el procedimiento lo exija, a fin de aplicar el nivel de protección correspondiente. Se prohíbe utilizar correo personal, mensajería informal o cuentas no autorizadas para gestionar asuntos administrativos, especialmente cuando involucren datos sensibles o información contractual y financiera.	Aplica a todos los colaboradores, contratistas, terceros, procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.	Muestras de documentos etiquetados; política difundida; evidencia de uso de correo o canales corporativos.
POL-ADM-006-RETENCION	Establecer directrices para la implementación y mantenimiento del control A.5.33 - Protección de los registros, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.	A.5.33 - Protección de los registros	La organización deberá definir y comunicar tiempos de retención y métodos de archivo, retiro o eliminación para la documentación administrativa física y digital. El personal administrativo deberá cumplir dichos lineamientos y asegurar que la eliminación se realice de forma segura y verificable cuando corresponda.	Aplica a todos los colaboradores, contratistas, terceros, procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.	Cronograma o tabla de retención; evidencia de archivo o eliminación; procedimiento vigente.
POL-ADM-007-PUESTO-SEGURO	Establecer directrices para la implementación y mantenimiento del control A.7.7 - Escritorio despejado y pantalla limpia, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la	A.7.7 - Escritorio despejado y pantalla limpia	Los documentos impresos, firmas, sellos, soportes y pantallas utilizados en actividades administrativas deberán permanecer bajo control del usuario responsable y ser resguardados cuando no estén en uso. Se prohíbe dejarlos expuestos en escritorios, bandejas, impresoras o áreas comunes sin supervisión.	Aplica a todos los colaboradores, contratistas, terceros, procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la	Observación en sitio; verificación de escritorio limpio; aceptación de política.

	gestión de seguridad de la información de la organización.			Información de la organización.	
POL-ADM-008-ANTIFRAUDE	Establecer directrices para la implementación y mantenimiento del control A.6.8 - Reporte de eventos de seguridad de la información, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.	A.6.8 - Reporte de eventos de seguridad de la información	Todo correo, llamada o mensaje sospechoso relacionado con pagos, datos personales, contratos, nómina o instrucciones urgentes fuera del procedimiento deberá reportarse de inmediato por el canal oficial. Se prohíbe ejecutar acciones sensibles sin validación previa cuando existan señales de fraude, suplantación o presión indebida.	Aplica a todos los colaboradores, contratistas, terceros, procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.	Capacitación o simulación; evidencia de reporte; conocimiento del canal de escalamiento.
POL-ADM-009-TERCEROS	Establecer directrices para la implementación y mantenimiento del control A.5.19 - Seguridad de la información en las relaciones con proveedores, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.	A.5.19 - Seguridad de la información en las relaciones con proveedores	Antes de compartir documentación con terceros, proveedores, auditores o entidades externas, el usuario deberá verificar permisos, finalidad, confidencialidad y medio autorizado de transferencia. La organización deberá asegurar que los terceros reciban únicamente la información necesaria y bajo condiciones claras de protección y uso.	Aplica a todos los colaboradores, contratistas, terceros, procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.	Acuerdo o cláusula de confidencialidad; validación de permisos; evidencia de revisión previa al envío.

Tabla E.6.

Políticas orientadas a gobernanza, continuidad, propiedad de activos críticos y toma de decisiones para microempresas (Dueño/Fundador)

Nombre	Objetivo	Control ISO	Lineamientos	Alcance	Evidencia
POL-DUF-001-CONTROL-CUENTAS	Establecer directrices para la implementación y mantenimiento del control A.5.9 - Inventario de información y otros activos asociados, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.	A.5.9 - Inventario de información y otros activos asociados	Formaliza la propiedad y control de las cuentas críticas del negocio para evitar dependencia exclusiva del fundador o de accesos personales no trazables.	Aplica a todos los colaboradores, contratistas, terceros, procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.	Listado de cuentas críticas, titularidad de dominio/hosting, correos de recuperación, accesos administrativos y responsables asignados.
POL-DUF-002-RIESGO-NEGOCIO	Establecer directrices para la implementación y mantenimiento del control A.5.1 - Políticas de seguridad de la información, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.	A.5.1 - Políticas de seguridad de la información	Establece criterios claros sobre qué riesgos son aceptables, cuáles no, y qué controles mínimos deben sostenerse para proteger operación, clientes y reputación.	Aplica a todos los colaboradores, contratistas, terceros, procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.	Documento de prioridades, acta, plan estratégico, matriz de riesgos o decisión formal del dueño/fundador.
POL-DUF-003-REDUCCION-DEPENDENCIA	Establecer directrices para la implementación y mantenimiento del control A.5.30 - Preparación de las TIC para la continuidad del negocio, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.	A.5.30 - Preparación de las TIC para la continuidad del negocio	Disminuye el riesgo de interrupción operativa definiendo accesos alternos, responsables suplentes y mecanismos de continuidad cuando el fundador no esté disponible.	Aplica a todos los colaboradores, contratistas, terceros, procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.	Plan de contingencia, accesos alternos, delegación documentada, respaldos administrativos o procedimiento de sustitución.

POL-DUF-004-SEPARACION RECURSOS	Establecer directrices para la implementación y mantenimiento del control A.5.10 - Uso aceptable de la información y otros activos asociados, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.	A.5.10 - Uso aceptable de la información y otros activos asociados	Evita mezclar recursos personales y empresariales para reducir pérdida de control, fuga de información y dependencia informal.	Aplica a todos los colaboradores, contratistas, terceros, procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.	Uso de correo corporativo, almacenamiento empresarial, dispositivos autorizados y evidencia de separación de cuentas.
POL-DUF-005-OBLIGACIONES - LEGALES	Establecer directrices para la implementación y mantenimiento del control A.5.31 - Requisitos legales, estatutarios, reglamentarios y contractuales, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.	A.5.31 - Requisitos legales, estatutarios, reglamentarios y contractuales	Reconoce y documenta los requisitos legales, regulatorios y contractuales que deben protegerse desde la toma de decisiones del negocio.	Aplica a todos los colaboradores, contratistas, terceros, procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.	Listado de obligaciones, política de datos, contratos, revisión legal o matriz de cumplimiento.
POL-DUF-006-PROVEEDORES-CRITICOS	Establecer directrices para la implementación y mantenimiento del control A.5.19 - Seguridad de la información en las relaciones con proveedores, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.	A.5.19 - Seguridad de la información en las relaciones con proveedores	Ubica los proveedores y plataformas cuya falla afectaría seriamente al negocio y define controles o alternativas de continuidad.	Aplica a todos los colaboradores, contratistas, terceros, procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.	Listado de proveedores críticos, mapa de dependencia, contratos, evaluación de riesgo o plan alterno.
POL-DUF-007-EVALUACION-	Establecer directrices para la implementación y mantenimiento del control A.5.8 -	A.5.8 - Seguridad de la información	Incorpora una validación mínima de riesgos de seguridad, privacidad y continuidad antes de adoptar	Aplica a todos los colaboradores, contratistas, terceros, procesos, activos	Checklist de evaluación, acta de aprobación, análisis

SEGURIDAD	Seguridad de la información en la gestión de proyectos, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.	en la gestión de proyectos	nuevas herramientas, servicios o integraciones.	de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.	previo, correo de validación o documento de proyecto.
POL-DUF-008-PRIORIZACION-INFORMACION	Establecer directrices para la implementación y mantenimiento del control A.5.30 - Preparación de las TIC para la continuidad del negocio, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.	A.5.30 - Preparación de las TIC para la continuidad del negocio	Define qué información y procesos deben recuperarse primero para sostener ingresos, atención al cliente y operación mínima viable.	Aplica a todos los colaboradores, contratistas, terceros, procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.	Listado de información crítica, prioridades de recuperación, plan de continuidad o respaldo de procesos clave.
POL-DUF-009-PROCEDIMIENTO-CIBERSEGURIDAD	Establecer directrices para la implementación y mantenimiento del control A.5.24 - Planificación y preparación para la gestión de incidentes de seguridad de la información, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.	A.5.24 - Planificación y preparación para la gestión de incidentes de seguridad de la información	Establece quién decide, quién comunica y cómo se escala una crisis de ciberseguridad para evitar improvisación en momentos críticos.	Aplica a todos los colaboradores, contratistas, terceros, procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.	Plan de crisis, procedimiento de escalamiento, responsables designados, comité o instructivo de actuación.

Tabla E.7.

Políticas orientadas a protección de datos comerciales, movilidad, clientes y prevención de suplantación (Ventas)

Nombre	Objetivo	Control ISO	Lineamientos	Alcance	Evidencia
POL-VTA-001-CRM	Establecer directrices para la implementación y mantenimiento del control A.5.34 - Privacidad y protección de la PII, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.	A.5.34 - Privacidad y protección de la PII	Toda información de clientes y prospectos deberá registrarse y mantenerse únicamente en el CRM o repositorio comercial autorizado por la organización. Se prohíbe administrar datos comerciales en listas personales, hojas sueltas o herramientas no aprobadas. La organización deberá definir responsables, permisos y mecanismos de control sobre la información comercial.	Aplica a todos los colaboradores, contratistas, terceros, procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.	Registro en CRM; evidencia de uso de repositorio autorizado; revisión de ausencia de bases personales.
POL-VTA-002-CANALES	Establecer directrices para la implementación y mantenimiento del control A.5.14 - Transferencia de información, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.	A.5.14 - Transferencia de información	La documentación comercial, incluyendo cotizaciones, contratos, propuestas y listas de precios, deberá enviarse únicamente por canales corporativos y herramientas aprobadas. Antes del envío, el usuario deberá verificar identidad, correo y necesidad del destinatario. Se prohíbe compartir documentación comercial sensible por canales informales o cuentas personales.	Aplica a todos los colaboradores, contratistas, terceros, procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.	Muestras de envío; permisos de repositorio; validación de destinatarios; uso de correo o plataforma corporativa.
POL-VTA-003-VALIDACION	Establecer directrices para la implementación y mantenimiento del control A.5.14 - Transferencia de información, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.	A.5.14 - Transferencia de información	Todo cambio inusual relacionado con cuentas de cobro, reembolsos, condiciones de pago, descuentos extraordinarios o solicitudes urgentes de clientes deberá validarse por un segundo canal antes de su ejecución. Se prohíbe actuar con base en una única comunicación no verificada cuando exista impacto financiero, contractual o reputacional.	Aplica a todos los colaboradores, contratistas, terceros, procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.	Registro de validación adicional; procedimiento comercial; evidencia de aprobación o confirmación.
POL-VTA-004-	Establecer directrices para la implementación y mantenimiento del	A.6.7 - Trabajo remoto	Durante visitas, viajes o trabajo remoto, el personal de ventas deberá proteger la información comercial y de	Aplica a todos los colaboradores, contratistas, terceros,	Declaración de cumplimiento; observación;

MOVILIDAD	control A.6.7 - Trabajo remoto, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.		clientes, evitando dejar equipos, documentos, pantallas o conversaciones expuestos a terceros. La organización definirá medidas mínimas para traslado, almacenamiento temporal, uso en reuniones y teletrabajo.	procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.	procedimiento de trabajo remoto o movilidad.
POL-VTA-005-CONEXION	Establecer directrices para la implementación y mantenimiento del control A.6.7 - Trabajo remoto, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.	A.6.7 - Trabajo remoto	El acceso a CRM, correo, repositorios y demás recursos comerciales fuera de la oficina deberá realizarse mediante redes o mecanismos seguros definidos por la organización. Se prohíbe utilizar redes públicas sin la protección autorizada o compartir información comercial en conexiones no confiables.	Aplica a todos los colaboradores, contratistas, terceros, procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.	Capacitación; evidencia de VPN o mecanismo seguro; aceptación de política.
POL-VTA-006-SERVICIOS-EXTERNOS	Establecer directrices para la implementación y mantenimiento del control A.5.10 - Uso aceptable de la información y de otros activos asociados, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.	A.5.10 - Uso aceptable de la información y de otros activos asociados	Se prohíbe cargar datos de clientes, contratos, listas de precios o información comercial a herramientas públicas, aplicaciones no aprobadas o servicios de inteligencia artificial no autorizados por la organización. Todo uso de servicios externos deberá estar previamente evaluado y autorizado conforme a la política corporativa.	Aplica a todos los colaboradores, contratistas, terceros, procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.	Política aceptada; revisión de herramientas aprobadas; evidencia de capacitación o restricción técnica.
POL-VTA-007-PERMISOS	Establecer directrices para la implementación y mantenimiento del control A.5.15 - Control de acceso, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la	A.5.15 - Control de acceso	Cuando se compartan propuestas, contratos, demos o archivos comerciales, el usuario deberá configurar permisos y enlaces de acceso de forma restrictiva, evitando exposición pública o acceso masivo no intencional. Los documentos deberán compartirse por tiempo, destinatario y finalidad definidos cuando la herramienta lo permita.	Aplica a todos los colaboradores, contratistas, terceros, procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de	Configuración de permisos; evidencia de enlaces restringidos; revisión de accesos en repositorio.

	gestión de seguridad de la información de la organización.			Seguridad de la Información de la organización.	
POL-VTA-008-PHISHING	Establecer directrices para la implementación y mantenimiento del control A.6.8 - Reporte de eventos de seguridad de la información, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.	A.6.8 - Reporte de eventos de seguridad de la información	Todo correo, archivo adjunto, mensaje o llamada sospechosa que aparente provenir de clientes, ejecutivos, aliados o plataformas comerciales deberá reportarse de inmediato por el canal oficial. Se prohíbe abrir adjuntos, hacer clic o entregar información sin validar la autenticidad cuando existan señales de suplantación o fraude.	Aplica a todos los colaboradores, contratistas, terceros, procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.	Evidencia de capacitación o simulación; reporte real o de prueba; conocimiento del canal oficial.
POL-VTA-009-DISPOSITIVO	Establecer directrices para la implementación y mantenimiento del control A.8.1 - Dispositivos terminales de usuario, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.	A.8.1 - Dispositivos terminales de usuario	Todo dispositivo móvil de trabajo o autorizado para actividades comerciales deberá mantenerse protegido con bloqueo, MFA y los controles definidos por la organización. En caso de pérdida, robo o compromiso, el usuario deberá reportarlo de inmediato para activar las medidas de contención, rastreo o borrado remoto que correspondan.	Aplica a todos los colaboradores, contratistas, terceros, procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.	Estado del dispositivo; evidencia de bloqueo y MFA; ticket o reporte de pérdida cuando aplique.

En las páginas siguientes se presenta un ejemplo del formato final utilizado para las políticas de seguridad de la información desarrolladas en el marco de CyberTrack 360. Estas políticas fueron elaboradas a partir de controles seleccionados de las normas ISO/IEC 27001:2022 e ISO/IEC 27002:2022 y están orientadas a facilitar su adopción en microempresas.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Sistema de gestión de seguridad de la información

Empresa: CyberTrack 360

Base legal: ISO/IEC 27001:2022

1. Objetivo

Establecer directrices para la implementación y mantenimiento del control A.5.17 - Información de autenticación, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos operativos y fortalecer la gestión de seguridad de la información de la organización.

2. Fundamento legal principal

ISO/IEC 27001:2022 Anexo A.5.17 - Información de autenticación

3. Lineamientos

- Toda comunicación laboral, acceso a plataformas corporativas, recuperación de credenciales e intercambio formal de información deberá realizarse exclusivamente mediante la cuenta institucional asignada por la organización.
- La autenticación multifactor será obligatoria en el correo institucional y en los servicios corporativos críticos o expuestos a Internet.
- Ningún usuario podrá desactivar, compartir, delegar o eludir los factores de autenticación sin autorización formal del área responsable.

4. Alcance

Aplica a todos los colaboradores, contratistas, terceros, procesos, activos de información, sistemas, dispositivos y recursos relacionados con el control establecido, dentro del alcance del Sistema de Gestión de Seguridad de la Información de la organización.

5. Evidencia

Captura o registro de MFA activo en correo institucional y servicios críticos; validación del administrador de identidad o TI; evidencia de cuenta corporativa asignada.

	ELABORÓ	REVISÓ	APROBÓ
FIRMA	*Jhon Fredy Aguirre*	*Flor Alba Tovar*	*Flor Alba Tovar*
NOMBRE	Jhon Fredy Aguirre	Flor Alba Tovar	Flor Alba Tovar
CARGO	Analista de seguridad de la información	Gerente General	Gerente General
FECHA	11-05-2026	14-05-2026	14-05-2026

CONTROL DE CAMBIOS

REVISÓ	FECHA	DESCRIPCIÓN DEL CAMBIO	FIRMA