



Universidad Nacional Mayor de San Marcos

Universidad del Perú. Decana de América

Dirección General de Estudios de Posgrado

Facultad de Ingeniería de Sistemas e Informática

Unidad de Posgrado

**Modelo basado en la Norma ISO 27001:2022 y PCI DSS para
la gestión de seguridad de la información en Pymes del sector
textil, Lima 2024**

TESIS

Para optar el Grado Académico de Magíster en Ingeniería de
Sistemas e Informática con mención en Gestión de Tecnología de
Información y Comunicaciones

AUTOR

Shonerly BUSTAMANTE GARCIA

ASESOR

Dr. Pedro Segundo CASTAÑEDA VARGAS

Lima, Perú

2026



Reconocimiento - No Comercial - Compartir Igual - Sin restricciones adicionales

<https://creativecommons.org/licenses/by-nc-sa/4.0/>

Usted puede distribuir, remezclar, retocar, y crear a partir del documento original de modo no comercial, siempre y cuando se dé crédito al autor del documento y se licencien las nuevas creaciones bajo las mismas condiciones. No se permite aplicar términos legales o medidas tecnológicas que restrinjan legalmente a otros a hacer cualquier cosa que permita esta licencia.

Referencia bibliográfica

Bustamante, S. (2026). *Modelo basado en la Norma ISO 27001:2022 y PCI DSS para la gestión de seguridad de la información en Pymes del sector textil, Lima 2024*. [Tesis de maestría, Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería de Sistemas e Informática, Unidad de posgrado]. Repositorio institucional Cybertesis UNMSM.

Metadatos complementarios

Datos de autor	
Nombres y apellidos	Shonerly Bustamante Garcia.
Tipo de documento de identidad	DNI
Número de documento de identidad	72222375
URL de ORCID	https://orcid.org/0000-0002-8173-203X
Datos de asesor	
Nombres y apellidos	Dr. Pedro Segundo Castañeda Vargas.
Tipo de documento de identidad	DNI
Número de documento de identidad	10744358
URL de ORCID	https://orcid.org/0000-0003-1865-1293
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	Mg. William Martín Enriquez Maguiña.
Tipo de documento	DNI
Número de documento de identidad	06179457
Miembro del jurado 1	
Nombres y apellidos	Mg. Carlos Ernesto Chavez Herrera.
Tipo de documento	DNI
Número de documento de identidad	40788722
Miembro del jurado 2	
Nombres y apellidos	Mg. César Augusto Angulo Calderón.
Tipo de documento	DNI
Número de documento de identidad	32907109
Datos de investigación	

Línea de investigación	No aplica
Grupo de investigación	No aplica
Agencia de financiamiento	Sin financiamiento
Ubicación geográfica de la investigación	País: Perú Departamento: Lima Provincia: Lima Distrito: Lurín Latitud: -12.25526 Longitud: -76.88507
Año o rango de años en que se realizó la investigación	2023 – 2024
URL de disciplinas OCDE	Ingeniería de sistemas y comunicaciones https://purl.org/pe-repo/ocde/ford#2.02.04



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
Universidad del Perú, Decana de América
Facultad de Ingeniería de Sistemas e Informática
Vicedecanato de Investigación y Posgrado
Unidad de Posgrado

**ACTA DE SUSTENTACIÓN DE TESIS PARA OPTAR EL GRADO ACADÉMICO DE
MAGÍSTER EN INGENIERÍA DE SISTEMAS E INFORMÁTICA CON MENCIÓN EN
GESTIÓN DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES**

A los veinte (20) días del mes de enero de 2026, siendo las 12:00 pm., se reunieron en el Auditorio Alfredo Celso Alva Bravo, el Jurado de Tesis conformado por los siguientes docentes:

Mg. William Martín Enriquez Maguiña (Presidente)
Mg. Carlos Ernesto Chavez Herrera (Miembro)
Mg. César Augusto Angulo Calderón (Miembro)
Dr. Pedro Segundo Castañeda Vargas (Miembro Asesor)

Se inició la Sustentación invitando al candidato a Magíster **Shonerly Bustamante Garcia**, para que realice la exposición oral de la tesis para optar el Grado Académico de Magíster en Ingeniería de Sistemas e Informática con mención en Gestión de Tecnología de Información y Comunicaciones, siendo la Tesis intitulada:

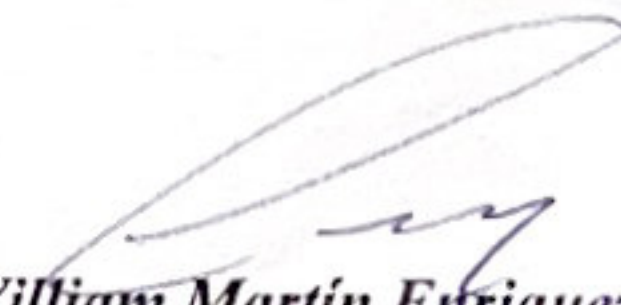
**“MODELO BASADO EN LA NORMA ISO 27001:2022 Y PCI DSS PARA LA GESTIÓN DE
SEGURIDAD DE LA INFORMACIÓN EN PYMES DEL SECTOR TEXTIL, LIMA 2024”**

Concluida la exposición, los miembros del Jurado de Tesis procedieron a formular sus preguntas que fueron absueltas por el graduando; acto seguido se procedió a la evaluación correspondiente, habiendo obtenido la siguiente calificación:

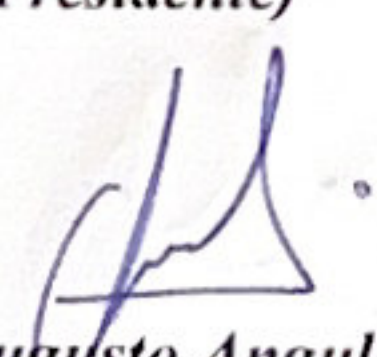
..... DIECISEIS (16) BUENO

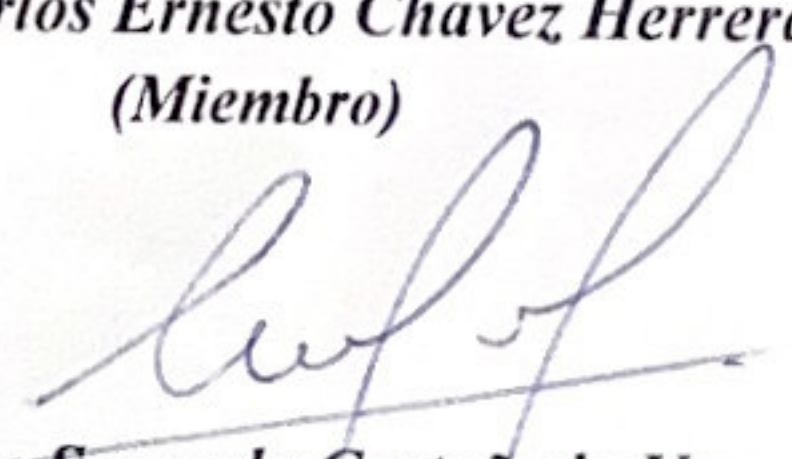
Por tanto, el presidente del Jurado, de acuerdo con el Reglamento General de Estudios de Posgrado, otorga al Bachiller **SHONERLY BUSTAMANTE GARCIA** el Grado Académico de Magíster en Ingeniería de Sistemas e Informática con mención en Gestión de Tecnología de Información y Comunicaciones.

Siendo las ...1:15... horas, el presidente del Jurado de Tesis, da por concluido el acto académico de Sustentación de Tesis.


Mg. William Martín Enriquez Maguiña
(Presidente)


Mg. Carlos Ernesto Chavez Herrera
(Miembro)


Mg. César Augusto Angulo Calderón
(Miembro)


Dr. Pedro Segundo Castañeda Vargas
(Miembro Asesor)



CERTIFICADO DE SIMILITUD

Yo, Pedro Segundo Castañeda Vargas en mi condición de asesor acreditado con Dictamen N° 000496-2024-UPG-VDIP-FISI/UNMSM de la tesis, cuyo título es **MODELO BASADO EN LA NORMA ISO 27001:2022 Y PCI DSS PARA LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN PYMES DEL SECTOR TEXTIL, LIMA 2024**, presentado por el egresado SHONERLY BUSTAMANTE GARCÍA para optar el grado Académico de Magíster en Ingeniería de Sistemas e Informática con mención en Gestión de Tecnología de Información y Comunicaciones,

CERTIFICO que se ha cumplido con lo establecido en la Directiva de Originalidad y de Similitud de Trabajos Académicos, de Investigación y Producción Intelectual. Según la revisión, análisis y evaluación mediante la plataforma PIDS, el documento evaluado cuenta con el 9 % de similitud, nivel **PERMITIDO** para continuar con los trámites correspondientes y para su **publicación en el repositorio institucional**.

Se emite el presente certificado en cumplimiento de lo establecido en las normas vigentes, como uno de los requisitos para la obtención del grado/ título/ especialidad correspondiente.

Lima, 08 de octubre de 2025

Firma del Asesor

Nombres y Apellidos del asesor: Pedro Segundo Castañeda Vargas

DNI: 10744358

Dedicatoria

A mis padres, quienes, con su amor incondicional, esfuerzo y ejemplo me enseñaron el valor del trabajo, la constancia y la honestidad. A mi familia, por su apoyo permanente y palabras de aliento en cada etapa de este proceso.

Agradecimientos

Expreso mi más profundo agradecimiento a Dios, por brindarme salud, fortaleza y sabiduría durante el desarrollo de esta investigación.

A la Universidad Nacional Mayor de San Marcos por la formación recibida y las oportunidades de crecimiento profesional.

A mi asesor el Dr. Pedro Segundo Castañeda Vargas, por su guía académica, exigencia y apoyo constante, que permitieron enriquecer el rigor y la calidad de este trabajo.

Índice general

Índice general	4
Lista de cuadros.....	5
Lista de figuras.....	6
CAPÍTULO 1: INTRODUCCIÓN	9
1.1. Situación problemática	9
1.2. Formulación del Problema	13
1.3. Justificación de la investigación.....	14
1.4. Objetivos de la investigación	15
CAPÍTULO 2: MARCO TEÓRICO.....	17
2.1. Marco filosófico o epistemológico de la investigación	17
2.2. Antecedentes del problema	18
2.3. Bases teóricas	22
2.4. Marcos conceptuales o glosario	39
CAPÍTULO 3: METODOLOGÍA.....	41
3.1. Tipo y diseño de investigación.....	41
3.2. Unidad de análisis	43
3.3. Población de estudio	43
3.4. Tamaño de muestra.....	43
3.5. Selección de la muestra.	44
3.6. Técnicas e instrumentos de recolección de datos	44
CAPÍTULO 4: RESULTADOS Y DISCUSIÓN.....	47
4.3. Análisis, interpretación y discusión de resultados.	47
2.3. Pruebas de hipótesis.	54
2.4. Discusiones.	62
CAPÍTULO 5: IMPACTOS.....	65
5.1. Propuesta para la solución del problema.....	65
5.2. Costos de la implementación de la propuesta.	90
5.3. Beneficios que aporta la propuesta.	91
CONCLUSIONES	91
RECOMENDACIONES.....	94
REFERENCIAS BIBLIOGRÁFICAS.....	96
ANEXOS.....	106

Lista de cuadros

Cuadro 1: <i>Personas afectadas según el origen del incidente</i>	10
Cuadro 2: <i>Principios y requisitos PCI DSS</i>	26
Cuadro 3: <i>Estándares y marcos de referencia</i>	37
Cuadro 4: <i>Validación de experto</i>	45
Cuadro 5: <i>Fiabilidad según Alfa de Cronbach</i>	46
Cuadro 6: <i>Representación sociodemográfica de la población</i>	47
Cuadro 7: <i>Distribución de frecuencia de la dimensión confidencialidad</i>	48
Cuadro 8: <i>Distribución de frecuencia de la dimensión integridad</i>	49
Cuadro 9: <i>Distribución de frecuencia de la dimensión disponibilidad</i>	50
Cuadro 10: <i>Representación sociodemográfica de la muestra de estudio</i>	51
Cuadro 11: <i>Resumen de medidas en las diferentes etapas</i>	52
Cuadro 12: <i>Prueba t para muestras relacionadas del pre y pos test</i>	56
Cuadro 13: <i>Prueba t de confidencialidad del pre y post test</i>	58
Cuadro 14: <i>Prueba t de integridad del pre y post test</i>	59
Cuadro 15: <i>Prueba t de disponibilidad del pre y post test</i>	61
Cuadro 16: <i>Plantilla para la lista de activos de información</i>	71
Cuadro 17: <i>Criterios para la evaluación</i>	72
Cuadro 18: <i>Nivel de criticidad de los activos</i>	73
Cuadro 19: <i>Lista de activos críticos</i>	74
Cuadro 20: <i>Matriz de calor</i>	75
Cuadro 21: <i>Matriz de riesgos</i>	76
Cuadro 22: <i>Criterios de aceptación</i>	78
Cuadro 23: <i>Riesgos con mayor impacto</i>	79
Cuadro 24: <i>Políticas de seguridad basadas en ISO 27001: 2022 y PCI DSS</i>	79
Cuadro 25: <i>Capacitaciones según su desempeño</i>	83
Cuadro 26: <i>Matriz de cumplimiento de políticas</i>	85
Cuadro 27: <i>Relación de políticas implementadas</i>	86

Lista de figuras

Figura 1: Categoría de ISO 27001:2022	24
Figura 2: <i>Ciclo PCDC o ciclo de DEMING</i>	24
Figura 3: <i>Proceso de pago</i>	28
Figura 4: <i>Procesos de gestión de riesgo de seguridad de la información</i>	29
Figura 5: <i>Triángulo de la información</i>	34
Figura 6: <i>Factores de seguridad de la información</i>	35
Figura 7: <i>Comparación de las diferentes pruebas</i>	53
Figura 8: <i>Representación gráfica del modelo</i>	65
Figura 9: <i>Organigrama para las pymes</i>	67
Figura 10: <i>Proceso de fase diagnóstica</i>	69
Figura 11: <i>Proceso de planificación</i>	74
Figura 12: <i>Proceso de ejecución</i>	82
Figura 13: <i>Proceso de supervisión</i>	84

RESUMEN

En la actualidad, las pymes textiles peruanas buscan incrementar su competitividad mediante la incorporación de tecnologías en sus procesos operativos; no obstante, esta transformación digital incrementa de manera considerable su exposición a amenazas y ciberataques, donde la carencia de infraestructura tecnológica robusta y de una gestión adecuada de protocolos de seguridad convierte a estas organizaciones en entornos altamente vulnerables. En este contexto, la presente investigación tuvo como finalidad determinar el grado de mejora del modelo basado en la Norma ISO 27001:2022 y PCI DSS sobre la gestión de seguridad de la información en las Pymes de la industria textil, Lima 2024. El estudio se enmarcó en un diseño pre-experimental con una muestra de 20 trabajadores, a quienes se aplicó un cuestionario en tres momentos distintos para identificar en qué medida el modelo mejora la seguridad de la información.

El análisis estadístico de las dimensiones claves como confidencialidad, integridad y disponibilidad reveló mejoras altamente significativas ($p < .001$), reflejadas en controles de acceso más estrictos, disminución del riesgo de divulgación no autorizada y disponibilidad confiable y oportuna de la información para usuarios autorizados. En síntesis, los resultados evidencian que la implementación del modelo no solo optimiza la eficacia en la protección de datos, sino que también produce cambios estructurales y sostenibles, reduce brechas iniciales y fomenta una cultura organizacional orientada a la seguridad de la información. Este estudio representa un aporte relevante para la gestión de riesgos en pymes textiles, ofrece un marco replicable en sectores con características afines y refuerza la gobernanza de la información como un recurso estratégico.

Palabras claves: Seguridad de la información, pymes textiles, gestión de riesgos, seguridad informática, políticas de seguridad.

ABSTRACT

Currently, Peruvian textile SMEs seek to increase their competitiveness by incorporating technologies into their operational processes. However, this digital transformation significantly increases their exposure to threats and cyberattacks. The lack of a robust technological infrastructure and adequate management of security protocols makes these organizations highly vulnerable. In this context, the purpose of this research was to determine the degree of improvement achieved by the model based on ISO 27001:2022 and PCI DSS for information security management in SMEs in the textile sector, Lima 2024. The study was framed within a pre-experimental design with a sample of 20 workers, who were administered a questionnaire at three different times to identify the extent to which the model improves information security.

Statistical analysis of key dimensions such as confidentiality, integrity, and availability revealed highly significant improvements ($p < .001$), reflected in stricter access controls, a reduced risk of unauthorized disclosure, and reliable and timely availability of information to authorized users. In summary, the results show that the implementation of the model not only optimizes the effectiveness of data protection but also produces structural and sustainable changes, reduces initial gaps, and fosters an organizational culture oriented toward information security. This study represents a relevant contribution to risk management in textile SMEs, offers a replicable framework in sectors with similar characteristics, and strengthens information governance as a strategic resource.

Keywords: Information security, textile SMEs, risk management, computer security, security policies.

CAPÍTULO 1: INTRODUCCIÓN

1.1. Situación problemática

En los tiempos recientes, la tecnología ha transformado significativamente nuestra sociedad, simplificando actividades diarias como el envío de archivos, las operaciones bancarias y la petición de diferentes servicios. Además, con la llegada de la pandemia de COVID-19, la tecnología se ha vuelto esencial en ámbitos como la educación, el empleo y el comercio, actuando como un medio para la transmisión veloz, eficaz y de calidad de la información (Bernate y Fonseca, 2023).

Silva-Giraldo et al. (2023) indican que la información juega un papel crucial en el éxito de las empresas; razón por la que se están creando plataformas tecnológicas innovadoras con sólidas medidas de seguridad buscando minimizar los riesgos informáticos y apoyar el crecimiento sostenible. En este sentido, Lee et al. (2023) argumentan que el uso de tecnologías y procedimientos seguros promueve la estabilidad laboral y el bienestar social, al ser resilientes y adaptarse con agilidad a los retos emergentes.

Además, el auge de la tecnología ha brindado bienestar en la vida de las personas, las mismas que son utilizadas como medio de almacenamiento y gestión de la información en muchas organizaciones; sin embargo, en paralelo a estos avances, se han desarrollado numerosos comportamientos fraudulentos y plataformas que permiten a los delincuentes informáticos llevar a cabo sus actividades delictivas, estas prácticas maliciosas han dado lugar a considerables pérdidas económicas y de información (Zhang y Dong, 2023).

En la actualidad, tanto gobiernos como empresas están incrementando sus demandas en cuanto a la implementación de estándares de seguridad; pues de acuerdo con una encuesta reciente llevada a cabo por Gartner, se observa que el 75 % de las organizaciones buscan activamente la consolidación de proveedores de seguridad en 2022, lo que marca un aumento significativo con respecto al 29 % en 2020, este aumento se atribuye a la creciente necesidad de garantizar una integración segura y la compatibilidad de los sistemas de Tecnologías de la Información y

Comunicación (TIC), esto en respuesta al rápido crecimiento de dispositivos IoT, sistemas ciberfísicos y sistemas integrados controlados por algoritmos (Djebbar y Nordstrom, 2023).

En una publicación realizada por IBM en el 2020 a organizaciones alemanas, informó que la pérdida producto de ataques informáticos a empresas con menos de 500 empleados superaban el promedio global de USD 3,86 millones y USD 2,64 millones, mientras que para organizaciones con más de 1,000 empleados, la pérdida promedio era de USD 24.000 millones y USD 462.000 millones, y entre los incidentes ocasionados estaban como daños a la reputación, costos por disputas legales, infracciones de patentes y pérdida de negocios (Skarczinski et al., 2023).

Según la investigación realizada por Tin et al. (2023) se destaca que la alteración de los datos puede ser originada por una diversidad de factores y por actos con intención maliciosa. Entre los aspectos más frecuentes se encuentran los errores derivados de la intervención humana, deficiencias en el tratamiento de la información y vulnerabilidades en los sistemas informáticos, además los autores presentan un informe que evidencia un aumento significativo en el número de personas afectadas, especialmente debido a la violación de la seguridad de los datos, tal como se detalla a continuación:

Cuadro 1:

Personas afectadas según el origen del incidente

Origen del incidente	Cantidad	Porcentaje	Personas afectadas
Servidores de red	1043	26%	227 686 822
Correo electrónico	965	24%	30 071 008
Papel	677	17%	5 315 442
Otros	460	11%	15 758 977
Ordenador portátil	344	9%	5 662 706
Ordenador de escritorio	308	8%	11 529 003
Registros electrónicos	229	5%	7 260 842

Nota: De “Cyberthreats: A primer for healthcare professionals”, por (Tin et al., 2023)

En el mismo contexto, un informe presentado por Kaspersky (2023) en América Latina, revela que aproximadamente el 25% de las organizaciones han experimentado pérdida de datos debido a diversos tipos de ataques, mientras que un 24% de estas pérdidas fue ocasionado por empleados internos, asimismo, un 18.4% de las organizaciones mencionaron que sus sistemas informáticos fueron objeto de exploración en busca de vulnerabilidades. Además, el informe señala que un 37.7% de las organizaciones expresan preocupación acerca de cómo obtener recursos económicos para implementar tecnología avanzada y mitigar el impacto de los riesgos.

Investigaciones recientes han puesto de manifiesto que la pandemia de la COVID-19 ha sido un factor determinante en el incremento de ataques y amenazas dirigidos hacia diversas organizaciones de distintos sectores, estas amenazas han abarcado desde ataques de ransomware, phishing, y malware, hasta violaciones de correos electrónicos comerciales, fraude en transferencias de fondos, desinformación y perturbación de procesos críticos (Coutinho et al., 2023) .

Kitsios et al. (2023) señalan que el rápido desarrollo de las organizaciones ha elevado el valor estratégico de la información para la toma de decisiones, por lo tanto, se destaca la necesidad imperante de proteger esta información, independientemente de su formato y durante su transmisión, a través de la implementación de estrategias de seguridad sólidas.

Cabe señalar que, en Perú, las Pequeñas y Medianas Empresas (Pymes) tienen un significativo impacto económico, ya que generan empleo para más del 70 % de la población y contribuyen con la mitad del Producto Bruto Interno nacional (Salazar et al., 2022), además, según estudios estadísticos del Banco Central de Reserva del Perú revelaron que las Pymes textiles alcanzaron el 51,17% de su capacidad en promedio para el año 2020 (Calsin et al., 2023). Sin embargo, debido a cuestiones administrativas y limitaciones presupuestales no logran alcanzar niveles óptimos de

competitividad, por lo tanto, resulta crucial asegurar el correcto funcionamiento y la continuidad de sus operaciones, con el propósito de lograr una toma de decisiones eficiente y el cumplimiento de sus objetivos estratégicos (Obiol, 2023).

Además, las pymes de hoy en día tienen como objetivo lograr una producción de servicios automatizada al incorporar tecnología en sus procesos claves para aumentar su competitividad en términos de tiempo, coste y calidad. Sin embargo, esta transición conlleva un aumento en las amenazas y ataques informáticos, lo que representa desafíos significativos que ponen en riesgo su éxito, donde la falta de una infraestructura tecnológica sólida y un manejo adecuado de protocolos de seguridad hacen que las PYMES sean especialmente vulnerables ante estas amenazas (Rodríguez-Baca et al., 2023).

De acuerdo con Bandari (2023), la formación deficiente, la supervisión constante y estrategias efectivas para responder a incidentes incrementa significativamente la vulnerabilidad de las Pymes ante potenciales brechas de seguridad y consecuentes perjuicios económicos, dada la magnitud de los retos que usualmente enfrentan en la protección de sus datos.

En tanto, Alraja et al. (2023), señala que una gran proporción de la pérdida o filtración de información se produce como resultado del incumplimiento de los mecanismos de seguridad, esto puede atribuirse a la carencia de un personal debidamente capacitado y comprometido en la mitigación de posibles ataques, y además, debido al incumplimiento frecuente de las directrices de seguridad, lo que genera una situación desafiante para los recursos de la organización y la exposición de vulnerabilidades en sus sistemas informáticos.

Dada la complicada y compleja situación mencionada previamente, es de suma importancia que las pymes textiles pongan énfasis en establecer directrices fundamentales para la seguridad de la información, en aras de mejorar la confiabilidad de la organización, atraer nuevos clientes y se mantener relaciones con los ya existentes, fortaleciendo así la posición competitiva en el entorno empresarial.

Por esta razón, está claro que estándares internacionales como ISO 27001 y PCI DSS ofrecen directrices y medidas de seguridad que posibilitan identificar deficiencias, reducir los costos vinculados a los procedimientos de seguridad de la información, atenuar las repercusiones de los riesgos, y al mismo tiempo, consolidar la confianza con los clientes, este conjunto de acciones contribuye de manera significativa a garantizar el éxito y la continuidad en las operaciones (Al-Khulaidi et al., 2023).

Sin embargo, Chatziamanetoglou y Rantos (2023) mencionan que una de las limitaciones más significativas para llevar a cabo la implementación de controles básicos de seguridad radica en la asignación insuficiente de recursos económicos, esta situación conduce a mantener una infraestructura tecnológica frágil y una comprensión insuficiente sobre cómo llevar a cabo operaciones de defensa, y como consecuencia, los activos de la organización se ven expuestos a riesgos inminentes y considerables.

1.2. Formulación del Problema

1.2.1. Problema general

¿En qué medida el modelo basado en la Norma ISO 27001:2022 y PCI DSS mejora significativamente la gestión de seguridad de la información en Pymes del sector textil, Lima 2024?

1.2.2. Problemas específicos

- ¿En qué medida el modelo basado en la Norma ISO 27001:2022 y PCI DSS mejora significativamente la confidencialidad de la información en las Pymes del sector textil, Lima 2024?
- ¿En qué medida el modelo basado la Norma ISO 27001:2022 y PCI DSS mejora significativamente la integridad de la información en las Pymes del sector textil, Lima 2024?
- ¿En qué medida el modelo basado en la Norma ISO 27001:2022 y PCI DSS mejora significativamente la disponibilidad la información en las Pymes del sector textil, Lima 2024?

1.3. Justificación de la investigación

1.3.1. Justificación teórica

La problemática de las pymes adquiere una mayor relevancia dado que los gastos asociados con la implementación de estándares de seguridad son exorbitantes, representando un obstáculo crítico. Por ende, AL-Dosari y Fetais (2023) afirman que existe la necesidad apremiante de soluciones adaptables, flexibles y económicamente viables, adaptadas a los procesos y requisitos particulares de las pequeñas y medianas empresas; esto implica la creación de marcos y/o modelos regulatorios que gestionen de manera eficiente la seguridad de la información.

La ejecución de medidas de seguridad demanda una planificación metódica y cuidadosa, con el objetivo de evitar la canalización de esfuerzos y recursos hacia áreas que carecen de necesidad. Asimismo, Coloma-Baños et al. (2022) sostienen que, para asegurar la eficacia de las medidas y mecanismos de protección, es esencial que se integren de manera coherente dentro de un sistema o modelo más amplio de gestión de la seguridad de la información.

Considerando el déficit identificado en el contexto problemático que adolece a las pymes del sector textil y la gran importancia que estas significan para el desarrollo del país, se planteó la formulación de un modelo enfocado a la administración de la seguridad de la información, a fin de proporcionar una salvaguardia adecuada y un uso apropiado de los activos de información, establecer una estructura organizativa de seguridad, y asegurar la continuidad de los procesos empresariales; de este modo, se busca garantizar la confidencialidad, integridad y disponibilidad de la información en su entorno operativo.

1.3.2. Justificación práctica

El modelo será de gran importancia para los ejecutivos y/o personal de las pymes, ya que ofrecerá pautas de tratamiento de riesgo, estrategias de acciones correctivas y preventivas y lineamientos básicos para un resguardo eficiente de los datos; para ello, basados en la Norma ISO 27001 y PCI DSS, se intenta:

- Fomentar la confianza del personal al someterse a políticas de seguridad de la información.
- Mejorar la eficacia y la productividad organizacional.
- Asegurar la continuidad operativa ante posibles incidentes de seguridad.
- Elevar el nivel de resiliencia y seguridad en el entorno laboral.
- Estimular el crecimiento económico mediante prácticas seguras y eficientes.
- Contribuir al fortalecimiento de la reputación organizativa como resultado del compromiso con estándares de seguridad informática.

Por otra parte, trabajar alineados a la norma ISO 27001 y conjuntamente con PCI DSS se optimizará el uso de los recursos, incluyendo el tiempo, el personal y los costos operativos, aumentar significativamente la confianza de los clientes y socios comerciales y por sobre todo proporcionar un enfoque holístico y efectivo para la detección, respuesta y mitigación de incidentes.

1.4. Objetivos de la investigación

1.4.1. *Objetivo General*

Determinar el grado de mejora del modelo basado en la Norma ISO 27001:2022 y PCI DSS sobre la gestión de seguridad de la información en las Pymes del sector textil, Lima 2024.

1.4.2. *Objetivos Específicos*

- Determinar el grado de mejora del modelo basado en la Norma ISO 27001:2022 y PCI DSS sobre la confidencialidad de la información en las Pymes del sector textil, Lima 2024.
- Determinar el grado de mejora del modelo basado en la Norma ISO 27001:2022 y PCI DSS sobre la integridad de la información en las Pymes del sector textil, Lima 2024.

- Determinar el grado de mejora del modelo basado en la Norma ISO 27001:2022 y PCI DSS sobre la disponibilidad de la información en las Pymes del sector textil, Lima 2024.

CAPÍTULO 2: MARCO TEÓRICO

2.1. Marco filosófico o epistemológico de la investigación

Resulta esencial, dentro de esta indagación, entender las bases filosóficas que moldearon el camino y el cómo se llevó a cabo la investigación. Aquí, se optó por una perspectiva pragmática que combina elementos tanto del constructivismo como del realismo crítico.

Pragmatismo

En el ámbito de la seguridad de la información, esta perspectiva adquiere una importancia particular, gracias a:

- ***Foco en la resolución de problemas:*** La meta central del estudio consistió en poner en marcha un esquema que facilite a las pequeñas y medianas empresas la gestión de su seguridad informática.
- ***Adaptabilidad en los métodos:*** El pragmatismo hace posible el uso de metodologías combinadas, integrando perspectivas cualitativas y cuantitativas para lograr un entendimiento integral del problema.
- ***Importancia de los resultados:*** La eficacia de las teorías y el modelo sugerido se juzga según su habilidad para solucionar inconvenientes concretos y optimizar la seguridad informática en las pymes.

Constructivismo

Dentro del marco de esta indagación, esta perspectiva se evidencia en:

- ***Ubicación del saber en su entorno:*** La puesta en práctica de normativas como ISO 27001 y PCI DSS cambia según la situación particular de cada pyme. Resulta clave comprender cómo estas ven y viven la seguridad de los datos.
- ***Intervención de los participantes:*** Hacer que los trabajadores y gerentes de las pymes se sumen a la creación y ajuste del modelo

asegura que las respuestas sean importantes y bien recibidas por los usuarios finales.

- ***Flexibilidad del esquema:*** Un esquema constructivista asume que no existe una solución que valga para todos, sino que las prácticas más adecuadas deben ajustarse a las necesidades y condiciones propias de cada pyme.

Realismo Crítico

Plantea la integración de componentes relativos a la presencia de un mundo real, siempre interpretado a través de elementos sociales y culturales. En el presente estudio:

- ***Aceptación de una realidad objetiva:*** Los peligros y puntos débiles en la protección de datos son concretos y tienen efectos palpables para las pequeñas empresas.
- ***Peso de los aspectos sociales:*** La forma en que las pymes manejan la seguridad de la información se ve afectada por factores sociales, culturales y de la propia empresa. Es fundamental estudiar estos factores para crear un esquema eficiente.
- ***Revisión y optimización constante:*** El realismo crítico facilita una valoración continua y una revisión del esquema planteado, modificándolo según nuevos datos y cambios en el contexto de seguridad.

2.2 Antecedentes del problema

En el estudio realizado por Avila (2023), se siguió una metodología bien definida para manejar la seguridad de la información. Esto se hizo poniendo en marcha un sistema diseñado para aplicar medidas de control que cumplieran con la norma ISO/IEC 27001:2013 en la administración local del cantón Naranjal. Como parte de este método, se realizó una encuesta a 55 trabajadores para conocer sus preocupaciones y entender mejor cómo estaban las cosas en ese momento. Para crear y llevar a cabo la propuesta, se utilizó el ciclo PHVA (Planificar, Hacer, Verificar y Actuar). Los resultados mostraron que la información se estaba manejando bien, con menos puntos

débiles y menos ataques a la base de datos, también se redujo el uso incorrecto de las contraseñas para acceder a los sistemas y recursos tecnológicos por parte de los empleados. Todo esto mejoró la seguridad, la disponibilidad y la fiabilidad de los datos, lo que hizo más fácil tomar decisiones.

Alshurideh et al. (2023) llevaron a cabo una investigación con el propósito de discernir el impacto de la seguridad de la información en la cadena de suministro electrónica en la industria de logística y distribución en los Emiratos Árabes Unidos (EAU). Al modelo de investigación propuesto se le aplicó un diseño descriptivo, causal y analítico con técnica de investigación cuantitativa. Para evaluar las variables elaboraron un cuestionario de 30 ítems en una escala tipo Likert de 5 puntos (desde 1, muy en desacuerdo hasta 5, muy de acuerdo) el cual fue aplicado a una muestra de 301 personas de los departamentos gerenciales de 176 empresas de logística y distribución en Dubai y Abu Dhabi. Los resultados obtenidos indicaron que el impacto de la seguridad de la información mostró una correlación positiva con la cadena de suministro electrónica. Como conclusión, los investigadores destacaron que los hallazgos obtenidos constituyen un fundamento robusto para la toma de decisiones estratégicas, respaldada por la implementación clara de políticas de seguridad de la información tanto interna como externamente.

En Ambato – Ecuador, Villarreal (2023) condujo una investigación centrada en cómo introducir un Sistema de Manejo de Datos en una universidad. El objetivo era proteger la información, confirmando que se mantuviera privada, completa y siempre accesible, usando la norma ISO 27001 como guía y el método Magerit para examinar a fondo los peligros relacionados con el manejo de la información. La investigación tomó un camino completo, mirando tanto los números como las cualidades. Se juntaron datos mediante encuestas con preguntas específicas y charlas, formas de ver cómo estaba la seguridad de la información al principio y entender los problemas y pasos para manejar los datos en la universidad. La conclusión subrayó lo importante que es analizar y evaluar los riesgos para poner en marcha un sistema de seguridad de la información que funcione bien. Este camino ayuda a entender bien cómo está la organización en ese

momento, lo que ayuda a tener más confianza en cada paso de la vida de la información, desde que se crea y se usa hasta que se guarda, se envía, se recupera y se borra bien.

En un estudio realizado en Pakistán, Asad et al. (2022) se propusieron determinar cómo la seguridad de la información, basada en la norma ISO 27001, impacta en los resultados económicos de las empresas. Para lograrlo, enviaron un cuestionario por correo electrónico a 190 empresas. Este cuestionario se dividió en cuatro partes, cada una con veinte preguntas de opción múltiple evaluadas mediante una escala de Likert. Los hallazgos revelaron que la gestión de la seguridad de la información es clave para el éxito y el rendimiento empresarial, lo que se traduce en una mejor reputación, imagen de marca y crecimiento económico.

En Perú, Lopez y Espinoza (2022) realizaron un estudio que buscó desarrollar una estrategia para implementar un Sistema de Gestión de Seguridad de la Información (SGSI) en una empresa de asesoría financiera ubicada en Lima, tomando como base la norma ISO/ IEC 27001:2013. Su investigación siguió un enfoque básico con un diseño experimental descriptivo; los datos se recolectaron a través de métodos como encuestas y observaciones, dirigidos a los 18 empleados de la empresa. Los investigadores determinaron que su trabajo produjo una propuesta completa para la gestión de la seguridad de la información, enfatizando su naturaleza crítica y urgente para mejorar la seguridad de los datos. En consecuencia, indicaron que la adopción de este sistema, según la norma ISO/IEC 27001:2013, permitió resguardar y proteger los recursos computacionales, asegurando la disponibilidad, integridad y confidencialidad de los datos. Además, señalaron que este esfuerzo ayudó a sostener la continuidad operacional durante emergencias o cuando se materializaban amenazas.

En su investigación, Silva (2022) subraya que la administración de datos en varias empresas a menudo carece del cuidado necesario. Así, la meta central del estudio fue poner en marcha un SGSI para aumentar la seguridad en una pyme. El método usado fue práctico, uniendo un esquema experimental con una visión mixta que juntó elementos cualitativos y cuantitativos. Para recoger datos, se hicieron entrevistas, cuestionarios con

preguntas cerradas y abiertas, y se usaron fichas de observación. Estos métodos se aplicaron a cada empleado de la empresa, elegidos por un muestreo no probabilístico y por conveniencia. Los resultados fueron buenos, ayudando mucho a mejorar la protección de la confidencialidad, integridad y acceso a los datos; también, se aseguró la continuidad de los servicios y labores de la empresa; además, la investigación creó una estructura interna para la defensa de la información, guiada por la norma NTP-ISO/IEC 27001:2014.

En la ciudad de Lima, se realizó un estudio por parte del investigador Aleman (2023) que tuvo como objetivo explorar los efectos que genera la implementación de la norma ISO 27001:2013 para la gestión de la seguridad de la información en una empresa consultora privada. Esta investigación, principalmente de tipo aplicativo, utilizó un plan preexperimental dentro de un marco correlacional cuantitativo. Los resultados se midieron mediante medidas de evaluación basadas en aspectos previamente establecidos para la variable dependiente, la recolección de datos implicó el uso de cuestionarios, cuya validez se aseguró mediante evaluaciones de tres expertos en el área. Los resultados mostraron un aumento considerable en áreas importantes como seguridad de la información, adaptabilidad, accesibilidad, protección y disponibilidad dentro de la empresa de consultoría. Este éxito garantizó que la empresa estuviera protegida por un sistema de gestión efectivamente en sintonía con las demandas del mercado.

El estudio conducido por Guizado (2024) se buscó determinar de qué manera el Sistema de Gestión de Seguridad de la Información (SGSI) incidía en la salvaguarda de la información en una municipalidad distrital de Lima, siguiendo los lineamientos de la norma ISO/IEC 27001:2022. Se optó por una metodología aplicada con un enfoque cuantitativo, de tipo correlacional-causal y diseño no experimental. El estudio involucró a 200 empleados, de los cuales se eligió una muestra de 132 especialistas en tecnología a través de un muestreo no probabilístico por conveniencia. La recopilación de datos se efectuó mediante encuestas, empleando dos cuestionarios que fueron previamente revisados y aprobados por un grupo de tres expertos. El análisis de los datos reveló que el SGSI logró un nivel de implementación óptimo,

mientras que la protección de la información se mantuvo en un nivel intermedio. Además, se encontró una correlación positiva moderada de 0.611, con una significancia de 0.032 ($p < 0.05$), lo que indica una relación estadísticamente importante entre ambas variables. En resumen, la implementación del SGSI, de acuerdo con la norma ISO/IEC 27001:2022, tuvo un efecto importante en la mejora de la seguridad de la información en la municipalidad distrital evaluada en 2023.

2.3. Bases teóricas

2.3.1. *Variable independiente.*

Norma ISO 27001

La norma ISO/IEC 27001, surgió producto de la unión entre la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC) en el 2005, y como evolución de la norma BS 7799. Dicho estándar define con detalle las pautas que se deben seguir para crear, poner en marcha, conservar y perfeccionar constantemente un Sistema de Gestión de la Seguridad de la Información (SGSI), tanto dentro como fuera de una empresa; también es importante señalar que algunos de los requisitos incluidos en esta norma son generales y válidos universalmente para cualquier organización, sin importar sus rasgos particulares de clase, dimensión o índole (De La Cruz et al., 2023).

La norma ISO/IEC 27001 ocupa una posición única en la serie ISO 27000 como el único estándar que permite a las empresas lograr la certificación de seguridad de la información. Por el contrario, las demás normas dentro de este grupo ofrecen asistencia clave, proporcionando orientación detallada y organizada para ayudar a crear e implementar un Sistema de Gestión de Seguridad de la Información (SGSI), garantizando su precisión y viabilidad continua.

Beneficios.

La norma ISO/IEC 27001 desempeña un papel significativo en asegurar la integridad de la información en una entidad y obtener la certificación correspondiente. De acuerdo con la perspectiva de Bouziani et al. (2022) se identifican una variedad de beneficios inherentes, destacándose entre ellos:

- Mejorar la eficacia en la salvaguardia de datos sensibles.
- Resaltar la singularidad distintiva de la entidad empresarial.
- Fomentar la confianza entre colaboradores comerciales, partes interesadas y clientes.
- Constituir un estándar globalmente reconocido y aceptado.
- Promover la priorización de la seguridad de la información como aspecto central de la dirección.
- Representar una norma abarcadora que engloba tanto la tecnología informática como la estructura organizativa, el personal y las instalaciones.
- Enfatizar la clara definición de responsabilidades para los empleados en el contexto de la seguridad de la información.

Norma ISO 27001:2022

La más reciente norma ISO/IEC 27001:2022, aborda temas de seguridad de la información, ciberseguridad y protección de la privacidad, además de presentar directrices esenciales. Los primeros segmentos de este estándar ofrecen detalles sobre el alcance, las referencias normativas pertinentes, así como la terminología y definiciones utilizadas en el contexto; adicionalmente, la ISO 27001:2022 especifica los requisitos esenciales para gestionar de manera continua un sistema de seguridad de la información adaptado a las características particulares de cada organización, también incorpora los requisitos para evaluar y gestionar los riesgos de seguridad de la información, ajustándolos de manera específica a las necesidades de cada entidad concernida (M. Hasan et al., 2023).

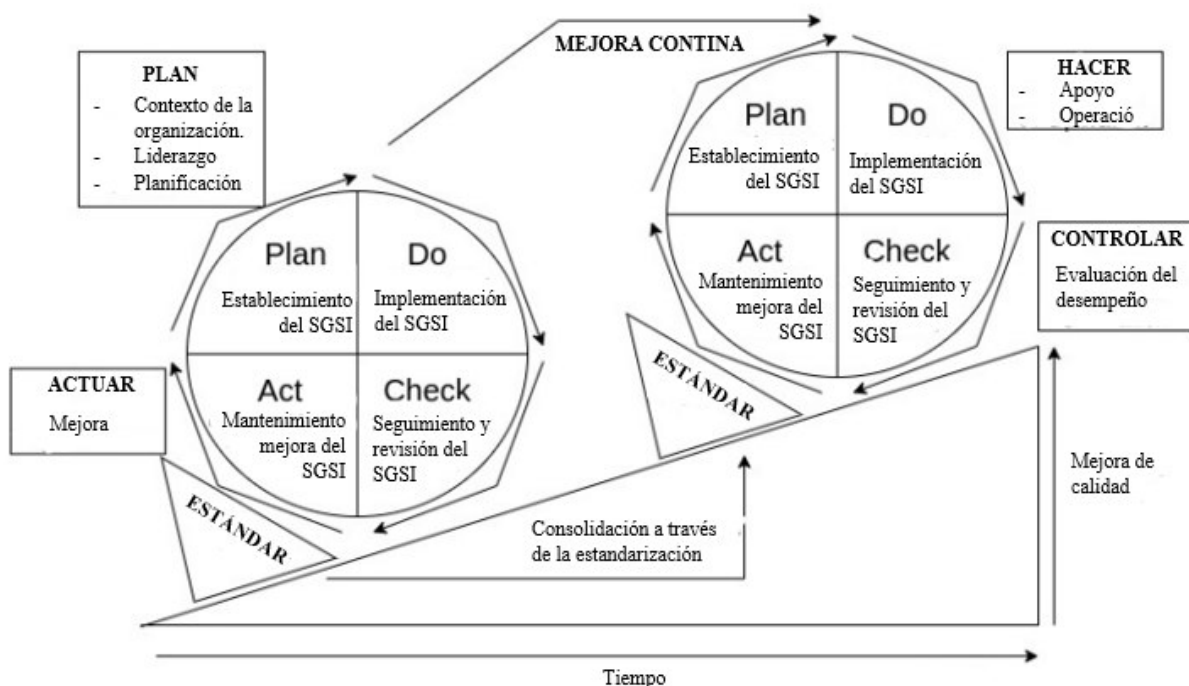
En líneas generales, las modificaciones realizadas en la norma ISO 27001 de 2013 se centran en la consolidación de ciertos controles existentes y la adición de 11 nuevos controles específicos para la versión del 2022, como se detalla más adelante. Esta actualización ha permitido reducir el número total de controles de 114, distribuidos en 14 grupos en la versión de 2013, a tan solo 93 controles agrupados en 4 categorías para la edición de 2022, como se muestra en la Figura 1.

Figura 1:*Categoría de ISO 27001:2022*

Nota: Adaptado de “A Systematic Review of Risk Management Methodologies for Complex Organizations in Industry 4.0 and 5.0”. por Barraza et al. (2023) *MDPI*, 2023.

Implementar los lineamientos de la norma ISO 27001 se facilita al usar el ciclo Planificar – Hacer – Verificar – Actuar (PHVA), buscando mejorar la gestión de procesos en términos de flexibilidad, claridad y enfoque. Este método se apoya en la idea de que siempre se puede mejorar, partiendo de que ningún proceso es perfecto ni totalmente eficiente desde el principio.

Figura 2:*Ciclo PCDC o ciclo de DEMING*



Nota: Adaptado y traducido de “Information Security Management Systems. Computer Science and Engineering” por Junaid (2023) Frankfurt University of Applied Sciences, 2023.

Planear: Implica tomar conocimiento de la situación actual real al recopilar y analizar datos.

Hacer: Se refiere a la ejecución de procesos basada en la planificación y análisis previos.

Verificar: Se lleva a cabo la supervisión y evaluación de los procesos y resultados, comparándolos con los objetivos y especificaciones iniciales.

Actuar: Se realizan las correcciones necesarias y alineando las modificaciones, todo para garantizar que se está mejorando constantemente el funcionamiento de las cosas.

A pesar de que numerosas organizaciones han establecido firmemente procedimientos de gestión de la información y han puesto en práctica medidas

de seguridad adecuada, han surgido diversas amenazas que ponen en peligro la integridad de sus datos.

PCI DSS

El estándar PCI DSS (Payment Card Industry Data Security Standard) fue creado por las principales compañías de tarjetas de crédito, como Visa, MasterCard, American Express, Discover y JCB, a fin de proteger la información de tarjetas de pago que es procesada, almacenada o transmitida por las organizaciones; este desarrollo responde a la necesidad creciente de seguridad en la industria de pagos, fomentando la implementación de prácticas de seguridad continuas, mejorando la flexibilidad y optimizando los procedimientos de seguridad (Paradongan et al., 2024).

El estándar PCI DSS delimita un grupo esencial de requerimientos, tanto técnicos como de funcionamiento, diseñados para blindar los detalles de cuentas financieras. Su meta central radica en prometer una defensa contundente de los datos confidenciales de los clientes y de sus instrumentos de pago, así como en evitar graves sucesos de seguridad (Lessa y Gebrehawariat, 2023).

Razack y Sorber (2022) señalan que esta norma es importante para distintos entes, desde comercios y bancos adquirentes hasta proveedores de servicios. No importa su envergadura, siempre que gestionen, tramiten o guarden información de pagos con tarjeta. Dichas entidades deben cumplir doce exigencias concretas concebidas para garantizar la seguridad de los datos (Hossain et al., 2023).

Cuadro 2:

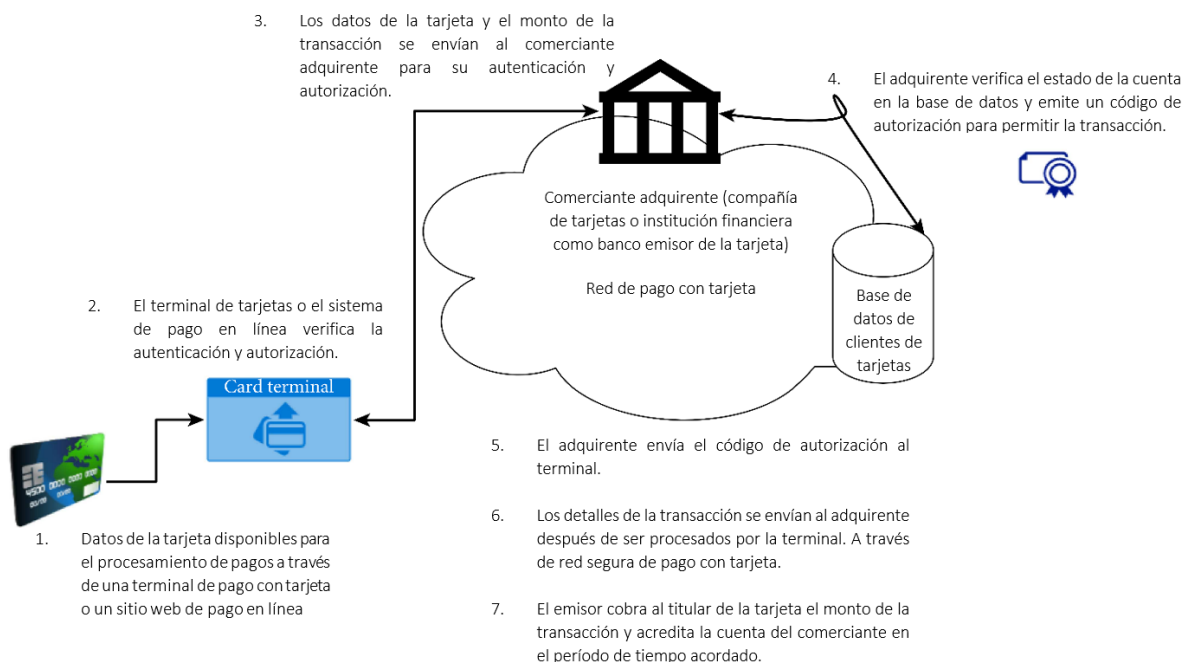
Principios y requisitos PCI DSS

ID	Principios	ID	Requisitos
P1	Desarrollar y mantener redes seguras.	R1	Instalar y mantener una configuración de firewall para proteger los datos del titular de la tarjeta.
		R2	No usar los valores predeterminados suministrados por el proveedor para las contraseñas del sistema y otros parámetros de seguridad.
P2		R3	Proteger los datos del titular de la tarjeta que fueron almacenados.

P3	Proteger los datos del titular de la tarjeta	R4	Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas.
	Mantener un programa de gestión de vulnerabilidades.	R5	Proteger todos los sistemas contra malware y actualizar los programas o software antivirus regularmente.
		R6	Desarrollar y mantener sistemas y aplicaciones seguros.
P4	Implementar medidas sólidas de control de acceso	R7	Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa.
		R8	Identificar y autenticar el acceso a los componentes del sistema.
		R9	Restringir el acceso físico a los datos del titular de la tarjeta.
P5	Supervisar y evaluar las redes con regularidad.	R10	Rastrear y supervisar todos los accesos a los recursos de red y a los datos del titular de la tarjeta.
		R11	Probar periódicamente los sistemas y los procesos de seguridad.
P6	Mantener una política de seguridad de la información.	R12	Mantener una política que aborde la seguridad de la información para todo el personal.

Nota: Traducido de “General Cybersecurity Maturity Assessment Model: Best Practice to Achieve Payment Card Industry-Data Security Standard (PCI-DSS) Compliance”, por (Razikin & Widodo, 2021)

Para entender completamente cómo estos requisitos son relevantes y aplicables, es esencial tener un conocimiento detallado del proceso de pago en su totalidad. Esto implica comprender cada etapa del proceso, desde la autorización de la transacción hasta la liquidación, así como los roles y responsabilidades de las partes involucradas, como los comerciantes, los adquirentes y los proveedores de servicios.

Figura 3:**Proceso de pago**

Nota: Adaptado y traducido de “Towards Secure IoT-Based Payments by Extension of Payment Card Industry Data Security Standard (PCI DSS)” por (Bhutta et al., 2022) *Wireless Communications and Mobile Computing*, 2022.

La implementación del estándar PCI-DSS contribuye a disminuir el riesgo de filtraciones de datos y a incrementar la confianza de los clientes, ya que garantiza que los datos de sus tarjetas de pago se gestionen de manera segura; además, ayuda a las empresas a mejorar su rendimiento general; no obstante, PCI-DSS es un estándar complejo que puede resultar difícil de entender e implementar para algunas organizaciones, ya que requiere monitoreo y mantenimiento continuo, consume una gran cantidad de recursos y demanda un esfuerzo considerable por parte de los equipos de TI (Mukati y Bhargava, 2023).

Riesgo

Algunas empresas aceptan el riesgo de forma pasiva y otras crean ventaja competitiva al exponerlos a riesgos de manera prudente y forma razonada, no hay riesgo cero y todas las actividades implican un cierto grado de riesgo, que debe ser entendido y manejado, de modo que se minimice al máximo. Para Fernandes et al. (2022), el concepto de riesgo ha adquirido amplia difusión social y protagonismo industrial, constituyendo un concepto operativo que se asocia a un evento, siendo una cantidad que resulta de la combinación de la probabilidad y la gravedad de las consecuencias debidas a fallas potenciales.

Gestión del riesgo

Manejar los riesgos debe hacerse poco a poco y de forma organizada, partiendo de la idea de entender bien de qué va cada riesgo. Hay que mirar con lupa las amenazas y por qué surgen, y también calcular bien los riesgos, pensando en cuánto daño podrían hacer y qué tan probable es que pasen; así, se pueden enfrentar los riesgos sabiendo bien qué se hace y actuando antes de que causen problemas, aplicando buenas estrategias para calmarlos y prevenirlos.

La gestión de riesgos es un reto importante para las empresas, pues las que usan estrategias para manejarlos trabajan con más confianza al reducir la duda y mejorar sus chances de lograr lo que quieren. Por eso, gestionar los riesgos en la seguridad de la información es clave, pues implica ver, entender, evaluar y calmar los riesgos, así como las debilidades que los causan y cómo afectan a la información (Mannes et al., 2022).

La gestión de riesgos es un proceso vital que busca encontrar rápido los riesgos en las empresas que puedan impedir que creen valor. Usando las estrategias correctas, se busca tener estos riesgos bajo control y, a la vez, mejorar siempre cómo se hacen las cosas; además, esta gestión efectiva ayuda a aprovechar las oportunidades de negocio y a dar estabilidad a la empresa en un mundo que cambia todo el tiempo (Gurtu y Johny, 2021).

Figura 4:

Procesos de gestión de riesgo de seguridad de la información



NOTA: De “Supply chain risk management: Literature review” por Gurtu y Johny (2021) *MDPI*, 2021.

Más allá de simplemente preparar el escenario, la gestión de riesgos realmente comienza determinando cuáles son los peligros potenciales. Detectar estas amenazas con precisión significa que puede implementar las medidas de protección adecuadas para mantener sus datos seguros. Luego, cuando estás en la fase de análisis, analizas qué probabilidad hay de que realmente ocurra cada riesgo y cuánto daño podría causar. Esto le ayudará a decidir qué riesgos abordar primero y a encontrar formas inteligentes de reducirlos (M. Wang et al., 2023).

Por último, en el tratamiento de riesgos, existen tres enfoques principales que una organización puede adoptar para abordar los riesgos identificados: i) **Aceptar**, aquí la organización decide conscientemente asumir el riesgo identificado sin aplicar medidas de tratamiento adicionales, esto ocurre cuando el costo o la complejidad de implementar medidas de control supera el impacto potencial del riesgo o cuando se considera que el riesgo es aceptable dentro de los límites establecidos; ii) **Transferir**, la organización opta por transferir el riesgo a otra entidad, como una compañía de seguros o un tercero, que esté dispuesto a asumir la responsabilidad y las

consecuencias económicas del riesgo en caso de que ocurra; y ii) **Mitigar**, aquí la organización aplica medidas para disminuir la probabilidad y el impacto de los riesgos, mediante controles de seguridad, políticas, capacitación, y actualización tecnológica.

Políticas de seguridad de la información

La información y los datos que residen en un sistema de información representan un valioso activo intangible para la organización, los mismos que se encuentran constantemente expuestos a desafíos derivados de intrusiones y ataques sorpresivos, ilícitos, camuflados y malintencionados. Estos riesgos pueden originarse tanto desde el interior como desde el exterior de la organización a través de vías no autorizadas, y ponen en entredicho la confidencialidad, integridad y disponibilidad de la información.

La política de seguridad, tal como se la suele entender, es en realidad el conjunto completo de reglas, estándares y pasos que utiliza una empresa para manejar, proteger y compartir información. Una buena política de seguridad no sólo debe cubrir todos los diferentes peligros potenciales que existen; también debe brindar asesoramiento sencillo sobre las mejores formas de abordarlos. Además, debe especificar claramente los deberes y trabajos del personal de TI, los usuarios habituales y los servicios, ya que todos ellos desempeñan un papel en mantener la red en funcionamiento, realizar copias de seguridad de las bases de datos, actualizar las licencias de software, supervisar el almacenamiento de datos, seguir las normas legales y ocuparse de otras cuestiones relacionadas con la seguridad.

Una política de seguridad debe ser formulada en un nivel de abstracción elevado y diseñada de manera que sea comprensible para todos los integrantes de la organización, debe ser de alcance general y no estar vinculada a tecnologías particulares, este enfoque asegura que la política de seguridad tenga una vigencia prolongada y requiera modificaciones poco frecuentes, no obstante, a partir de la política de seguridad de nivel general, es posible desarrollar procedimientos más específicos relacionados con tecnologías particulares (Arogundade, 2023). Con el paso del tiempo, es probable que sea necesario actualizar estos procedimientos, pero la política

de seguridad en sí misma debería mantener su relevancia a lo largo del tiempo.

2.3.2. *Variable dependiente.*

Seguridad de la información

Salvaguardar la información implica proteger los datos importantes, tanto en formato físico como digital, como los detalles personales, los datos financieros o la información confidencial. Para lograr esto, se utilizan medidas de seguridad como el cifrado, la administración de accesos, los firewalls, las copias de seguridad, la formación del personal y la adhesión a las regulaciones de seguridad.

El objetivo de la seguridad de la información, según Kamariotou y Kitsios (2023), es defender los datos personales y los recursos corporativos durante la creación y el funcionamiento de los sistemas, asegurando la confidencialidad, la integridad y la disponibilidad de la información, fortaleciendo así la protección de la organización, la confianza del cliente y la continuidad operativa.

Importancia de la seguridad de la información

Hoy en día, con la globalización y lo digital tan presentes, proteger la información es crucial para todos los países. La información es vital en áreas como las finanzas, el comercio, lo personal y el gobierno. Por eso, gestionar bien la seguridad de la información es clave para cuidar la privacidad, evitar pérdidas de dinero, mantener la confianza de los clientes y proteger los bienes de cualquier organización (Lykhova et al., 2022).

En cuanto a la seguridad de la información, Ramos et al. (2023) indican que ha cambiado mucho: ya no solo se trata de usar herramientas tecnológicas, sino de evitar que entren sin permiso y ataquen los sistemas. Por eso, se necesita una gestión que cambie constantemente en vez de ser algo fijo. Para estar seguros, hay que contar con la ayuda de varias áreas que influyan en esto. Pero ojo, aunque tengamos un buen sistema de gestión, no podemos asegurar que los riesgos a la información desaparezcan por completo.

El informe anual de 2021 sobre seguridad muestra que la principal causa de pérdida de información es que la gente no está muy atenta, en dos sentidos: no entienden bien cómo proteger la información y no están dispuestos a seguir las normas de la empresa (Fadlika et al., 2023). Para solucionar esto y estar más seguros, se propone mejorar tres cosas:

- Educación: Aquí se busca explicar por qué la seguridad de la información es importante para la empresa.
- Capacitación: En este punto, se enseña a los usuarios cómo usar las opciones de seguridad que hay en el sistema y en su trabajo.
- Concientización: Esto se basa en lo que se ha enseñado y formado, animando a la gente a entender y seguir las mejores prácticas de seguridad y privacidad.

La norma ISO 27001 es una herramienta útil para gestionar y proteger bien la información. Sirve tanto si la empresa quiere obtener un certificado como si solo quiere usar buenas prácticas de seguridad de la información. Además, se aplica tanto a lo que ocurre dentro de la empresa como a lo que hace fuera.

Gestión de seguridad de la información

Se trata de un grupo de métodos y acciones delineados con precisión para reconocer, sopesar y manejar los peligros que ponen en riesgo los recursos de información de una empresa. Esto requiere usar reglas, principios y mecanismos de control enfocados en salvaguardar la privacidad, exactitud y acceso a los datos. Abarca desde el registro de recursos y estudio de puntos débiles, hasta la puesta en marcha de defensas, manejo de problemas, capacitación del equipo y acatamiento de las leyes actuales.

Para Bemenet et al. (2023) la gestión de la seguridad de la información, implica coordinar de forma integral los recursos tecnológicos, humanos y normativos para garantizar la continuidad operativa y el alineamiento con los objetivos organizacionales, pues el avance y la expansión de las tecnologías de la información en todos los niveles empresariales, ha hecho que esta gestión sea más crítica, que es imposible abordarse con controles estáticos;

el entorno actual, dinámico y centrado en los datos, exige enfoques más flexibles y adaptativos.

Principios de la gestión de seguridad de la información

Los principios se describen bajo confidencialidad, integridad y disponibilidad, las mismas que conforman lo que se conoce como el "triángulo de la seguridad de la información". Bolek et al. (2023) consideran que el equilibrio adecuado entre estos tres principios es esencial para proteger la información y garantizar una postura sólida de seguridad en cualquier entorno, ya sea en sistemas informáticos, redes, aplicaciones o cualquier otro ámbito donde se maneje información sensible o crítica.

Figura 5:

Triángulo de la información



Nota: Adaptado de “Seguridad de la información en el comercio electrónico basado en ISO 27001: Una revisión sistemática” por De La Cruz et al. (2023) *Innovación y Software*, 2023.

Confidencialidad alude a un pilar esencial en la protección de datos. Hablamos de la cualidad que confirma que solo gente autorizada vea y entienda la información. En el mundo de la seguridad digital, se logra mediante cifrado, verificación y gestión de accesos, pues los datos privados deben resguardarse de accesos ajenos, asegurando que solo individuos o sistemas con permiso accedan a ellos.

La **integridad** de la información concierne a su calidad, asegurando que los datos sigan sin alteraciones indebidas, sean accidentales o intencionadas.

Mantener la integridad supone preservar la exactitud, lógica y totalidad de los datos durante su almacenamiento, envío y tratamiento.

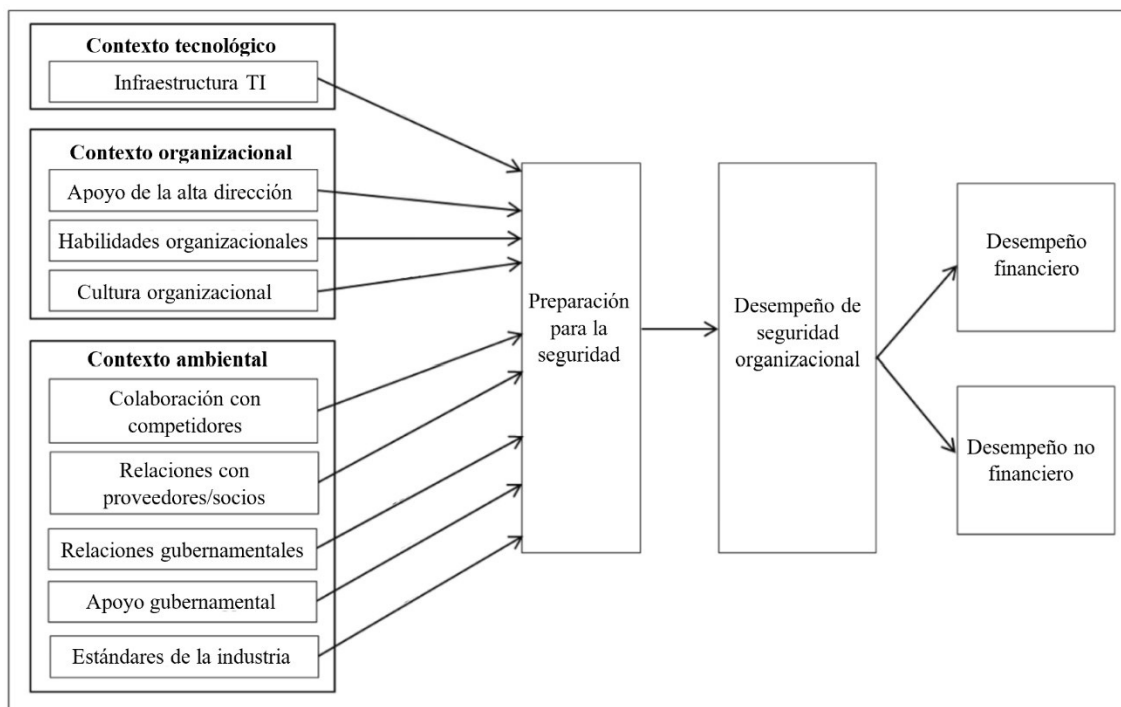
La **disponibilidad** es la capacidad de la información para estar accesible y operativa cuando se requiere. En seguridad de la información, se asegura manteniendo los sistemas y recursos funcionales y preparados para responder a usuarios autorizados, mediante medidas que evitan interrupciones inesperadas, ataques de denegación de servicio y otros eventos que puedan impedir el acceso legítimo.

Factores de la gestión de seguridad de la información

Hasan et al. (2021) introducen una estructura compuesta por nueve factores que inciden en la seguridad de la información dentro de las organizaciones, clasificándolos en tres categorías distintas: tecnológicos, organizacionales y ambientales, presentando una perspectiva integral que abarca los elementos tecnológicos, la dinámica organizativa y las influencias ambientales que contribuyen a la seguridad de la información en el contexto empresarial, tal cual se muestra en la figura.

Figura 6:

Factores de seguridad de la información.



Nota: Adaptado de “Evaluating the cyber security readiness of organizations and its influence on performance” por Hasan et al. (2021) *Journal of Information Security and Applications*, 2021.

Según Veiga et al. (2020), los factores ambientales ejercen una influencia significativa en la gestión de seguridad en organizaciones, ya que permite establecer vínculos con socios comerciales, consumidores y proveedores; además, estos factores pueden tener efectos indirectos, como el estado económico, los avances tecnológicos y los cambios políticos, científicos y socioculturales, los cuales pueden no manifestarse de manera inmediata en las operaciones empresariales.

Se ha evidenciado que el factor humano representa uno de los elementos más determinantes en el ámbito de la seguridad de la información (Dada et al., 2021), ya que los empleados y los directivos son quienes forjan conexiones tanto internas como externas, y desempeñan un papel crucial en el mantenimiento y la adhesión a los protocolos de seguridad establecidos (Bahrami et al., 2021).

Podrecca et al. (2022) señalan que el entorno tecnológico guarda una estrecha relación con la gestión de la seguridad de la información, dado que

las empresas manejan datos en formatos digitales y operan en entornos virtuales, lo que las expone potencialmente a amenazas y ataques cibernéticos.

2.3.3. Estándares y marcos.

Cuadro 3:

Estándares y marcos de referencia.

Estándar	Objetivo	Público objetivo	Descripción
ISO 27001	Gestión de seguridad de la información	Organizaciones en general	La norma ISO 27001 , lanzada por primera vez en 2005 , brinda instrucciones detalladas sobre cómo construir , implementar , cuidar y mejorar constantemente el sistema de gestión de seguridad de la información de una empresa (Podrecca & Sartor, 2023); aparte, no solo define una estructura compartida para la creación de reglas y estrategias efectivas en la gestión de la seguridad, sino que también ayuda a construir confianza en las operaciones y los vínculos comerciales al producir reportes creíbles (Amirinnisa y Rahadian, 2023). Es un marco de referencia de aceptación mundial en el ámbito de la gestión de los servicios de las tecnologías de la información, que destaca por presentar un compendio ordenado de métodos y procedimientos pensados para la administración eficiente de los servicios de TI. Se centra principalmente en la administración de dichos servicios, ofreciendo orientación concreta para la mejora constante en la provisión y el funcionamiento seguro de los servicios; su valor reside en su habilidad para ofrecer una visión pormenorizada de los procesos que intervienen, localizar puntos susceptibles de mejora y dar a conocer a los profesionales la metodología de trabajo concreta vinculada a la gestión de servicios de TI (Minaya et al., 2023).
ITIL	Gestión de servicios	Organizaciones en general	

COBIT	Gobierno de TI como base de seguridad cibernética	Organizaciones en general	Desde su inicio en 1996, COBIT ha crecido constantemente en cuanto a su amplitud. Este esquema de trabajo ofrece una perspectiva completa y una estrategia para dirigir y administrar los sistemas de tecnología informática (TI) (Cortés, 2023). Busca principalmente armonizar la creación de ganancias, la mejora de los grados de riesgo y el uso efectivo de los medios; sobresale al proponer una serie de prácticas recomendadas, con una atención más dirigida a la supervisión que a la puesta en práctica, y también, define criterios de supervisión basados en demandas de calidad, fiabilidad y protección, suministrando una estructura organizada para la administración eficaz de los bienes de información (Coronel y Quirumbay, 2022). Establecida en mayo de 1987, la metodología BS 7799 surgió con un doble propósito: en primer lugar, asistir a los proveedores de productos de seguridad de tecnología de la información mediante el establecimiento de un conjunto de criterios de evaluación; en segundo lugar, proporcionar un esquema de certificación. La finalidad subyacente de esta metodología radica en salvaguardar la información contra una amplia variedad de amenazas, asegurando la continuidad del negocio y minimizando los posibles perjuicios. Además, brinda a los directivos la oportunidad de obtener el reconocimiento de la alta dirección respecto a la importancia de implementar procedimientos y mecanismos que mejoren la seguridad de la información (Masaev et al., 2020). Fue concebida con el propósito de estimular y perfeccionar la seguridad de los datos del titular de la tarjeta, al mismo tiempo que facilita la implementación de
BS 7799-3	Seguridad de la información	Organizaciones en general	
PCI DSS	Seguridad de las transacciones de información y	Sector de pagos tarjeta (Payment	

datos en Card movimientos Industry) bancarios.	medidas de seguridad coherentes a nivel global. La Norma de Seguridad de Datos del Sector de Tarjetas de Pago (PCI DSS) constituye una guía que establece requisitos técnicos y operativos destinados a resguardar la información, este marco engloba requisitos fundamentales para la protección de los datos y se ofrece como un fundamento adaptable, permitiendo mejoras mediante la incorporación de controles y prácticas adicionales con el objetivo de mitigar riesgos; además, la PCI DSS se ajusta a las leyes y regulaciones locales, regionales y sectoriales pertinentes (Mujica y Monges, 2022).
--	--

2.4. Marcos conceptuales o glosario

Información: Resultan cruciales para desarrollar saberes y apoyar la toma de decisiones en campos como la ciencia, tecnología, educación y economía. Su veracidad depende de fuentes objetivas, lo cual garantiza su validez. En la era digital, la buena gestión de los datos es clave para el correcto desempeño de la sociedad y las organizaciones (Benjamin y Nabende, 2023).

Activo de información: Es un conjunto de saberes estructurados y manejados como una unidad, cuya definición es amplia y siempre se transforma. Este dato activo primordial incluye todos los conocimientos que están en constante evolución y avance. Igualmente, se le valora por su utilidad para los usuarios, sus posibles usos y su posesión (Fathullah y Subbarao, 2022).

Gestión de la información: Abarca procesos, técnicas y estrategias para adquirir, ordenar, guardar, recuperar, analizar y usar los datos de manera eficiente en una organización. Busca mejorar el ciclo de vida de los datos, desde su inicio hasta el final, para optimizar las decisiones, fomentar la unión, potenciar la innovación y proteger los datos clave para lograr los objetivos (Zhao, 2022).

Amenaza: Se trata de sucesos naturales o causados por personas que pueden pasar en cualquier momento, y causar efectos negativos en elementos frágiles y expuestos, como daños a sistemas e infraestructuras tecnológicas. También, se refiere al uso de fallos para alterar el funcionamiento de un sistema para sacar provecho (Egoshin et al., 2023).

Vulnerabilidades: Son una debilidad propia de un sistema, que puede ser usada por gente mala para poner en riesgo su integridad y seguridad. Estos puntos débiles pueden surgir por errores en el diseño, fallos en la configuración o métodos incorrectos. En las empresas, son la principal causa de ataques a los sistemas (Sánchez-Bautista y Ramírez-Chávez, 2022).

Activos: Son elementos que dan valor a una organización, ya sea para sus negocios o su forma de operar, incluyendo los datos que apoyan su misión. Se dividen en dos tipos: las cosas valiosas principales, que son los negocios, las acciones y los datos, y las cosas valiosas secundarias, como equipos, programas, redes y la estructura física y relaciones (Velepucha et al., 2022).

Probabilidad: La probabilidad representa la expectativa de ocurrencia del riesgo evaluado, reconociendo que nos referimos, a una probabilidad teórica, ya que la cuantificación precisa es inalcanzable dado que el riesgo absoluto no puede ser eliminado por completo (Daoud et al., 2023).

Impacto: Podemos concebir el impacto como la repercusión tangible que surgirá como resultado de la aplicación de un tratamiento específico o conjunto de tratamientos de datos a individuos concretos, en términos más sencillos, el impacto representa la consecuencia, ya sea beneficiosa o perjudicial, que un tratamiento de datos particular pueda tener en la persona a la cual se han recolectado dichos datos (Dronov y Dronova, 2022).

CAPÍTULO 3: METODOLOGÍA

3.1. Tipo y diseño de investigación

Tipo de investigación

Debido a las características particulares observadas en la investigación, se clasificó como un estudio de tipo aplicada, conceptualizada según Castro et al. (2023) como investigaciones inéditas orientadas hacia la adquisición de conocimientos novedosos con el propósito de abordar una problemática concreta, valiéndose de hallazgos previos en la investigación básica; estos estudios, son caracterizados por su brevedad en la obtención de resultados, y suelen ejercer un impacto sobresaliente en la sociedad.

La investigación adoptó un enfoque cuantitativo, centrado en la recolección de datos numéricos y su análisis estadístico. Para ello, se emplearon cuestionarios como instrumentos de obtención de información y se formularon hipótesis para validar el estudio.

Por su parte, Acosta (2023) refiere que el enfoque cuantitativo se destaca por su capacidad para realizar predicciones, las cuales representan interpretaciones de los eventos observados, y como resultado, su trayectoria es predecible; además, señalan que este enfoque se caracteriza por ser un proceso analítico que descompone un todo en sus componentes elementales.

Diseño de investigación

El diseño de la investigación fue preexperimental, ya que se manipuló intencionalmente la variable independiente, correspondiente al modelo basado en las normas ISO 27001:2022 y PCI DSS, para evaluar su efecto sobre la variable dependiente, la Gestión de Seguridad de la Información. El estudio incluyó mediciones (pretest y posttest) realizadas en un único grupo de muestras apareadas para comprobar el cumplimiento de los objetivos (Ramos, 2021), cuyo diagrama inicial es el siguiente:

$$G \rightarrow O_1 \rightarrow X \rightarrow O_2$$

Donde:

G: Grupo al que se la hará el seguimiento.

O₁: Pre test, que permitió diagnosticar el estado de seguridad antes de la implantación de las políticas.

X: Implantación del modelo.

O₂: Post test, que permitió determinar la influencia del modelo sobre la Gestión de Seguridad de la información.

El modelo conceptual presentado describe la estructura fundamental del diseño: una medición previa (pretest), la aplicación de la intervención y una medición posterior (posttest). Este tipo de diseño es ampliamente reconocido en la literatura metodológica como uno de los esquemas básicos de experimentación (Campbell y Stanley, 1966; Hernández-Sampieri et al., 2014).

Sin embargo; durante el desarrollo de la intervención, se incluyeron dos evaluaciones después del tratamiento. Estas evaluaciones adicionales no transforman el tipo de diseño, sino que profundizan el análisis del cambio, permitiendo observar variaciones en el desempeño de los participantes a lo largo del proceso. Por ello, la secuencia real es representada como:

$$G \rightarrow O_1 \rightarrow X \rightarrow O_2 \rightarrow O_3$$

Es importante aclarar que esta estructura no constituye un diseño de series temporales, ya que dicho diseño exige un número amplio de observaciones repetidas y espaciadas regularmente antes y después de la intervención para modelar patrones, tendencias o autocorrelaciones temporales. En cambio, en este estudio, la inclusión de dos evaluaciones posteriores al tratamiento busca refinar la comparación pretest–posttest típica del diseño preexperimental, permitiendo observar la estabilidad, retención o posible decaimiento del efecto sin asumir un comportamiento longitudinal complejo.

Este enfoque es coherente con estudios recientes de evaluación que utilizan secuencias como diagnóstico – monitoreo – cierre para profundizar el

análisis del cambio sin pretender constituir una serie temporal (Herrera et al., 2023). Asimismo, la literatura actual sobre evaluación formativa señala que las mediciones adicionales funcionan como estrategias de seguimiento para mejorar la validez interpretativa del cambio, no como observaciones sistemáticas propias de un diseño longitudinal o de series temporales (Vega et al., 2025; Vargas-Pimentel et al., 2024; Velandia-Mesa et al., 2021). De manera similar, informes técnicos de intervenciones recientes reportan la aplicación de postests múltiples para fortalecer la evidencia de impacto sin modificar la naturaleza preexperimental del diseño (Ramos-Galarza, 2021).

3.2. Unidad de análisis

Para efectos de la presente investigación, se tomó como unidad de análisis a las pymes dedicadas al sector textil en Lima metropolitana, 2024.

3.3. Población de estudio

La población estuvo conformada por 5 pymes textiles, ubicadas en el distrito de Lurín, dicha información fue brindada por el Ministerio de Producción mediante el portal de transparencia, de las cuales se aplicó el cuestionario a aproximadamente 20 trabajadores de cada pyme entre gerenciales, administrativos y técnicos.

3.4. Tamaño de muestra

En el marco de la presente investigación, el tamaño muestral se ha establecido en 20 participantes, abarcando perfiles gerenciales, administrativos y técnicos. Esta decisión responde a restricciones en los recursos financieros y a la limitada accesibilidad a la población objetivo. La selección se sustenta en los principios expuestos en X. Wang y Ji (2020) que indican que, en estudios experimentales, la potencia estadística puede ajustarse estratégicamente para optimizar el balance entre viabilidad económica y validez de los resultados. Asimismo, Lakens (2022) enfatiza que la disponibilidad de recursos es un factor determinante en las decisiones metodológicas relacionadas con el tamaño de la muestra.

Por otro lado, Rendón-Macías y Villasís-Keever (2017) señala que, en investigaciones donde la accesibilidad a la muestra es limitada, es posible

emplear estrategias para reducir el tamaño sin afectar la validez interna del estudio. Además, resalta que los diseños experimentales con tamaños muestrales reducidos pueden ser metodológicamente válidos permitiendo obtener resultados confiables a pesar de la restricción en la cantidad de participantes.

3.5. Selección de la muestra.

La muestra de la presente investigación es no probabilística de tipo por conveniencia, ya que se seleccionó a aquella pyme accesible que aceptó ser incluida; este enfoque se justificó siguiendo la definición de Reales et al. (2022) que lo describen como un método que se limita a incluir en el estudio únicamente a aquellos elementos de la población que cumplen criterios prácticos como disponibilidad, accesibilidad, cercanía geográfica o disposición para participar.

3.6. Técnicas e instrumentos de recolección de datos

En la investigación, se emplearon la técnica de la encuesta online, la cual se utilizó como medio para recopilar la información necesaria mediante la aplicación de su herramienta asociada, el cuestionario.

Para Cisneros-Caicedo et al. (2022), la encuesta online es la técnica de recolección de datos más utilizada en investigaciones científicas, ya que ofrece flexibilidad temporal y privacidad para los participantes; además, al eliminar la presencia del encuestador, se minimiza el riesgo de sesgos o influencias en las respuestas. Esta técnica requiere el uso de un cuestionario estructurado y cuidadosamente diseñado, el cual debe ser evaluado previamente antes de su aplicación a la población objetivo para garantizar su validez y fiabilidad.

Como instrumento en la investigación, se empleó un cuestionario previamente organizado, que incluyó alternativas de respuesta tipo Likert, posibilitando la clasificación de las opiniones y su cuantificación, con el propósito de posteriormente representar estos datos a través de tablas estadísticas.

El instrumento en consideración estuvo compuesto por 20 ítems, los cuales se encontraron estructurados en tres dimensiones distintas. La primera dimensión, denominada confidencialidad, abarca los ítems del 1 al 6, adicionalmente la dimensión de integridad, compuesta por los ítems del 7 al 13, y la dimensión de disponibilidad, que engloba los ítems del 14 al 20; cada uno de estos elementos presenta cinco opciones de respuesta estructuradas según una escala Likert, que varía desde nunca, casi nunca, algunas veces, casi siempre y siempre (Anexo 01).

Validez

Para garantizar la validez del instrumento de recolección de datos, se llevó a cabo una evaluación mediante juicio de expertos, donde profesionales especializados revisaron y validaron los ítems o dimensiones que componen el constructo de interés, ya sea proponiéndolos o evaluándolos (Nápoles y Barrueta, 2023).

Entre los expertos, se seleccionaron a 3 ingenieros con maestría que se encargaron de evaluar el instrumento y certificaron a través de un informe que el instrumento cumple con las condiciones necesarias para ser aplicado a los trabajadores de las Pymes que conforman la muestra (Anexo 02).

Cuadro 4:

Validación de experto.

Nombre y apellido	Grado	Entidad donde labora	Calificación
Nilton César, Mori León	Magister	Mi banco	Aplicable
Ruben Oscar, Cerda García	Magister	IA Inversiones Palo Alto II SAC	Aplicable
Teodoro Manuel, Andrade Mogollón.	Magister	IFF	Aplicable

Confiabilidad

Después de validar el instrumento de recolección de datos mediante juicio de expertos, se procedió a evaluar su confiabilidad. Para ello, se seleccionó una muestra piloto de 10 trabajadores, a quienes se les aplicó el

instrumento; posteriormente, se analizó utilizando el coeficiente Alfa de Cronbach, calculado con SPSS v26, obteniendo un resultado de 0.904

Cuadro 5:

Fiabilidad según Alfa de Cronbach.

Alfa de Cronbach	N de elementos
0.904	20

CAPÍTULO 4: RESULTADOS Y DISCUSIÓN

4.3. Análisis, interpretación y discusión de resultados.

En la siguiente sección, se exponen los resultados derivados del estudio realizado. En primer lugar, se describen los datos obtenidos de las pymes textiles que participaron en el análisis, junto con las características relevantes de la muestra utilizada para evaluar la viabilidad y la eficacia del estudio. En la segunda parte, se presentan los resultados del contraste de hipótesis, los cuales permiten validar y medir la efectividad del modelo propuesto en relación con los objetivos planteados.

4.3.1. Análisis descriptivo de la población.

En el Cuadro 6 se presentan los datos sociodemográficos de los N = 100 participantes de la población estudiada, cuyas edades oscilan entre 17 y 61 años, con una media (ME) de 33 años y una desviación estándar (DE) de 9 años.

Cuadro 6:

Representación sociodemográfica de la población

		fi	%
Género	Femenino	42	42
	Masculino	58	58
Nivel de educación	Secundaria	20	20
	Técnico	25	25
	Universitario	55	55
	Administrativo	66	66
Cargo u ocupación	Gerencial	7	7
	Operario	12	12
	Técnico	15	15
	Menos de 1 año	9	9
Años de servicio	1 a 3 años	45	45
	4 a 6 años	35	35
	7 a 10 años	6	6
	Más de 10 años	5	5
Tipo de vivienda	Casa independiente	33	33
	Cuarto	37	37
	Departamento	29	29
	Dúplex	1	1

Se puede observar que un 58% de los encuestados fueron hombres y un 42% mujeres, destacando una presencia equilibrada de géneros. La mayoría de los participantes (56.6%) se encuentra en la franja de 31 a 45 años, lo que indica una fuerza laboral en plena etapa productiva. En términos de formación académica, el 56% posee un grado universitario, mientras que un 20% cuenta con educación secundaria, mostrando una variabilidad en los niveles de instrucción.

Dentro del entorno laboral encuestado, casi dos tercios, o el 66 %, están involucrados en tareas administrativas, lo que indica un fuerte enfoque en los roles gerenciales y la toma de decisiones dentro de las pymes textiles. En cuanto a la duración del empleo, alrededor del 45% ha trabajado en su puesto actual durante uno a tres años, pero sólo el 5% ha permanecido más de una década, lo que puede implicar cierta dificultad para retener el talento durante períodos prolongados. Esta información ofrece una visión general de la composición y la dinámica del personal, subrayando tanto las oportunidades como los desafíos en materia de experiencia y continuidad laboral.

A continuación, se muestran las tablas de frecuencia porcentual para cada aspecto. Cabe señalar que se utilizó una escala de medición tipo Likert, cuyos valores representan: 1 = Nunca, 2 = Rara vez, 3 = A veces, 4 = A menudo y 5 = Siempre. Si bien estos detalles sirven como base descriptiva, a continuación, se realizarán pruebas de hipótesis para evaluar la efectividad real del modelo propuesto.

Cuadro 7:

Distribución de frecuencia de la dimensión confidencialidad.

Pregunta	1	2	3	4	5
P1	4	29	50	13	4
P2	5	39	37	11	8
P3	7	44	28	13	8
P4	3	31	44	17	5
P5	30	35	26	6	3
P6	8	45	33	10	4

En la primera dimensión analizada (Cuadro 7), los resultados muestran que la mayoría de las respuestas se concentran en las opciones 2 ("Casi

nunca") y 3 ("Algunas veces"). Esto indica que realmente no existen reglas o medidas sólidas para mantener la información privada. Lo que esto significa es que, muchas de las empresas no están haciendo un buen trabajo a la hora de establecer reglas claras para evitar que información confidencial llegue a personas que no deberían verla.

Esta situación demuestra que las pequeñas empresas que analizamos podrían encontrarse en serios problemas en lo que respecta a cómo gestionan sus actividades y cómo son percibidas por los demás. No mantener la privacidad podría significar perder datos importantes, perder la confianza de clientes y socios e incluso enfrentar sanciones legales.

Cuadro 8:

Distribución de frecuencia de la dimensión integridad.

Pregunta	1	2	3	4	5
P7	7	17	49	16	11
P8	0	7	64	18	11
P9	2	16	50	22	10
P10	6	12	17	55	10
P11	2	13	72	11	2
P12	5	27	50	14	4
P13	5	24	50	15	6

En la segunda dimensión analizada (Cuadro 8), los resultados muestran que la mayor proporción de respuestas se concentra en las opciones 3 ("Algunas veces") y 4 ("Casi siempre"). Esto sugiere que, a pesar de la ausencia de políticas claras y de ciertas limitaciones tecnológicas, los encuestados perciben que los datos se mantienen mayoritariamente íntegros y que el manejo de la información es, en general, adecuado.

Este hallazgo indica una percepción positiva respecto a la conservación y uso correcto de los datos, lo que podría atribuirse a prácticas informales o al esfuerzo individual de los colaboradores para garantizar la integridad de la información. Sin embargo, la falta de políticas definidas y las deficiencias tecnológicas representan riesgos latentes que podrían comprometer la sostenibilidad de este manejo favorable en el largo plazo.

Cuadro 9:

Distribución de frecuencia de la dimensión disponibilidad.

Pregunta	1	2	3	4	5
P14	2	2	20	60	16
P15	1	3	29	53	14
P16	17	15	62	5	1
P17	3	11	65	18	3
P18	11	46	24	11	8
P19	9	8	63	15	5
P20	3	3	18	50	26

En la tercera dimensión de seguridad (Cuadro 9), los resultados muestran una tendencia diferenciada según los grupos de preguntas analizadas. En las preguntas 14, 15 y 20, las respuestas predominantes se encuentran en las opciones 3 ("Algunas veces") y 4 ("Casi siempre"), lo que implica que los usuarios generalmente pueden obtener la información que necesitan. Este resultado da una impresión bastante buena de lo fácil que es encontrar y utilizar datos.

Sin embargo, en las preguntas 16 a 19, las respuestas más frecuentes corresponden a las opciones 2 ("Casi nunca") y 3 ("Algunas veces"). Esto demuestra que a menudo es bastante difícil obtener información, especialmente cuando se necesita acceso constante, como en operaciones las 24 horas del día.

En general, estos resultados sugieren que, si bien las personas pueden acceder a cierta información, aún existen obstáculos para obtenerla de manera consistente; esto podría deberse a problemas técnicos, malos procesos o falta de personal. Para solucionar estos problemas es necesario mejorar los sistemas de soporte, facilitar el acceso e implementar tecnología que permita un acceso confiable e ininterrumpido.

4.3.2. Análisis descriptivo de la muestra

En relación con la muestra del estudio, se seleccionaron $n = 20$ elementos de la población, con edades que varían entre 20 y 61 años. La media de edad (M) es de 35 años, con una desviación estándar (DE) de 10

años, lo que indica una dispersión moderada en los rangos de edad representados en la muestra.

Cuadro 10:

Representación sociodemográfica de la muestra de estudio

		fi	%
<i>Género</i>	Femenino	11	55
	Masculino	9	45
<i>Nivel de educación</i>	Secundaria	4	20
	Técnico	5	25
	Universitario	11	55
<i>Cargo u ocupación</i>	Administrativo	11	55
	Gerencial	2	10
	Operario	1	5
	Técnico	6	30
<i>Años de servicio</i>	1 a 3 años	9	45
	4 - 6 años	7	35
	7 - 10 años	1	5
	Más de 10 años	1	5
	Menos de 1 año	2	10
<i>Tipo de vivienda</i>	Casa independiente	7	35
	Cuarto	8	40
	Departamento	5	25

En el Cuadro 10 se detalla la distribución de los participantes del estudio. En términos de género, los resultados muestran una composición equilibrada, con un 55% de mujeres y un 45% de varones. En cuanto al nivel educativo, la mayoría de los encuestados (55%) reportó haber completado estudios universitarios.

Respecto al cargo u ocupación, un 55% de los participantes desempeñaba roles administrativos, lo que resalta la predominancia de posiciones vinculadas a la gestión en la muestra. En relación con la variable de años de servicio, el 80% de los encuestados contaba con menos de 6 años de experiencia laboral. Finalmente, sobre el tipo de vivienda, los datos reflejan que la mayoría residía en casas independientes (35%) o en cuartos (40%), lo que sugiere cierta heterogeneidad en las condiciones de vivienda de los participantes.

4.3.3. *Análisis descriptivo de la evaluación del modelo implementado.*

En esta sección, se presenta un análisis basado en resultados obtenidos a partir de tres evaluaciones que permitieron medir la efectividad del modelo. La primera medición, conocida como Pre test o Evaluación Diagnóstica, se realizó antes de la implementación para establecer un punto de referencia; posteriormente, tras un mes de aplicación del modelo, se llevó a cabo una Medición Intermedia o Prueba de Proceso, con el objetivo de monitorear avances y posibles ajustes. Finalmente, luego de tres meses, se aplicó una Prueba de Impacto o Post Test, con el propósito de realizar un análisis comparativo y determinar la efectividad sostenida del modelo en el tiempo.

El cuadro 11 muestra los valores estadísticos descriptivos de cada dimensión en las distintas pruebas, incluyendo la media, la desviación estándar (DE), así como los valores máximos y mínimos obtenidos.

Cuadro 11:

Resumen de medidas en las diferentes pruebas.

Prueba	Media	Mediana	DE	Mínimo	Máximo
Pre Test	62	60	7.82	54	80
D1 - Confidencialidad	16.7	15	4.975	10	29
D2 - Integridad	22.2	21	2.802	19	27
D3 - Seguridad	23.1	23	1.586	21	27
Prueba de Proceso	84.8	85	1.843	81	88
D1 - Confidencialidad	27.3	27	1.174	25	30
D2 - Integridad	27.4	27.5	1.432	25	31
D3 - Seguridad	30.1	30	1.071	27	32
Pos Test	88	88	1.605	83	90
D1 - Confidencialidad	29.4	30	0.995	27	30
D2 - Integridad	27.3	27	1.07	24	29
D3 - Seguridad	31.3	31	0.571	30	32

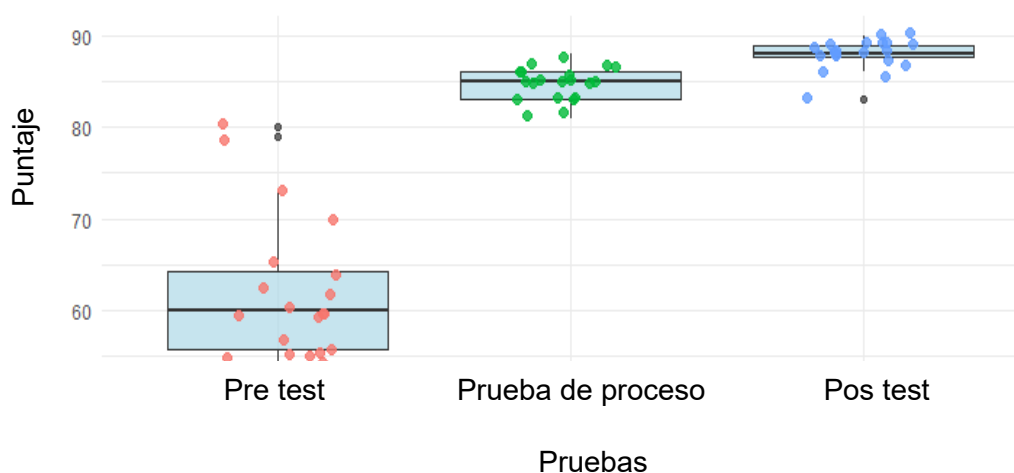
El Cuadro 11 refleja un incremento en las medias de cada prueba, lo que sugiere una tendencia positiva en los resultados generales. De manera similar, la mayoría de las dimensiones presentan un comportamiento ascendente, excepto la dimensión 2, Integridad, cuya media se ha mantenido prácticamente estable entre la Prueba de Proceso (27.4 ± 1.4) y el Post Test

(27.3 ± 1.07). No obstante, se observa una reducción en la desviación estándar, lo que indica una menor dispersión en los datos de esta dimensión.

Para facilitar la interpretación de las comparaciones entre las tres pruebas, se presenta el gráfico de caja y bigote en la Figura 7, el cual permite visualizar la distribución, dispersión y posibles valores atípicos de los datos.

Figura 7:

Comparación de las diferentes pruebas.



En la Figura 7, se puede observar la evolución de los puntajes a lo largo de las tres pruebas:

Pre test (rojo): Punto de partida con alta dispersión

En esta primera medición, la mediana del puntaje se encuentra alrededor de 60, lo que indica que, antes de la implementación del modelo, el rendimiento general era moderado o bajo. La gran dispersión de los datos, evidenciada por un amplio rango intercuartílico, indica que había una alta variabilidad en los puntajes; es decir, algunas personas evaluadas tenían un desempeño significativamente mejor o peor que otras; además, la presencia de valores atípicos fuera de los límites esperados indica la existencia de individuos que se desviaban considerablemente de la tendencia general.

Prueba de proceso (verde): Incremento en el desempeño con reducción de variabilidad

Un mes después de la implementación del modelo, se observa un incremento sustancial en la mediana, que ahora se sitúa cerca de 80. Este aumento revela que el modelo comenzó a generar un impacto positivo en los resultados. Paralelamente, la reducción en la dispersión de los datos (caja más estrecha) indica que los puntajes están más concentrados en torno a la mediana, es decir existe una mayor homogeneidad en el rendimiento de los participantes. Sin embargo, aún se presentan algunos valores atípicos, lo que implica que ciertos individuos continúan mostrando resultados que se alejan del comportamiento general del grupo.

Post test (azul): Consistencia y consolidación del impacto

Tras tres meses de implementación, la mediana alcanza aproximadamente 90, evidenciando una mejora sostenida en los resultados. Más relevante aún, la reducción drástica del rango intercuartílico y la casi desaparición de valores atípicos indican que el impacto del modelo no solo fue positivo, sino que también logró estabilizar los puntajes dentro de un rango más predecible y homogéneo. La menor dispersión en los datos indica que el modelo ha favorecido la consistencia en el desempeño, reduciendo desigualdades iniciales y permitiendo que los participantes alcancen niveles similares de mejora.

El análisis de los datos permite inferir que la intervención ha tenido un impacto positivo y sostenido en la población estudiada; es más, la disminución de la dispersión refuerza la idea de que la mejora no fue puntual, sino estructural, beneficiando de manera equitativa a los participantes.

2.3. Pruebas de hipótesis.

A continuación, se procede a realizar las pruebas de hipótesis que corresponden con cada uno de los objetivos planteados en esta investigación.

Resulta crucial, para elegir la prueba estadística correcta, confirmar si los datos muestran una distribución normal; así, se utilizó la prueba de normalidad de Shapiro-Wilk con un nivel de significancia del 5%, la cual nos ayuda a determinar si los datos que analizamos se ajustan a una distribución normal.

Las hipótesis planteadas para esta prueba son las siguientes:

Hipótesis nula (H_0): Los datos siguen una distribución normal ($p \geq 0.05$).

Hipótesis alterna (H_a): Los datos no siguen una distribución normal ($p < 0.05$).

Los resultados obtenidos en la prueba de Shapiro-Wilk se presentan en el Cuadro 12, permitiendo determinar la estrategia estadística más adecuada en los siguientes análisis.

Cuadro 12:

Prueba de normalidad de Shapiro - Wilk

Prueba	Estadístico	gl	p
Pre Test	0.842	20	0.004
D1 - Confidencialidad	0.888	20	0.025
D2 - Integridad	0.869	20	0.011
D3 - Seguridad	0.866	20	0.01
Prueba de Proceso	0.939	20	0.232
D1 - Confidencialidad	0.924	20	0.117
D2 - Integridad	0.934	20	0.183
D3 - Seguridad	0.817	20	0.002
Pos Test	0.844	20	0.004
D1 - Confidencialidad	0.638	20	<0.001
D2 - Integridad	0.811	20	0.001
D3 - Seguridad	0.736	20	<0.001

Los resultados de la prueba de Shapiro-Wilk indican que la mayoría de los test y sus dimensiones presentan valores de significancia menores a 0.05, excepto en la Prueba de Proceso y sus dimensiones D1 y D2, donde $p > 0.05$; esto implica que, en general, los datos no siguen una distribución normal, lo que impulsa a emplear pruebas no paramétricas.

Dado que el objetivo es comparar las medias en tres momentos distintos dentro de una misma muestra, se seleccionó el Test de Friedman como la prueba estadística más adecuada y para realizar comparaciones detalladas entre cada par de mediciones, con el objetivo de identificar cuál tiene el "mejor" promedio, se utilizó la prueba de Durbin - Conover como análisis Post Hoc. Este examen ayudó a identificar con precisión cuándo ocurren diferencias

significativas, ofreciendo una comprensión más clara de cómo cambian los resultados con el tiempo.

Con un nivel de significancia del 5% ($\alpha = 0.05$), se plantean las siguientes hipótesis para la contrastación estadística:

Regla de decisión de hipótesis.

H₀: $p \geq 0.05$ = No existen diferencias significativas entre las medias de los grupos, es decir, las tres mediciones presentan valores similares.

H_a: $p < 0.05$ = Al menos una de las medias es significativamente diferente, lo que indicaría cambios en los resultados a lo largo del tiempo.

Estas hipótesis fueron aplicadas tanto al objetivo general como a los objetivos específicos del estudio, permitiendo evaluar la efectividad del modelo y la variabilidad de los resultados en cada dimensión analizada.

Objetivo general (OG)

OG: Determinar el grado de mejora del modelo basado en la Norma ISO 27001:2022 y PCI DSS sobre la gestión de seguridad de la información en las Pymes de la industria textil, Lima 2024.

H₀: El modelo basado en la Norma ISO 27001:2022 y PCI DSS no mejora significativamente la gestión de seguridad de la información en las Pymes de la industria textil, Lima 2024.

H_a: El modelo basado en la Norma ISO 27001:2022 y PCI DSS mejora significativamente la gestión de seguridad de la información en las Pymes de la industria textil, Lima 2024.

Se aplicó el Test de Friedman a las evaluaciones totales correspondientes al Pre Test, Prueba de Proceso y Post Test con el fin de determinar si existen diferencias significativas entre las tres mediciones. Los resultados obtenidos en este análisis se presentan en la Cuadro 13, donde se detalla el valor de chi-cuadrado (χ^2), los grados de libertad (gl) y el nivel de significancia (p).

Cuadro 13:

Test de Friedman de las tres pruebas tomadas.

χ^2	gl	p
38.7	2	< .001

Dado que el valor de p obtenido es menor a 0.05, se acepta la hipótesis alternativa (H_a), es decir que existe una diferencia significativa entre al menos una de las mediciones (Pre Test, Prueba de Proceso y Post Test), esto indica que el modelo propuesto ha generado una mejora significativa en la gestión de la seguridad de la información en las pymes del sector textil en Lima durante el año 2024.

Para determinar específicamente entre qué pruebas existen diferencias significativas, se aplicó la prueba Post Hoc de Durbin–Conover. Esta prueba permitió realizar comparaciones dos a dos entre las mediciones, identificando cuál presenta la "mejor" media y dónde se localizan las diferencias más relevantes, tal como se muestra en el Cuadro 14.

Cuadro 14:

Comparaciones con el Test de Durbin-Conover

Pares de evaluación	Estadístico	p
Pretest - Prueba Proceso	18.6	< .001
Pretest - Post Test	33.2	< .001
Prueba Proceso - Post Test	14.7	< .001

Dado que en todas las comparaciones se obtuvo un p menor a 0.05, se confirma que las puntuaciones de las tres pruebas (Pre Test, Prueba de Proceso y Post Test) son significativamente diferentes entre sí.

Este resultado respalda la existencia de cambios estadísticamente significativos en cada fase de la evaluación. En términos prácticos, estos hallazgos refuerzan la eficacia del modelo implementado, ya que no solo se observan mejoras al comparar la primera y la última medición, sino que también se evidencian avances significativos desde las etapas intermedias, indicando que los cambios fueron constantes y sostenibles en el tiempo.

Objetivos específicos (OE)

OE1: Determinar el grado de mejora del modelo basado en la Norma ISO 27001:2022 y PCI DSS sobre la confidencialidad de la información en las Pymes de la industria textil, Lima 2024.

Ho: El modelo basado en la Norma ISO 27001:2022 y PCI DSS no mejora significativamente la confidencialidad de la información en las Pymes de la industria textil, Lima 2024.

Ha: El modelo basado en la Norma ISO 27001:2022 y PCI DSS mejora significativamente la confidencialidad de la información en las Pymes de la industria textil, Lima 2024.

Para evaluar el objetivo específico 1, se analizó la primera dimensión: Confidencialidad en las tres pruebas realizadas (Pre Test, Prueba de Proceso y Post Test). Los resultados obtenidos se presentan en el Cuadro 15, permitiendo determinar si hubo cambios significativos en esta dimensión a lo largo del proceso.

Cuadro 15:

Test de Friedman de la dimensión confidencialidad.

χ^2	gl	p
36.5	2	< .001

Con un nivel de significancia del 5% y dado que el valor de p en la dimensión de confidencialidad fue menor a 0.05 (Cuadro 15), se acepta la hipótesis alterna; es decir existe diferencia significativa entre las pruebas tomadas, confirmando que el modelo implementado fue efectivo en mejorar la confidencialidad de la información, evidenciando un alto nivel de protección de los datos en las pymes textiles y reflejando avances significativos en las prácticas de seguridad para garantizar la preservación de la información.

A continuación, el Cuadro 16 muestra los resultados de la prueba Post Hoc de Durbin–Conover, con las comparaciones dos a dos entre las tres pruebas (Pre Test, Prueba de Proceso y Post Test) dentro de la dimensión Confidencialidad. Esta prueba complementaria nos permitió identificar entre qué pruebas específicas se presentan dichas diferencias y determinar si los cambios observados siguen un patrón de mejora progresiva.

Cuadro 16:*Comparaciones con el Test de Durbin-Conover - dimensión confidencialidad*

Pares de evaluación	Estadístico	p
Conf. Pretest - Conf. P Proceso	9.62	< .001
Conf. Pretest - Conf. Post Test	20.04	< .001
Conf. P Proceso - Conf. Post Test	10.42	< .001

Los resultados de la prueba Post Hoc de Durbin–Conover muestran que todas las comparaciones por pares son significativas; es decir el valor que obtiene p es menos a 0.05, indicando que la dimensión confidencialidad presenta diferencias estadísticamente relevantes en cada una de las pruebas evaluadas.

Este hallazgo revela una mejora progresiva y sostenida en la dimensión confidencialidad a lo largo del tiempo, ya que la significancia en todas las comparaciones indica que cada fase representa un avance significativo respecto a la anterior, reforzando la efectividad del modelo, y respaldando la idea de que la intervención tuvo un impacto positivo, continuo y consistente.

OE2: Determinar el grado de mejora del modelo basado en la Norma ISO 27001:2022 y PCI DSS sobre la integridad de la información en las Pymes de la industria textil, Lima 2024.

Ho: El modelo basado en la Norma ISO 27001:2022 y PCI DSS no mejora significativamente la integridad de la información en las Pymes de la industria textil, Lima 2024.

Ha: El modelo basado en la Norma ISO 27001:2022 y PCI DSS mejora significativamente la integridad de la información en las Pymes de la industria textil, Lima 2024.

Para analizar el objetivo específico 2, se evalúa la segunda dimensión: Integridad en las tres pruebas realizadas (Pre Test, Prueba de Proceso y Post Test). Los resultados obtenidos se presentan en la Cuadro 17, el cual permitió determinar si hubo cambios significativos en la dimensión a lo largo del tiempo.

Cuadro 17:*Test de Friedman de la dimensión integridad*

χ^2	gl	p
29.3	2	< .001

Con un nivel de significancia del 5% y dado que el valor de p en la dimensión de integridad fue menor a 0.05 (Cuadro 17), se acepta la hipótesis alterna, esto indica que existen diferencias significativas en la dimensión integridad entre las tres pruebas, confirmando que el modelo implementado fue efectivo en mejorar la integridad de la información, evidenciando un fortalecimiento en la precisión, consistencia y confiabilidad de los datos manejados por las pymes textiles, y subrayando el impacto positivo del modelo en la preservación de la calidad y exactitud de la información.

El Cuadro 18 presenta los resultados de la prueba Post Hoc de Durbin–Conover, el cual examina las diferencias entre cada par de evaluaciones (Pre Test, Prueba de Proceso y Post Test) dentro de la dimensión Integridad, ayudando a precisar en qué momentos específicos ocurrieron cambios y si la evolución de los puntajes refleja un patrón de mejora constante a lo largo del tiempo.

Cuadro 18:

Comparaciones con el Test de Durbin-Conover - dimensión integridad.

Pares de evaluación	Estadístico	p
Integ. Pretest - Integ. P Proceso	9.39	< .001
Integ. Pretest - Integ. Post Test	8.16	< .001
Integ. P Proceso - Integ. Post Test	1.23	0.226

Los resultados muestran que, en los dos primeros pares de comparaciones (Integ. Pretest - Integ. P Proceso y Integ. Pretest - Integ. Post Test), se identifican diferencias estadísticamente significativas, dado a que el valor que tiene p es menor a 0.05, indicando que la dimensión Integridad presentó un cambio relevante en estas fases, evidenciando una mejora sustancial en los puntajes tras la implementación del modelo.

Sin embargo, en la comparación entre la Prueba de Proceso y el Post Test, no se encontró una diferencia significativa, ya que p obtiene un valor mayor a 0.05 ($p = 0.226$). Esto sugiere que, si bien hubo una evolución notable

en la primera etapa de la intervención, los valores de integridad se estabilizaron después de la Prueba de Proceso, sin una variación significativa en la fase final.

Es decir, el resultado indica que la mayor mejora en integridad ocurrió en la primera etapa de intervención y que, posteriormente, los puntajes se mantuvieron consistentes; además, se puede interpretar como una rápida asimilación de los cambios en esta dimensión, donde los beneficios del modelo se consolidaron sin necesidad de mayores fluctuaciones en el tiempo.

OE3: Determinar el grado de mejora del modelo basado en la Norma ISO 27001:2022 y PCI DSS sobre la disponibilidad de la información en las Pymes de la industria textil, Lima 2024.

Ho: El modelo basado en la Norma ISO 27001:2022 y PCI DSS no mejora significativamente la disponibilidad la información en las Pymes de la industria textil, Lima 2024.

Ha: El modelo basado en la Norma ISO 27001:2022 y PCI DSS mejora significativamente la disponibilidad la información en las Pymes de la industria textil, Lima 2024.

Para abordar el objetivo específico 3, se examinó la evolución de la dimensión disponibilidad en las tres pruebas realizadas (Pre Test, Prueba de Proceso y Post Test), tal como se presentan en el Cuadro 19, lo cual permitió determinar si la intervención produjo cambios significativos en la percepción de la disponibilidad.

Cuadro 19:

Test de Friedman de la dimensión integridad.

χ^2	gl	p
38	2	< .001

Con un nivel de significancia del 5% y dado que el valor de p en la dimensión de disponibilidad fue menor al 0.05 (según el Cuadro 19), se acepta la hipótesis alterna, esto indica que existen diferencias significativas en la dimensión entre las tres pruebas (Pre Test, Prueba de Proceso y Post Test);

es decir, el modelo implementado fue efectivo en mejorar la disponibilidad de la información, evidenciando un acceso más oportuno y consistente a los datos cuando estos son requeridos, garantizando que la información esté accesible para los usuarios autorizados de manera confiable y continua.

Para determinar en qué momentos específicos se producen diferencias, se procedió con la prueba Post Hoc de Durbin–Conover, que permitió analizar comparaciones dos a dos entre las pruebas y establecer si la evolución sigue un patrón de mejora progresiva o si hubo fases de estabilización. Los resultados detallados se presentan en el Cuadro 20.

Cuadro 20:

Comparaciones con el Test de Durbin-Conover - dimensión disponibilidad.

Pares de evaluación	Estadístico	p
Disp. Pretest - Disp. P Proceso	16	< .001
Disp. Pretest - Disp. Post Test	26.7	< .001
Disp. P Proceso - Disp. Post Test	10.7	< .001

Los resultados muestran que, en todas las comparaciones entre todas las pruebas, el valor de p es menor a 0.05, lo que confirma la existencia de diferencias estadísticamente significativas en todos los casos.

Esto sugiere que la dimensión disponibilidad ha experimentado cambios significativos y sostenidos a lo largo del tiempo, reforzando la conclusión de que la dimensión confidencialidad mejoró de manera consistente en cada una de las pruebas evaluadas.

2.4. Discusiones.

Para el objetivo general, el análisis global del modelo evidenció diferencias significativas entre las tres evaluaciones, con un valor de $p = 0.001$ respaldando la hipótesis de que el modelo mejora significativamente la gestión de seguridad de la información en las pymes del sector textil, los cuales se alinean con los hallazgos de Contador y Tapia (2023) quienes, en un estudio realizado en una empresa minera en Lima, evidenciaron que la adopción de la norma ISO/IEC 27001 mejoró la seguridad de la información, con un valor

de significancia $p = 0.000$, inferior al umbral de 0.05. Del mismo modo, la indagación de Rodríguez et al. (2020) demostró que la implementación de la ISO/IEC 27001 promueve una mejora continua en la gestión de la seguridad de la información, dado que obtuvo un valor de $p = 0.005$, confirmando su impacto positivo y sostenido en la protección de datos organizacionales.

Los resultados logrados en esta investigación, sumados a otros análisis ya realizados sobre la aplicación de la norma ISO/IEC 27001 para la gestión de la seguridad de la información, se ven reforzados por la investigación de (Avila, 2023), en su estudio, enfocado en el sector público de Ecuador, se hizo evidente una baja importante en las vulnerabilidades del sistema y una mejora en el control de accesos. Asimismo, el trabajo de Asad et al. (2022), hecho en el entorno corporativo, mostró que implementar un SGSI basado en ISO/IEC 27001 no solo refuerza la seguridad de la información, sino que también influye de forma positiva en el rendimiento económico de las empresas.

Respecto al primer objetivo específico, el estudio revela que el aspecto de confidencialidad demostró un nivel de significancia de $p = 0.001$. Esto apunta a avances constantes y estadísticamente relevantes en lo que respecta a la gestión de la seguridad de la información. Estos resultados se alinean con la investigación de Trujillo (2023), que señaló una fuerte correlación de 0.532 y un valor p de 0.000 mientras examinaba la aplicación de la norma ISO/IEC 27001 dentro de un departamento de TI del sector público en Lima, enfatizando el impacto sustancial de la norma en la disponibilidad de la información.

De manera similar, el estudio de Lopez y Espinoza (2022), conducida en una firma de gestión económica con 18 personas, mostró que usar un SGSI mejoró bastante las defensas de acceso a la información; por otro lado, Alshurideh et al. (2023), al analizar el campo de la logística, probaron que poner en práctica normas de seguridad sólidas eleva la protección de los datos, notando la relevancia de mandos concretos para guardar la confidencialidad.

La dimensión integridad mostró un nivel de significancia de $p = 0.001$. Esto apunta a mejoras considerables, junto con un patrón que indica

estabilización después de alcanzar un nivel de control ideal. Estos resultados encuentran correspondencia con el estudio de Coronado (2024) donde se reportó un valor de $p = 0.000$ (< 0.05); es decir que la implementación de controles específicos del SGSI basado en la ISO/IEC 27001:2022 garantizó la protección de la integridad de los activos de información en una entidad pública del sector defensa en la ciudad de Lima.

Así mismo, estos resultados fueron semejantes con la investigación de Asqui y Torres (2023) ejecutada dentro de una institución educativa en Lima, donde indicaron que los controles basados en la ISO 27001 mejoran la integridad de la información, esto tras identificar que el valor de p es igual 0,025. Complementariamente, la investigación de Villarreal (2023) en el ámbito universitario, demostraron mejoras sustanciales en la precisión y consistencia de los datos, esto tras la aplicación de metodologías mixtas y normas internacionales; del mismo modo, el trabajo de Guizado (2024) en una municipalidad de Lima respalda la idea de que la implementación de un SGSI establece una alta integridad generando garantía en sus bases de datos que dispone, además de prevenir a cualquier cambio no autorizado.

La dimensión disponibilidad arrojó un $p = 0.001$, lo que indica mejoras continuas, significativas y la accesibilidad de la información de manera oportuna para los usuarios autorizados; estos hallazgos son consistentes con la investigación de Aleman (2023) que en un estudio pre-experimental en una firma de consultoría privada evidenció que la implementación de la ISO 27001:2013 mejora y gestiona correctamente la disponibilidad de la información, esto tras encontrar que el valor de $p = 0.000$

Del mismo modo, los hallazgos de Medina (2023) en el área TI de una empresa industrial en Lima revelaron un valor de $p = 0.021$ evidenciando que la ISO 27001 influye de manera positiva en la disponibilidad de la información, optimizando la accesibilidad y continuidad operativa de los sistemas; así mismo, Silva (2022) aportó evidencia adicional al demostrar que una adecuada estructuración organizacional, junto con el fortalecimiento de los sistemas de seguridad, incrementa la disponibilidad de la información, permitiendo un acceso confiable y constante a los datos.

asimismo, desempeñan un papel crucial como generadoras principales de empleo a escala nacional (Jauregui, 2023).

Sin embargo, son estas entidades las que exhiben un nivel de madurez inferior y una mayor susceptibilidad en relación con los riesgos de seguridad de la información y la capacidad de recuperación. Según (Bustillos & Rojas, 2022) el 57 % de las pymes señalan que, en caso de un ataque, es probable que sufran quiebras o cese de operaciones; esto se debe a que las medidas de seguridad se perciben como demasiado complicadas, lentas y demandantes en términos de conocimientos técnicos, así como recursos financieros elevados.

Según las afirmaciones, (Jelovčan et al., 2022) estas empresas deben llevar a cabo un análisis exhaustivo de sus capacidades y necesidades antes de tomar decisiones respecto a la gestión de la seguridad de la información, considerando criterios claves, como la continuidad del negocio y la supervisión administrativa y gerencial, permitiendo adoptar decisiones estratégicas basadas en una evaluación rigurosa de sus propias capacidades y contextos particulares.

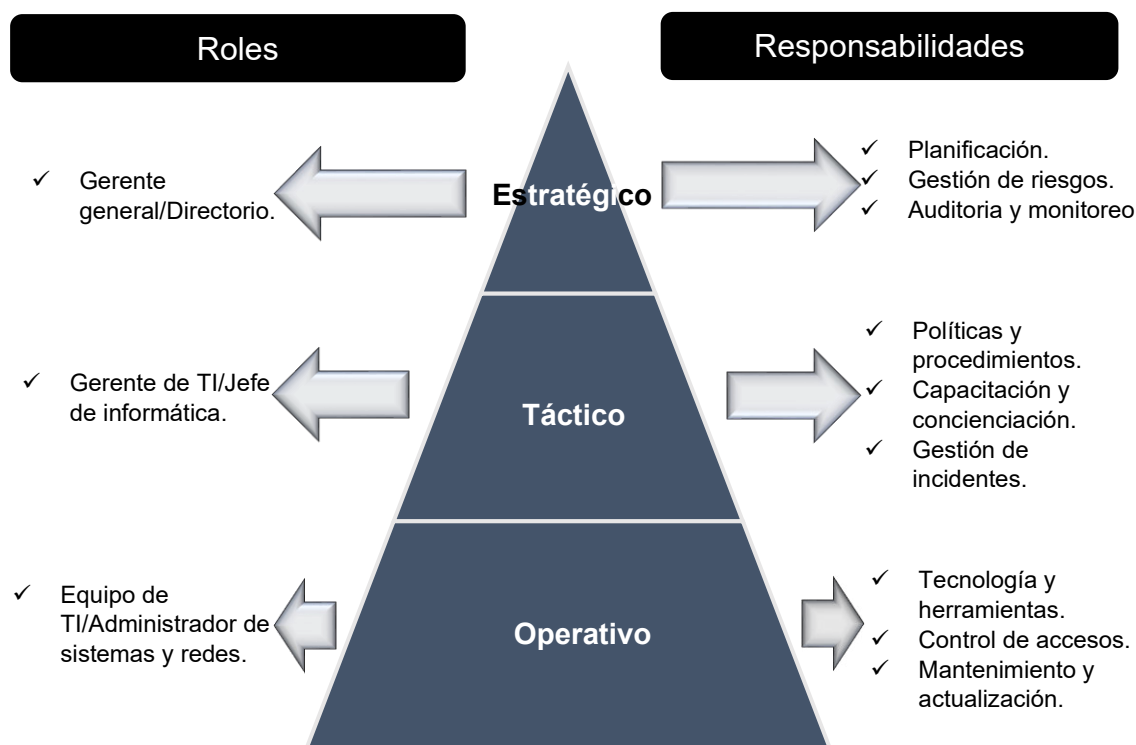
En ese sentido, coincidimos con (Alotaibi et al., 2023) donde garantizar la seguridad de la información requiere la integración de modelos o conjuntos de políticas de seguridad de la información para asegurar tanto la protección de datos sensibles como el funcionamiento óptimo de los sistemas informáticos; abarcando aspectos como la seguridad física, el control de acceso, el cifrado de datos y la autenticación de usuarios, evitando el acceso no autorizado, la alteración, divulgación o destrucción no deseada; además, (Shaikh & Siponen, 2023) sostienen que éstas directrices deben ser adaptadas dependiendo al nivel de riesgo y al perfil de cada pyme.

Así mismo, es importante que las pymes textiles establezcan una estructura organizativa dedicada a la gestión de la seguridad de la información, incorporando procesos estratégicos, tácticos y operativos. Este organigrama debe garantizar la protección de datos críticos, el cumplimiento de normativas y la continuidad operativa, y fortalecer la confianza de los

clientes y socios al mantener segura la información empresarial, tal como a continuación se presenta (Figura 9).

Figura 9:

Organigrama para las pymes.



Como se ilustra en la Figura 9 en el nivel superior, el gerente general y los miembros del directorio están organizados en el proceso estratégico, donde sus principales responsabilidades incluyen la planificación de la estrategia empresarial, la gestión de riesgos, la programación de auditorías y el monitoreo continuo de las operaciones, a fin de asegurar el cumplimiento de los objetivos a largo plazo de la pyme y mantener un control efectivo sobre las actividades y recursos.

Dentro del proceso táctico, el gerente o jefe de TI juega un papel fundamental, ya que sus responsabilidades incluyen la implementación y el cumplimiento de las políticas de seguridad, asegurando que los sistemas, redes y bases de datos estén configurados y gestionados adecuadamente para mitigar vulnerabilidades ante posibles amenazas; además, deben organizar y ejecutar capacitaciones en aras de desarrollar una cultura de

seguridad, donde cada empleado entienda su rol en la protección de los datos empresariales y conozca los protocolos a seguir en situaciones de riesgo.

También son responsables del proceso de identificación temprana de problemas, respuesta inmediata, y resolución de incidentes de seguridad, esto no solo incluye la contención de los daños, sino también un análisis posterior para identificar las causas y evitar que se repitan en el futuro. Esta función requiere una preparación constante, protocolos de comunicación definidos, y la capacidad de coordinar con otros departamentos para restaurar rápidamente las operaciones.

En el nivel inferior, el equipo de TI o administrador de sistemas y redes pertenecen al proceso operativo porque, a nivel práctico, sus funciones aseguran que la tecnología, el software, el hardware, y las herramientas informáticas estén alineados con las necesidades diarias de la pyme; además, la gestión de controles de acceso es una tarea central, el equipo de TI debe establecer y supervisar los niveles de permisos para cada usuario, minimizando así el riesgo de accesos no autorizado.

Por otro lado, el mantenimiento y la actualización de sistemas y equipos informáticos son esenciales para el funcionamiento sin interrupciones, estas actividades incluyen la reparación de hardware, la actualización de software para incorporar parches de seguridad y mejoras de funcionalidad, y la monitorización continua del rendimiento de los sistemas. Al asegurar que la infraestructura tecnológica esté en óptimas condiciones, el equipo de TI contribuye directamente a que los procesos empresariales se realicen de manera fluida y eficiente, minimizando el riesgo de paradas o fallos en el sistema que puedan afectar la operatividad general de las pymes textiles.

Es así, que el enfoque planteado se fundamenta en un modelo de gestión de seguridad de la información, cuyo eje central es la Norma ISO 27001:2022; adicionalmente, incorpora ciertas políticas del estándar PCI DSS enfocadas en proteger la información sensible de las tarjetas de pago, ello considerando la relevancia de las transacciones bancarias en las operaciones diarias de las pymes textiles. Este modelo está estructurado en cuatro fases principales, las cuales se detallan a continuación:

5.1.3. Fases del modelo.

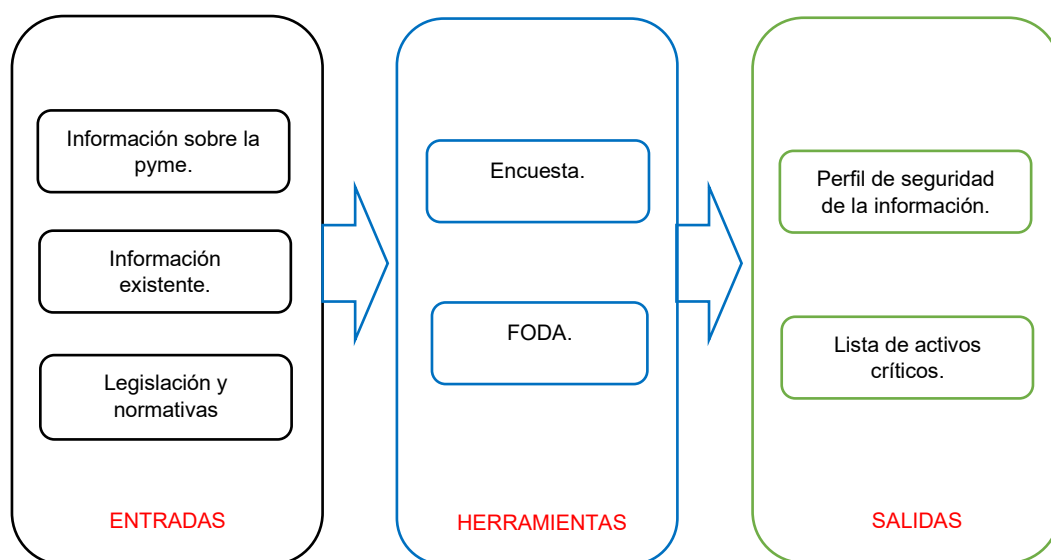
Fase I: Diagnóstico

En esta fase, la meta central consiste en analizar cómo están las pequeñas y medianas empresas textiles respecto a las exigencias del esquema de protección de datos. Para conseguirlo, es necesario cumplir los siguientes propósitos:

- ✓ Averiguar cómo se maneja hoy la información en las pymes textiles mediante una encuesta.
- ✓ Entender el entorno en que se desenvuelven las pymes textiles, incluyendo su forma, actividades y medios disponibles.
- ✓ Señalar y ordenar los elementos de información cruciales para las pymes textiles, tales como datos de usuarios, proveedores, información económica, bienes tangibles y demás datos delicados.

Figura 10:

Proceso de fase diagnóstica.



En una pequeña empresa, el diagnóstico comienza con un análisis a fondo de su estado presente. Esto se logra por medio de actividades específicas que reúnen y revisan datos esenciales sobre su rendimiento, recursos y organización. Estas "entradas" son vitales porque ofrecen una

perspectiva completa del estado actual, lo que hace posible evaluar de forma realista las fortalezas y las áreas que deben mejorarse.

Durante esta etapa, se reúne y se valora una variedad de información, como registros operativos, informes de finanzas y métricas de productividad, junto con cualquier regla o ley que se aplique al sector; esto también considera el análisis de políticas internas y de seguridad, garantizando que cumplen con los criterios de la industria y las leyes.

Para obtener esta información, es fundamental utilizar herramientas de diagnóstico que permitan capturar una visión completa de las pequeñas empresas textiles. Una de las técnicas clave es la encuesta dirigida a las partes interesadas, que abarca tanto a empleados como a otros actores relevantes, lo que posibilita reunir perspectivas internas y externas sobre el funcionamiento y las necesidades.

La encuesta debe tener preguntas previamente revisadas y valoradas por expertos, quienes certifiquen que están orientadas con precisión a la recopilación de la información requerida y que se eliminan los sesgos en la investigación. Asimismo, se sugiere dividir las preguntas según los principios de confidencialidad, integridad y disponibilidad, con opciones de respuesta tipo Likert; esta estructura facilitará un análisis detallado y cuantificable de cada aspecto crítico de la seguridad de la información, lo que permite identificar las áreas de mejora de manera precisa y eficaz.

Por otro lado, el análisis FODA (Fortalezas, Oportunidades, Debilidades y Amenazas) es otra herramienta esencial en esta etapa, puesto que ayuda a estructurar y evaluar diversos factores que afectan a las pequeñas empresas textiles. A través de este análisis, la empresa puede reconocer sus ventajas competitivas y puntos débiles, así como detectar oportunidades de crecimiento y posibles peligros en su entorno. Al combinar estas herramientas, se logra una comprensión profunda y estructurada del estado actual de la empresa, estableciendo las bases para la formulación de estrategias y acciones de mejora.

Toda la información recopilada en esta fase diagnóstica tiene como objetivo crear un perfil de seguridad detallado para las pequeñas empresas

textiles, lo que proporciona una visión clara de sus prácticas y necesidades en seguridad de la información; este perfil incluirá una lista de activos, identificando aquellos datos, software, hardware, personas e infraestructura que son fundamentales para la continuidad y el éxito de las operaciones. En el Cuadro 21, se muestra una plantilla para los activos, que debe llenarse de acuerdo con el contexto de la empresa; estos activos se someterán a un proceso de evaluación para determinar su nivel de criticidad y cuáles necesitan medidas de seguridad adicionales.

Cuadro 21:

Plantilla para la lista de activos de información

Categoría	Activo	Descripción
Datos		
Software		
Hardware		
Personas		
Infraestructura		

Clasificar los activos en categorías como datos, software, hardware, personas e infraestructura permite una identificación más completa y detallada de todos los recursos esenciales para alcanzar los objetivos estratégicos. Esta segmentación facilita la identificación de las interdependencias entre los activos y asegura que cada uno reciba la atención adecuada según su importancia en los procesos operativos; además, este enfoque contribuye a una gestión más eficiente, priorizando la protección y optimización de los elementos críticos para la continuidad y el éxito de las pymes textiles; tal como se muestra en el Anexo 3, como parte de la evaluación dentro de una pyme objeto de estudio.

Valoración de los activos de información.

Tras la identificación de los activos claves dentro de los procesos fundamentales de las pymes textiles, es imprescindible proceder con su valoración. Esta evaluación es esencial para establecer el valor específico de cada activo y estimar las consecuencias que su posible fallo tendría en la continuidad operativa. A continuación, se presenta el Cuadro 22, que describe los criterios aplicables para efectuar esta valoración, los valores asignados y su descripción en el contexto operativo.

Cuadro 22:

Criterios para la evaluación.

Criterios	Valor	Descripción
Confidencialidad	0	No es relevante
	1	Inconvenientes menores, pero la operación se mantiene.
	2	Pérdida de competitividad o demoras en la producción.
	3	Pérdidas financieras significativas, daño reputacional y posible pérdida de clientes claves.
Integridad	0	No es relevante
	1	Impacto mínimo en las operaciones o productos.
	2	Pérdida de precisión en la producción o calidad de los productos.
	3	Graves consecuencias, afectando significativamente la operación y los productos.
Disponibilidad	0	No es relevante
	1	Afectaría ligeramente las operaciones, pero es recuperable.
	2	Afectaría significativamente las operaciones durante un tiempo limitado.
	3	Causaría una interrupción grave, deteniendo operaciones críticas.

Es esencial que los criterios utilizados para la valoración de los activos en las pymes textiles se basen en la confidencialidad, integridad y disponibilidad, porque así se asegura una revisión completa y adaptada a las necesidades propias del sector. Por un lado, la **confidencialidad** protege la información delicada, como los datos de clientes y proveedores, restringiendo el acceso a personal autorizado y protegiendo la propiedad intelectual. Por otro lado, la **integridad** asegura que los datos operativos y financieros sean exactos y sin cambios no permitidos, evitando errores en la producción. Finalmente, la **disponibilidad** garantiza que los sistemas y datos esenciales

estén disponibles cuando se requieran, ayudando a la empresa a cumplir con los tiempos de producción sin pausas.

Para calcular la puntuación final de un activo, se suman los valores asignados a su confidencialidad, integridad y disponibilidad, cada uno de ellos entre 0 y 9. El total determina entonces qué tan crítico es el activo y se clasifica en las siguientes categorías:

- ✓ **No Aplica (0):** Activos que no requieren medidas especiales de seguridad.
- ✓ **Bajo (1-3):** Activos que, en caso de fallo, causan un impacto mínimo a la operación diaria.
- ✓ **Medio (4-6):** Activos cuya falla provoca un impacto moderado en la eficiencia y calidad de la operación.
- ✓ **Alto (7-9):** Activos críticos cuya falla ocasiona interrupciones graves, pérdidas financieras significativas y daño a la reputación de la empresa.

Para manejar este proceso, el Cuadro 23 muestra un diseño propuesto que organiza los datos en siete secciones, lo que simplifica la clasificación y el estudio de los activos de la pequeña empresa. Estas secciones van desde “ID de activo”, que otorga a cada recurso un código único, hasta la sección de “Críticidad”, que identifica qué tan clave es cada activo en función de su efecto en el funcionamiento de la empresa y su seguridad. Cada sección se completará utilizando los resultados de la evaluación, cubriendo aspectos como confidencialidad, integridad y disponibilidad, como se detalla en el Anexo 4.

Cuadro 23:

Nivel de criticidad de los activos.

ID	Activo	CRITERIOS DE VALORIZACIÓN			Valor final	Críticidad
		Confidencialidad	Integridad	Disponibilidad		
1	---	0	0	0	0	No aplica
2	---	1	1	1	3	Bajo
3	---	2	2	2	6	Medio
4	---	3	3	3	9	Alto

Al completar la evaluación de activos, se identificarán aquellos con una criticidad excepcionalmente alta debido a su impacto potencial en la continuidad del negocio y la seguridad de la información para las pymes textiles. Estos activos se presentarán luego siguiendo el marco esbozado en el Gráfico 24, que ofrece una plantilla específica, y el mismo que se muestra en el Anexo 5.

Cuadro 24:

Lista de activos críticos.

ID	Activo
1	---
2	---
3	---

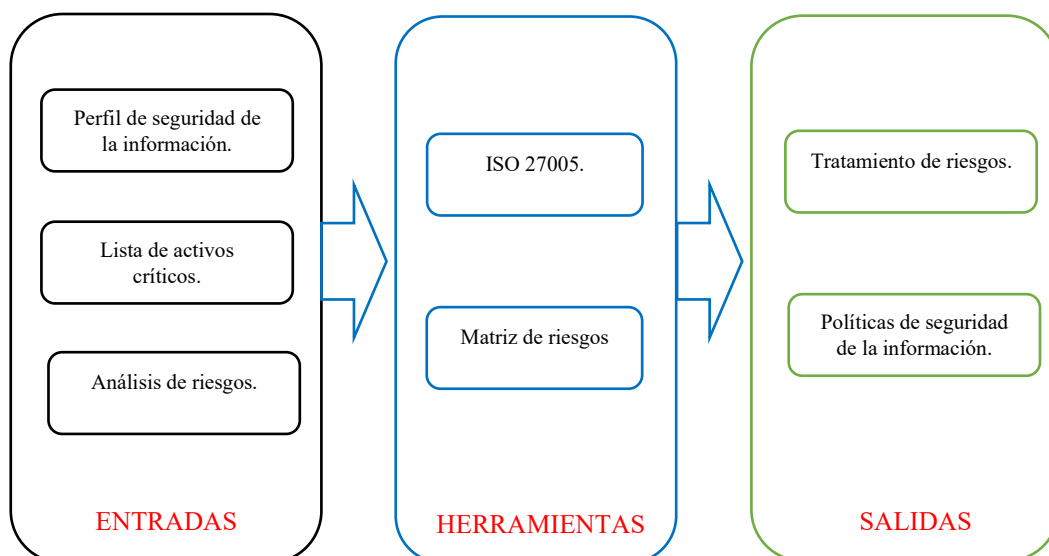
Fase II: Planificación

En esta etapa, nos adentramos en los diferentes aspectos y acciones claves que servirán para la construcción efectiva del modelo bajo el respaldo de la Norma ISO 27001:2022 e incorporando políticas del estándar PCCI DSS que estén íntimamente ligadas a la protección de tarjetas de pago, para lo cual es necesario:

- ✓ Realizar la identificación y **evaluación de riesgos** para determinar las amenazas y vulnerabilidades, evaluar impacto y probabilidad, y sobre todo priorizar acciones de mitigación.
- ✓ Identificar y seleccionar **políticas de seguridad** estipulados en la ISO 27001:2022 y PCI DSS que sean los adecuados para mitigar los riesgos.

Figura 11:

Proceso de planificación.



El proceso de planificación se basa en las salidas de la fase diagnóstica, ahora puntos de partida clave: la instantánea de seguridad de las pymes textiles y la lista que señala los activos críticos. También se incorpora algo crucial: El análisis de riesgos, lo que significa evaluar las amenazas y vulnerabilidades vinculados a esos activos, determinando el riesgo que corre cada uno de ellos ante problemas de seguridad.

Identificación y análisis de riesgos.

Para llevar a cabo la evaluación de los riesgos, se recomienda apoyarse en instrumentos como las pautas de la norma ISO 27005, las cuales entregan métodos para una estimación exacta. En el Cuadro 25 se puede observar una matriz de calor que calcula la probabilidad de que una amenaza aproveche una vulnerabilidad y el posible efecto ligado.

Cuadro 25:

Matriz de calor.

		PROBABIIDAD				
		Muy baja	Baja	Media	Alta	Muy Alta
IMPACTO	Muy bajo	Bajo	Bajo	Bajo	Bajo	Moderado
	Bajo	Bajo	Bajo	Bajo	Moderado	Relevante
	Medio	Moderado	Moderado	Relevante	Alto	Crítico

	Alto	Relevante	Relevante	Alto	Alto	Crítico
	Muy alto	Relevante	Relevante	Alto	Crítico	Crítico

Al utilizar esta matriz de calor, el objetivo es obtener una evaluación efectiva y detectar rápidamente riesgos altos o críticos, exigiendo una acción rápida porque podrían causar daños importantes. Al identificar estos niveles de riesgo, la matriz nos permite asignar recursos y tomar decisiones inteligentes para implementar políticas precisas y efectivas, garantizando que los riesgos más graves se gestionen de forma prioritaria y diferenciada especialmente en comparación con aquellos que son menos severos.

Probabilidad:

- *Muy baja*: Escasamente probable que ocurra.
- *Baja*: Poca probabilidad de ocurrencia.
- *Media*: Posibilidad moderada.
- *Alta*: Probabilidad considerable.
- *Muy alta*: Extremadamente probable.

Impacto:

- *Muy Bajo*: Impacto insignificante o sin efectos apreciables.
- *Bajo*: Interrumpe las operaciones hasta un máximo de 10 horas.
- *Medio*: Afecta las operaciones por hasta 24 horas.
- *Alto*: Interrumpe las operaciones por hasta 72 horas.
- *Muy Alto*: Impacto severo que afecta las operaciones por más de una semana.

Después de analizar y clasificar tanto la probabilidad como el impacto, se determina el nivel del riesgo los cuales son presentados en una matriz del Cuadro 26. Este proceso permitirá visualizar qué riesgos requieren atención prioritaria y cuáles tienen un impacto menor en las operaciones diarias a fin de diseñar estrategias efectivas de mitigación y asegurar la continuidad del negocio. Los resultados de la evaluación se presentan en el Anexo 6.

Cuadro 26:

Matriz de riesgos.

MATRÍZ DE RIESGO						
ID riesgo	Activo	Vulnerabilidad	Amenaza	Probabilidad	Impacto	Nivel riesgo
R1	---	---	---	---	---	Crítico
R2	---	---	---	---	---	Alto
R3	---	---	---	---	---	Relevante
R4	---	---	---	---	---	Moderado
R5	---	---	---	---	---	Bajo

Un riesgo se clasifica como **crítico** cuando su impacto es tan severo que afecta casi por completo la operatividad o viabilidad de las pymes textiles, poniendo en riesgo su continuidad; mientras que los riesgos **altos** son aquellos que, aunque no llegan a paralizar toda la organización, generan consecuencias graves que pueden afectar significativamente procesos claves, la reputación o los ingresos.

Los riesgos **relevantes** representan un nivel de amenaza considerable que exige atención, ya que afectan de manera importante ciertos aspectos de la organización, aunque sin comprometer totalmente su funcionamiento. Por otro lado, los riesgos **moderados** son aquellos con un impacto menor que puede gestionarse con acciones correctivas sin afectar de forma notable la operación, y los riesgos **bajos** presentan un nivel de amenaza mínimo, con consecuencias poco significativas y controlables con medidas rutinarias o preventivas.

Tratamiento de riesgos

Tras evaluar detalladamente los niveles de riesgo en función de las vulnerabilidades de cada activo y las amenazas que pueden comprometer su integridad, confidencialidad o disponibilidad, se establecerán criterios específicos para aceptar riesgos, tal como se muestran en el Cuadro 27. Estos criterios determinan si un riesgo es manejable dentro de los márgenes aceptables o si requiere acciones de mitigación adicionales. Con base en esta evaluación, se desarrollará el tratamiento de riesgos, abordando de manera proactiva y estratégica los riesgos identificados anteriormente, a fin de

proteger no solo los activos críticos, sino también garantizar la continuidad de las operaciones en las pymes textiles.

Cuadro 27:

Criterios de aceptación.

Nivel de riesgo	Criterio de aceptación
Bajo	Riesgo aceptable
Moderado	Riesgo aceptable
Relevante	Riesgo aceptable
Alto	Riesgo no aceptable
Crítico	Riesgo no aceptable

Un riesgo en las pymes textiles se clasifica como **aceptable** cuando su nivel se encuentra entre bajo, moderado y relevante, ya que, en estos casos el impacto en la operación es limitado y las consecuencias no compromete gravemente la continuidad de las actividades ni la estabilidad de la empresa, por lo que se considera manejable dentro de los procesos habituales y con recursos disponibles; además permiten a la pyme concentrarse en su actividad principal sin necesidad de implementar medidas complejas o costosas de mitigación.

Mientras que un riesgo clasificado como alto o crítico se considera **no aceptable**, ya que su potencial de impacto es significativo y podría poner en peligro la viabilidad del negocio; en estos casos, es fundamental tomar acciones de mitigación inmediatas, como implementar políticas de seguridad, rediseñar procesos o incluso contar con un plan de contingencia para reducir la probabilidad de ocurrencia o el daño en caso de materializarse.

Para abordar eficazmente los riesgos, es necesario identificar todos aquellos que, de acuerdo con los criterios de aceptación, se consideran no aceptables, como se muestra en el Cuadro 28; esta selección permitirá enfocar los esfuerzos en los riesgos con mayor impacto, garantizando que sean gestionados mediante medidas de mitigación adecuadas. Además, el Anexo 7 presenta los resultados de la evaluación realizada en una pyme.

Cuadro 28:

Riegos con mayor impacto.

MATRÍZ DE RIESGO						
ID riesgo	Activo	Vulnerabilidad	Amenaza	Probabilidad	Impacto	Nivel riesgo
R1	---	---	---	---	---	Alto
R2	---	---	---	---	---	Alto
R3	---	---	---	---	---	Crítico
R4	---	---	---	---	---	Crítico

Una vez identificados los riesgos no aceptables, es fundamental proponer políticas de seguridad que se ajusten a estándares reconocidos. En esta situación particular, las políticas antes mencionadas se organizan siguiendo los lineamientos de la norma ISO 27001:2022 y PCI DSS, tal como se muestra a modo de ejemplo en el Cuadro 29. Estas políticas deben abordar exhaustivamente los riesgos identificados y mantener a las pequeñas y medianas empresas en línea con las prácticas de seguridad de primer nivel a nivel mundial. El Anexo 8 presenta la lista de políticas identificadas.

Políticas de seguridad de la información:

Cuadro 29:

Políticas de seguridad basadas en ISO 27001: 2022 y PCI DSS.

Políticas de uso de los activos lógicos.	
1	La documentación física será almacenada correctamente en lugares con acceso a personas autorizadas.
2	Se realizarán copias de seguridad regulares para asegurar la disponibilidad de los datos.
3	No se revelará información de clientes y el estado de su crédito a ningún agente externo a la pyme.
4	Se prohíbe el almacenamiento de datos sensibles de autenticación, como códigos CVV, después de la autorización de la transacción.
5	Retener los datos de tarjetas solo durante el tiempo necesario para cumplir con los fines comerciales legítimos.

Políticas de uso de los activos físicos.	
1	Se prohíbe la alteración de las configuraciones ya establecidas.
2	Se utilizarán identificaciones personales y tarjetas de acceso para verificar la identidad.
3	Las áreas seguras serán definidas y categorizadas según la sensibilidad de los datos.
4	Los visitantes deberán registrarse y recibir una identificación temporal.
5	Se controlarán factores como temperatura, humedad y sistemas de detección de incendios.
Políticas de control de accesos.	
1	Todos los sistemas y aplicaciones deberán requerir autenticación mediante credenciales únicas para cada usuario.
2	Las contraseñas deberán cumplir con requisitos de complejidad, incluyendo longitud mínima, uso de caracteres especiales, números y letras.
3	Los accesos deberán ser desactivados inmediatamente cuando un empleado deje la pyme textil o cambie de rol.
4	Los trabajadores deben bloquear sus equipos de trabajo inmediatamente al salir del escritorio.
5	Restringir el acceso a los datos de tarjetas únicamente al personal autorizado mediante autenticación multifactor.
Políticas contra amenazas externas e internas	
1	Implementar y mantener firewalls y sistemas de detección de intrusos (IDS).
2	Realizar evaluaciones de vulnerabilidad periódicas en todos los sistemas que manejan datos de tarjetas.
3	Asegurar que todos los sistemas y software estén actualizados con los parches y actualizaciones de seguridad más recientes.
4	Configurar segmentación de la red para limitar el alcance de un posible ataque.
5	Monitorear todas las actividades en los sistemas y redes para detectar comportamientos inusuales o no autorizados.

Este enfoque segmentado de política de seguridad garantiza un manejo integral y una protección exhaustiva, adaptando cada sección a las distintas clases de activos y los peligros específicos que enfrenta la empresa, mejorando así la seguridad de la infraestructura y el flujo de trabajo operativo. Los segmentos se detallan a continuación:

- ✓ **Políticas de uso de los activos lógicos:** Establecen directrices para el manejo seguro de sistemas de información, datos y software, definiendo el uso adecuado y las restricciones necesarias para proteger la información digital contra accesos indebidos y pérdidas de integridad.
- ✓ **Políticas de uso de los activos físicos:** Regulan el acceso y manejo de equipos tangibles, como computadoras, dispositivos móviles y servidores, asegurando su correcto funcionamiento y protección frente a daños, robos o accesos no autorizados.
- ✓ **Políticas de control de accesos:** Establecen directrices claras sobre quién y bajo qué condiciones puede acceder a información y recursos críticos, limitando el acceso únicamente a personal autorizado y minimizando el riesgo de brechas de seguridad.
- ✓ **Políticas contra amenazas externas e internas:** Se centran en prevenir y mitigar ataques o vulnerabilidades, tanto de origen externo (ciberataques) como interno (como el uso indebido por empleados), mediante medidas de seguridad proactivas y reactivas.

Fase II: Ejecución

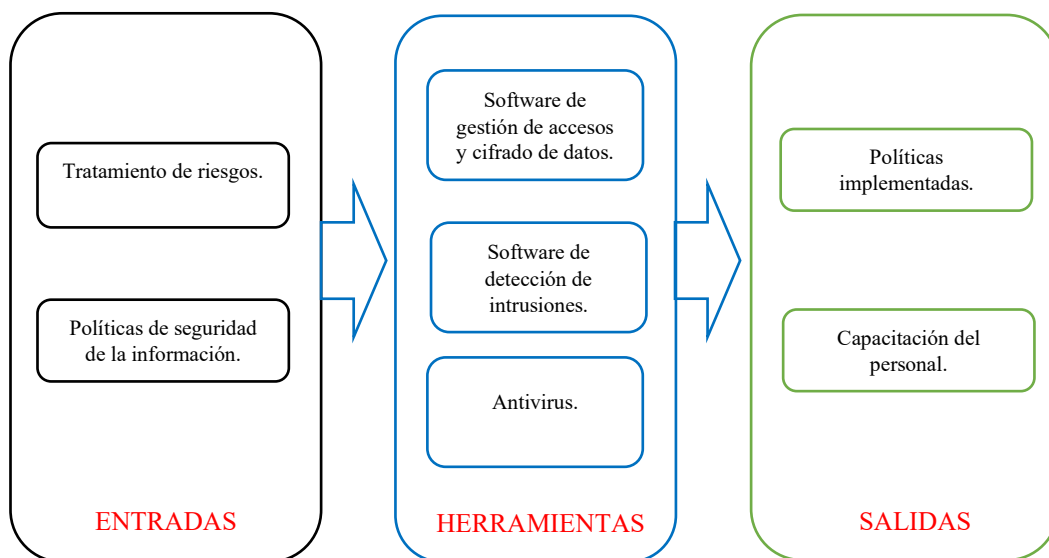
En esta fase se implementarán las políticas seleccionadas en la fase de planificación. Para lograr esto, se realizarán las siguientes actividades:

- ✓ Aplicar las políticas de seguridad identificadas.
- ✓ Mantener la **comunicación** efectiva para generar una cultura de seguridad dentro de las pymes textiles, y ejecutar **capacitaciones** periódicas a fin de mantener al personal informado sobre las políticas de seguridad, los riesgos y las mejores prácticas para proteger la información.
- ✓ Proporcionar **documentación** con una visión clara y transparente de los procesos, procedimientos y políticas, ayudando a garantizar que todos los involucrados comprendan sus roles y

responsabilidades, así como los requisitos de seguridad que deben seguir.

Figura 12:

Proceso de ejecución.



Para poner en marcha las políticas de seguridad, es esencial seleccionar herramientas adecuadas, ya que estas actuarán como facilitadoras para alcanzar los objetivos planteados. En esta situación específica, se usarán programas como **software de gestión de accesos y cifrado de datos**, que dará un control total sobre quién mira la información y cuidará los datos privados; **software de detección de intrusiones**, que permitirá monitorear continuamente los sistemas y emitir alertas en caso de accesos no autorizados; y **antivirus**, que dará un escudo ante los peligros y ataques de software dañino. La mezcla de estos medios hará una defensa fuerte para la estructura técnica de la empresa, cuidando que sus bienes digitales estén enteros, secretos y accesibles.

Una vez implantadas las políticas, es muy importante crear programas de capacitación para asegurarse de que todos conozcan y asuman sus obligaciones para mantener la seguridad de los datos, en función de su desenvolvimiento, como se ve en el Cuadro 30. Estos programas serán claves para informar y enseñar al personal sobre las principales formas, reglas y

pasos necesarios para proteger los activos y desarrollar una mentalidad de seguridad completa y con visión de futuro en todas las pymes textiles

Programas de capacitación al personal.

Cuadro 30:

Capacitaciones según su desempeño.

Estrategia	Tarea
Evaluación del personal.	Verificar si el personal asignado cuenta con la habilidad y competencia para cumplir con las tareas asignadas, mediante evaluaciones que consideren sus funciones y requisitos. Esto implica revisar tanto su formación académica como la experiencia laboral adquirida. Si se detecta alguna deficiencia, será necesario que la persona tome un curso de actualización o capacitación, o bien, buscar un sustituto adecuado para el puesto según corresponda.
Capacitación del personal.	Se aplicará al personal que haya demostrado carencias en el desempeño de su rol en la pyme, así como a aquellos que se incorporen como nuevos miembros. En el caso de estos últimos, la capacitación deberá adaptarse a las habilidades y competencias específicas que posean, con el fin de optimizar su formación.
Concientización del personal.	Es necesario implementar charlas periódicas de concientización para el personal, con el objetivo de recordarles los diversos riesgos de seguridad de la información presentes en el día a día, los cuales pueden afectar a la pyme textil.
Control	Toda evaluación, capacitación y charla de concientización impartida al personal debe registrarse formalmente para asegurar la trazabilidad y demostrar que se han cumplido con los

	procedimientos necesarios para el desarrollo de competencias y la concientización en temas relevantes, especialmente en seguridad de la información. Estos registros servirán como evidencia ante auditorías internas y externas, y permitirán evaluar el progreso y la efectividad de las medidas implementadas para minimizar riesgos y optimizar el rendimiento del personal en sus funciones.
--	---

Clasificar las capacitaciones en función del desempeño en evaluación, capacitación, concientización del personal y control permitirá a las pymes textiles concentrar sus esfuerzos y facilitar la comprensión de la información por parte de su equipo. Este enfoque sistemático no solo mejora la efectividad de los programas de capacitación, sino que también asegura que cada empleado reciba la formación adecuada según sus necesidades específicas; además, facilita una transmisión eficiente del conocimiento, fortaleciendo las competencias necesarias para desempeñarse eficazmente.

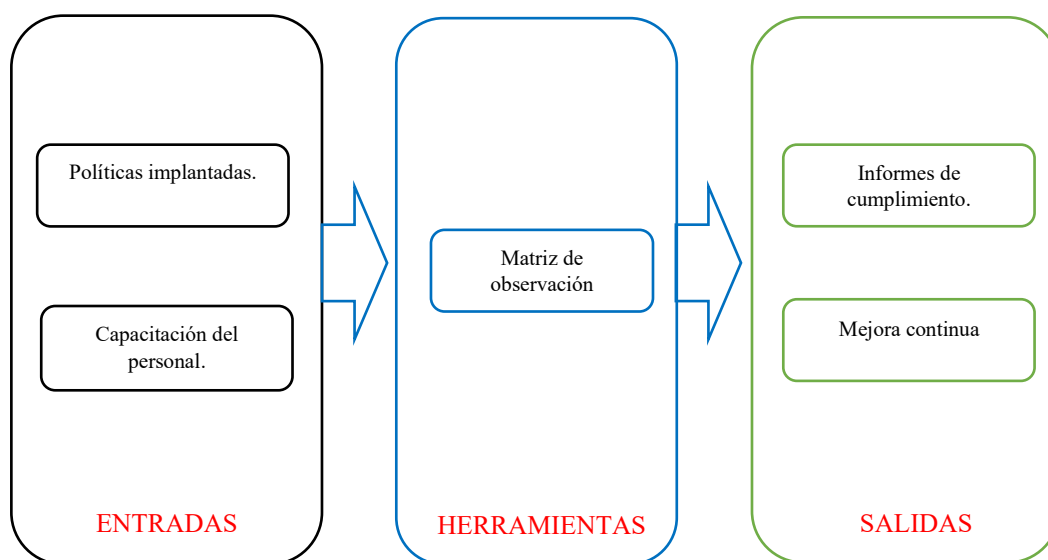
Fase III: Supervisión.

En esta última fase, se analizarán los resultados de la fase anterior, permitiendo:

- ✓ Establecer un proceso de **mejora continua** para **evaluar el desempeño** integrando retroalimentación o feedback para identificar áreas de mejora y tomar acciones.
- ✓ Establecer **medidas correctivas** o **preventivas** según sea el caso, y se determinará si el modelo influye de manera positiva para con la gestión de seguridad de la información, y cuán eficiente resulta ser para la pyme.

Figura 13:

Proceso de supervisión.



El proceso de supervisión toma como insumos el reporte de políticas implantadas y las capacitaciones del personal, que se definieron como resultados en la fase anterior. Estos elementos sirven de base para poner en marcha la herramienta denominada matriz de observación de políticas del Cuadro 31, la cual evalúa el grado de implantación de cada política mediante un rango de niveles que va desde el 0% (no existe) hasta el 100% (completado).

Esta matriz permite un seguimiento claro del avance en la adopción de las políticas de seguridad, facilitando la identificación de áreas que requieren ajustes o refuerzo para alcanzar el cumplimiento total, y ser tratadas en el ciclo de mejora continua.

Cuadro 31:

Matriz de observación de políticas.

Descripción	Puntaje	Nivel de cumplimiento	Descripción
No existe	1	0%	La política no existe.
Inicio	2	40%	La política está planificada implementarse, pues se ha identificado la necesidad de implementarse.
En proceso	3	70%	La política se encuentra en procesos de implementación.
Completado	4	100%	La política se ha implementado y se encuentra aprobado por la alta dirección.

Definidos los criterios de la matriz de observación, necesitamos enumerar las políticas implementadas que se mostraron anteriormente. Esto permitirá evaluar qué tan bien se está siguiendo cada uno. Para agilizar esta evaluación, es importante incluir comentarios específicos para cada política, destacando las mejoras necesarias para alcanzar plenamente los objetivos previstos, como se ejemplifica en el Cuadro 32.

Cuadro 32:

Relación de políticas implementadas.

Políticas de uso de los activos lógicos.		Nivel de cumplimiento				Comentarios
		0%	25%	50%	100%	
1	La documentación física será almacenada correctamente en lugares con acceso a personas autorizadas.					
2	Se realizarán copias de seguridad regulares para asegurar la disponibilidad de los datos.					
3	No se revelará información de clientes y el estado de su crédito a ningún agente externo a la pyme.					
4	Se prohíbe el almacenamiento de datos sensibles de autenticación, como códigos CVV, después de la autorización de la transacción.					
5	Retener los datos de tarjetas solo durante el tiempo necesario para cumplir con los fines comerciales legítimos.					
Políticas de uso de los activos físicos.		Nivel de cumplimiento				Comentarios
		0%	25%	50%	100%	
1	Se prohíbe la instalación de aplicativos que alteren el rendimiento.					

2	Se prohíbe la alteración de las configuraciones ya establecidas.					
3	Las áreas seguras serán definidas y categorizadas según la sensibilidad de los datos.					
4	Los visitantes deberán registrarse y recibir una identificación temporal.					
5	Se controlarán factores como temperatura, humedad y sistemas de detección de incendios.					
Políticas de control de accesos.		Nivel de cumplimiento				Comentarios
		0%	25%	50%	100%	
1	Todos los sistemas y aplicaciones deberán requerir autenticación mediante credenciales únicas para cada usuario.					
2	Las contraseñas deberán cumplir con requisitos de complejidad, incluyendo longitud mínima, uso de caracteres especiales, números y letras.					
3	Los accesos deberán ser desactivados inmediatamente cuando un empleado deje la pyme o cambie de rol.					
4	Los trabajadores deben bloquear sus equipos de trabajo inmediatamente al salir del escritorio.					
5	Restringir el acceso a los datos de tarjetas únicamente al personal autorizado mediante autenticación multifactor.					
Políticas contra amenazas externas e internas		Nivel de cumplimiento				Comentarios
		0%	25%	50%	100%	
1	Implementar y mantener firewalls y sistemas de detección de intrusos (IDS).					
2	Realizar evaluaciones de vulnerabilidad periódicas en					

	todos los sistemas que manejan datos de tarjetas.					
3	Asegurar que todos los sistemas y software estén actualizados con los parches y actualizaciones de seguridad más recientes.					
4	Configurar segmentación de la red para limitar el alcance de un posible ataque.					
5	Monitorear todas las actividades en los sistemas y redes para detectar comportamientos inusuales o no autorizados.					

Tras finalizar la verificación del cumplimiento según el formato del Anexo 9, es necesario crear un reporte con los hallazgos. Esto debe incluir observaciones detalladas de las áreas examinadas, junto con sugerencias concisas para futuras mejoras.

La **mejora continua** se enfocará en cada punto débil identificado, aplicando medidas correctivas y perfeccionando los procesos de protección. El objetivo es robustecer de manera continua la infraestructura de seguridad y reducir al mínimo los riesgos a futuro, garantizando que las pymes textiles se adapten a las nuevas amenazas y cumplan con las normativas fijadas.

Mejora continua.

Para llevar a cabo una mejora continua, es necesario organizarse según las ideas del ciclo PDCA (Planificar, Hacer, Verificar, Actuar), lo que hace posible aplicar cambios de manera ordenada y constante. Este ciclo, explicado más adelante, ayuda a tener un método estructurado para analizar, realizar y optimizar los procesos, garantizando que cada paso se ajuste a los propósitos de las pequeñas y medianas empresas textiles.

Planificar (Plan)

- ✓ Identificar las deficiencias actuales o las áreas que funcionan por debajo de las expectativas.

- ✓ Diseñar una estrategia bien definida con soluciones y salvaguardas adaptadas a cada objetivo de mejora.
- ✓ Establecer indicadores clave de desempeño (KPI) que hagan seguimiento a los avances y midan la efectividad de las estrategias implementadas.

Hacer (Do)

- ✓ Implementar las mejoras y correcciones necesarias en los procesos y sistemas encontrados durante la etapa de planificación.
- ✓ Confirmar que el equipo esté completamente consciente y listo para realizar las nuevas acciones o manejar actualizaciones de procedimientos.
- ✓ Documentar cada acción realizada y todos los problemas encontrados para facilitar cualquier control posterior.

Verificar (Check)

- ✓ Analiza los resultados obtenidos tras la implementación de las acciones de mejora, comparando estos datos con los indicadores de éxito definidos en la fase de planificación.
- ✓ Realiza revisiones para asegurar que los cambios han tenido el efecto deseado e identificar si existen áreas donde los objetivos no se cumplieron totalmente.
- ✓ Obtén retroalimentación del equipo y de otras partes interesadas para evaluar el impacto y la efectividad de las acciones.

Actuar (Act)

- ✓ Registrar los aprendizajes clave, las estrategias efectivas y cualquier área que aún necesite ajuste, lo cual servirá para futuros ciclos de mejora.
- ✓ La mejora continua es un proceso sin fin, ya que una vez implementados y documentados los cambios, se identificarán nuevas oportunidades de mejora y se repite el ciclo PDCA para avanzar continuamente.

5.2. Costos de la implementación de la propuesta.

5.2.1. Costos de personal.

Cuadro 33:

Costos de personal.

Ítem	Descripción	Costo (S/.)
1	Personal	S/ 1,500.00
Sub total		S/ 1,500.00

5.2.2. Costos de servicios y materiales.

Cuadro 34:

Costos de servicios y materiales.

Ítem	Descripción	Costo (S/.)
1	Consultoría externa	S/ 1,600.00
2	Servicio de internet	S/ 700.00
3	Servicios telefónicos	S/ 200.00
4	Energía eléctrica	S/ 900.00
Sub total		S/ 3,400.00

5.2.3. Costos de hardware.

Cuadro 35:

Costos de hardware.

Ítem	Descripción	Costo (S/.)
1	Laptop	S/ 2,300.00
Sub total		S/ 2,300.00

5.2.4. Otros gastos.

Cuadro 36:

Otros gastos.

Ítem	Descripción	Costo (S/.)
------	-------------	-------------

1	Papelería (Documentación)	S/ 2,300.00
2	Alimentación	S/ 950.00
3	Movilidad	S/ 300.00
Sub total		S/ 3,550.00

5.2.5. Resumen de costos.

Cuadro 37:

Resumen de costos.

Ítem	Descripción	Costo (S/.)
1	Costo de personal	S/ 1,500.00
2	Costo de servicios y materiales	S/ 3,400.00
3	Costos de hardware	S/ 2,300.00
4	Otros gastos	S/ 3,550.00
Costo total		S/ 10,750.00

5.1. Beneficios que aporta la propuesta.

La propuesta se fundamenta en un modelo integral de gestión de seguridad de la información que se apoya en estándares internacionales como la ISO 27001:2022 y el PCI DSS para optimizar la infraestructura de protección en pymes textiles. Este enfoque se estructura en un modelo jerárquico que distribuye las funciones y responsabilidades en tres niveles (estratégico – táctico - operativo).

Al identificar y evaluar cuantitativamente los activos críticos mediante criterios rigurosos y usar metodologías analíticas, como las matrices de riesgos y el análisis FODA, la propuesta promueve un enfoque holístico que refuerza la resiliencia organizacional, optimiza la asignación de recursos, permite una evaluación sistemática y cuantitativa de vulnerabilidades y amenazas y fortalece la cultura de seguridad en el entorno altamente competitivo y tecnológicamente exigente del sector textil.

Así mismo, la incorporación de ciclos de mejora continua mediante el modelo PDCA (Planificar, Hacer, Verificar, Actuar) en conjunto con programas

de capacitación sistemática permite establecer un proceso de retroalimentación constante que optimiza procesos y políticas, asegurando la actualización y competencias del personal en normativas y mejores prácticas; además, al identificar y mitigar de manera proactiva áreas de vulnerabilidad, se fortalece la resiliencia operativa, lo que resulta crucial para la sostenibilidad organizacional.

CONCLUSIONES

En la dimensión de confidencialidad, los resultados revelaron que el modelo implementado mejoró sustancialmente los métodos de control de acceso y redujo en gran medida los riesgos relacionados con la revelación de detalles privados. Esto demostró una estrategia más sólida para gestionar permisos y limitaciones, garantizando que los datos vitales se mantengan a salvo del ingreso no autorizado o el manejo inadecuado.

Respecto a la dimensión de integridad, los resultados mostraron una mejora significativa en la consistencia, precisión y confiabilidad de los datos. El modelo agilizó los procedimientos para evitar cambios indebidos, garantizando que la información procesada y guardada mantuviera su calidad y precisión, asegurando que fuera adecuada para la toma de decisiones estratégicas y operativas.

En lo que respecta a la dimensión confidencialidad, se observó una mejora en la habilidad del sistema para dar a los usuarios validados un acceso constante y rápido a los datos que necesitan. El modelo optimizó la base tecnológica y el manejo de operaciones, dando como resultado una mayor firmeza y mejor reacción ante mucha demanda o problemas inesperados.

En líneas generales, el esquema adoptado probó ser útil para mejorar el manejo de la protección de los datos en sus tres aspectos clave: confidencialidad, integridad y disponibilidad. Esto comprueba su efecto bueno al robustecer la seguridad en las pequeñas empresas textiles, elevando los grados de resguardo, confianza y facilidad de acceso de los recursos de datos esenciales.

RECOMENDACIONES

Para abarcar la totalidad de las pequeñas y medianas empresas, se debe expandir el modelo de gestión de seguridad de la información, generando un resguardo absoluto de la información en cada sector. Dicha expansión solidificará la seguridad en cada fase funcional, certificando la protección adecuada de los procesos de importancia; aparte, la fusión del sistema en cada sector hará posible un manejo constante de los peligros, aminorando las debilidades que pongan en riesgo los datos y la operación constante.

Priorizar un liderazgo activo y un seguimiento riguroso por parte de la alta dirección. Se aconseja que las empresas pequeñas y medianas fomenten activamente un entorno en donde la seguridad sea primordial, cosa que se consigue fijando planes definidos y proveyendo las herramientas indispensables. Por ende, es vital que se invierta en comunicación y formación constantes, para asegurar que cada empleado entienda por completo su función y deberes en la salvaguarda de los datos. Si se aplica esta visión global, en la que los líderes dan el ejemplo y cada quien se siente clave para la seguridad, la defensa de la información mejorará notablemente.

Fomentar el compromiso del personal con las actividades relacionadas con la seguridad de la información para evaluar su desempeño frente al modelo de gestión implementado y alcanzar los objetivos establecidos. Revisar seguido si se cumplen las normas ayuda a ver qué se puede mejorar y a perfeccionar los controles internos. Además, si los empleados colaboran buscando y reduciendo peligros, la seguridad de los procesos será mayor y habrá menos chances de que ocurran problemas.

Las pymes deben asumir el reto de obtener la Certificación ISO/IEC 27001:2022 para capitalizar su reputación hacia sus clientes y mejorar su percepción en el mercado nacional. La certificación no solo permitirá demostrar el compromiso con la seguridad de la información, sino que también ofrecerá una ventaja competitiva al garantizar el cumplimiento de estándares internacionales, facilitará el acceso a nuevas oportunidades comerciales,

mejorará la confianza de los clientes y socios estratégicos, y fortalecerá la resiliencia de la empresa frente a las amenazas cibernéticas.

REFERENCIAS BIBLIOGRÁFICAS

- Acosta, S. (2023). Los enfoques de investigación en las Ciencias Sociales. *Revista Latinoamericana Ogmios*, 3(8), 82-95. <https://doi.org/10.53595/RLO.V3.I8.084>
- AL-Dosari, K., & Fetais, N. (2023). Risk-Management Framework and Information-Security Systems for Small and Medium Enterprises (SMEs): A Meta-Analysis Approach. *Electronics (Switzerland)*, 12(17), 3629. <https://doi.org/10.3390/electronics12173629>
- Aleman, F. (2023). Norma ISO 27001 para el control de la seguridad de información en una consultoría privada, Lima 2023 [Universidad Cesar Vallejo]. En *Repositorio Institucional - UCV*. <https://repositorio.ucv.edu.pe/handle/20.500.12692/106824>
- Al-Khulaidi, A. A. G., Al-Ashwal, M. M. Y., Nasser, A. A., & Al-Anesi, N. K. (2023). Information Security Risk Management in Yemeni Banks: An Evaluation of Current Practices. *International Journal of Engineering Trends and Technology*, 71(4), 225-237. <https://doi.org/10.14445/22315381/IJETT-V71I4P220>
- Alotaibi, F., Al-Dhaqm, A., Yafooz, W., & Al-Otaibi, Y. (2023). A Novel Administration Model for Managing and Organising the Heterogeneous Information Security Policy Field. *Applied Sciences (Switzerland)*, 13(17), 9703. <https://doi.org/10.3390/app13179703>
- Alraja, M. N., Butt, U. J., & Abbod, M. (2023). Information security policies compliance in a global setting: An employee's perspective. *Computers and Security*, 129. <https://doi.org/10.1016/J.COSE.2023.103208>
- Alshurideh, M., Alquqa, E., Alzoubi, H., Al Kurdi, B., & Hamadneh, S. (2023). The effect of information security on e-supply chain in the UAE logistics and distribution industry. *Uncertain Supply Chain Management*, 11(1), 145-152. <https://doi.org/10.5267/J.USCM.2022.11.001>
- Amirinnisa, M., & Rahadian, B. (2023). Analisis Penilaian Risiko Keamanan Informasi Berdasarkan Iso 27005 Untuk Persiapan Sertifikasi Iso 27001 pada Pemerintah Kota Madiun. *Journal of Emerging Information System and Business Intelligence (JEISBI)*, 4(4), 47-58. <https://ejournal.unesa.ac.id/index.php/JEISBI/article/view/56250>
- Arogundade, O. (2023). Network Security Concepts, Dangers, and Defense Best Practical. *Computer Engineering and Intelligent Systems*, 14(2), 25-38. <https://doi.org/10.7176/CEIS/14-2-03>
- Asad, S., Bokhari, A., & Manzoor, S. (2022). Impact of Information Security Management System on Firm Financial Performance: Perspective of Corporate Reputation and Branding. *American Journal of Industrial and Business Management*, 12, 934-954. <https://doi.org/10.4236/ajibm.2022.125048>

- Asqui, J., & Torres, J. (2023). *ISO 27001 para mejorar la seguridad de la información en una institución educativa, Lima 2022*. <https://hdl.handle.net/20.500.13053/8519>
- Avila, A. (2023). Modelo de Sistema e Gestión de Seguridad de la Información, para establecer Controles basados en la Norma ISO/IEC 27001:2013 mediante el Código de Prácticas de Seguridad de la Información ISO/IEC 27002:2022 en el Departamento de Tecnologías de la Información del Gobierno Autónomo Descentralizado Municipal del Cantón Naranjal [Universidad Estatal de Milagro]. En *Repositorio de la Universidad Estatal de Milagro*. <http://repositorio.unemi.edu.ec/xmlui/handle/123456789/6971>
- Bahrami, L., Safaie, N., & Hamidi, H. (2021). Effect of Motivation, Opportunity and Ability on Human Resources Information Security Management Considering the Roles of Attitudinal, Behavioral and Organizational Factors. *International Journal of Engineering*, 34(12), 2624-2635. <https://doi.org/10.5829/ije.2021.34.12C.07>
- Bandari, V. (2023). Enterprise Data Security Measures: A Comparative Review of Effectiveness and Risks Across Different Industries and Organization Types. *International Journal of Business Intelligence and Big Data Analytics*, 6(1), 1-11. <https://research.tensorgate.org/index.php/IJBIBDA/article/view/3>
- Barraza, J., Rodríguez-Picón, L., Morales-Rocha, V., & Torres-Argüelles, S. (2023). A Systematic Review of Risk Management Methodologies for Complex Organizations in Industry 4.0 and 5.0. *Systems 2023, Vol. 11, Page 218, 11(5)*, 218. <https://doi.org/10.3390/SYSTEMS11050218>
- Bemenet, G., Gideon, J., & Sileshi, Y. (2023). Information security challenges during digital transformation. *Procedia Computer Science*, 219, 44-51. <https://doi.org/10.1016/J.PROCS.2023.01.262>
- Benjamin, A., & Nabende, P. (2023). The Institutionalisation of information security management practices in selected organisations in Uganda. *International Journal of Advanced Research*, 6(1), 48-63. <https://doi.org/10.37284/IJAR.6.1.1155>
- Bernate, J., & Fonseca, I. (2023). Impacto de las tecnologías de información y comunicación en la educación del siglo XXI: revisión bibliométrica. *Revista de ciencias sociales, ISSN-e 1315-9518, Vol. 29, Nº. 1, 2023, págs. 227-242*, 29(1), 227-242. <https://dialnet.unirioja.es/servlet/articulo?codigo=8822438&info=resumen&idioma=ENG>
- Bhutta, M., Bhattia, S., Alojail, M., Nisar, K., Cao, Y., Chaudhry, S., & Sun, Z. (2022). Towards Secure IoT-Based Payments by Extension of Payment Card Industry Data Security Standard (PCI DSS). *Wireless Communications and Mobile Computing*, 2022, 1-10. <https://doi.org/10.1155/2022/9942270>

- Bolek, V., Romanová, A., & Korček, F. (2023). The Information Security Management Systems in E-Business. *Journal of Global Information Management*, 31(1). <https://doi.org/10.4018/JGIM.316833>
- Bouziani, M., Merbah, M., Tiskar, M., Et-tahir, A., & Chaouch, A. (2022). When can we talk about implementing an Information Security Management System, according to ISO 27001? *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, 13(2), 394-401. <https://turcomat.org/index.php/turkbilmat/article/view/12256>
- Bustillos, O., & Rojas, J. (2022). Protocolo básico de ciberseguridad para pymes. *Interfases*, 016, 168-186. <https://doi.org/10.26439/INTERFASES2022.N016.6021>
- Calsin, E., Dueñas, L., & Taquía, J. (2023). Proposed Improvement Plan with Lean Manufacturing to Increase Productivity in a SME in the Textile Sector in Peru. *Proceedings of the 6th European Conference on Industrial Engineering and Operations Management*, 767-775.
- Campbell, D., & Stanley, J. (1966). *Experimental and quasi-experimental designs for research*. https://www.jameslindlibrary.org/wp-data/uploads/2016/01/Campbell_St Stanley-Experimental_and_Quasi-Experimental_Designs_for_Research_1963.pdf
- Castro, J., Gómez, L., Camargo Casallas, E., Castro Maldonado, J. J., Gómez Macho, L. K., & Camargo Casallas, E. (2023). La investigación aplicada y el desarrollo experimental en el fortalecimiento de las competencias de la sociedad del siglo XXI. *Tecnura*, 27(75), 140-174. <https://doi.org/10.14483/22487638.19171>
- Chatziamanetoglou, D., & Rantos, K. (2023). Blockchain-Based Security Configuration Management for ICT Systems. *Electronics (Switzerland)*, 12(8). <https://doi.org/10.3390/ELECTRONICS12081879>
- Cisneros-Caicedo, A., Urdánigo-Cedeño, J., Guevara-García, A., & Garcés-Bravo, J. (2022). Técnicas e Instrumentos para la Recolección de Datos que Apoyan a la Investigación Científica en Tiempo de Pandemia. *Dominio de las Ciencias*, 8(1), 58. <https://doi.org/10.23857/dc.v8i41.2546>
- Coloma-Baños, N., Cañizares-Galarza, F., Romero-Fernández, A., & Quintana-Cifuentes, M. (2022). La seguridad informática para la toma de decisiones en el distrito de educación 12d03. Mocache-Ecuador. *CIENCIAMATRIA*, 8(4), 897-915. <https://doi.org/10.35381/CM.V8I4.898>
- Contador, J., & Tapia, C. (2023). *Diseño e implementación de la ISO 27001 para mejorar la seguridad de información de la Empresa Minera Colibri S.A.C.* Lima - 2023. <https://repositorio.unjfsc.edu.pe/handle/20.500.14067/8975>
- Coronado, G. (2024). SGSI basado en ISO/IEC_27001:2022 para la protección de activos de información de una entidad pública del Sector

- Defensa, Lima 2024. *Repositorio Institucional - UCV*.
<https://repositorio.ucv.edu.pe/handle/20.500.12692/153916>
- Coronel, I., & Quirumbay, D. (2022). Seguridad informática, metodologías, estándares y marco de gestión en un enfoque hacia las aplicaciones web. *Revista Científica y Tecnológica UPSE*, 9(2), 97-108.
<https://doi.org/10.26423/RCTU.V9I2.672>
- Cortés, A. (2023). Propuesta de método basado en COBIT 2019, para la evaluación de procesos tecnológicos en la municipalidad de Carrillo. *InterSedes*, 24(49), 277-306.
<https://doi.org/10.15517/ISUCR.V24I49.50024>
- Coutinho, B., Ferreira, J., Yevseyeva, I., & Basto-Fernandes, V. (2023). Integrated cybersecurity methodology and supporting tools for healthcare operational information systems. *Computers and Security*, 129.
<https://doi.org/10.1016/J.COSE.2023.103189>
- Dada, O., Irunokhai, E., Shawulu, C., Nuhu, A., & Daniel, E. (2021). Information security awareness, a tool to mitigate information security risk: A literature review. *Innovative Journal of Science*, 3(3), 29-54.
<https://journals.rasetass.org/index.php/ij/article/view/106>
- Daoud, W., Othmen, S., Hamdi, M., Khedhir, R., & Hamam, H. (2023). Fog computing network security based on resources management. *Eurasip Journal on Wireless Communications and Networking*, 2023(1), 1-18.
<https://doi.org/10.1186/S13638-023-02256-1>
- De La Cruz, G., Méndez, R., & Méndez, C. (2023). Seguridad de la información en el comercio electrónico basado en ISO 27001: Una revisión sistemática. *Innovación y Software*, 4(1), 219-236.
<https://doi.org/10.48168/innosoft.s11.a79>
- Djebbar, F., & Nordstrom, K. (2023). A Comparative Analysis of Industrial Cybersecurity Standards. *IEEE Access*, 11, 85315-85332.
<https://doi.org/10.1109/ACCESS.2023.3303205>
- Dronov, V. Y., & Dronova, G. A. (2022). Principles of information security management system. *Conference Series*, 2182(1), 012092.
<https://doi.org/10.1088/1742-6596/2182/1/012092>
- Egoshin, N., Konev, A., & Shelupanov, A. (2023). Model of Threats to the Integrity and Availability of Information Processed in Cyberspace. *Symmetry* 2023, Vol. 15, Page 431, 15(2), 431.
<https://doi.org/10.3390/SYM15020431>
- Fadlika, R., Ruldeviyani, Y., Butarbutar, Z., Istiqomah, R., & Fariz, A. (2023). Employee Information Security Awareness in the Power Generation Sector of PT ABC. *International Journal of Advanced Computer Science and Applications*, 14(4), 594-603.
<https://doi.org/10.14569/IJACSA.2023.0140465>

- Fathullah, M., & Subbarao, A. (2022). Security Risk Analysis for Information Asset. *System and Management Sciences*, 12(3), 191-204. <http://www.aasmr.org/jsms/Vol12/JSMS%20august%202022/Vol.12.No.04.12.pdf>
- Fernandes, R., Castro, A., & Menezes, A. (2022). Methodology for risk management in dams from the event tree and FMEA analysis. *Soils and Rocks*, 45(3), 1-15. <https://doi.org/10.28927/SR.2022.070221>
- Guizado, J. (2024). SGSI según ISO/IEC 27001:2022 y su incidencia en la protección de información en una municipalidad distrital, Lima 2023 [Tesis, Universidad César Vallejo]. En *Repositorio Institucional - UCV*. <https://repositorio.ucv.edu.pe/handle/20.500.12692/135503>
- Gurtu, A., & Johny, J. (2021). Supply chain risk management: Literature review. *Risks*, 9(1), 1-16. <https://doi.org/10.3390/RISKS9010016>
- Hasan, M., Habib, A., Shukur, Z., Ibrahim, F., Islam, S., & Razzaque, M. (2023). Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations. *Network and Computer Applications*, 209, 103540. <https://doi.org/10.1016/J.JNCA.2022.103540>
- Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications*, 58, 1-16. <https://doi.org/10.1016/J.JISA.2020.102726>
- Hernández-Sampieri, R., Fernández, C., & Baptista, M. (2014). Metodología de la investigación. En *Metodología de la investigación*. McGraw Hill España. <https://dialnet.unirioja.es/servlet/libro?codigo=775008&info=resumen&idoma=SPA>
- Herrera, C., AguirreDo, P., Honores, F., & Riveros, N. (2023). ¿Cómo se articula la normativa vigente sobre evaluación, calificación y promoción escolar en los reglamentos de evaluación en Antofagasta? *Revista Enfoques Educativos*, 20(2), 1-26. <https://doi.org/10.5354/2735-7279.2023.71690>
- Hossain, S., Akter, S., & Ferdous, K. (2023). Evaluation of ICT Security Implementation in Banks: Bangladesh Perspective. *European Journal of Computer Science and Information Technology*, 11(6), 22-41. <https://doi.org/10.37745/EJCSIT.2013/VOL11N62241>
- Jauregui, R. (2023). Estilos de liderazgo en las pequeñas empresas textiles en el Perú. *Económicas CUC*, 44(1), 137-152. <https://doi.org/10.17981/econcuc.44.1.2023.Org.2>
- Jelovčan, L., Mihelič, A., & Prislan, K. (2022). Outsource or not? An AHP Based Decision Model for Information Security Management. *Organizacija*, 55(2), 142-159. <https://doi.org/10.2478/orga-2022-0010>

- Junaid, T.-S. (2023). ISO 27001: Information Security Management Systems. *Computer Science and Engineering*. <https://doi.org/10.13140/RG.2.2.36267.52005>
- Kamariotou, M., & Kitsios, F. (2023). Information systems strategy and security policy: A conceptual framework. *Electronics* 2023, Vol. 12, Page 382, 12(2), 1-12. <https://doi.org/10.3390/ELECTRONICS12020382>
- Kaspersky. (2023, marzo 21). *La negligencia de los empleados es ahora tan preocupante para las empresas como las filtraciones de datos por ciberataques*. https://latam.kaspersky.com/about/press-releases/2023_la-negligencia-de-los-empleados-es-ahora-tan-preocupante-para-las-empresas-como-las-filtraciones-de-datos-por-ciberataques
- Kitsios, F., Chatzidimitriou, E., & Kamariotou, M. (2023). The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector. *Sustainability (Switzerland)*, 15(7). <https://doi.org/10.3390/SU15075828>
- Lakens, D. (2022). Sample Size Justification. *Collabra: Psychology*, 8(1). <https://doi.org/10.1525/COLLABRA.33267/120491>
- Lee, J., Babcock, J., Pham, T. S., Bui, T. H., & Kang, M. (2023). Smart city as a social transition towards inclusive development through technology: a tale of four smart cities. *International Journal of Urban Sciences*, 27(S1), 75-100. <https://doi.org/10.1080/12265934.2022.2074076>
- Lessa, L., & Gebrehawariat, D. (2023). Effectiveness of banking card security in the Ethiopian financial sector: PCI-DSS security standard as a lens. *International Journal of Industrial Engineering and Operations Management*, 5(2), 135-147. <https://doi.org/10.1108/IJIEOM-10-2021-0015>
- Lopez, C., & Espinoza, J. (2022). *Propuesta de un sistema de gestión de seguridad de la información para una empresa de consultoría financiera en Lima, 2021, según la norma ISO/IEC 27001:2013* [Universidad Peruana de Ciencias Informáticas]. <http://repositorio.upci.edu.pe/handle/upci/722>
- Lykhova, S., Sysoieva, V., Servatiuk, L., Shamsutdinov, O., & Hurina, D. (2022). International and national standards on societal information security. *Revista Científica General José María Córdova*, 20(38), 247-264. <https://doi.org/10.21830/19006586.898>
- Mannes, S., Beuren, I., & Souza, E. (2022). Cooperative Behavior and Knowledge Sharing: Interaction of Risk Management. *Revista Brasileira de Gestão de Negócios*, 24(4), 692-707. <https://doi.org/10.7819/rbgn.v24i4.4203>

- Masaev, S., Minkin, A., Bezborodov, Y., Edimichev, D., & Salal, Y. (2020). Information security control as a task of control a dynamic system. *Journal of Physics: Conference Series*, 1679(3), 032012. <https://doi.org/10.1088/1742-6596/1679/3/032012>
- Medina, J. (2023). ISO 27001 para la gestión de seguridad de la información en el área TI de una empresa industrial, Lima 2023. *Repositorio Institucional* - UCV. <https://repositorio.ucv.edu.pe/handle/20.500.12692/121182>
- Minaya, M., Minaya, R., Intriago, M., & Intriago, J. (2023). Normas y estándares en auditoría: una revisión de su utilidad en la seguridad informática. *Revista Científica Arbitrada Multidisciplinaria PENTACIENCIAS*, 5(4), 584-599. <https://doi.org/10.59169/PENTACIENCIAS.V5I4.700>
- Mujica, F., & Monges, M. (2022). Implementación del Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago en una Procesadora de Tarjetas. *Revista sobre estudios de investigaciones del saber*, 17, 1-8. <https://revistas.uni.edu.py/index.php/rseisa/article/view/324>
- Mukati, A., & Bhargava, A. (2023). Comparative Study between PCI-DSS v4.0 and ISO/IEC 27001:2022. *International Journal of Science and Research (IJSR)*, 12(6), 2936-2951. <https://doi.org/10.21275/SR23711142455>
- Nápoles, M., & Barrueta, N. (2023). Metodología para la validación de instrumentos de medición. *A3manos*, 10(19), 1-10. <https://a3manos.isdi.co.cu/index.php/a3manos/article/view/337/347>
- Obiol, E. (2023). Pensamiento estratégico gerencial y su incidencia en la sostenibilidad de las PYME de Chiclayo, Perú 2020-2022. *Revista de la Facultad de Derecho y Ciencias Políticas*, 53(138), 1-17. <https://doi.org/10.18566/RFDPCP.V53N138.A4>
- Paradongan, P., Legowo, N., & Rydarto, D. (2024). STRENGTHENING PAYMENT CARD DATA SECURITY: A study on compliance enhancement and risk mitigation through MFA implementation under PCI DSS 4.0. *Journal of Theoretical and Applied Information Technology*, 15(9), 4093-4102. www.jatit.org
- Podrecca, M., Culot, G., Nassimbeni, G., & Sartor, M. (2022). Information security and value creation: The performance implications of ISO/IEC 27001. *Computers in Industry*, 142, 103744. <https://doi.org/10.1016/J.COMPIND.2022.103744>
- Podrecca, M., & Sartor, M. (2023). Forecasting the diffusion of ISO/IEC 27001: a Grey model approach. *TQM Journal*, 35(9), 123-151. <https://doi.org/10.1108/TQM-07-2022-0220>
- Ramos, C. (2021). Diseños de investigación experimental. *CienciAmérica*, 10(1), 1-7.

<https://dialnet.unirioja.es/servlet/articulo?codigo=7890336&info=resumen&idioma=ENG>

- Ramos, R., Cahuaya, R., & Llanqui, R. (2023). Política informática y la gestión de la seguridad de la información en base a la norma ISO 27001. *Innovación y Software*, 4(1), 96-106. <https://doi.org/10.48168/innosoft.s11.a57>
- Ramos-Galarza, C. (2021). Diseños de investigación experimental. *CienciAmérica*, 10(1), 1-7. <https://doi.org/10.33210/CA.V10I1.356>
- Razack, Y., & Sorber, T. (2022). A Security Awareness Program for PCI DSS Compliance. *ISACA*, 1(4), 1-9. <https://doi.org/10.1080/08874417.2016.1258679>
- Razikin, K., & Widodo, A. (2021). General Cybersecurity Maturity Assessment Model: Best Practice to Achieve Payment Card Industry-Data Security Standard (PCI-DSS) Compliance. *CommIT (Communication & Information Technology)*, 15(2), 91-104. <https://doi.org/10.21512/COMMIT.V15I2.6931>
- Reales, L., Robalino, G., Peñafiel, A., Cárdenas, J., & Cantuña-Vallejo, P. (2022). El Muestreo Intencional No Probabilístico como herramienta de la investigación científica en carreras de Ciencias de la Salud. *Universidad y Sociedad*, 14(S5), 681-691. <https://rus.ucf.edu.cu/index.php/rus/article/view/3338>
- Rendón-Macías, M., & Villasís-Keever, M. (2017). The research protocol V: The calculation of sample size. *Alergia*, 64(2), 220-227. <http://www.revistaalergia.mx>
- Rodriguez, L., Cruzado, C., Mejía, C., & Alarcón, M. (2020). Aplicación de ISO 27001 y su influencia en la seguridad de la información de una empresa privada peruana. *Propósitos y Representaciones*, 8(3), 786. <https://doi.org/10.20511/PYR2020.V8N3.786>
- Rodriguez-Baca, L. S., Allagi, S., Larrea-Serquen, R., Cruzado, C. F., Diaz, M. A., Garcia-Hernández, S., & Monteiro, J. D. (2023). Experimental Study based on the Implementation of a Regulatory Framework for the Improvement of Cyber Resilience in SMEs. *International Journal on Recent and Innovation Trends in Computing and Communication*, 11(3), 199-205. <https://doi.org/10.17762/IJRITCC.V11I3.6337>
- Salazar, D., Huayllani, F., & Ramos, R. (2022). Balanced scorecard y el crecimiento empresarial de las Pymes de la ciudad de Huancavelica. *Ciencia Latina Revista Científica Multidisciplinar*, 6(5), 1840-1855. https://doi.org/10.37811/CL_RCM.V6I5.3200
- Sánchez-Bautista, G., & Ramírez-Chávez, L. (2022). Amenazas de seguridad a considerar en el desarrollo de software. *XIKUA Boletín Científico de la*

- Escuela Superior de Tlahuelilpan*, 10(19), 31-37.
<https://doi.org/10.29057/XIKUA.V10I19.8118>
- Shaikh, F., & Siponen, M. (2023). Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. *Computers & Security*, 124, 102974. <https://doi.org/10.1016/J.COSE.2022.102974>
- Silva, A. (2022). Implementación de un sistema de gestión de seguridad de la información para mejorar la seguridad de la información en una empresa MyPE, 2021 [Universidad Tecnológica del Perú]. En *Repositorio Institucional* - UTP. <http://repositorio.utp.edu.pe/handle/20.500.12867/5705>
- Silva-Giraldo, C. A., Rueda-Mahecha, Y. M., & Moreno-Suarez, A. M. (2023). La innovación en las MIPYMES por medio de redes colaborativas y el uso de las TIC. *TECHNO REVIEW. International Technology, Science and Society Review /Revista Internacional de Tecnología, Ciencia y Sociedad*, 14(1), 1-13. <https://doi.org/10.37467/REVTECHNO.V14.4822>
- Skarczynski, B., Raschke, M., & Teuteberg, F. (2023). Modelling maximum cyber incident losses of German organisations: an empirical study and modified extreme value distribution approach. *The Geneva Papers on Risk and Insurance - Issues and Practice*, 48(2), 463-501. <https://doi.org/10.1057/S41288-023-00293-X>
- Tin, D., Hata, R., Granholm, F., Ciottone, R. G., Staynings, R., & Ciottone, G. R. (2023). Cyberthreats: A primer for healthcare professionals. *American Journal of Emergency Medicine*, 68, 179-185. <https://doi.org/10.1016/J.AJEM.2023.04.001>
- Trujillo, F. (2023). ISO 27001 en la Gestión de Seguridad de la Información en el área TI en una institución pública, Lima 2023. *Repositorio Institucional* - UCV, 1-96. <https://repositorio.ucv.edu.pe/handle/20.500.12692/120927>
- Vargas-Pimentel, R., Mejía-Janampa, M., & Huamancha-Aguilar, M. (2024). Tendencias de la evaluación formativa en la educación básica. *Revista Tecnológica-Educativa Docentes 2.0*, 17(2), 376-389. <https://doi.org/10.37843/RTED.V17I2.572>
- Vega, P., Gómez, M., Feijoo, D., & Maldonado, C. (2025). Evaluación formativa y su incidencia en el desarrollo del pensamiento crítico en la educación superior. *Revista de Investigación en Comunicación y Desarrollo*, 3(2), 1-13. <https://doi.org/10.33595/2226-1478.13.2.672>
- Veiga, A., Astakhova, Liudmila., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. *Computers & Security*, 92, 1-23. <https://doi.org/10.1016/J.COSE.2020.101713>

- Velandia-Mesa, C., Serrano-Pastor, F., & Martínez-Segura, M. (2021). Evaluación de la investigación formativa: Diseño y validación de escala. *Revista Electrónica Educare*, 25(1), 35-54. <https://doi.org/10.15359/REE.25-1.3>
- Velepucha, M., Morales, J., & Pazmiño, M. (2022). Análisis y evaluación de riesgos aplicados a la seguridad de la información bajo la norma ISO. *Informática y Sistemas: Revista de Tecnologías de la Informática y las Comunicaciones*, 6(1), 63-78. <https://doi.org/10.33936/ISRTIC.V6I1.4473>
- Villarreal, V. (2023). *Sistema de gestión de seguridad de la información en la Universidad Estatal Amazónica*. <https://repositorio.uta.edu.ec:8443/jspui/handle/123456789/37329>
- Wang, M., Qin, Y., Liu, J., & Li, W. (2023). Identifying personal physiological data risks to the Internet of Everything: the case of facial data breach risks. *Humanities and Social Sciences Communications*, 10(1). <https://doi.org/10.1057/S41599-023-01673-3>
- Wang, X., & Ji, X. (2020). Sample Size Estimation in Clinical Research: From Randomized Controlled Trials to Observational Studies. *Chest*, 158(1), S12-S20. <https://doi.org/10.1016/J.CHEST.2020.03.010>
- Zhang, Y., & Dong, H. (2023). Criminal law regulation of cyber fraud crimes—from the perspective of citizens' personal information protection in the era of edge computing. *Journal of Cloud Computing*, 12(1). <https://doi.org/10.1186/S13677-023-00437-3>
- Zhao, W. (2022). Blockchain-Based Information Security Management: A Brief Review. *Electronics and Information Science*, 7(2), 21-26. <https://doi.org/10.23977/JEIS.2022.070204>

ANEXOS

Anexo 01: Instrumento

PARA MEDIR LA SEGURIDAD DE LA INFORMACIÓN EN LAS PYMES DE LA INDUSTRIA TEXTIL, LIMA 2024.

Fecha: ____/____/____

Edad: Género: Femenino [☐] Masculino [☐]

El objeto del presente cuestionario es conocer el estado actual sobre la seguridad de la información. Marcar con una equis (X) de acuerdo a la valoración que usted crea conveniente, considerando la siguiente escala:

1) Nunca 2) Casi nunca 3) Algunas veces 4) Casi siempre 5) Siempre

	Dimensiones	Escala				
		1	2	3	4	5
Ítem	Confidencialidad					
1	¿Con qué frecuencia se gestionan las contraseñas a través de políticas, directivas o mecanismos de restricción basados en roles o perfiles?					
2	¿Con qué frecuencia se siguen medidas de seguridad para el uso y/o acceso a los dispositivos móviles y el teletrabajo?					
3	¿Con qué frecuencia la gestión de recursos humanos antes, durante y después de la relación laboral se ciñe a protocolos de seguridad?					
4	¿Con qué frecuencia se aplican medidas y protocolos para supervisar y regular el acceso a determinados sitios o sistemas informáticos?					
5	¿Con qué frecuencia se llevan a cabo programas de capacitación anuales en temas de seguridad de la información a los empleados y usuarios?					
6	¿Con qué frecuencia se sigue procedimientos y políticas para la gestión y segregación de la redes sociales e intercambio de información?					
	Integridad					
7	¿Con qué frecuencia la entidad administra y actualiza los antivirus instalados en sus equipos?					
8	¿Con qué frecuencia la información es almacenada en sitios seguros y con acceso a personas autorizadas?					
9	¿Con qué frecuencia la documentación física se protege siguiendo políticas de seguridad?					
10	¿Con qué frecuencia extrae y/o comparte información de su área mediante dispositivos como USB, medios compartidos, red y correo?					
11	¿Con qué frecuencia la capacidad de los equipos tecnológicos se ve afectada por caídas o lentitudes extremas?					
12	¿Con qué frecuencia se optimiza la capacidad de los equipos tecnológicos mediante mantenimiento preventivo?					
13	¿Con qué frecuencia se definen y/o se revisan medidas de contingencia que respondan ante incendios, inundaciones y cortes eléctricos imprevistos?					

	Disponibilidad					
14	¿Con qué frecuencia la información que necesita para hacer su trabajo está disponible las 24 horas al día?					
15	¿Con qué frecuencia la disponibilidad de su equipo de cómputo satisface las necesidades de su área?					
16	¿Con qué frecuencia se ha reportado incidentes como pérdida de información, ataques internos y suplantación de identidad en su computador o sistema informático?					
17	¿Con qué frecuencia los sistemas presentan una recuperación temprana de potenciales reveses?					
18	¿Con qué frecuencia se revisan y/o se actualizan los inventarios para la gestión de activos y la definición de reglas de uso aceptables?					
19	¿Con qué frecuencia el área de TI le ha proporcionado una copia de seguridad para recuperar la información eliminada por error?					
20	¿Con qué frecuencia el ancho de banda de internet que tiene le permite trabajar normalmente y evitar la saturación de datos?					

Anexo 02: Informes de validación



UNIVERSIDAD NACIONAL MAYOR DE
SAN MARCOS
Universidad del Perú, Decana de América

INFORME DE OPINIÓN SOBRE INSTRUMENTO DE INVESTIGACIÓN CIENTÍFICA

I. DATOS GENERALES

Apellidos y nombre del experto: Mori León, Nilton Cesar
Grado y especialidad : MBA, Ingeniero Industrial
Entidad donde labora : Mibanco
Instrumento de evaluación : Encuesta para medir la seguridad de la información en las pymes de la industria textil, Lima 2024.

II. ASPECTOS DE VALIDACIÓN

MUY DEFICIENTE (1) - DEFICIENTE (2) - ACEPTABLE (3) - BUENA (4) - EXCELENTE (5)

CRITERIOS	INDICADORES	1	2	3	4	5
CLARIDAD	Los ítems están redactados con lenguaje apropiado y libre de ambigüedades acorde con los sujetos muestrales.					X
OBJETIVIDAD	Las instrucciones de los ítems del instrumento permiten recoger la información objetiva sobre la variable: Gestión de seguridad de la información en las PYMES de la industria textil en Lima, en todas sus dimensiones e indicadores.					X
ACTUALIDAD	El instrumento presenta acorde con el conocimiento científico, tecnológico, innovación y legal inherente a la variable: Gestión de seguridad de la información en las PYMES de la industria textil en Lima.					X
SUFICIENCIA	Los ítems del instrumento son suficientes en cantidad y calidad acorde con la variable: Gestión de seguridad de la información en las PYMES de la industria textil en Lima.				X	
INTENCIONALIDAD	Los ítems del instrumento son coherentes con el tipo de investigación y responden a los objetivos, hipótesis y variable de estudio: Gestión de seguridad de la información en las PYMES de la industria textil en Lima.					X
CONSISTENCIA	La información que se recoja a través de los ítems del instrumento permitirá analizar, describir y explicar la realidad motivo de la investigación.				X	
COHERENCIA	Los ítems del instrumento expresan relación con los indicadores de cada dimensión de la variable: Gestión de seguridad de la información en las PYMES de la industria textil en Lima.					X
METODOLOGÍA	La relación entre la técnica la técnica y el instrumento propuesto responden al propósito de la investigación, desarrollo tecnológico e innovación.				X	
PERTINENCIA	La redacción de los ítems concuerda con la escala valorativa del instrumento.					X
PUNTAJE TOTAL						

NOTA: Tener en cuenta que el instrumento se considera como válido si se tiene un puntaje mayor o igual a 41 "Excelente", sin embargo, un puntaje mejor se considera el instrumento no válido ni aplicable.

III. OPINIÓN DE APLICABILIDAD

El instrumento de investigación va a permitir conocer la situación y contexto sobre el que se encuentra la pyme, es importante conocer el nivel de seguridad, integridad y facilidad de acceso a la información requerida ante escenarios de caídas y/o imprevistos técnicos u otros.

PROMEDIO DE VALORACIÓN:

42


Firma



UNIVERSIDAD NACIONAL MAYOR DE
SAN MARCOS
Universidad del Perú, Decana de América

INFORME DE OPINIÓN SOBRE INSTRUMENTO DE INVESTIGACIÓN CIENTÍFICA

I. DATOS GENERALES

Apellidos y nombre del experto: CERDA GARCÍA, RUBEN OSCAR
Grado y especialidad : MAESTRO - INGENIERO DE COMPUTACION Y SISTEMAS
Entidad donde labora : IA INVERSIONES PALO ALTO II SAC .CANVIA
Instrumento de evaluación : Encuesta para medir la seguridad de la información en las pymes de la industria textil, Lima 2024.

II. ASPECTOS DE VALIDACIÓN

MUY DEFICIENTE (1) - DEFICIENTE (2) - ACEPTABLE (3) - BUENA (4) - EXCELENTE (5)

CRITERIOS	INDICADORES	1	2	3	4	5
CLARIDAD	Los ítems están redactados con lenguaje apropiado y libre de ambigüedades acorde con los sujetos muestrales.					X
OBJETIVIDAD	Las instrucciones de los ítems del instrumento permiten recoger la información objetiva sobre la variable: Gestión de seguridad de la información en las PYMES de la industria textil en Lima, en todas sus dimensiones e indicadores.					X
ACTUALIDAD	El instrumento presenta acorde con el conocimiento científico, tecnológico, innovación y legal inherente a la variable: Gestión de seguridad de la información en las PYMES de la industria textil en Lima.					X
SUFICIENCIA	Los ítems del instrumento son suficientes en cantidad y calidad acorde con la variable: Gestión de seguridad de la información en las PYMES de la industria textil en Lima.					X
INTENCIONALIDAD	Los ítems del instrumento son coherentes con el tipo de investigación y responden a los objetivos, hipótesis y variable de estudio: Gestión de seguridad de la información en las PYMES de la industria textil en Lima.					X
CONSISTENCIA	La información que se recoja a través de los ítems del instrumento permitirá analizar, describir y explicar la realidad motivo de la investigación.					X
COHERENCIA	Los ítems del instrumento expresan relación con los indicadores de cada dimensión de la variable: Gestión de seguridad de la información en las PYMES de la industria textil en Lima.					X
METODOLOGÍA	La relación entre la técnica la técnica y el instrumento propuesto responden al propósito de la investigación, desarrollo tecnológico e innovación.					X
PERTINENCIA	La redacción de los ítems concuerda con la escala valorativa del instrumento.					X
PUNTAJE TOTAL						

NOTA: Tener en cuenta que el instrumento se considera como válido si se tiene un puntaje mayor o igual a 41 "Excelente", sin embargo, un puntaje menor se considera el instrumento no válido ni aplicable.

III. OPINIÓN DE APLICABILIDAD

PROMEDIO DE VALORACIÓN:

5

Firma



UNIVERSIDAD NACIONAL MAYOR DE
SAN MARCOS
Universidad del Perú, Decana de América

INFORME DE OPINIÓN SOBRE INSTRUMENTO DE INVESTIGACIÓN CIENTÍFICA

I. DATOS GENERALES

Apellidos y nombre del experto: Andrade Mogollon Teodoro Manuel
Grado y especialidad : Magister - TIC
Entidad donde labora : IFF
Instrumento de evaluación : Encuesta para medir la seguridad de la información en las pymes de la industria textil, Lima 2024.

II. ASPECTOS DE VALIDACIÓN

MUY DEFICIENTE (1) - DEFICIENTE (2) - ACEPTABLE (3) - BUENA (4) - EXCELENTE (5)

CRITERIOS	INDICADORES	1	2	3	4	5
CLARIDAD	Los ítems están redactados con lenguaje apropiado y libre de ambigüedades acorde con los sujetos muestrales.					X
OBJETIVIDAD	Las instrucciones de los ítems del instrumento permiten recoger la información objetiva sobre la variable: Gestión de seguridad de la información en las PYMES de la industria textil en Lima, en todas sus dimensiones e indicadores.				X	
ACTUALIDAD	El instrumento presenta acorde con el conocimiento científico, tecnológico, innovación y legal inherente a la variable: Gestión de seguridad de la información en las PYMES de la industria textil en Lima.					X
SUFICIENCIA	Los ítems del instrumento son suficientes en cantidad y calidad acorde con la variable: Gestión de seguridad de la información en las PYMES de la industria textil en Lima.				X	
INTENCIONALIDAD	Los ítems del instrumento son coherentes con el tipo de investigación y responden a los objetivos, hipótesis y variable de estudio: Gestión de seguridad de la información en las PYMES de la industria textil en Lima.					X
CONSISTENCIA	La información que se recoja a través de los ítems del instrumento permitirá analizar, describir y explicar la realidad motivo de la investigación.					X
COHERENCIA	Los ítems del instrumento expresan relación con los indicadores de cada dimensión de la variable: Gestión de seguridad de la información en las PYMES de la industria textil en Lima.					X
METODOLOGÍA	La relación entre la técnica la técnica y el instrumento propuesto responden al propósito de la investigación, desarrollo tecnológico e innovación.					X
PERTINENCIA	La redacción de los ítems concuerda con la escala valorativa del instrumento.					X
PUNTAJE TOTAL		43				

NOTA: Tener en cuenta que el instrumento se considera como válido si se tiene un puntaje mayor o igual a 41 “Excelente”, sin embargo, un puntaje menor se considera el instrumento no válido ni aplicable.

III. OPINIÓN DE APLICABILIDAD

El instrumento es aplicable dada la directa relación con el objetivo de la investigación, lo que va a permitir un estudio de calidad en cuanto a la “Gestión de seguridad de la información en las PYMES de la industria textil en Lima “

PROMEDIO DE VALORACIÓN:

4,3

Teodoro Andrade

Firma

Anexo 3: Relación de activos categorizados.

Categoría	Activo	Descripción
Datos	Salario	Remuneración periódica que recibe un trabajador por su labor, usualmente en términos monetarios.
	Datos del personal	Información relacionada con los empleados de las pymes, como nombres, puestos, historial laboral y datos de contacto.
	Datos de los clientes	Información de contacto y detalles relevantes sobre los clientes, incluyendo historial de compras y preferencias.
	Datos de los proveedores	Información de contacto y detalles sobre los proveedores que abastecen bienes y servicios, incluyendo contratos y condiciones de suministro.
	Órdenes de compra	Documentos que especifican los productos o servicios que se desea adquirir de un proveedor, incluyendo cantidades, precios y fechas de entrega.
	Órdenes de venta	Documentos que registran los productos o servicios que las pymes venden a sus clientes, incluyendo detalles de los artículos, precios y condiciones de venta.
	Estados de cuenta	Resúmenes financieros que detallan el balance y las transacciones de una cuenta específica durante un período de tiempo determinado.
Software	Página web	Página electrónica que residen en un servidor web y accesible a través de internet.
	Sistema operativo	Software que gestiona el hardware de una computadora y proporciona servicios comunes para los programas de aplicación, como Windows, macOS o Linux.
	Correo electrónico	Un servicio de transmisión de mensajes digitales a través de una red informática, que permite la comunicación rápida y eficiente entre usuarios.
Hardware	Computadoras	Dispositivos electrónicos que procesan datos y ejecutan programas para realizar una variedad de tareas, desde cálculos simples hasta aplicaciones complejas.
	Dispositivos de red	Equipos que facilitan la comunicación y el intercambio de datos entre computadoras y otras tecnologías de información, como routers, switches y modems.
	Impresoras	Dispositivos que transfieren texto e imágenes desde una computadora u otro dispositivo digital a papel u otros medios físicos.
Personas	Directivos	Ejecutivos de alto nivel que toman decisiones estratégicas y supervisan la dirección general de las pymes.

	Jefes de área	Responsables de coordinar y gestionar actividades específicas dentro de sus departamentos.
	Administrativos	Personal encargado de tareas de soporte y gestión, como la administración de documentos y la asistencia en tareas operativas.
	Operarios	Trabajadores encargados de la producción y operación de equipos en la línea de producción.
Infraestructura	Oficinas	Espacios dentro de las pymes, donde la planificación, coordinación y ejecución de proyectos y actividades laborales se llevan a cabo.

Anexo 4: Nivel de criticidad de los activos.

ID	Activo	CRITERIOS DE VALORIZACIÓN			Valor final	Criticidad
		Confidencialidad	Integridad	Disponibilidad		
1	Salarios	1	1	1	3	BAJO
2	Datos del personal	2	1	1	4	MEDIO
3	Datos de los clientes	3	3	2	8	ALTO
4	Datos de los proveedores	3	2	2	7	ALTO
5	Órdenes de compra	3	2	2	7	ALTO
6	Órdenes de venta	3	2	2	7	ALTO
7	Estados de cuenta	2	1	1	4	MEDIO
8	Página web	3	2	2	7	ALTO
9	Sistema operativo	2	2	3	7	ALTO
10	Correo electrónico	1	1	1	3	BAJO
11	Computadoras	3	3	3	9	ALTO
12	Dispositivos de red	2	2	2	6	MEDIO
13	Impresoras	1	1	1	3	BAJO
14	Directivos	3	3	3	9	ALTO
15	Jefes de área	3	2	2	7	ALTO
16	Administrativos	2	2	2	6	MEDIO
17	Operarios	2	2	2	6	MEDIO
18	Oficinas	2	3	3	8	ALTO

Anexo 5: Lista de activos físicos.

ID	Activo
1	Datos de los clientes
2	Datos de los proveedores
3	Órdenes de compra
4	Órdenes de venta
5	Página web
6	Sistema operativo
7	Computadoras
8	Directivos
9	Jefes de área
10	Oficinas

Anexo 6: Matriz de riesgos.

MATRÍZ DE RIESGO						
ID riesgo	Activo	Vulnerabilidad	Amenaza	Probabilidad	Impacto	Nivel riesgo
R1	Datos de los clientes.	Autenticaciones débiles	Ciberataques	Alto	Alto	Alto
R2	Datos de los clientes.	Errores humanos.	Robo o manipulación	Alto	Alto	Alto
R3	Datos de los proveedores.	Accesos mal controlados.	Espionaje industrial.	Medio	Alto	Alto
R4	Datos de los proveedores.	Ausencia de políticas robustas.	Robo o manipulación	Muy alto	Alto	Crítico
R5	Datos de los proveedores	Uso de canales poco seguros.	Acciones fraudulentas.	Medio	Alto	Alto
R6	Órdenes de compra	Errores humanos.	Robo o manipulación	Muy alto	Alto	Crítico
R7	Órdenes de compra	Accesos mal controlados.	Fraude.	Medio	Alto	Alto
R8	Órdenes de compra	Trasmisión de información no cifrada.	Suplantación de identidad	Media	Alto	Alto
R9	Órdenes de venta	Errores humanos.	Robo o manipulación	Muy alto	Alto	Crítico
R10	Órdenes de venta	Accesos mal controlados.	Fraude.	Medio	Alto	Alto
R11	Órdenes de venta	Trasmisión de información no cifrada.	Suplantación de identidad.	Medio	Alto	Alto
R12	Página web	Defectos en el funcionamiento.	Abuso de privilegios.	Medio	Medio	Relevante
R13	Página web	Errores de configuración.	Instalación de software malicioso.	Alto	Medio	Alto
R14	Página web	Falta de pruebas.	Abuso de privilegios.	Bajo	Medio	Moderado
R15	Sistema operativo	Software no actualizado.	Malware.	Alto	Muy alto	Crítico
R16	Sistema operativo	Permisos mal configurados.	Exploits.	Alto	Muy alto	Crítico

R17	Sistema operativo	Ausencia de monitoreo de eventos.	Ransomware	Medio	Muy alto	Alto
R18	Computadoras	Sensibilidad a la humedad, polvo y calor.	Lentitudes extremas, congelamiento.	Muy alto	Muy alto	Crítico
R19	Computadoras	Falta de cierre de sesión al salir del área de trabajo.	Manipulación de información.	Muy alto	Muy alto	Crítico
R20	Computadoras	Susceptibilidad a variaciones en el voltaje.	Pérdida de suministro de energía eléctrica.	Alto	Muy alto	Crítico
R21	Computadoras	Deficiente seguridad en contraseñas.	Divulgación de información.	Alto	Muy alto	Crítico
R22	Directivos	Suplantación de identidad.	Phishing.	Medio	Muy alto	Alto
R23	Directivos	Ausencia de capacitación en seguridad.	Espionaje industrial.	Bajo	Muy alto	Relevante
R24	Directivos	Excesivo control de accesos.	Empleados desleales pueden abusar de sus permisos.	Alto	Muy alto	Crítico
R25	Directivos	Indisponibilidad o ausencia accidental.	Falta de personal para desempeñar el rol.	Bajo	Muy alto	Relevante
R26	Jefes de área	Desconocimiento de protocolos de seguridad.	Phishing.	Alto	Alto	Alto
R27	Jefes de área	Ausencia de capacitación en seguridad.	Espionaje industrial.	Medio	Alto	Alto
R28	Jefes de área	Indisponibilidad o ausencia accidental.	Falta de personal para desempeñar el rol.	Bajo	Alto	Relevante
R29	Oficinas	Accesos físicos no controlados.	Personas no autorizadas accediendo a las instalaciones.	Alto	Alto	Alto

R30	Oficinas	Equipos desprotegidos.	Sustracción de equipos con datos sensibles	Medio	Alta	Alto
R31	Oficinas	Falta de políticas de seguridad.	Eventos que comprometan la operación física sin planes de contingencia.	Bajo	Alto	Relevante
R32	Oficinas	Fallas en la infraestructura.	Interrupción en los servicios eléctricos o de red.	Bajo	Alto	Relevante

Anexo 7: Riesgo con mayor impacto.

MATRÍZ DE RIESGO						
ID riesgo	Activo	Vulnerabilidad	Amenaza	Probabilidad	Impacto	Nivel riesgo
R1	Datos de los clientes.	Autenticaciones débiles	Ciberataques	Alto	Alto	Alto
R2	Datos de los clientes.	Errores humanos.	Robo o manipulación	Alto	Alto	Alto
R3	Datos de los proveedores.	Accesos mal controlados.	Espionaje industrial.	Medio	Alto	Alto
R4	Datos de los proveedores.	Ausencia de políticas robustas.	Robo o manipulación	Muy alto	Alto	Crítico
R5	Datos de los proveedores	Uso de canales poco seguros.	Acciones fraudulentas.	Medio	Alto	Alto
R6	Órdenes de compra	Errores humanos.	Robo o manipulación	Muy alto	Alto	Crítico
R7	Órdenes de compra	Accesos mal controlados.	Fraude.	Medio	Alto	Alto
R8	Órdenes de compra	Trasmisión de información no cifrada.	Suplantación de identidad	Media	Alto	Alto
R9	Órdenes de venta	Errores humanos.	Robo o manipulación	Muy alto	Alto	Crítico
R10	Órdenes de venta	Accesos mal controlados.	Fraude.	Medio	Alto	Alto

R11	Órdenes de venta	Trasmisión de información no cifrada.	Suplantación de identidad.	Medio	Alto	Alto
R13	Página web	Errores de configuración.	Instalación de software malicioso.	Alto	Medio	Alto
R15	Sistema operativo	Software no actualizado.	Malware.	Alto	Muy alto	Crítico
R16	Sistema operativo	Permisos mal configurados.	Exploits.	Alto	Muy alto	Crítico
R17	Sistema operativo	Ausencia de monitoreo de eventos.	Ransomware.	Medio	Muy alto	Alto
R18	Computadoras	Sensibilidad a la humedad, polvo y calor.	Lentitudes extremas, congelamiento	Muy alto	Muy alto	Crítico
R19	Computadoras	Falta de cierre de sesión al salir del área de trabajo.	Manipulación de información.	Muy alto	Muy alto	Crítico
R20	Computadoras	Susceptibilidad a variaciones en el voltaje.	Pérdida de suministro de energía eléctrica.	Alto	Muy alto	Crítico
R21	Computadoras	Deficiente seguridad en contraseñas.	Divulgación de información.	Alto	Muy alto	Crítico
R22	Directivos	Suplantación de identidad.	Phishing.	Medio	Muy alto	Alto
R24	Directivos	Excesivo control de accesos.	Empleados desleales pueden abusar de sus permisos.	Alto	Muy alto	Crítico
R26	Jefes de área	Desconocimiento de protocolos de seguridad.	Phishing.	Alto	Alto	Alto
R27	Jefes de área	Ausencia de capacitación en seguridad.	Espionaje industrial.	Medio	Alto	Alto
R29	Oficinas	Accesos físicos no controlados.	Personas no autorizadas accediendo a las instalaciones.	Alto	Alto	Alto
R30	Oficinas	Equipos desprotegidos.	Sustracción de equipos con	Medio	Alta	Alto


Anexo 8: Políticas de seguridad de la información.

Políticas de uso de los activos lógicos.	
1	Cada jefe de área es responsable de la información asignada.
2	La información debe estar protegida contra adulteración con claves seguras.
3	La documentación física será almacenada correctamente en lugares con acceso a personas autorizadas.
4	Los datos serán clasificados en categorías tales como pública, interna, confidencial y sensible.
5	Se prohíbe circular información de proveedores.
6	Se implementarán medidas de encriptación para proteger los datos sensibles en tránsito y en reposo.
7	Se establecerán procedimientos seguros para la eliminación de datos que ya no sean necesarios.
8	Los datos personales serán recolectados y procesados únicamente para fines legítimos y específicos.
9	Cualquier alteración de los datos deberá ser registrada y monitorizada.
10	Se establecerán planes de recuperación ante desastres.
11	Se realizarán copias de seguridad regulares para asegurar la disponibilidad de los datos.
12	No se revelará información de clientes y el estado de su crédito a ningún agente externo a la pyme.
13	Está prohibido el uso de dispositivos externos de almacenamiento.
14	Todos los programas a utilizar deberán ser licenciados.
15	Wi-fi y bluetooth serán desactivados.
16	Los canales y programas de entretenimiento serán bloqueados.
17	Se encriptarán todos los datos de tarjetas durante la transmisión a través de redes públicas y privadas utilizando protocolos seguros como TLS.
18	Se prohíbe el almacenamiento de datos sensibles de autenticación, como códigos CVV, después de la autorización de la transacción.

19	Retener los datos de tarjetas solo durante el tiempo necesario para cumplir con los fines comerciales legítimos.
Políticas de uso de los activos físicos.	
1	El personal que recepcione algún dispositivo, será responsable de su cuidado.
2	Se prohíbe la instalación de aplicativos que alteren el rendimiento.
3	El monitoreo de cámaras de seguridad estará a cargo del jefe de informática.
4	Se prohíbe la alteración de las configuraciones ya establecidas.
5	Se prohíbe la ingesta de comidas y bebidas en las estaciones de trabajo.
6	Se utilizarán identificaciones personales y tarjetas de acceso para verificar la identidad.
7	Las áreas seguras serán definidas y categorizadas según la sensibilidad de los datos.
8	Los visitantes deberán registrarse y recibir una identificación temporal.
9	Se controlarán factores como temperatura, humedad y sistemas de detección de incendios.
10	Se realizarán pruebas periódicas de seguridad, incluyendo simulacros y pruebas de intrusión.
Políticas de control de accesos.	
1	Definir roles de usuarios en función al trabajo que desempeña.
2	Todos los sistemas y aplicaciones deberán requerir autenticación mediante credenciales únicas para cada usuario.
3	Todos los roles y permisos de acceso serán documentados y revisados periódicamente.
4	Se asignarán permisos mínimos necesarios para realizar las tareas laborales específicas, siguiendo el principio de menor privilegio.
5	Las contraseñas deberán cumplir con requisitos de complejidad, incluyendo longitud mínima, uso de caracteres especiales, números y letras.
6	Las contraseñas deberán cambiarse regularmente, al menos cada 90 días.
7	No se permitirá la reutilización de contraseñas antiguas.
8	Se limitará el acceso de terceros a los sistemas y datos estrictamente necesarios para sus funciones.

9	Los accesos deberán ser desactivados inmediatamente cuando un empleado deje la pyme o cambie de rol.
10	Los trabajadores deben bloquear sus equipos de trabajo inmediatamente al salir del escritorio.
11	Restringir el acceso a los datos de tarjetas únicamente al personal autorizado mediante autenticación multifactor.
Políticas contra amenazas externas e internas	
1	Implementar y mantener firewalls y sistemas de detección de intrusos (IDS).
2	Realizar evaluaciones de vulnerabilidad periódicas en todos los sistemas que manejan datos de tarjetas.
3	Asegurar que todos los sistemas y software estén actualizados con los parches y actualizaciones de seguridad más recientes.
4	Establecer un calendario regular de actualización y parcheo.
5	Configurar segmentación de la red para limitar el alcance de un posible ataque.
6	Monitorear todas las actividades en los sistemas y redes para detectar comportamientos inusuales o no autorizados.
7	Fomentar una cultura de seguridad dentro de la pyme.
8	Realizar simulacros de incidentes para asegurar que todos los empleados sepan cómo reaccionar ante una amenaza.

Anexo 9: Matriz de cumplimiento de políticas.

Políticas de uso de los activos lógicos.		Nivel de cumplimiento				Comentarios
		0%	40%	70%	100%	
1	Cada jefe de área es responsable de la información asignada.			X		- Algunos jefes de área pueden no estar completamente informados sobre sus responsabilidades. - Puede haber dificultades en la adopción de nuevas prácticas de seguridad. - No hay un sistema de recompensas o sanciones para motivar el cumplimiento total.
2	La información debe estar protegida contra adulteración con claves seguras.			X		- No todos los responsables cambian sus claves regularmente, lo que aumenta el riesgo de accesos no autorizados. - Puede haber usuarios que utilicen contraseñas fáciles de adivinar o compartan credenciales.
3	La documentación física será almacenada correctamente en lugares con acceso a personas autorizadas.				X	
4	Los datos serán clasificados en categorías tales como pública, interna, confidencial y sensible.			X		- Algunos colaboradores pueden estar clasificando los datos de manera incorrecta o no hacerlo en absoluto.
5	Se prohíbe circular información de proveedores.				X	

6	Se implementarán medidas de encriptación para proteger los datos sensibles en tránsito y en reposo.			X		- Puede que algunos datos en reposo no estén cifrados correctamente. - Algunos métodos pueden ser inseguros o no cumplir con estándares actuales.
7	Se establecerán procedimientos seguros para la eliminación de datos que ya no sean necesarios.			X		- No hay reglas claras sobre cuándo y cómo eliminar datos de manera segura. - No se utilizan software o técnicas especializadas para la eliminación segura de datos digitales y físicos.
8	Los datos personales serán recolectados y procesados únicamente para fines legítimos y específicos.			X		- Falta una supervisión adecuada para asegurar que los datos sean usados solo para los fines declarados. - No siempre se informa a los titulares sobre el propósito específico de la recolección.
9	Cualquier alteración de los datos deberá ser registrada y monitorizada.				X	
10	Se establecerán planes de recuperación ante desastres.			X		- No hay roles y responsabilidades bien definidos en caso de un desastre. - No se han realizado pruebas regulares para evaluar la efectividad del plan.
11	Se realizarán copias de seguridad regulares para asegurar la disponibilidad de los datos.				X	
12	No se revelará información de clientes y el estado de su crédito a ningún agente externo a la pyme.				X	

13	Está prohibido el uso de dispositivos externos de almacenamiento.				X	
14	Todos los programas a utilizar deberán ser licenciados.			X		- Algunos programas utilizados pueden no contar con licencias oficiales. - Algunos empleados pueden estar utilizando herramientas no autorizadas.
15	Wi-fi y bluetooth serán desactivados.				X	
16	Los canales y programas de entretenimiento serán bloqueados.				X	
17	Se encriptarán todos los datos de tarjetas durante la transmisión a través de redes públicas y privadas utilizando protocolos seguros como TLS.			X		- Puede haber puntos en el proceso donde los datos no estén debidamente cifrados.
18	Se prohíbe el almacenamiento de datos sensibles de autenticación, como códigos CVV, después de la autorización de la transacción.				X	
19	Retener los datos de tarjetas solo durante el tiempo necesario para cumplir con los fines comerciales legítimos.				X	
Políticas de uso de los activos físicos.		Nivel de cumplimiento				Comentarios
		0%	40%	70%	100%	

1	El personal que recepcione algún dispositivo, será responsable de su cuidado.				X	
2	Se prohíbe la instalación de aplicativos que alteren el rendimiento.				X	
3	El monitoreo de cámaras de seguridad estará a cargo del jefe de informática.				X	
4	Se prohíbe la alteración de las configuraciones ya establecidas.				X	
5	Se prohíbe la ingesta de comidas y bebidas en las estaciones de trabajo.			X		- Algunos empleados no comprenden los riesgos asociados, como daños a equipos o contaminación de materiales. - Si no hay áreas designadas para el consumo de alimentos, los trabajadores podrían ignorar la política.
6	Se utilizarán identificaciones personales y tarjetas de acceso para verificar la identidad.				X	
7	Las áreas seguras serán definidas y categorizadas según la sensibilidad de los datos.			X		- No hay supervisión activa (como cámaras o registros de ingreso/salida) en áreas críticas.
8	Los visitantes deberán registrarse y recibir una identificación temporal.			X		- En algunos casos, los visitantes no se registran adecuadamente o se omite información clave (nombre, motivo, hora de ingreso/salida).

						- Algunos trabajadores pueden no exigir el cumplimiento del protocolo de visitas.
9	Se controlarán factores como temperatura, humedad y sistemas de detección de incendios.			X		- Algunas zonas podrían no contar con detectores de humo o alarmas operativas.
10	Se realizarán pruebas periódicas de seguridad, incluyendo simulacros y pruebas de intrusión.				X	- Los trabajadores no están debidamente capacitados o no toman en serio los ejercicios. - No se realizan con regularidad o no involucran a todo el personal.
Políticas de control de accesos.		Nivel de cumplimiento				Comentarios
		0%	40%	70%	100%	
1	Definir roles de usuarios en función al trabajo que desempeña.				X	
2	Todos los sistemas y aplicaciones deberán requerir autenticación mediante credenciales únicas para cada usuario.				X	
3	Todos los roles y permisos de acceso serán documentados y revisados periódicamente.				X	
4	Se asignarán permisos mínimos necesarios para realizar las tareas laborales específicas, siguiendo el principio de menor privilegio.			X		- Algunos usuarios tienen acceso a sistemas, archivos o funciones que no requieren para su rol. - Algunos trabajadores no comprenden los límites de sus accesos ni las consecuencias de su mal uso.

5	Las contraseñas deberán cumplir con requisitos de complejidad, incluyendo longitud mínima, uso de caracteres especiales, números y letras.				X	
6	Las contraseñas deberán cambiarse regularmente, al menos cada 90 días.				X	
7	No se permitirá la reutilización de contraseñas antiguas.				X	
8	Se limitará el acceso de terceros a los sistemas y datos estrictamente necesarios para sus funciones.				X	
9	Los accesos deberán ser desactivados inmediatamente cuando un empleado deje la pyme o cambie de rol.				X	
10	Los trabajadores deben bloquear sus equipos de trabajo inmediatamente al salir del escritorio.				X	
11	Restringir el acceso a los datos de tarjetas únicamente al personal autorizado mediante autenticación multifactor.				X	
Políticas contra amenazas externas e internas		Nivel de cumplimiento				Comentarios
		0%	40%	70%	100%	

1	Implementar y mantener firewalls y sistemas de detección de intrusos (IDS).			X		- No todos los puntos de entrada o segmentos de red están protegidos.
2	Realizar evaluaciones de vulnerabilidad periódicas en todos los sistemas que manejan datos de tarjetas.			X		- Las evaluaciones pueden ser manuales o básicas, lo que limita su profundidad.
3	Asegurar que todos los sistemas y software estén actualizados con los parches y actualizaciones de seguridad más recientes.			X		- Algunos equipos o software antiguos no permiten actualizaciones, representando puntos vulnerables. - No todos los sistemas siguen un calendario establecido para parches.
4	Establecer un calendario regular de actualización y parcheo.				X	
5	Configurar segmentación de la red para limitar el alcance de un posible ataque.			X		- Algunos encargados de infraestructura no tienen claridad sobre cómo mantener una segmentación segura y eficiente.
6	Monitorear todas las actividades en los sistemas y redes para detectar comportamientos inusuales o no autorizados.			X		- Las alertas generadas por el monitoreo no están siendo gestionadas correctamente, lo que puede generar un "ruido" de notificaciones sin que se tomen acciones.
7	Fomentar una cultura de seguridad dentro de la pyme.				X	
8	Realizar simulacros de incidentes para asegurar que todos los empleados sepan cómo reaccionar ante una amenaza.				X	