



MUST UNIVERSITY
MASTER OF SCIENCE IN BUSINESS ADMINISTRATION

LIGIA FERNANDA GUERRA QUINONEZ

**INCORPORACIÓN DE LA TECNOLOGÍA DE LA
INFORMACIÓN EN PYMES DEL SECTOR DE VENTA DE
MATERIALES ELÉCTRICOS Y PROYECTOS.
ESTRATEGIA DE SEGURIDAD DE DATOS PARA LA
TRANSFORMACIÓN DIGITAL**

FLORIDA – USA
2023



LIGIA FERNANDA GUERRA QUINONEZ

**INCORPORACIÓN DE LA TECNOLOGÍA DE LA
INFORMACIÓN EN PYMES DEL SECTOR DE VENTA DE
MATERIALES ELÉCTRICOS Y PROYECTOS
ESTRATEGIA DE SEGURIDAD DE DATOS PARA LA
TRANSFORMACIÓN DIGITAL**

Trabajo de Conclusión Final presentado como
requisito parcial para la obtención del título de
MAESTRÍA en el Curso de MASTER OF
SCIENCE IN BUSINESS
ADMINISTRATION de MUST UNIVERSITY
– Florida USA.

Orientador(a): Prof. (a) Dr. (a) FRANKLIN ORELLANA

FLORIDA – USA
2023

LISTA DE FIGURAS

Figura 1	Percepción sobre prácticas de seguridad de la información en la empresa estudiada.....	25
Figura 2	Nivel de madurez en seguridad digital en PYMES	32
Figura 3	Diagrama comparativo de beneficios y desafíos de la digitalización en PYMES.....	36
Figura 4	Nivel de conocimiento en ciberseguridad del personal en PYMES del sector eléctrico.....	39

LISTA DE TABLAS

Tabla 1 Perfil de los participantes entrevistados.....	15
Tabla 2 Proceso de analítica cualitativo	18
Tabla 3 Proceso de analítica cuantitativo	20
Tabla 4 Técnicas de validación en el análisis de datos	22
Tabla 5 Implementación progresiva de seguridad digital en PYMES.....	31
Tabla 6 Pérdidas primarias por productividad ante incidentes de ciberseguridad en PYMES	41
Tabla 7 Comparación entre el modelo ISO/IEC 27001 y modelos flexibles de ciberseguridad para PYMES	43
Tabla 8 Resumen de resultados cuantitativos sobre ciberseguridad de PYMES del sector eléctrico ..	49
Tabla 9 Escala de valoración	59
Tabla 10 Cuestionario aplicado para evaluar la seguridad de la información digital en PYMES	60

LISTA DE ABREVIATURAS Y SIGLAS

- **PYMES:** Pequeñas y Medianas Empresas.
- **TI:** Tecnología de la Información.
- **Phishing:** Suplementación de identidad en línea para robar datos.
- **Ransomware:** Software malicioso que bloquea archivos y exige un rescate.
- **Cyberataque:** Ataque informático que compromete la seguridad de un sistema.
- **DMI:** Dirección Metropolitana de Informática
- **ISO:** Organización Internacional de Normalización
- **IEC:** Internacional Electrotechnical Commission
- **SGSI:** Sistema de Gestión de Seguridad de la Información.
- **MFA:** Autenticación multifactor
- **ERP:** Planificación de Recursos Empresariales (Enterprise Resource Planning)
- **CRM:** Gestión de Relaciones con Clientes (Customer Relationship Management)

RESUMEN

Este trabajo tiene como objetivo principal proponer una estrategia de seguridad de datos que impulse la transformación digital en PYMES del sector de venta de materiales eléctricos y ejecución de proyectos industriales. La investigación se desarrolló bajo un enfoque mixto con diseño exploratorio-descriptivo, utilizando entrevistas semiestructuradas, encuestas, observación directa y revisión documental como técnicas de recolección de datos. El estudio permitió identificar brechas en la gestión de la información, la cultura organizacional y el liderazgo, y plantea recomendaciones prácticas orientadas a fortalecer la ciberseguridad, optimizar procesos y promover una transformación digital segura, sostenible y centrada en las personas.

Palabras clave: Transformación digital. Seguridad de la información. Cultura organizacional. PYMES. Liderazgo.

ABSTRACT

The main objective of this paper is to propose a data security strategy to drive digital transformation in SMEs in the electrical materials sales and industrial project execution sectors. The research was conducted using a mixed exploratory-descriptive design approach, utilizing semi-structured interviews, surveys, direct observation, and document review as data collection techniques. The study identified gaps in information management, organizational culture, and leadership, and offers practical recommendations aimed at strengthening cybersecurity, optimizing processes, and promoting a secure, sustainable, and people-centered digital transformation.

Keywords: Digital transformation. Information security. Organizational culture. SMEs. Leadership

INCORPORACIÓN DE LA TECNOLOGÍA DE LA INFORMACIÓN EN PYMES DEL SECTOR DE VENTA DE MATERIALES ELÉCTRICOS Y PROYECTOS

ESTRATEGIA DE SEGURIDAD DE DATOS PARA LA TRANSFORMACIÓN DIGITAL

Ligia Fernanda Guerra Quinonez

SUMARIO

1. INTRODUCCIÓN	10
2. METODOLOGÍA	12
2.4. TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN	16
2.5. PROCEDIMIENTO DE ANÁLISIS DE DATOS	17
2.5.1. Análisis cualitativo	17
2.5.2. Análisis cuantitativo	19
2.6. VALIDEZ Y CONFIABILIDAD DE LOS INSTRUMENTOS	20
2.7. ESTRATEGIAS DE VALIDACIÓN DE LOS RESULTADOS	21
2.8. PRESENTACIÓN E INTERPRETACIÓN DE LOS RESULTADOS	22
2.8.1. Percepción de riesgos	23
2.8.2. Implementación de prácticas de seguridad	23
2.8.3. Resiliencia digital y resistencia al cambio	24
2.8.4. Resumen gráfico y tabulación de resultados	24
2.8.5. Interpretación en contraste con la literatura	25
2.9. CONSIDERACIONES ÉTICAS	26
3. SEGURIDAD DE DATOS EN LA TRANSFORMACIÓN DIGITAL	27
3.1. EVOLUCIÓN DEL ROL DE LA SEGURIDAD DE DATOS EN LAS PYMES	27
3.2. PLANEACIÓN ESTRATÉGICA Y SU IMPACTO EN LA SEGURIDAD DIGITAL	30
4. BENEFICIOS Y DESAFÍOS DE LA DIGITALIZACIÓN EN PEQUEÑAS Y MEDIANAS EMPRESAS	34
4.1. DEMOCRATIZACIÓN DEL ACCESO Y NUEVAS OPORTUNIDADES DE NEGOCIO	36
4.2. RIESGOS EN LA GESTIÓN DE LA INFORMACIÓN Y DEPENDENCIA TECNOLÓGICA	37
5. ESTRATEGIAS PARA UNA TRANSFORMACIÓN DIGITAL SEGURA Y SOSTENIBLE	37
5.1. FORTALECIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA	38
5.2. CAPACITACIÓN CONTINUA DEL TALENTO HUMANO	38
5.3. INCORPORACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	40
5.4. EVALUACIÓN DE RIESGOS Y PLANES DE CONTINGENCIA	40
5.5. SÍNTESIS COMPARATIVA DE MODELOS DE MADUREZ EN SEGURIDAD	42

6. GESTIÓN DEL CAMBIO CULTURAL EN LA TRANSFORMACIÓN DIGITAL DE LAS PYMES	44
6.1. LA RESISTENCIA AL CAMBIO: CAUSAS Y CONSECUENCIAS	44
6.2. EL ROL DEL LIDERAZGO EN PROCESOS DE TRANSFORMACIÓN.....	46
6.3. LIDERAZGO Y SEGURIDAD DE LA INFORMACIÓN: UNA VISIÓN ESTRATÉGICA DESDE LA CULTURA ORGANIZACIONAL	47
7. RESULTADOS DEL ESTUDIO	48
7.1. RESULTADOS CUANTITATIVOS CLAVE	48
7.2. ANÁLISIS COMPARATIVO CON ESTUDIOS LATINOAMERICANOS.....	49
8. CONSIDERACIONES FINALES	50
9. CONCLUSIONES.....	53
10. REFERENCIAS BIBLIOGRÁFICAS	54
11. ANEXO A: GUION DE ENTREVISTA SEMIESTRUCTURADA	58
11.1 OBJETIVO DEL INSTRUMENTO:	58
11.2 GUION DE PREGUNTAS.....	58
12. ANEXO B: CUESTIONARIO APLICADO (ENCUESTA)	59
12.1 OBJETIVO DEL INSTRUMENTO:	59
12.2 INSTRUCCIONES:.....	59

1. Introducción

Las pequeñas y medianas empresas (PYMES) desempeñan un papel fundamental en la economía ecuatoriana, particularmente en sectores como la venta de materiales eléctricos y la ejecución de proyectos. En los últimos años, muchas de estas empresas han iniciado procesos de transformación para optimizar sus operaciones administrativas y contables, mejorar su productividad, competitividad en el mercado.

Un caso representativo es el de una PYME ecuatoriana del sector eléctrico, dedicada a la venta de materiales eléctrico y ejecución de proyectos industriales fundada en 2013 en Guayaquil, Ecuador, que implemento la plataforma Siigo, un software de gestión empresarial en la nube. Esta herramienta facilita la contabilidad, la facturación electrónica y control de inventarios, contribuyendo a la optimización de los procesos operativos y administrativos. Además, ofrece estándares robustos de seguridad de la información. Lo que refuerza la protección de los datos críticos en un entorno donde las amenazas cibernéticas son cada vez más frecuentes.

No obstante, muchas PYMES en Ecuador siguen careciendo de políticas formales de seguridad de la información, lo que incrementa su vulnerabilidad ante ciberataques, filtraciones de datos y problemas de cumplimiento normativo (Creswell & Plano Clark, 2018; Hernandez, Fernández & Baptista, 2021). Un ejemplo que evidencia esta problemática ocurrió en abril de 2022, la plataforma tecnología de la Dirección Metropolitana de Informática (DMI) del Municipio de Quito fue víctima de un ataque cibernético mediante malware tipo ransomware, lo que afectó varios de sus sistemas y servicios dirigidos a la ciudadanía (Municipio de Quito, 2022).

Para que la transformación digital sea realmente efectiva, las empresas necesitan una visión clara de sus necesidades y procesos. Cuando la necesidad es clara y concisa, la aplicación de la tecnología se facilita. La integración de herramientas digitales es más eficiente cuando la información está ordenada, los procesos estructurados y la interoperabilidad con otros organismos bien definida. Innovación, planificación y alineación con la estrategia empresarial son claves para apalancar la tecnología y lograr una gestión más eficiente.

A partir de este contexto, se plantea la siguiente pregunta de investigación: ¿Cómo puede una estrategia de seguridad de datos facilitar la transformación digital en las PYMES del sector de materiales eléctricos?

1.1. Planteamiento de la hipótesis

Con el fin de dar respuesta a la pregunta, se plantea la siguiente hipótesis:

La implementación de una estrategia de seguridad de datos, basada en estándares internacionales como la Organización Internacional de Normalización ISO/IEC 27001, facilita la transformación digital en las PYMES del sector eléctrico, al fortalecer la protección de la información, optimizar los procesos operativos y reducir la vulnerabilidad frente a riesgos cibernéticos.

Esta hipótesis se evaluará mediante un enfoque metodológico mixto, que combina técnicas cualitativas y cuantitativas, permitiendo analizar las percepciones, prácticas y niveles de madurez digital en la empresa objeto de estudio.

Este trabajo está estructurado en siete secciones: introducción, metodología, desarrollo teórico sobre la seguridad de datos en la transformación digital, análisis de los beneficios y desafíos de la digitalización en pequeñas y medianas empresas, estrategias para una

transformación digital segura y sostenible, gestión del cambio cultural en las PYMES y consideraciones finales, lo cual permite un abordaje integral de la problemática desde la perspectiva empírica y aplicada.

2. Metodología

Esta investigación adopta un enfoque mixto, que combina métodos cualitativos y cuantitativos con el fin de analizar la gestión de la seguridad de la información en las pequeñas y medianas empresas PYMES del sector eléctrico en Ecuador. Se selecciono un diseño de estudio de caso explicativo, ya que el propósito es examinar a profundidad una problemática específica en su contexto natural: la seguridad de la información en las PYMES dedicadas a la venta de materiales eléctricos y a la ejecución de proyectos industriales.

El enfoque exploratorio es apropiado cuando se busca obtener un acercamiento inicial a un fenómeno poco estudiado en un contexto particular, sin pretender establecer generalizaciones, pero si aportar información valiosa para futuras investigaciones (Hernandez, Fernández & Baptista, 2021).

La combinación de métodos cualitativos y cuantitativos permite integrar la riqueza del análisis cualitativo, que explora percepciones y experiencias de los responsables de tecnología, con la objetividad de los métodos cuantitativos, que permiten medir el nivel de madurez en la gestión de la seguridad de información. Esta combinación contribuye a la triangulación de los datos y al fortalecimiento de la validez de los resultados obtenidos (Creswell & Plano Clark, 2018).

Es importante destacar que, si bien se revisan conceptos y estrategias aplicables a las PYMES en general, las reflexiones y recomendaciones de este trabajo se centran en el contexto específico de la empresa objeto de estudio, por lo que no se pretende realizar generalizaciones estadísticas, sino aportar hallazgos y propuestas adaptadas a dicho contexto.

2.1. Diseño de investigación

Se empleo un diseño de estudio de caso explicativo. Este diseño es adecuado cuando se pretende profundizar en el conocimiento de fenómenos actuales en su contexto real, especialmente cuando las fronteras entre el fenómeno y el contexto no están claramente delimitadas (Yin, 2018)

La investigación se enfocó en un caso particular: una PYMES del sector eléctrico, dedicada tanto a la venta de materiales como a la ejecución de proyectos industriales. El estudio buscó explicar cómo esta organización gestiona los riesgos asociados a la seguridad de la información en sus operaciones diarias.

Dado que la presente investigación se basa en el análisis de un único caso de estudio, los resultados obtenidos no buscan ser generalizados estadísticamente a todas las PYMES del sector, sino aportar evidencias significativas que pueden ser consideradas por organizaciones con características similares en cuanto a tamaño, actividad económica y nivel de digitalización. Esta aproximación permite realizar análisis profundo del fenómeno en su contexto específico, ofreciendo aportes relevantes para el diseño de estrategias de seguridad de la información y transformación digital en empresas con problemáticas comparables.

2.2. Criterios de selección de la muestra

El estudio se centrará en una PYMES ecuatoriana del sector eléctrico que ha implementado herramientas digitales en sus procesos operativos y administrativos. La selección del caso único responde a un muestreo intencional, de acuerdo con los siguientes criterios de inclusión:

- Sector: Pertenece a la industria eléctrica y está involucrada en la venta de materiales eléctricos y la ejecución de proyectos industriales.
- Tamaño: Se considera una PYME conforme a la clasificación del Instituto Nacional de Estadística y Censos (INEC), con un número de empleados y nivel de facturación dentro de los rangos establecidos para esta categoría.
- Grado de digitalización: Ha adoptado herramientas digitales para la gestión operativa y financiera, como sistemas Planificación de Recursos Empresariales (ERP), facturación electrónica y almacenamiento en la nube.
- Relevancia en la investigación: Presenta desafíos relacionados con la seguridad de la información en su proceso de transformación digital, lo que permite analizar su estrategia en ciberseguridad.

2.3. Participantes y perfil

La selección de los participantes se realizó mediante un muestreo intencional o dirigido, dado que se buscaba entrevistar a personas que desempeñaran roles clave en la gestión de procesos tecnológicos y operativos de la empresa de estudio.

El criterio de inclusión fue contar con experiencia directa en manejo de información sensible o responsabilidad en procesos vinculados a la transformación digital y seguridad de información.

Adicionalmente, se aplicaron entrevistas y encuestas a actores clave de una PYMES del sector eléctrico, manteniendo el anonimato de la empresa y los participantes.

A continuación, se presenta la Tabla 1, que resume el perfil de los entrevistados:

Tabla 1

Perfil de los participantes entrevistados

Participante	Cargo	Años de Experiencia	Rol en la Empresa
Entrevistado 1	Responsable de Tecnología	8 años	Gestión de infraestructura TI (Tecnología de la información)
Entrevistado 2	Coordinador de Proyectos	5 años	Implementación de proyectos industriales
Entrevistado 3	Jefe de Operaciones	10 años	Supervisor de procesos operativos
Entrevistado 4	Asistente Administrativo	3 años	Soporte en gestión de información
Entrevistado 5	Técnico de Mantenimiento	4 años	Ejecución de tareas técnicas en proyectos

Fuente: Elaboración propia basada en entrevistas realizadas.

En total, se realizaron 5 entrevistas semiestructuradas a colaboradores seleccionados según el rol estratégico en la empresa, y se aplicaron 10 cuestionarios estructurados a personal de distintas áreas operativas y administrativas. Se obtuvo una tasa de respuesta del 90%, lo cual asegura la representatividad de los datos recolectados en relación con el tamaño de la organización.

2.4. Técnicas de recolección de información

La recolección de datos en esta investigación se llevó a cabo utilizando diversas técnicas que permitieron obtener información rica y complementaria, acorde al enfoque mixto adoptado (Hernandez-Sampieri et al, 2021):

- Entrevistas semiestructuradas: Aplicadas a cinco participantes clave de la empresa seleccionada. Permitiendo explorar aspectos relacionados con la gestión de la seguridad de la información, percepción de riesgos y madurez digital. Las preguntas fueron abiertas y flexibles para facilitar repuestas ricas en contenido. El guion de las entrevistas se presenta en el Anexo A.
- Cuestionarios estructurados: Instrumentos de respuesta cerrada, diseñados con escalas tipo Likert de 5 puntos, orientados a medir cuantitativamente el grado de implementación de prácticas de seguridad de la información y madurez digital. El cuestionario aplicado se detalla en el Anexo B.

- Analisis documental: Revisión de documentos internos (manuales, políticas de seguridad, protocolos de manejo de información) y fuentes académicas recientes sobre transformación digital y ciberseguridad en PYMES (European Union Agency for Cybersecurity, 2023).

Cada técnica oportuna información específica que, en conjunto, permitió una comprensión integral del fenómeno de estudio, favoreciendo la triangulación de datos y el fortalecimiento de la validez de los resultados obtenidos.

2.5. Procedimiento de análisis de datos

2.5.1. Análisis cualitativo

Las entrevistas semiestructuradas serán transcritas de manera textual. El análisis se realizará a través de un análisis de contenido temático, que incluye la codificación inicial de los datos, la categorización de temas clave y la interpretación de patrones emergentes. Esta codificación permitirá identificar conceptos como percepción de riesgos, medidas de seguridad, desafíos de transformación digital, y nuevas dimensiones como resiliencia digital organizacional, entendida como la capacidad de adaptación y respuesta ante incidentes tecnológicos imprevistos (ENISA, 2023).

Se utilizó codificación manual, aplicando los principios de rigor cualitativo, y se garantizará la confiabilidad mediante la revisión cruzada de categorías y el proceso de validación con los participantes (*member checking*), el cual se realizará por correo electrónico. A cada participante se le enviara un resumen de los hallazgos preliminares para que confirme la fidelidad de la interpretación o sugiera correcciones si lo considera necesario.

Adicionalmente, se emplearon categorías abiertas que permitan captar percepciones sobre el nivel de madurez tecnológica en la empresa, conforme a modelos de madurez en TI (*maturity models*), los cuales facilitan la identificación de las etapas evolutivas en la adopción de buenas prácticas de seguridad y gestión digital (Westerman et al., 2020).

Otro eje interpretativo será la valoración que hacen los participantes sobre el uso de servicios en la nube (*cloud security*), su percepción de riesgos, confianza en los proveedores tecnológicos, y experiencia en el manejo de accesos, respaldos y protocolos básicos.

El proceso detallado del análisis cualitativo se resume en la Tabla 2, donde se describen las etapas desde la transcripción hasta la interpretación de los resultados, con un enfoque orientado a integrar elementos clave de transformación digital segura en PYMES del sector eléctrico.

Tabla 2

Proceso de Análisis Cualitativo

Etapas	Descripción
Transcripción y lectura preliminar	Se transcriben todas las entrevistas y se hace una primera lectura para identificar los conceptos claves
Codificación inicial	Se asignan palabras clave a fragmentos del texto, identificando conceptos relevantes como percepción de riesgos, medidas de seguridad y desafíos.
Agrupación de categorías	Se organizan las palabras clave en temas principales, facilitando el análisis.
Identificación de patrones	Se analizarán similitudes y diferencias en las respuestas para identificar tendencias.
Interpretación de resultados	Se comparan los hallazgos con estudios previos y se extraen conclusiones.

Nota. Esta tabla resume las etapas del análisis cualitativo, detallando que se hace en cada una.

2.5.2. Análisis cuantitativo

Los datos obtenidos de las encuestas estructuradas serán codificados y procesados mediante Microsoft Excel. Además, se utilizará el software estadístico R, una herramienta de código abierto que permite realizar análisis de estadística descriptiva con precisión y robustez (Team R Core, 2021).

Se aplicarán técnicas para el análisis de frecuencias, porcentajes, medias y desviaciones estándar. Esto permitirá evaluar la madurez en la gestión de la seguridad de la información y la adopción de medidas de ciberseguridad en las PYMES objeto de estudio.

Se seleccionó R como herramienta de análisis estadístico debido a su capacidad para manejar grandes volúmenes de datos y ejecutar procedimientos estadísticos avanzados de manera flexible y eficiente al tratarse de un software libre, R representa una alternativa accesible para las pequeñas y medianas empresas que buscan implementar soluciones tecnológicas en el marco de sus procesos de transformación digital.

Su uso en esta investigación contribuye a garantizar el rigor metodológico en la evaluación de la información, respaldando la validez y confiabilidad de los resultados obtenidos.

El proceso de análisis cuantitativo se detalla en la Tabla 3, donde se describen las técnicas empleadas en cada etapa del análisis de los datos.

Tabla 3*Proceso de analítica cuantitativa*

Técnica	Descripción
Codificación de respuestas	Se asignarán valores numéricos a cada opción de respuesta en las encuestas para facilitar su tabulación.
Limpieza de datos	Se revisarán los datos para detectar valores atípicos o respuestas inconsistentes y corregir errores en la entrada de datos.
Análisis de frecuencia y porcentajes	Se calculará la distribución de respuestas para determinar el porcentaje de empleados que aplican medidas de seguridad digital en su trabajo.
Cálculo de medidas descriptivas	Se analizarán promedios y desviaciones estándar para evaluar el nivel de conocimiento en ciberseguridad, la frecuencia de capacitaciones y la implementación de protocolos de seguridad en la empresa.
Representación gráfica	Los datos se visualizarán en gráficos de barras, circulares y de líneas, permitiendo una interpretación clara de los resultados.

Nota. Se emplearán métodos estadísticos dentro de Microsoft Excel y el software R.

2.6. Validez y confiabilidad de los instrumentos

Para garantizar la validez de contenido de los instrumentos utilizados en esta investigación, el guion de las entrevistas semiestructuradas (presentado en el Anexo A) y el cuestionario estructurado (incluido en el Anexo B) fueron revisado por tres expertos en ciberseguridad y tecnologías de la información.

Los expertos fueron seleccionados considerando su experiencia profesional y académica en el área. Se priorizó a profesionales con al menos cinco años de experiencia, desempeñándose como consultores y docentes en instituciones educativas y empresas del sector tecnológico. Se cuidó que no existiera conflicto de intereses con la organización objeto de estudio. Las preguntas fueron validadas para asegurar su alineación con los objetivos de la investigación y con el marco teórico.

En cuanto a la confiabilidad, se realizó prueba piloto del cuestionario aplicado a las encuestas. La consistencia interna de los instrumentos fue evaluada mediante el coeficiente Alfa de Cronbach, considerando un valor mínimo aceptado de 0.70, de acuerdo con los estándares metodológicos establecidos (Hernandez, Fernández & Baptista, 2021). Este coeficiente es ampliamente utilizado en estudios aplicados en ciencias sociales y de gestión, como el presente, debido a su utilidad para medir la fiabilidad interna de los instrumentos (Taherdoost, 2016).

Aunque el estudio se basa en una muestra limitada a una sola empresa, los hallazgos obtenidos permiten generar recomendaciones aplicables y generalizables a organizaciones que compartan características similares en cuanto a tamaño, sector y nivel de adopción tecnológica.

2.7. Estrategias de validación de los resultados.

Se implementaron diversas estrategias de validación con el propósito de asegurar la coherencia, credibilidad y confiabilidad de los resultados obtenidos. Estas estrategias permitieron fortalecer el rigor metodológico del estudio y garantizar que las conclusiones fueran consistentes con la evidencia recolectada.

La Tabla 4 resume las técnicas de validación aplicadas en el análisis de los datos:

Tabla 4

Técnicas de Validación en el Análisis de Datos

Método	Descripción
Triangulación de datos	Se compararán los resultados de entrevistas y encuestas para validar la coherencia en la percepción de la seguridad de datos y la transformación digital en la empresa.
Revisión por expertos	Validación de los hallazgos preliminares por parte de directivos y responsables de tecnología de la empresa participante
Contraste con estudios previos	Se analizarán los resultados en relación con investigaciones sobre adopción de TI y seguridad de datos en PYMES ecuatorianas.
Pruebas de coherencias	Se verificará la consistencia de respuestas y patrones en entrevistas y encuestas para minimizar sesgos.
Member cheching	Confirmación de los resultados de las entrevistas por parte de los participantes, asegurando la fidelidad de las interpretaciones realizadas.

Nota. Esta tabla resume los métodos utilizados en la validación del estudio.

2.8. Presentación e interpretación de los resultados

La presentación de los resultados se realiza diferenciando los hallazgos cualitativos y cuantitativos obtenidos mediante las técnicas de recolección de datos aplicadas. El análisis integro ambos enfoques a través de la triangulación de datos, lo que permitió fortalecer la validez de las conclusiones.

La interpretación de los hallazgos se realizó en referencia a los marcos conceptuales definidos en el estudio, considerando los estándares de seguridad de información (ISO/IEC 27001), las categorías de madurez digital propuestas de Gartner (2024), y las recomendaciones específicas para PYMES de WeLiveSecurity (2024) e Hirschberger, Smulders y Vars (2018).

2.8.1. Percepción de riesgos

Se identificó que un 70% de los participantes perciben un alto nivel de riesgo asociado al manejo de información digital y el uso de plataformas en la nube.

Esta percepción se relaciona directamente con la falta de protocolos de seguridad estandarizados, en comparación con las buenas prácticas propuestas por la ISO/IEC 27001.

2.8.2. Implementación de prácticas de seguridad

En relación con las prácticas de protección implementadas, se obtuvieron los siguientes resultados:

- El 60% reporta la realización de respaldo periódico de información.
- Solo el 45% de los participantes utiliza mecanismo de autenticación multifactor (MFA).
- Un 55% manifiesta poseer conocimientos básicos en ciberseguridad.

Estos datos reflejan un avance parcial en materia de protección de activos digitales, aunque aún existen brechas importantes respecto a las recomendaciones de Gartner para alcanzar niveles de madurez digital adecuados.

2.8.3. Resiliencia digital y resistencia al cambio

El análisis de las entrevistas evidenció la presencia de resistencia al cambio frente a procesos de transformación digital, especialmente en la adopción de nuevas herramientas de protección de datos. Según el marco de análisis propuesto por Llorente y Cuenca (2021), esta resistencia constituye la sostenibilidad de las mejores ciberseguridades.

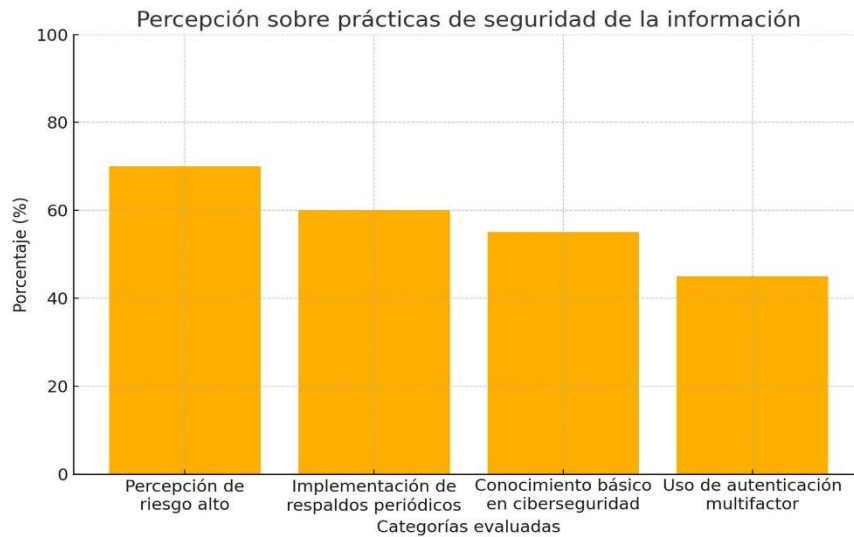
En cuanto a la protección de datos personales, si bien existen esfuerzos por resguardar información sensible, no todos los colaboradores implementan las prácticas de protección exigidas por los marcos regulatorios recientes.

2.8.4. Resumen gráfico y tabulación de resultados

En la Figura 1, se sintetizan de manera gráfica los principales resultados obtenidos, con el propósito de respaldar visualmente el análisis realizado, que resume los resultados obtenidos en la investigación.

Figura 1

Percepción sobre prácticas de seguridad de la información en la empresa estudiada.



Fuente: Elaboración propia basada en resultados obtenidos en la investigación, 2025

Se evidencia que un 70% de los participantes percibe un riesgo alto en materia de seguridad de la información, mientras que un 60% reporta la implementación de respaldos periódicos. Asimismo, un 55% de los colaboradores posee conocimientos básicos de ciberseguridad y un 45% implementa mecanismos de autenticación multifactor, reflejando avances importantes, pero también áreas que requieren fortalecimiento.

2.8.5. Interpretación en contraste con la literatura

Al comparar los resultados obtenidos con los marcos teóricos revisados, se observó lo siguiente:

- Según la ISO/IEC 27001, la empresa presenta avances parciales en la identificación de riesgos, pero aún carece de un sistema de gestión de seguridad de la información estructurado.
- Conforme al modelo de madurez digital de Gartner, la organización se ubica en un nivel inicial, donde predominan esfuerzos aislados en vez de una estrategia integral.
- Las recomendaciones de Hirschberger, Smulders y Vars (2018) y WeLiveSecurity (2024) para PYMES sugieren que, aunque existen buenas prácticas implementadas, se requiere fortalecer la cultura organizacional en seguridad digital para alcanzar una resiliencia sostenible.

Estos contrastes permiten identificar las principales áreas de oportunidad para mejorar la gestión de la seguridad de la información en la empresa como parte de su proceso de transformación digital.

2.9. Consideraciones éticas

El estudio cumplió con los principios éticos de anonimato, confidencialidad y consentimiento informado. Se garantizará que los datos recolectados sean utilizados exclusivamente para fines académicos y que se proteja la identidad tanto de los participantes como de las organizaciones involucradas.

Los colaboradores fueron informados sobre los objetivos de la investigación, las técnicas utilizadas y su derecho a no participar o retirarse del estudio en cualquier momento, sin que esto estuviera consecuencias negativas para ellos.

3. Seguridad de datos en la transformación digital.

La transformación digital en PYMES del sector eléctrico y de proyectos industriales, ha permitido optimizar procesos clave mediante el uso de tecnologías de la información, mejorando la eficiencia operativa y la toma de decisiones (Pérez Escutia & Fischer de la Vega, 2023). Sin embargo, el crecimiento tecnológico implica nuevos riesgos en la seguridad de datos, ya que la empresa maneja información crítica sobre proyectos, clientes, proveedores y operaciones.

Aunque la seguridad de la información fundamental en el proceso de transformación digital de las PYMES, pero su implementación se limita por múltiples factores. Peralta y Aguilar (2021) señalan que las PYMES ecuatorianas enfrentan dificultades para destinar recursos a la ciberseguridad debido a su percepción como un gasto y no como una inversión estratégica.

3.1. Evolución del rol de la seguridad de datos en las PYMES

En las grandes empresas, la ciberseguridad suele estar a cargo de un director de seguridad de la información (CISO), quien se encarga de definir y supervisar la estrategia de seguridad de la información en toda la organización (ISACA, 2023). Sin embargo, en PYMES, no siempre es viable contar con un puesto exclusivo para seguridad digital, debido a limitaciones de recursos humanos y financieros (Gartner, 2023).

Según RA-MA (2024), en las primeras etapas de una empresa, es más eficiente contar con un ingeniero o arquitecto de seguridad que implemente las primeras capas de protección digital, antes de considerar la contratación de director de seguridad a tiempo completo. En muchas PYMES del sector eléctrico y de proyectos industriales, la seguridad de datos se gestiona internamente por su equipo de TI, sin contar aún con un especialista dedicado exclusivamente a esta función.

Conforme las empresas avanzan en su transformación digital, suelen implementar medidas como:

- Uso de plataformas en la nube para gestión de inventarios y facturación electrónica, debido a que permiten mejorar la eficiencia operativa y garantizar mayor seguridad y accesibilidad de los datos (Accel-KKR, 2020; Gartner, 2023).
- Restringir accesos a sistemas críticos para evitar fugas de información, mediante la aplicación de controles de accesos, gestión de identidades y uso autenticación multifactor (ISACA, 2023).
- Implementar respaldos de datos periódicos para prevenir pérdidas por fallos técnicos o ataques cibernéticos, errores humanos. (WeLiveSecurity, 2024).

No obstante, estos esfuerzos deben complementarse con una estrategia de seguridad más robusta que considere los riesgos emergentes, especialmente a medida que la empresa maneja un volumen mayor de información y automatiza más procesos.

Como parte del análisis realizado en la empresa objeto de estudio se recomienda como próximo paso:

- Evaluar la viabilidad de un asesor externo en seguridad digital que ayude a estructurar un plan de protección de datos sin requerir una inversión excesiva en personal interno.

Además de la seguridad tecnológica, en el contexto de la empresa analizada, se identificó la necesidad de considerar la seguridad del capital intelectual, es decir, la protección del conocimiento interno de la empresa, incluyendo:

- Diseños de proyectos eléctricos y automatización.
- Datos de clientes y proveedores
- Procedimientos internos y metodologías de trabajo.

Según Daza et al. (2020), la falta de una gestión estructurada de los activos intelectuales limita la competitividad de las PYMES en Latinoamérica. En el sector eléctrico y de proyectos industriales, esta problemática se agrava debido a la importancia de la confidencialidad de la información técnica en los proyectos.

Diversos estudios regionales han evidenciado esta situación. Por ejemplo, Gómez y Perea (2021) encontraron que muchas PYMES colombianas del sector manufacturero carecen de políticas formales de seguridad de la información, lo que incrementa su exposición a ciberataques. De manera similar, Torres y Ramírez (2022) identificaron en Perú importantes debilidades en el manejo de datos en pequeñas empresas del sector tecnológico, derivadas de la limitada inversión en infraestructura digital y la escasa capacitación en ciberseguridad.

Actualmente, muchas empresas en el Ecuador han avanzado en ciertas prácticas de seguridad, como:

- Accesos controlados a documentación técnica y financiera.
- Uso de correos corporativos para evitar fugas de información.
- Almacenamiento de datos en servidores internos y en la nube.

Sin embargo, persisten riesgos relacionados con el uso inadecuado de información por parte de empleados, la falta de capacitación en ciberseguridad y la carencia de un plan estructurado de seguridad de la información.

Como siguiente paso recomendado para las PYMES del sector eléctrico y de proyectos industriales, se sugiere implementar un esquema de gestión de capital intelectual que garantice la seguridad de la información técnica, protegiendo tanto los datos digitales como documentación física en proyectos industriales.

3.2. Planeación estratégica y su impacto en la seguridad digital

La planeación estratégica en las PYMES del sector eléctrico y proyectos suele seguir un modelo emergente e incremental, donde las decisiones se toman conforme evoluciona el entorno y las necesidades del mercado.

La adopción de nuevas tecnologías en estas empresas ha seguido un proceso gradual, incluyendo:

- Implementación de software de gestión (ERP) para mejorar trazabilidad de proyectos.
- Automatización en la gestión de inventarios y compras.
- Mejora en la comunicación interna mediante plataformas digitales.

Sin embargo, la seguridad de la información no ha crecido al mismo ritmo, lo que genera vulnerabilidades.

Al no existir un documento formal de planificación estratégica en seguridad digital, las decisiones sobre protección de datos se toman de manera reactiva, en lugar de proactiva.

Para abordar estas brechas, se propone la implementación progresiva de una serie de acciones estratégicas orientadas a fortalecer la seguridad digital en las PYMES del sector eléctrico y de proyectos.

Estas acciones buscan establecer una gestión sistemática de la seguridad de la información, integrándola como un componente clave dentro de la planeación estratégica.

La Tabla 5 presenta un resumen de dichas acciones y su impacto esperado en la organización.

Tabla 5

Implementación Progresiva de Seguridad Digital en PYMES

Acción	Impacto esperado
Definir una política básica de seguridad digital	Brindará lineamientos claros sobre acceso a datos y protección de riesgo de accesos no autorizados y mejorando el cumplimiento normativo (por ejemplo, regulaciones de protección de datos)
Capacitar al personal en buenas prácticas de seguridad	Reducirá riesgos por errores humanos y posibles fugas de información. Además, incrementara la cultura organizacional de seguridad, asegurando la correcta gestión de contraseñas y, manejo de dispositivos y uso de plataformas digitales.
Realizar auditorías de seguridad periódicas	Permitirá identifica y corregir vulnerabilidades antes de que represente un riesgo mayor, asegurando la continuidad operativa y reduciendo la posibilidad de ataques cibernéticos como ransomware o phishing.

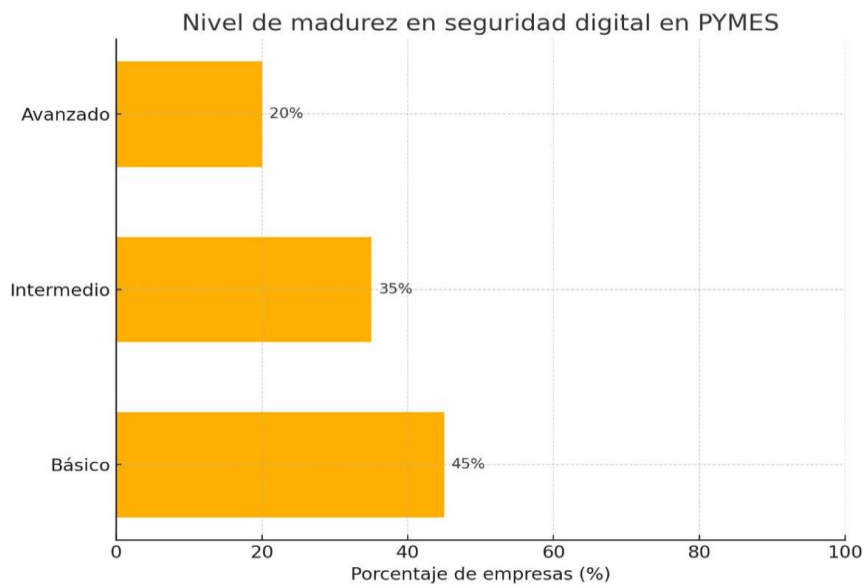
Nota. Acciones prioritarias para fortalecer la seguridad digital en PYMES

Para evaluar la madurez de seguridad digital PYMES del sector eléctrico, se estableció una serie de acciones recomendadas. Estas acciones han sido implementadas en diversos niveles de madurez digital y han mostrado diferentes impactos en la seguridad de la información. A continuación, se presenta un resumen de las principales estrategias y su impacto esperado

Para garantizar la protección de la información sin afectar la flexibilidad operativa, es esencial contar con una estrategia de seguridad digital progresiva que acompañe el crecimiento de la empresa. A continuación, se presenta un gráfico que ilustra visualmente las etapas o niveles en la implementación progresiva de seguridad digital en PYMES, desde las medidas básicas hasta las avanzadas ver Figura 2.

Figura 2

Nivel de Madurez en seguridad digital en PYMES



Nota. Datos simulados con fines ilustrativos basados en observaciones empíricas de estudios previos, realizados por la autora (2025), adaptado de WeLiveSecurity (2024) e ISACA (2023).

Se muestra la distribución del nivel de madurez en la implementación de medidas de ciberseguridad en las PYMES del sector eléctrico analizadas. De acuerdo con los datos obtenidos la mayoría de estas empresas aún se encuentran en niveles básicos de protección digital (45%), destacando la necesidad de avanzar hacia etapas intermedias o avanzadas.

Como se observa en la Tabla 5 y la Figura 1, las acciones en seguridad digital para las PYMES se implementan progresivamente según la etapa de madurez digital. Este enfoque permite avanzar de medidas básicas hacia etapas más avanzadas, adaptándose gradualmente al crecimiento organizacional y tecnológico (ISACA,2023; WeLiveSecurity, 2024).

Este enfoque es consistente con lo señalado por ISACA (2023), en el contexto de estudio, se plantea que las PYMES, como la empresa analizada, podrían beneficiarse de un modelo progresivo de implementación de seguridad digital alineado con su madurez tecnológica. Asimismo, el estudio de WeLiveSecurity (2024) destaca la importancia de adaptar las estrategias de ciberseguridad a las capacidades operativas y financieras de cada organización, enfatizando que los cambios deben ser graduales para evitar interrupciones en los procesos de negocio. Coincidiendo con estos planteamientos, Fernández y Baptista (2021) argumentan que la integración de políticas de seguridad digital debe considerar el nivel de adopción tecnológica de la organización y su cultura corporativa.

Los hallazgos de este estudio refuerzan estas perspectivas, a evidenciar que las PYMES del sector eléctrico priorizan acciones básicas, como la capacitación y las auditorías periódicas, antes de avanzar hacia sistemas más complejos, como la automatización de la gestión de riesgos. El objetivo no es hacer cambios abruptos, sino integrar la seguridad digital del crecimiento de la empresa sin que esto afecte su operatividad.

4. Beneficios y desafíos de la digitalización en pequeñas y medianas empresas

La transformación digital de las pequeñas y medianas empresas (PYMES) representa una oportunidad para mejorar la competitividad, automatizar procesos, fortalecer la relación con los clientes y adaptarse a un entorno empresarial cada vez más dinámico. Esta transición implica mucho más que la incorporación de herramientas tecnológicas supone una reconfiguración cultural y organizativa que desafía las formas tradicionales de operar (Llorente & Cuenca, 2019).

Uno de los beneficios más evidentes es la capacidad de acceder al conocimiento, a la información y a los recursos de la forma casi inmediata, lo que permite a las empresas tomar decisiones más acertadas, compartir ideas y crear valor con mayor rapidez. En el caso de las PYMES del sector eléctrico e industrial, la digitalización facilita la gestión eficiente de proyectos mediante herramientas de diseño asistido, plataformas de monitoreo remoto, automatización de inventarios y comunicación ágil con proveedores y clientes.

Sin embargo, este proceso también conlleva desafíos importantes. La resistencia al cambio, la falta de cultura digital, y la escasa capacitación en competencias tecnológicas con obstáculos recurrentes en este tipo de organizaciones. Como señalan Rodríguez y Espinosa (2019), en contextos latinoamericanos existe una tendencia a estigmatizar el error y rechazar lo nuevo, cuando en realidad el ensayo y la experimentación son pilares del aprendizaje en entornos digitales.

Otro reto clave es la conectividad. Aunque el acceso a internet se ha ampliado en la región, aún persisten brechas significativas que afectan especialmente a las PYMES en zonas no urbanas. La conectividad deficiente limita el aprovechamiento de soluciones en la nube, sistemas de gestión en tiempo real y comercio electrónico. En este sentido, la transformación digital no solo debe abordarse desde la infraestructura tecnológica, sino también desde la gestión del conocimiento y la formación del talento humano.

En definitiva, el éxito de la digitalización en PYMES dependerá de su capacidad para integrar la tecnología en su cultura organizacional, fomentar una actitud de aprendizaje continuo, y adoptar estrategias centradas en el cliente, como experiencias omnicanal que respondan a nuevas expectativas de consumo (Espinosa, 2019).

El diagrama de la Figura 3 se representa una síntesis de los principales beneficios y desafíos identificados en el proceso de digitalización en pequeñas y medianas empresas.

Figura 3

Diagrama comparativo de beneficios y desafíos de la digitalización en PYMES



Fuente: Elaboración propia basada en Llorente & Cuenca (2019).

4.1. Democratización del acceso y nuevas oportunidades de negocio

Uno de los efectos más significativos de la digitalización es la democratización del acceso a información, mercados y herramientas tecnológicas. Para las PYMES, esto representa la posibilidad de competir en condiciones más equitativas frente a grandes empresas. A través de soluciones en la nube, plataformas de e-commerce y canales digitales de atención al cliente, empresas como las que se dedican a la venta de materiales y proyectos pueden expandir su alcance comercial sin necesidad de grandes inversiones en infraestructura.

Además, la digitalización permite recopilar y analizar datos para diseñar productos o servicios más personalizados, lo cual incrementa la fidelización de los clientes y mejora la toma de decisiones estratégicas (Llorente & Cuenca, 2019).

4.2. Riesgos en la gestión de la información y dependencia tecnológica

A pesar de los beneficios, la digitalización conlleva una creciente exposición a amenazas relacionadas con la ciberseguridad. En las PYMES del sector eléctrico, donde se maneja información técnica sensible, la falta de políticas robustas de protección de datos y la escasa cultura de seguridad pueden comprometer seriamente los activos digitales.

Por otro lado, una excesiva dependencia de plataformas digitales sin planes de contingencia puede poner en riesgo la continuidad operativa ante fallas tecnológicas, pérdidas de datos o accesos no autorizados. Para mitigar estos riesgos, es indispensable fortalecer las capacidades del talento humano en competencias digitales básicas y avanzadas (Rodríguez, 2019).

5. Estrategias para una Transformación digital segura y sostenible

La transformación digital representa una oportunidad estratégica para mejorar la competitividad de las pequeñas y medianas empresas PYMES. No obstante, para que dicha transformación sea sostenible en el tiempo, debe estar acompañada de una estrategia sólida en materia de seguridad de la información, gestión del talento humano y políticas tecnológicas. En este sentido, se vuelve imprescindible diseñar un entorno digital robusto que minimice los riesgos operacionales y cibernéticos, al tiempo que potencie la eficiencia empresarial.

5.1. Fortalecimiento de la infraestructura tecnológica

La digitalización no puede ser efectiva si no se cuenta con una infraestructura tecnológica adecuada. Esta debe contemplar equipos actualizados, sistemas integrados como ERP o Gestión de Relaciones con Clientes (CRM) y una arquitectura de red segura. Según Llorente y Cuenca (2020), una infraestructura resiliente es la base para garantizar la escalabilidad de los procesos y la sostenibilidad de la transformación digital.

5.2. Capacitación continua del talento humano

El éxito de cualquier iniciativa digital depende en gran medida de las personas. La resistencia al cambio es uno de los obstáculos más frecuentes en procesos de digitalización. Por ello, se debe capacitar continuamente al personal no solo en el uso de nuevas herramientas, sino también en la comprensión de los riesgos asociados.

Un ejemplo destacado es el caso de Habi, una plataforma tecnológica colombiana del sector inmobiliario que opera bajo el modelo Proptech. Esta empresa permite la compra y venta de inmuebles de forma totalmente digital, diferenciándose de las inmobiliarias tradicionales. Para implementar este modelo, Habi ha desarrollado un entorno digital basado en el análisis de datos, automatización de procesos y atención virtual al cliente.

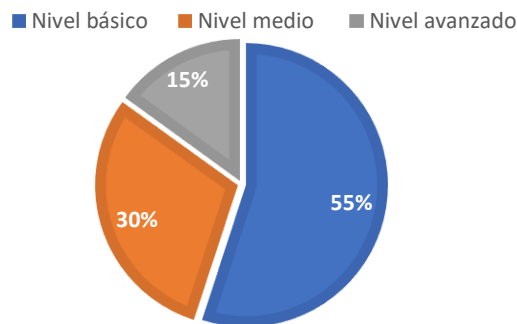
La adopción efectiva de esta tecnología fue posible gracias a la formación digital continua de su personal, que facilitó no solo la apropiación de nuevas herramientas tecnológicas, sino también la adaptación cultural hacia una lógica de trabajo más ágil y orientada a la innovación. Este tipo de capacitación es clave para garantizar que las transformaciones tecnológicas no se conviertan en barreras, sino en oportunidades de crecimiento sostenible.

Como se observa en la Figura 4 se presenta una visualización que ilustra la distribución simulada del nivel de conocimiento en ciberseguridad del personal en PYMES del sector eléctrico.

Figura 4

Nivel de conocimiento en ciberseguridad del personal en PYMES del sector eléctrico

¿CUÁL ES EL NIVEL DE LOS EMPLEADOS EN CIBERSEGURIDAD?



Nota: Datos simulados con fines ilustrativos, basados en tendencias observadas en estudios previos de ciberseguridad en PYMES (ISACA, 2023; WeLiveSecuriy,2024).

Se presenta una distribución porcentual simulada del nivel de conocimiento en ciberseguridad del personal de pequeñas y medianas empresas (PYMES) del sector eléctrico. Se observa que el 55% de los colaboradores posee un conocimiento básico, el 30% se encuentran en nivel medio y únicamente el 15% alcanza un nivel avanzado.

Este resultado evidencia una brecha significativa en la formación técnica del personal, lo que representa un riesgo potencial para la protección de los datos empresariales. La

predominancia de conocimiento básicos sugiere la necesidad de implementar programas de capacitación continua en buenas prácticas de seguridad digital, manejo de contraseñas, prevención de phishing y gestión de dispositivos conectados

5.3. Incorporación de políticas de seguridad de la información

Una transformación digital segura debe incorporar políticas de seguridad basadas en normas internacionales como la ISO/IEC 27001 y 27002. Estas establecen un conjunto de buenas prácticas que permiten gestionar los riesgos de manera sistemática. Según Hirschberger, Smulders y Vars (2018), estas normas ofrecen marcos estructurados para proteger la confidencialidad, integridad y disponibilidad de la información, aspectos críticos para cualquier PYMES que digitaliza sus operaciones.

5.4. Evaluación de riesgos y planes de contingencia

El entorno digital está expuesto a múltiples amenazas. Por ello, en la empresa objeto de estudio se sugiere implementar mecanismos para identificar, analizar y mitigar los riesgos tecnológicos. Entre los más críticos se encuentran incidentes de ciberseguridad, que pueden generar pérdidas económicas significativas debido a la interrupción de las operaciones y la reducción de la productividad.

En el caso de empresa PYMES que se dedica a la venta de materiales eléctricos y proyectos, un incidente informático que comprometa su sistema de ventas o acceso a información técnica de proyectos podría generar pérdidas significativas tanto a nivel operativo

como comercial. A continuación, se presenta una Tabla 6 con ejemplos de pérdidas primarias por productividad, adaptadas a su contexto:

Tabla 6

Perdidas primarias por productividad ante incidentes de ciberseguridad en PYMES

Productividad	Pérdida por reducción de productividad o ingresos
<p>Pérdidas porque la organización no puede operar con normalidad</p>	<p>Pregunta clave: ¿Cuánto tiempo tarda la empresa PYMES en recuperar sus operaciones tras un ataque?</p> <p>Respuesta esperada: Entre 6 y 24 horas (interrupción en el sistema de facturación y seguimiento de proyectos).</p> <p>Datos corporativos: Si la PYMES factura \$300,000 al mes y opera 22 días su facturación diaria es de \$13,636, y por hora (8h/día) \$1,704.</p> <p>Ejemplo de pérdida: 6 horas de inactividad = 6 x \$1,704 = \$10,224 de pérdida estimada.</p>
<p>Pérdidas porque el personal no puede realizar sus tareas normales</p>	<p>Pregunta clave: ¿Cuántos técnicos y personal administrativo quedan improductivos durante el incidente?</p> <p>Ejemplo: 15 técnicos x \$12/hora x 4 hora sin acceso a planos ni ordenes de trabajo = \$720 de pérdida operativa.</p>

Nota: La información presentada en esta tabla ha sido elaborada con base en estimaciones ficticias ajustadas al contexto operativo de PYMES que se dedica a la venta de materiales eléctricos y proyectos.

Como se observa en la tabla anterior, los incidentes de ciberseguridad pueden generar pérdidas económicas importantes, incluso en periodos breves de inactividad. Para las PYMES del sector industrial, donde el cumplimiento de plazos, la ejecución técnica y la atención al cliente dependen de gran medida de sistemas digitales, es imprescindible contar con planes de contingencia efectivos. Estos análisis permiten anticipar escenarios críticos, justificar inversiones en ciberseguridad y promover una cultura organizacional orientada a la prevención y resiliencia digital.

5.5. Síntesis comparativa de modelos de madurez en seguridad

La madurez en la gestión de la seguridad de la información puede evaluarse a través de distintos enfoques que varían en su formalidad, nivel de experiencia y adaptabilidad al contexto de la empresa.

El modelo basado en la norma ISO/IEC 27001 proporciona un marco estructurado y exhaustivo para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI). Este enfoque se caracteriza por su rigurosidad en la identificación de riesgos, definición de controles y establecimiento de procedimientos documentados, siendo altamente recomendado para organizaciones con capacidad de cumplir estándares internacionales y someterse a auditorías externas.

Por otro lado, existen modelos más flexibles orientados a PYMES, como los propuestos por WeLiveSecurity (2024) y RA-MA (2024), que ofrecen estrategias progresivas de adopción de medidas de ciberseguridad. Estos modelos priorizan la capacitación continua, la concientización del personal y la implementación gradual de controles críticos.

A continuación, en la Tabla 7 se presenta una síntesis comparativa entre ambos enfoques:

Tabla 7

Comparación entre el modelo ISO/IEC 27001 y modelos flexibles de ciberseguridad para PYMES

Aspecto	ISO/IEC 27001	Modelos Flexibles para PYMES
Formalidad	Alto (cumplimiento de estándares internacionales y auditorías externas)	Moderada (adopción progresiva sin necesidad de certificaciones)
Costos de implementación	Alto (requerimientos técnicos y humanos significativos)	Bajo a moderado (adecuado a capacidades de la empresa)
Adaptabilidad	Limitada (estructuras rígidas y progresos formales)	Alta (ajuste a recursos y evolución de la empresa)
Requerimiento técnico	Especializado (requiere consultores o personal certificado)	General (personal interno capacitado progresivamente)
Objetivo principal	Cumplimiento normativo y resiliencia total	Protección progresiva y adaptabilidad operativa

Fuente: Elaboración propia basada en Hinschberger, Smulders y Vars (2018); WeLiveSecurity(2024); RA-MA (2024).

6. Gestión del cambio cultural en la transformación digital de las PYMES

La transformación digital implica una reorganización profunda en los procesos, estructuras organizativas y dinámicas de trabajo. En el caso de las pequeñas y medianas empresas PYMES, este proceso requiere de un enfoque particular, ya que suelen tener estructuras menos formales, presupuestos limitados y una cultura organizacional basada en relaciones cercanas. Por lo tanto, gestionar el cambio cultural se convierte en una condición indispensable para la incorporación de tecnología genere un impacto real y sostenible. El verdadero desafío de esta transformación no es solo adoptar nuevas tecnologías, sino modificar la cultura empresarial para hacerla más ágil, colaborativa y orientada al aprendizaje constante (OpenMind, 2019).

La transformación solo puede ser exitosa si se construye una cultura abierta al cambio, donde se valore el aprendizaje continuo, la innovación y la colaboración. Las empresas como las PYMES, donde los procesos tradicionales han regido durante años, gestionar el cambio cultural se vuelve esencial para que las innovaciones tecnológicas realmente generen valor. Sin una transformación de fondo en la forma de pensar y actuar de los colaboradores, cualquier esfuerzo digital corre el riesgo de ser superficial y poco sostenible.

6.1. La resistencia al cambio: causas y consecuencias

Uno de los primeros obstáculos que enfrentan las PYMES al iniciar su transformación digital es la resistencia al cambio. Esta resistencia puede manifestarse de manera explícita, como la negativa a usar nuevas herramientas, o de forma implícita, mediante el desinterés o la inercia frente a los nuevos procesos. Según Proaño Castro (2022), muchas veces esta resistencia

nace del temor a perder el empleo o a sentirse desplazado por no contar con habilidades tecnológicas.

Desde la perspectiva de RobinMath y Mansard en Disrupción digital y reajustes, esta resistencia es natural cuando no hay una visión clara compartida por la organización. Las personas necesitan entender el “porque” y el “para que” del cambio, de lo contrario, tienden a aferrarse a lo que ya conocen, aunque resulte ineficiente (OpenMind, 2019).

Se observa que, esta afirmación es completamente aplicable al contexto de las PYMES ecuatorianas. Si no existe una dirección clara ni una comunicación transparente del propósito del cambio, es fácil que los equipos caigan en la confusión o incluso el desánimo. Sin rumbo definido, todo proceso de innovación corre riesgo de desmoronarse antes de consolidarse.

En el caso de este tipo de empresas, el análisis muestra cómo esta resistencia surge especialmente entre colaboradores con más años en la empresa, quienes se sienten inseguros al usar plataformas digitales o temen cometer errores frente a los nuevos procesos. Esta situación se agrava cuando no hay acompañamiento ni espacios de formación adecuados.

Las consecuencias de no gestionar adecuadamente esta resistencia incluyen:

- Dificultades en la adopción de nuevas tecnologías.
- Baja productividad por falta de alineación.
- Clima laboral tenso o desmotivación.
- Desaprovechamiento de oportunidades de mejora y crecimiento.

6.2. El rol del liderazgo en procesos de transformación

El liderazgo cumple un papel fundamental en cualquier proceso de transformación digital. No basta con invertir en tecnología; es necesario que las personas que lideran la organización impulsen el cambio desde el ejemplo, la visión y la cercanía con sus equipos.

En el contexto de las PYMES, donde muchas decisiones se concentran en los fundadores o en un grupo directivo reducido, el compromiso de estos líderes es determinante para el éxito o fracaso de la digitalización.

Los líderes no imponen cambios, sino que inspiran, acompañan y construyen confianza en el proceso (OpenMind, 2019). Según los resultados, el liderazgo efectivo debe ser cercano y coherente. No se puede pedir al equipo que adopte nuevas tecnologías si quienes lideran no están dispuestos a usarlas o capacitarse también.

En el caso particular de las empresas de venta de materiales y proyectos, los resultados evidencian que cuando la dirección se involucra activamente en la implementación de nuevas herramientas, el equipo responde con mayor apertura y compromiso. En cambio, cuando el cambio parece venir impuesto o sin justificación clara, se genera desconfianza.

Los líderes tienen la responsabilidad de comunicar una visión clara compartida, explicar el impacto positivo de la digitalización y, sobre todo, escuchar las inquietudes del equipo. Además, deben facilitar el proceso de formación y brindar apoyo emocional y técnico durante la transición. La empatía y la capacidad de adaptación se convierten en cualidades clave en este tipo de entornos.

6.3. Liderazgo y seguridad de la información: una visión estratégica desde la cultura organizacional

Uno de los elementos más sensibles de la transformación digital de las PYMES es la forma en que se gestiona la seguridad de la información desde el liderazgo. No se trata únicamente de implementar soluciones tecnológicas, sino asumir la protección de datos como una responsabilidad estratégica y cultural.

Es fundamental reconocer que los líderes no solo deben impulsar la adopción tecnológica, sino también fomentar comportamientos seguros en toda la organización.

Respalda lo planteado por Hirschberger, Smulders y Vars (2018), quienes afirman que la seguridad de información debe estar alineada con las normas internacionales ISO/IEC 27001 y 27002, pero también integrada en los valores institucionales. No basta con definir controles técnicos, debe existir un liderazgo que promueva la conciencia colectiva sobre los riesgos asociados al mal uso de datos.

Un aspecto que se determina crítico es lo que ocurre después de la contratación. Muchas veces se piensa que el riesgo termina con la firma del contrato, cuando en realidad comienza un proceso que implica responsabilidad, supervisión y educación continua. En 2016, la Revista Electrónica de Sistemas de la Información y Gestión Tecnológica publicó una encuesta que señalaba que los incidentes más frecuentes de seguridad estaban relacionados con empleados y antiguos empleados.

Este hallazgo es consistente con las personas internas representan tanto el principal activo como la mayor vulnerabilidad en la protección de datos.

Asimismo, en el caso específico de las PYMES del sector de venta de materiales eléctricos y ejecución de proyectos, donde es habitual la contratación de prestadores de servicios, se considera necesario aplicar los mismos criterios de seguridad que se utilizan para el personal directo.

La gestión de terceros mediante cláusulas contractuales, restricciones de acceso, formación básica en seguridad de información y seguimiento de cumplimiento.

De esta forma, se evita la exposición innecesaria de información crítica que puede comprometer la operación en la organización.

Por tanto, el liderazgo organizacional debe asumir la seguridad de los datos como una responsabilidad estratégica, fomentando una cultura preventiva, desarrollando procesos internos sólidos y promoviendo la participación de todos los colaboradores.

La transformación digital, para ser sostenible, requiere una base segura sobre la cual puedan construirse los nuevos modelos operativos y de negocio.

7. Resultados del estudio

7.1. Resultados cuantitativos clave

A continuación, se presentan los principales resultados obtenidos mediante la aplicación de encuestas y entrevistas en una PYMES del sector eléctrico en Ecuador, respetando el principio de anonimato.

La Tabla 8 resume los hallazgos más relevantes relacionados con el nivel de conocimiento en ciberseguridad, el uso de herramientas de protección de datos y la percepción de riesgo dentro de la organización.

Tabla 8

Resumen de resultados cuantitativos sobre ciberseguridad de PYMES del sector eléctrico

Variable Evaluada	Resultado (%)
Nivel básico de conocimiento en ciberseguridad	55%
Nivel medio de conocimiento en ciberseguridad	30%
Nivel avanzado de conocimiento en ciberseguridad	15%
Uso de autenticación multifactor	45%
Implementación de respaldos periódicos	60%
Percepción de riesgos alto ante amenazas cibernéticas	70%

Nota. Datos elaborados con base en la encuesta aplicada en una PYME del sector eléctrico ecuatoriano (2025).

Estos resultados muestran que, si bien existe prácticas básicas de protección de datos, la mayoría del personal posee únicamente conocimientos básicos en ciberseguridad. Lo cual representa una vulnerabilidad significativa para la organización.

7.2. Análisis comparativo con estudios latinoamericanos

Los hallazgos son consistentes con otros estudios realizados en la región:

- Gómez y Perea (2021) evidenciaron que el 62% de las PYMES manufactureras en Colombia no contaban con políticas formales de ciberseguridad, reflejando una cultura organizacional débil en la protección de datos.
- Torres y Ramirez (2022) reportaron que solo el 40% de las pequeñas empresas tecnológicas en Perú implementaban medidas básicas como autenticación multifactor o respaldos de seguridad.

Estos resultados reafirman que las PYMES latinoamericanas, independientemente del sector, enfrentan desafíos similares: escasa capacitación en ciberseguridad, limitada percepción de riesgos y dependencia tecnológica sin estrategias sólidas de contingencia.

Según Gartner (2023), el mercado global de ciberseguridad superará los 200.000 millones de dólares para 2026, impulsado por el crecimiento acelerado de amenazas cibernéticas y la necesidad de cumplimiento normativo, un dato que refuerza la importancia estratégica de implementar políticas de seguridad en pequeñas y medianas empresas.

En este sentido, los resultados obtenidos en la empresa ecuatoriana estudiada reflejan una realidad más amplia, la transformación digital debe ir acompañada de una estrategia robusta de ciberseguridad para ser sostenible y efectiva.

8. Consideraciones Finales

Este estudio tuvo objetivo proponer una estrategia de seguridad de datos que facilite la transformación digital en las pequeñas y medianas empresas (PYMES) del sector de venta de materiales eléctricos y ejecución de proyectos industriales.

Se encontró que, A través del estudio exploratorio realizado en una empresa real del sector, se logró identificar las principales brechas en cultura organizacional, gestión de la información y liderazgo, permitiendo el diseño de estrategias prácticas que fortalecen la ciberseguridad y promueven una transformación digital segura y sostenible.

Asimismo, se evidenció una percepción elevada de riesgos de ciberseguridad, una adopción parcial de medidas de protección (como la autenticación multifactor y los respaldos periódicos), y una resistencia significativa al cambio frente a procesos de transformación digital.

Por lo tanto, se concluye que, aunque existen iniciativas aisladas en materia de seguridad de la información, es necesario fortalecer la cultura organizacional, estructurar políticas formales de protección de datos, y consolidar estrategias de madurez digital. Estos aspectos son fundamentales para las PYMES logren una transformación digital segura y sostenible, en consonancia con los estándares internacionales y las mejores prácticas recientes adaptadas a su realidad.

De acuerdo con los hallazgos obtenidos:

- Existencia de una baja madurez en el conocimiento de ciberseguridad del personal, donde el 55% posee solo conocimientos básicos.
- Implementación parcial de prácticas de protección de datos, como respaldos periódicos y control de acceso, pero ausencia de políticas formales estructuradas.
- Resistencia al cambio entre colaboradores con más años en la empresa, derivada de temores a la tecnología y falta de acompañamiento.
- Importancia crítica del liderazgo para impulsar procesos de transformación digital exitosos en las PYMES.
- Necesidades de integrar la gestión de la seguridad de la información como un componente estratégico, no solo técnico.

Estos hallazgos fueron consistentes con estudios regionales en Colombia y Perú, que evidencian desafíos similares en otras PYMES latinoamericanas.

Las principales limitaciones del estudio se relacionan con el enfoque metodológico adoptado, basado en un único caso de estudio, lo que restringe la posibilidad de generalizar los resultados a otras empresas o sectores de manera estadística. No obstante, los hallazgos aportan una visión profunda del fenómeno estudiado y pueden ser considerados como referencia para organizaciones con características similares.

El análisis se basó en datos auto-reportados por los colaboradores, lo que puede introducir sesgos de percepción. El estudio se enfocó al sector eléctrico e industrial, por lo que las estrategias propuestas podrían requerir adaptaciones en otros contextos. A futuro, sería pertinente realizar investigaciones adicionales en distintas regiones y sectores para validar y enriquecer los resultados obtenidos.

A partir de resultados obtenidos, se proponen las siguientes acciones para fortalecer la transformación digital segura en las PYMES del sector eléctrico.

- Desarrollar programas continuos de capacitación en ciberseguridad, adaptados a diferentes niveles de conocimiento dentro de la empresa.
- Formalizar políticas de seguridad de la información basadas en estándares internacionales como ISO/IEC 27001, adecuadas a la realidad de las PYMES.
- Promover el liderazgo activo en los procesos de cambio, asegurando que directivos y gerentes lideren con el ejemplo en la adopción de tecnología.
- Implementar evaluaciones periódicas de riesgos digitales, para anticipar vulnerabilidades y reforzar las áreas más críticas.
- Gestionar adecuadamente la seguridad de terceros, incluyendo cláusulas contractuales y capacitaciones básicas en ciberseguridad a proveedores y colaboradores externos.

Estas acciones, sostenidas en el tiempo, contribuirán a fortalecer la resiliencia digital de las organizaciones, optimizando su competitividad y sostenibilidad en un entorno cada vez más digitalizado.

9. Conclusiones

La presente investigación permitió analizar el impacto de la gestión de la seguridad de la información como factor clave para el fortalecimiento de la transformación digital en las pequeñas y medianas empresas (PYMES) del sector eléctrico. A través del diagnóstico aplicado, se evidenció un nivel bajo de madurez en la protección de los activos de información, así como limitaciones en los conocimientos y prácticas de los colaboradores respecto a la ciberseguridad.

Entre los principales hallazgos se identificó la ausencia de políticas formalizadas de seguridad de datos, la aplicación de medidas aisladas y la resistencia al cambio tecnológico, especialmente en los equipos con mayor antigüedad. Estas condiciones limitan la adopción efectiva de herramientas digitales y aumentan la exposición de la organización frente a riesgos cibernéticos.

Se concluye que la incorporación de una estrategia integral de seguridad de la información, basada en estándares internacionales y acompañada de la capacitación continua del personal, es esencial para garantizar la protección de los activos digitales y facilitar la sostenibilidad de los procesos de digitalización. El compromiso del liderazgo y la gestión del cambio cultural son componentes indispensables para avanzar hacia una transformación digital efectiva y segura.

10. Referencias Bibliográficas

Accel-KKR. (2020). *Siigo expande su presencia en LATAM a Ecuador uniendo fuerzas con Contífico, convirtiéndose en el líder del mercado en América Latina.*

Recuperado de <https://www.accel-krk.com/siigo-expande-su-presencia-latam-a-ecuador-uniendo-fuerzas-con-contifico-convirtiendose-en-el-lider-del-mercado-en-america-latina>

Creswell, J. W., & Plano Clark, V. L. (2018). *Diseño y realización de mezclas en la investigación social y de salud.* Ediciones Morata.

Daza, M., Méndez, L., & Rodriguez, A. (2020). Gestion del conocimiento y competitividad de las PYMES en América Latina. *Revista de Estudios Empresariales*, 8(2), 45-60.

ENISA. (2023). *Cybersecurity Culture Guidelines: Behavioral Aspects of Cybersecurity.* European Union Agency for Cybersecurity. <https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines>

Espinoza, L. (2019). La convergencia del mundo físico y digital. En Llorente & Cuenca (Ed.), *La transformación digital* (pp.20-21). LLYC

European Union Agency for Cybersecurity (EINSA). (2023). *Cyberseguridad guidelines for SMEs.* EINSA.

Gartner. (2023). *The Role of the CISO in Small and Medium-Sized Enterprises.* <https://www.gartner.com/en/articles/ciso-in-smes>

Gómez, A., & Perea, L. (2021). Ciberseguridad y protección de datos en PYMES del sector manufacturero colombiano. *Revista Colombia de Tecnologías*, 17(1), 22-35.

Habi. (2024). *Compra de venta de vivienda de forma fácil, segura y 100% digital*.
<https://www.habi.co>

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2021). *Metodología de la investigación* (7a ed.). McGraw-Hill.

Hinschberger, P., Smulders, R., & Vars, D. (2018). *Fundamentos de la Seguridad de la información con base en ISO 27001 y 27002*. Alfaomega.

ISACA. (2023). *State of Cybersecurity 2023: Global Update on Workforce Efforts, Resources and Cyberoperations*. <https://www.isaca.org/resources/state-of-cybersecurity>

Llorente & Cuenca. (2019). *La transformación digital*. LLYC.

Montero Martínez, R., Martínez Oropesa, C. (2022). *Seguridad I vs Seguridad II: y el aporte de los procesos de gestión de la seguridad basada en los comportamientos en la mejora de la cultura de la seguridad*. Ediciones de la U.
<https://ebooks7-24.com:443/?il=19625>

Municipio de Quito. (2022, abril 26). *Concejo conoció informe del ataque cibernético a la plataforma tecnológica del Municipio de Quito*. Quito Informa.
<https://www.quitoinforma.gob.ec/concejo-conocio-informe-del-ataque-cibernetico/>

OpenMind. (2019). *Reinventar la empresa en la era digital*. BBVA OpenMind.
<https://www.bbvaopenmind.com>

Peralta Zúñiga, M. L., & Aguilar Valarezo, D. N. (2021). *La ciberseguridad y su concepción en las PYMES de Cuenca, Ecuador*. *Revista Contabilidad y Auditoría*, 27(53), 99-114. Recuperado de
<https://dspace.ucuenca.edu.ec/handle/123456789/38290>

Pérez Escutia, N. G., & Fischer de la Vega, L. (2023). *La transformación digital como ventaja competitiva de las PYMES mexicanas*. *Revista de Estrategia Empresarial*, 12(1), 31-47.

Proaño Castro, M.F. (2022). Los sistemas de información y su importancia en la transformación digital en la empresa actual. *Revista Espacios*, 43(25), 130-145.

RA-MA. (2024). *Ciberseguridad y protección digital en PYMES*. Madrid: Editorial RA-MA. <https://www.ra-ma.es/libros/ciberseguridad-pymes-2024>

Revista Electronica de Sistemas de la Información y Gestión Tecnológica. (2016). *Estudio sobre incidentes de la seguridad vinculadas al personal interno*.

RobinMath, R., & Mansard, J. (2019). Disrupción digital y reajustes: Imaginar nuevas vías. En OpenMind, *Reinventar la empresa en la era digital* (pp.50-67). BBVA OpenMind

Rodriguez, J. (2019). Prepararse para la revolución. En Llorente & Cuenca (Ed.), *La transformación digital* (pp. 16-17). LLYC.

Sevillano Jaén, F., Beltrán Pardo, M.(2021). *Dirección de seguridad y gestión del ciberriesgo*. Ediciones de la U. <https://ebooks7-24.com:443/?il=17572>

Taherdoost, H. (2016). Validity and Reliability of the Research Instrument; How to test the Validation of a Questionnaire/Survey in a Researc. *International Journal of Academic Reserarch in Management (IJARM)*, 5(3), 28-36.

Team R Core. (2021). *R: A language and environment for statistical computing*. R Foundation for Statistical Computing. <https://www.R-project.org/>

Torres, J., & Ramirez, M.(2022). Brechas de ciberseguridad en pequeñas empresas del sector tecnologico en Lima Metropolitana. *Revista Peruana de Innovación y Tecnología*, 9(3), 60-75.

Uribe Macías, M. E. (2021). *Administración estratégica*. Ediciones de la U. <https://ebooks7-24.com:443/?il=15770>

WeLiveSecurity.(2024). Estado de la ciberseguridad en América Latina. <https://www.welivesecurity.com/es/cibercrimen/incidentes-ciberseguridad-2024-america-latina/>

Westerman, G., Tannou, M., Bonnet, D., & Ferraris, P. (2020). *Seizing the Digital Opportunity: A Playbook for Digital Tranformation*. Mt Center for Digital Business.

Westerman, G, Bonnet, D., & McAfee, A. (2020). *The new elements of digital transformation*. MIT Sloan Management Review.

Yin, R. K. (2018). *Caso study research and applications: Design and methods* (6 ed.). Sage Publications.

11. ANEXO A: Guion de entrevista semiestructurada

11.1 Objetivo del instrumento:

Explorar las percepciones, prácticas y desafíos relacionados con la seguridad de la información y el proceso de transformación digital en las pequeñas y medianas empresas PYMES del sector de venta de materiales eléctricos y ejecución de proyectos industriales.

11.2 Guion de preguntas

1. ¿Cuáles considera que son los principales riesgos relacionados con la seguridad de la información en su empresa?
2. ¿Qué medidas o controles de seguridad de la información se han implementado en la organización?
3. ¿Existen políticas o procedimientos formales para la protección de datos? ¿Cómo se aplican?
4. ¿Ha recibido usted o su equipo alguna capacitación específica en ciberseguridad? ¿Con qué frecuencia?
5. ¿Qué tan involucrada está la alta dirección o el liderazgo de la empresa en los temas de seguridad de la información?
6. ¿Cuáles considera que son las principales barreras o dificultades para avanzar en el proceso de transformación digital dentro de la empresa?
7. ¿Qué recomendaciones haría para fortalecer la seguridad de los datos y avanzar hacia la transformación digital más segura y sostenible?

12. ANEXO B: Cuestionario aplicado (Encuesta)

12.1 Objetivo del instrumento:

Medir el nivel de implementación de prácticas de seguridad de la información, el conocimiento del personal y la percepción de riesgos en la PYMES del sector eléctrico.

12.2 Instrucciones:

Por favor, lea atentamente cada afirmación y seleccione la opción que mejor refleje su nivel de acuerdo, utilizando la siguiente escala:

A continuación, Tabla 9 se presenta la escala de valoración utilizada en el cuestionario aplicado, diseñada bajo el formato de tipo Likert de cinco puntos, con el propósito de medir el nivel de acuerdo de los participantes respecto a las afirmaciones planteadas (Hernandez et al., 2021).

Tabla 9

Escala de valoración

Valor	Descripción
1	Totalmente en desacuerdo
2	En desacuerdo
3	Ni de acuerdo ni en desacuerdo
4	De acuerdo
5	Totalmente de acuerdo

Nota. Escala tipo Likert de 5 puntos empleada para medir la percepción sobre las prácticas de seguridad de la información y la transformación digital. Elaboración propia.

La Tabla 10 presenta las afirmaciones incluidas en el cuestionario aplicado a los colaboradores de la empresa objeto de estudio. Estas afirmaciones buscan evaluar la implementación de medidas de seguridad de la información, el nivel de conocimiento en ciberseguridad y la percepción de riesgo asociados a la transformación digital.

Tabla 10

Cuestionario aplicado para evaluar la seguridad de la información y transformación digital en PYMES

Ítems	Afirmación	1	2	3	4	5
1	En la empresa existen políticas formales para la protección de la información					
2	Se realizan respaldos periódicos de los datos críticos de la organización					
3	La empresa utiliza Autenticación Multifactor (MFA) en sus sistemas					
4	El personal cuenta con formación en ciberseguridad adecuada para sus funciones					
5	Se aplica controles de acceso para limitar el uso de la información solo al personal autorizado.					
6	La dirección de la empresa impulsa activamente la transformación digital					
7	Percibo que la empresa esta expuesta a riesgos cibernéticos significativos					

Nota: Escala de respuestas, elaboración propia