MAESTRÍA EN CIBERSEGURIDAD

PROYECTO DE GRADUACIÓN

Sometido al Tribunal Examinador de Postgrados para optar por el grado de Maestría en Ciberseguridad

Diseño de una propuesta de evaluación de vulnerabilidades basada en buenas prácticas de ciberseguridad para el Local 6 Inversiones Hamburgo, en el cantón central de Golfito, durante el segundo semestre de 2025

AUTOR
Mainor Cruz Alvarado

TUTOR: Randall Artavia Delgado
LECTOR: Irvin Sáenz Córdoba

Pérez Zeledón, Costa Rica
diciembre, 2025

UNIVERSIDAD SAN ISIDRO DEL LABRADOR
MAESTRÍA EN CIBERSEGURIDAD

TRIBUNAL EXAMINADOR

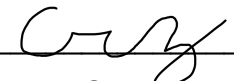
Ing. Ruddy Rodriguez Acuña
Director de Maestría

Msc. Randall Artavia Delgado
Tutor

Ing. Irvin Argenis Sáez Cordoba
Lector

DECLARACIÓN JURADA

Yo, Mainor Cruz Alvarado, mayor, casado, egresado de la carrera de Maestría Profesional en Ciberseguridad de la Universidad San Isidro Labrador, domiciliado en la ciudad de Golfito, portador de la cédula de identidad número 702090041, en este acto, debidamente apercibido y entendido de las penas y consecuencias con las que se castiga, en el Código Penal, el delito del perjurio, ante quienes se constituyen en el Tribunal Examinador de mi Trabajo Final de Graduación para optar por el título de maestría, juro solemnemente que mi trabajo final de graduación titulado "**Diseño de una propuesta de evaluación de vulnerabilidades basada en buenas prácticas de ciberseguridad para el Local 6 Inversiones Hamburgo, en el cantón central de Golfito, durante el segundo semestre de 2025**" es una obra original que ha respetado todo lo preceptuado por las Leyes Penales así con la Ley de Derechos de Autor y Derechos Conexos, número 6683 de 14 de octubre de 1982 y sus reformas, publicada en la Gaceta número 226 de 25 de noviembre de 1982; incluyendo el numeral 70 de dicha ley que advierte: artículo 70º: Es permitido citar a un autor transcribiendo los pasajes pertinentes siempre que estos no sean tantos y seguidos, que puedan considerarse como una producción simulada y sustancial, que redunde en perjuicio del autor y de la obra original. Asimismo, quedo advertido que la Universidad San Isidro Labrador se reserva el derecho de protocolizar este documento ante Notario Público. En fe de lo anterior firmo en la ciudad de Pérez Zeledón, al ser el 6 del mes de diciembre del año dos mil veinticinco.



Mainor Cruz Alvarado
Cédula: 702090041

DEDICATORIA

A mi esposa por todo el amor y apoyo incondicional para cumplir mis metas.

A mis padres y hermanas por brindarme su tiempo y cariño a pesar de la distancia.

A mis amigos por siempre estar presentes y ser mis guías.

AGRADECIMIENTOS

Agradezco a mi esposa y familia por todo el sacrificio realizado, sobre todo por esos momentos que no hemos podido estar juntos.

A mis amigos por el apoyo incondicional, por hacer que esta travesía fuera más fácil.

A la Universidad Internacional San Isidro Labrador, por brindarme la posibilidad de crecer profesionalmente.

CARTA DE AUTORIZACIÓN DEL TUTOR

Pérez Zeledón, 06 de diciembre de 2025

Licenciado
Ruddy Rodríguez Acuña
Coordinador de la Escuela de Informática
Universidad Internacional San Isidro Labrador

Estimado señor Coordinador:

Yo, Randall Mauricio Artavia Delgado, mayor, Ingeniero en informática, con domicilio en la Trinidad de Moravia San José, portador de la cédula de identidad número 205740823, en mi condición de tutor del Proyecto de Graduación titulado Diseño de una propuesta de evaluación de vulnerabilidades basada en buenas prácticas de ciberseguridad para el Local 6 Inversiones Hamburgo, en el cantón central de Golfito, durante el segundo semestre de 2025. Propuesta por el estudiante Mainor Alberto Cruz Alvarado, manifiesto lo siguiente:

1. Que el proceso de trabajo final de graduación culmina satisfactoriamente.
2. Que se ha incorporado en el documento final las sugerencias hechas por el Tribunal Examinador.
3. Que he cumplido con el acompañamiento encomendado por la Universidad en forma y fondo.
4. Que considero que el documento final responde a las exigencias académicas establecidas por la Universidad.

Atentamente,

MATI Randall Mauricio Artavia Delgado
Tutor

CARTA DE APROBACIÓN DEL LECTOR

Pérez Zeledón, 06 de diciembre de 2025

Licenciado
Ruddy Rodríguez Acuña
Coordinador de la Escuela de Informática
Universidad Internacional San Isidro Labrador

Estimado señor Coordinador:

Yo, Irvin Argenis Sáenz Córdoba, mayor, Divorciado, Ing. Sistemas y docente, vecino de Guápiles, portador de la cédula de identidad número 7-0197-0839, en mi condición de lector del Proyecto de Graduación titulado Diseño de una propuesta de evaluación de vulnerabilidades basada en buenas prácticas de ciberseguridad para el Local 6 Inversiones Hamburgo, en el cantón central de Golfito, durante el segundo semestre de 2025. Propuesta por el estudiante Mainor Alberto Cruz Alvarado, manifiesto lo siguiente:

1. Que la lectura del trabajo final de graduación concluye satisfactoriamente.
2. Que he leído el documento final y he hecho mis observaciones en el mismo.
3. Que he cumplido con las labores de lector encomendadas por la Universidad en forma y fondo.
4. Que considero que el documento final responde a las exigencias académicas establecidas por la Universidad.

Atentamente,

Máster Irvin Argenis Sáenz Córdoba
Lector

TABLA DE CONTENIDOS

ÍNDICE DE GRÁFICOS, FIGURAS E ILUSTRACIONES

ÍNDICE DE TABLAS Y CUADROS

LISTA DE PALABRAS CLAVE

Ciberseguridad

Evaluación de vulnerabilidades

Gestión de riesgos

ISO/IEC 27001

ISO/IEC 31000

NIST Cybersecurity Framework

Pequeñas y medianas empresas (PYMES)

Continuidad del negocio

Controles de seguridad

Capacitación y concienciación del personal.

RESUMEN EJECUTIVO

El presente Trabajo Final de Graduación desarrolla un diagnóstico y una propuesta de mejora en ciberseguridad para el Local 6 Inversiones Hamburgo, ubicado en el cantón central de Golfito. En un contexto donde las pequeñas y medianas empresas incrementan su dependencia de sistemas digitales para facturación, inventario y operaciones financieras, se plantea como objetivo general diseñar una propuesta de evaluación de vulnerabilidades basada en buenas prácticas internacionales de ciberseguridad, que permita identificar riesgos y fortalecer la postura de seguridad digital del negocio durante el segundo semestre de 2025.

Metodológicamente, se utiliza un enfoque aplicado y descriptivo, con recolección de información mediante tres instrumentos: una entrevista semiestructurada a personas clave de la organización, una encuesta estructurada tipo Likert sobre controles básicos de seguridad, y una lista de chequeo técnica basada en el NIST Cybersecurity Framework y los CIS Controls. A partir de estos insumos se construye una matriz de riesgos conforme a los lineamientos de ISO/IEC 31000, considerando probabilidad e impacto, y se diseña una herramienta práctica de evaluación de vulnerabilidades apoyada en marcos como ISO/IEC 27001, ISO/IEC 31000, NIST CSF, NIST SP 800-50 y los CIS Controls.

Los resultados del diagnóstico evidencian un nivel de madurez bajo en ciberseguridad. Si bien el local cuenta con algunos controles básicos, como el uso de antivirus y la realización de respaldos semanales, se constató la ausencia de políticas documentadas, de un responsable formal de seguridad, de un programa de capacitación, de monitoreo sistemático de eventos y de procedimientos de respuesta a incidentes. La matriz de riesgos identifica como críticos o altos aspectos como la ausencia de autenticación multifactor en accesos sensibles, la debilidad en la gestión de contraseñas, la falta de pruebas de restauración de respaldos, la inexistencia de registros mínimos de seguridad y la alta dependencia de servicios externos sin análisis formal de continuidad. Asimismo, se detecta una brecha

relevante entre la percepción del personal, que tiende a sobreestimar el grado de control existente y la realidad operativa observada.

En respuesta a este diagnóstico, se diseñó una herramienta de evaluación compuesta por un checklist de 23 controles esenciales, una evaluación de madurez por dominios (Identify, Protect, Detect, Respond, Recover) y una matriz de riesgos integrada, que permite valorar de forma estructurada el estado de la ciberseguridad del Local 6, priorizar riesgos y orientar la toma de decisiones. Esta herramienta, adaptada al tamaño y contexto de la empresa, facilita la aplicación práctica de marcos normativos usualmente asociados a organizaciones de mayor escala.

El estudio concluye que la principal necesidad del Local 6 no es únicamente tecnológica, sino de gestión: formalizar políticas, asignar responsabilidades, establecer procesos básicos de monitoreo, respuesta y continuidad, e incorporar la capacitación del personal como eje transversal. Las recomendaciones propuestas se centran en la adopción gradual de controles de alto impacto y bajo costo, en la institucionalización del uso periódico de la herramienta diseñada y en la posibilidad de replicar el modelo en otras PYMES de la región, contribuyendo así al fortalecimiento de la seguridad digital en contextos similares.

CAPÍTULO I. INTRODUCCIÓN

1.1. Introducción

En la actualidad, las pequeñas y medianas empresas, también denominadas pymes enfrentan múltiples desafíos en materia de ciberseguridad. A pesar de tener un papel fundamental en la economía costarricense, muchas de estas empresas no tienen los recursos y conocimientos necesarios para protegerse adecuadamente contra amenazas cibernéticas. Por su parte, la dependencia de tecnologías digitales, combinada con una falta de educación digital, las convierte en objetivos atractivos para ciberdelincuentes.

En este contexto, es indispensable contar con herramientas adaptadas que permitan a las pymes identificar sus vulnerabilidades digitales y tomar decisiones informadas para reducir los riesgos. Esta investigación se enfoca en el Local 6 Inversiones Hamburgo, una PYME ubicada en el cantón central de Golfito, que opera en un entorno comercial altamente expuesto a las amenazas digitales, pero con recursos limitados para gestionarlas. Por ello, el propósito del proyecto es diseñar una propuesta de evaluación de vulnerabilidades basada en buenas prácticas internacionales, como las promovidas por el NIST (National Institute of Standards and Technology, 2022), los CIS Controls y la norma ISO/IEC 27001 (ISO, 2022), adaptadas a la realidad operativa del negocio.

Para ello, se hará una indagación de trabajos relacionados con la implementación de los tópicos de ciberseguridad aplicados a pymes tanto a nivel nacional como internacional, que permitan brindar precedentes y fortalezca el trabajo de esta investigación. Este tipo de indagatoria es indispensable ya que permite establecer contexto del estado actual, así como presentar una base teórica para justificar la propuesta investigativa.

Posteriormente, se sientan las bases teóricas de este trabajo, en donde se exponen todos aquellos conceptos importantes fundamentales para entender el origen y objetivo principal.

En consecuencia, se explica el modelo metodológico que permite guiar la elaboración de la propuesta. Esto fortalece el ejercicio de cumplir a cabalidad con los objetivos planteados y brindar un producto acorde a las necesidades evaluadas. Todo respondiendo a una necesidad concreta bajo estándares respaldados y objetivamente correctos.

1.2. Antecedentes

El presente trabajo surge del interés por contribuir a la mejora de la ciberseguridad en las pequeñas y medianas empresas ubicadas en zonas rurales de Costa Rica, específicamente en el cantón central de Golfito. El proyecto nació a partir de una experiencia directa con el negocio Local 6 Inversiones Hamburgo, el cual mostró una ausencia de mecanismos formales de evaluación de riesgos informáticos y con ello posibles vulnerabilidades en su infraestructura digital. Esta situación despertó una preocupación profesional al observar cómo muchas PYMES, al igual que este local, operan con escaso conocimiento sobre seguridad digital, lo cual las expone a incidentes que pueden comprometer seriamente su operación.

El interés por el tema se consolidó durante los primeros meses 2025, tras conversaciones con dueños de pequeños negocios. Fue evidente que, a pesar de los esfuerzos nacionales en materia de ciberseguridad, las empresas rurales no cuentan con herramientas prácticas y adaptadas a su realidad operativa. Esta motivación, combinada con la necesidad de aplicar conocimientos adquiridos en el área de tecnología y gestión del riesgo, llevó a formular esta investigación que busca diseñar una propuesta de evaluación de vulnerabilidades informáticas con base en buenas prácticas reconocidas internacionalmente.

A nivel nacional, el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT, 2023) ha impulsado políticas y recomendaciones orientadas a fortalecer la seguridad digital de empresas mediante la estrategia de Ciberseguridad 2023-2027. Sin embargo, estas iniciativas han estado más enfocadas en grandes organizaciones o entidades gubernamentales, dejando a las pymes con herramientas generales poco adaptadas a su realidad operativa y

presupuestaria. La ausencia de instrumentos prácticos de evaluación con enfoque rural limita la capacidad para detectar riesgos e implementar acciones antes de que estos se materialicen.

Bajo este escenario, existen investigaciones que abordan temas de ciberseguridad en las organizaciones. Por ejemplo, en la Universidad Técnica Nacional (UTN), se desarrolló una propuesta enfocada en el fortalecimiento del tratamiento de datos personales mediante la implementación de un estándar de cifrado en bases de datos, conforme a la Ley 8968 (Calvo & Sánchez, 2015).

Por su parte, la Universidad de Costa Rica (UCR) ha promovido recursos educativos sobre ciberseguridad a través del Centro de Informática, los cuales buscan concientizar a la comunidad sobre las amenazas digitales y el manejo seguro de la información (Centro de Informática, 2025).

No obstante, si bien estas iniciativas contribuyen al fortalecimiento de la ciberseguridad en el país, se evidencia una falta de herramientas prácticas de evaluación e incluso de autoevaluación con enfoque que permita a las pymes acceder a estos recursos, especialmente en aquellas pequeñas empresas que se ubican en zonas rurales.

Desde el ámbito académico, diversas investigaciones respaldan la importancia del tema, por lo que se han clasificado los antecedentes en dos grandes categorías: antecedentes nacionales e internacionales, con el fin de mostrar cómo distintas iniciativas han abordado la ciberseguridad en las pequeñas y medianas empresas.

1.2.1. Antecedentes nacionales

En Bustillos Ortega & Rojas Segura (2022) se expone de forma clara una realidad crítica que enfrentan las pequeñas y medianas empresas (PYMES) en el contexto post pandemia a raíz del COVID-19, su creciente exposición a riesgos cibernéticos como consecuencia de la digitalización forzada. La migración hacia plataformas tecnológicas, aunque necesaria para su supervivencia económica, las ha dejado

vulnerables frente a actores maliciosos que aprovechan su limitada preparación en ciberseguridad.

Dicha investigación destaca la urgencia de sensibilizar a las PYMES sobre la protección de sus activos digitales. Muchas veces, estas empresas perciben la ciberseguridad como un tema técnico complejo y económicamente inaccesible, lo cual contribuye a que no adopten medidas preventivas adecuadas. Este criterio es especialmente peligroso en un entorno donde los ataques informáticos no distinguen entre grandes corporaciones y pequeños negocios.

La propuesta investigativa busca construir un protocolo básico de seguridad como una herramienta concreta y adaptada a las posibilidades de las PYMES. Este tipo de soluciones, cuando se basan en estándares técnicos, estudios previos y buenas prácticas, pueden ser clave para generalizar la ciberseguridad y fomentar una cultura de protección digital sostenible.

También, Bustillos Ortega & Rojas Segura (2023) presentan una visión estratégica y necesaria sobre el papel activo que deben asumir los Estados en la protección de las pequeñas y medianas empresas (PYMES) frente a las amenazas cibernéticas. La digitalización global, aunque ha traído consigo múltiples beneficios para la productividad y conectividad, también ha expuesto a las PYMES a riesgos crecientes debido a sus limitaciones financieras y técnicas para implementar medidas de seguridad efectivas.

En este trabajo se reconoce que la ciberseguridad no puede ser abordada únicamente desde el sector privado. Las PYMES, requieren del acompañamiento institucional para fortalecer sus capacidades de prevención, respuesta y recuperación ante incidentes cibernéticos. Es por ello, que abordar la ciberseguridad desde una perspectiva interdisciplinaria y multilateral es la forma correcta, la cooperación entre diferentes sectores y países es fundamental para construir una verdadera cultura de ciberseguridad, especialmente en un entorno donde los ataques no respetan fronteras.

1.2.2. Antecedentes internacionales

El trabajo de investigación desarrollado por Inoguchi Rojas & Macha Moreno (2017) titulado *"Gestión de la ciberseguridad y prevención de los ataques cibernéticos en las PYMES del Perú"*, expone la problemática que enfrentan las pequeñas y medianas empresas peruanas en cuanto a la protección de sus activos informáticos. Los autores identifican que muchas PYMES no cuentan con una adecuada comprensión sobre la importancia de la ciberseguridad, ni sobre conceptos fundamentales como la confidencialidad, integridad y disponibilidad de la información.

El objetivo del estudio fue proponer una estrategia de gestión y prevención en seguridad informática aplicable a PYMES de distintos sectores, con la premisa de que estas empresas tomen conciencia sobre la necesidad de salvaguardar la información que circula en sus redes privadas. Para ello, realizaron un análisis de los riesgos informáticos y formularon recomendaciones específicas orientadas a mejorar la protección de los sistemas informáticos.

Este antecedente internacional resulta relevante, ya que evidencia que los problemas de concientización, falta de inversión y ausencia de políticas de ciberseguridad no son exclusivos de un país, sino que afectan a las PYMES en diversos contextos latinoamericanos, subrayando la necesidad de desarrollar modelos de gestión viables y contextualizados para este sector empresarial.

De la Rosa (2019) destaca el trabajo realizado en España, cuyo objetivo fue acercar el concepto de ciberseguridad al público general y, particularmente, a las pequeñas y medianas empresas (PYMES), reconociendo que muchas de ellas no cuentan con conocimientos técnicos suficientes para identificar sus riesgos digitales ni para implementar medidas efectivas de protección. Esta investigación plantea una estructura educativa y práctica en la que se exponen los principales conceptos de ciberseguridad, se identifican las vulnerabilidades más comunes en el entorno digital, y se analizan herramientas disponibles que las empresas pueden utilizar para elevar sus niveles de protección.

El trabajo también incluyó un enfoque legal, abordando el cumplimiento del Reglamento General de Protección de Datos (RGPD) y la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (LOPDGDD) de España, resaltando la importancia de que las empresas estén al tanto de sus obligaciones legales en materia de protección de datos. Además, se incorporó una parte práctica basada en entrevistas a cinco empresas españolas con presencia en línea, con el fin de conocer sus medidas de ciberseguridad y cómo enfrentan los riesgos en sus operaciones cotidianas.

Este trabajo es significativo porque no solo expone conceptos técnicos de forma accesible, sino que también propone una guía integral y progresiva para la mejora de la ciberseguridad en PYMES, adaptada a un entorno cambiante y con limitaciones presupuestarias.

Valero Bueno & Haz López (2022) exponen un trabajo titulado *"Ciberseguridad post Covid-19 y su impacto en las PYMES del Ecuador"*, el cual analiza cómo las pequeñas y medianas empresas ecuatorianas han percibido y gestionado la ciberseguridad en el contexto posterior a la pandemia de COVID-19. La investigación reconoce que la digitalización, acelerada por la crisis sanitaria, obligó a muchas empresas a tecnificar sus procesos sin una preparación previa suficiente en materia de seguridad informática, lo que aumentó su exposición a riesgos cibernéticos.

Mediante una metodología cualitativa basada en una revisión bibliográfica y la aplicación de encuestas a representantes de PYMES, el estudio tuvo como objetivo principal identificar el nivel de interés y compromiso de estas empresas en la implementación de mecanismos de ciberseguridad tras la pandemia. Los resultados revelaron múltiples debilidades en la infraestructura tecnológica de las empresas, especialmente relacionadas con el desconocimiento, los errores y las omisiones en el manejo adecuado de la seguridad de la información.

El estudio concluye con la formulación de un conjunto de buenas prácticas de ciberseguridad, fundamentadas en normas internacionales como ISO/IEC 27001 y

COBIT 5.0. Estas prácticas están orientadas a mitigar los efectos de amenazas que comprometen los principios fundamentales de la información: confidencialidad, integridad y disponibilidad. Este trabajo es significativo, ya que no solo identifica las áreas críticas de vulnerabilidad, sino que también ofrece una guía práctica y estandarizada que puede ser replicada en otros contextos similares.

Por tanto, diseñar una propuesta de evaluación de vulnerabilidades basada en buenas prácticas de ciberseguridad para el Local 6 Inversiones Hamburgo, busca cubrir el vacío que existe actualmente mediante una propuesta aplicada y contextualizada, adaptada a las características y necesidades específicas de una pyme del cantón central de Golfito.

1.3. Planteamiento del problema

La falta de conocimiento expone a las pymes a amenazas persistentes como ransomware, phishing o violaciones de datos sin tener la capacidad de prevenirlas ni de reaccionar adecuadamente. Bajo esta situación surge la necesidad urgente de contar con una herramienta de evaluación práctica que le permita a las pequeñas empresas a identificar y mitigar vulnerabilidades antes de que sufran consecuencias graves.

En noviembre de 2020, la Municipalidad de Golfito emitió una alerta pública advirtiendo sobre intentos de estafa mediante suplantación de identidad por correo electrónicos, donde se utilizaron direcciones falsas como info@munigolfito.go.cr para engañar a ciudadanos y obtener información confidencial o inducir a realizar pagos no autorizados (Municipalidad de Golfito, 2020). Esta es una de las de situaciones de incidentes de ciberseguridad en instituciones locales y así como el posible desconocimiento de la población sobre cómo identificar estas amenazas.

Asimismo, el en febrero del 2025 el Depósito Libre Comercial de Golfito denunció la publicación de sitios falsos de ventas en línea que simulaban representar al comercio oficial, generando pérdidas económicas entre compradores que fueron víctimas de engaños (May-Grosser, 2025).

Ambos hechos revelan una creciente exposición de entidades públicas, empresas locales y ciudadanos a ciberamenazas básicas pero efectivas, como el phishing, lo que confirma la urgencia de dotar a las pymes locales de herramientas prácticas para reconocer y evaluar vulnerabilidades de ciberseguridad.

Los antecedentes revisados en esta investigación evidencian que la falta de concienciación, capacitación y evaluación estructurada de vulnerabilidades constituye un patrón común en muchas pymes dentro y fuera del país. Diversos estudios han señalado que este tipo de organizaciones tiende a priorizar recursos hacia funciones operativas o comerciales, relegando la ciberseguridad a un segundo plano e incluso mayor.

Frente a este escenario, surge la necesidad de diseñar una propuesta específica que permita a la empresa objeto de estudio identificar sus vulnerabilidades, evaluarlas con base en estándares reconocidos y establecer medidas de control acordes a su capacidad organizativa. Este abordaje contribuirá no solo a fortalecer su postura de seguridad, sino también a promover una cultura organizacional orientada a la gestión del riesgo tecnológico de forma sostenible y adaptada a su realidad local.

1.4. Justificación

Las pymes del cantón central de Golfito enfrentan desafíos particulares en cuanto a su protección digital. En particular, el Local 6 Inversiones Hamburgo el cual se encuentra inmerso dentro del Depósito Libre Comercial de Golfito no contempla dentro de su estructura organizacional una instancia especializada en tecnologías de información, su condicionada capacidad técnica y humana, incluso financiera impide que adopten marcos de ciberseguridad avanzados o consultorías externas.

A nivel nacional, el MICITT lanzó la estrategia nacional de ciberseguridad enfocada en la gobernanza, gestión de riesgos y protección de infraestructuras criticas (MICITT, 2023). Sin embargo, estas acciones no son prácticas para pymes rurales.

En este contexto, surge la necesidad urgente e importante de desarrollar soluciones prácticas, económicas y contextualizadas a pymes para identificar sus vulnerabilidades y con ello contribuir directamente en mejorar sus condiciones cibernéticas, lo que permite tomar conciencia de sus debilidades y actuar de forma preventiva.

Esta investigación aborda estas deficiencias al diseñar una herramienta de evaluación de vulnerabilidades basadas en buenas prácticas internacionales como las ISO/IEC 27001, ISO/IEC 31000. Tiene como beneficiario el Local 6 Inversiones Hamburgo, no obstante, este trabajo no solo busca este comercio identifique y mitigue sus debilidades cibernéticas, si no que sirva como modelo replicable para el sector pyme del sector rural de la zona sur del país.

El aporte principal de esta investigación es cerrar una brecha entre las buenas prácticas internacionales y su aplicación contextualizada en pymes rurales, transformar la teoría institucional y académica en una solución tangible. Se podría considerar que su utilidad radica en ofrecer un insumo que influye en la toma de decisiones estratégicas y promueve la cultura de protección digital basada en la prevención, análisis de riesgos y mejora continua.

El impacto de este proyecto va más allá del ámbito académico, ya que ofrece un producto aplicable, que fortalece la seguridad digital de la pyme desde una perspectiva de educación y mejora continua. Responde a un vacío práctico y contextual, con el propósito de promover y difundir de que la ciberseguridad no tiene por qué ser inaccesible o exclusiva de grandes empresas.

1.5. Objetivos

1.5.1. Objetivo general

Diseñar una implementación de evaluación de vulnerabilidades informáticas basada en buenas prácticas de ciberseguridad para el Local 6 Inversiones Hamburgo, ubicado en el cantón central de Golfito, que permita identificar riesgos y fortalecer su postura de seguridad digital durante el segundo semestre de 2025.

1.5.2. Objetivos específicos

- Realizar un diagnóstico de la situación actual de la ciberseguridad en el Local 6 Inversiones Hamburgo, mediante una revisión de su infraestructura digital, prácticas operativas y políticas de seguridad existentes.

- Identificar los riesgos existentes a través de la probabilidad y el impacto que puedan tener las vulnerabilidades informáticas presentes en el negocio, a través de una evaluación exploratoria basada en ISO/IEC 31000.

- Diseñar una herramienta práctica de evaluación de vulnerabilidades, adaptada a las características técnicas y operativas del Local 6 Inversiones Hamburgo, fundamentada en buenas prácticas internacionales de ciberseguridad.

1.6. Alcance

El proyecto se enfocará en el diseño de una metodología y herramienta de evaluación de vulnerabilidades para el Local 6 Inversiones Hamburgo, fundamentada en buenas prácticas internacionales de ciberseguridad, incluyendo ISO/IEC 27001, ISO/IEC 31000, NIST, y CIS Controls. Como parte del alcance, se realizará un diagnóstico integral de la infraestructura tecnológica, las políticas de seguridad y las prácticas operativas del personal, con el objetivo de identificar y priorizar riesgos en función de su probabilidad e impacto.

Para la recolección de información se utilizarán encuestas estructuradas dirigidas a colaboradores, entrevistas semiestructuradas a responsables técnicos y de gestión, y listas de verificación basadas en marcos normativos internacionales. A partir de estos insumos, se desarrollará una herramienta práctica adaptada al contexto de la organización, capaz de evaluar de manera sistemática las vulnerabilidades y riesgos presentes en el entorno digital.

Es importante destacar que este proyecto se limita a la identificación, análisis y priorización de riesgos, sin incluir la implementación de medidas correctivas, mitigación activa de vulnerabilidades ni adquisición de hardware o software especializado. Asimismo, no contempla servicios de consultoría externa a largo plazo.

Los principales entregables serán: el informe de diagnóstico de ciberseguridad, los instrumentos aplicados (encuestas, entrevistas y listas de verificación), la matriz de riesgos priorizados, la herramienta de evaluación de vulnerabilidades y el informe final con recomendaciones estratégicas para fortalecer la postura de seguridad digital del Local 6.

En la Imagen 1 muestra de manera gráfica la composición del alcance del proyecto, destacando sus características principales, elementos incluidos y aspectos excluidos.

Imagen 1.

Alcance del proyecto: Inclusiones y Exclusiones

Nota. Elaboración propia.

Finalmente, el proyecto se llevará a cabo entre septiembre y diciembre de 2025, concluyendo con la entrega de todos los resultados y la herramienta diseñada.

CAPÍTULO II. MARCO TEÓRICO

2.1. Introducción

Este capítulo presenta los conceptos teóricos que permiten dar contexto a este trabajo, con ello situar por qué en esta era digital, las pequeñas y medianas empresas se han convertido objetivos potenciales para ataques cibernéticos (Junior et al., 2023). En una primera instancia (sección 2.2) se exponen los fundamentos necesarios sobre ciberseguridad, con el fin de dar a conocer principios, su importancia y tendencias actuales.

En segunda instancia, en la sección 2.3 se presentan vulnerabilidades. Luego, en la sección 2.4 buenas prácticas y estándares.

2.2. Las Pymes en la era digital

Las tecnologías emergentes han transformado el horizonte de las pequeñas y medianas empresas, ofrece nuevas oportunidades para mejorar la productividad, la competitividad y la capacidad de innovación. No obstante, la adopción de estas herramientas continúa enfrentando limitaciones vinculadas a la falta de capacitación, los recursos económicos insuficientes y la baja conectividad. Un estudio reciente elaborado por Paula Yugsi et al. (2024) y titulado “Tecnologías emergentes para las PYMES en los cantones Sigchos y Latacunga” reveló que, si bien las PYMEs muestran familiaridad con ciertos recursos digitales como los asistentes virtuales, el conocimiento en áreas críticas como la ciberseguridad sigue siendo reducido, alcanzando apenas el 6.52% de los encuestados. Esta situación refleja la existencia de una brecha significativa entre el potencial de las tecnologías emergentes y su aplicación real en el entorno empresarial. En este contexto, resulta indispensable analizar cómo las PYMEs en su proceso de digitalización pueden integrar de manera efectiva herramientas tecnológicas que, además de optimizar procesos, fortalezcan sus prácticas de seguridad informática y reduzcan su exposición a vulnerabilidades (Paula Yugsi et al., 2024).

2.2.1. Pymes

Para tratar de definir el término PYME se debe considerar analizar una serie de elementos. No obstante, se establece que una PYME es básica en la producción industrial, sin embargo, su definición no se ha estandarizado internacionalmente y pueden existir algún tipo de diferencias y clasificación según entes gubernamentales hasta de un mismo país (Orlandi, 2006). Estas clasificaciones pueden estar relacionadas al número de empleados o volumen de ventas. Por consiguiente, Cardozo et al. (2012) indican que la definición de PYME es:

> En su concepción más amplia una PYME, es una unidad económica productora de bienes y servicios, dirigida por su propietario, de una forma personalizada y autónoma, de pequeña dimensión en cuanto a número de trabajadores y cobertura de mercado (Cardozo et al., 2012, p. 3).

La definición de las pequeñas y medianas empresas en la región continúa siendo un desafío debido a la diversidad de criterios utilizados para su clasificación. No obstante, la propuesta de González-Díaz & Becerra-Pérez (2021) sugiere la necesidad de avanzar hacia una definición estandarizada que, tomando como base variables cuantificables como el número de empleados y las ventas brutas anuales, permita estratificar a las empresas de forma homogénea por sector productivo. Bajo este enfoque, Centroamérica establece rangos que oscilan entre microempresas de hasta 10 trabajadores, pequeñas de hasta 50 y medianas de hasta 150, lo que ofrece un marco de referencia regional que facilita la comparación y el diseño de políticas económicas (González-Díaz & Becerra-Pérez, 2021).

2.2.2. Transformación digital en las Pymes

La transformación digital se entiende como parte de una evolución de la industria a un mundo digitalizado, pasando de ser una oportunidad tecnológica a una necesidad para gestionar los deseos y expectativas de una población (Kraus et al., 2022).

Para Calle Herencia (2022) la transformación digital se define como:

> Es el conjunto de los elementos de la organización para transformar los lineamientos, procesos y productos a un contexto virtual involucrando un cambio organizacional en la cultura, comportamiento, competencias y habilidades teniendo como principal objetivo al consumidor(Calle Herencia, 2022, p. 67).

La digitalización de las pequeñas y medianas empresas en América Latina se ha convertido en un requisito indispensable para mantener la competitividad. No obstante, gran parte de estas organizaciones aún operan con bajos niveles de madurez digital, lo que limita la adopción efectiva de tecnologías como servicios en la nube, plataformas de comercio electrónico o sistemas de gestión empresarial (Pozo-Benites et al., 2025). Factores como la insuficiente infraestructura tecnológica, la escasez de personal calificado y las restricciones presupuestarias dificultan la consolidación de entornos digitales seguros. Esta situación expone a las organizaciones a mayores riesgos de seguridad informática, al no contar con medidas adecuadas de protección frente a amenazas cibernéticas, lo que refuerza la necesidad de estrategias que integren no solo tecnología, sino también cultura de seguridad y gestión de recursos digitales.

Por consiguiente, las PYMEs enfrentan problemáticas de ciberseguridad equivalentes a las de las grandes corporaciones; sin embargo, su principal limitación radica en la escasez de recursos financieros y técnicos para gestionar los riesgos de manera eficaz (Sánchez-Sánchez et al., 2021).

2.3. Fundamentos de ciberseguridad

2.3.1. Ciberseguridad

De acuerdo con el *Cyber Security Body of Knowledge* (CyBOK), la ciberseguridad comprende la protección de los sistemas de información, esto incluye hardware, software e infraestructura, así como los datos y servicios que estos proporcionan frente a accesos no autorizados, daños o usos no correctos. Esta protección incluye tanto amenazas intencionales generadas por operadores maliciosos, como errores

accidentales ocasionados por la omisión de procedimientos de seguridad (CyBOK, 2021; UK National Cyber Security Strategy, 2016)

La definición proporcionada enfatiza la protección técnica, sin embargo, el mismo CyBOK expone que también deberían contemplarse los efectos sobre los usuarios, la confianza en los sistemas y la necesidad de equilibrar la seguridad con la usabilidad. Asimismo, se reconoce que una parte significativa de la ciberseguridad proviene del campo de la seguridad de la información, que de acuerdo con la norma ISO/IEC 27000, se basa en la preservación de la confidencialidad, integridad y disponibilidad de la información (ISO, 2018a).

A continuación, se exponen algunas de las definiciones presentadas por diferentes actores.

> *Según la Cybersecurity and Infrastructure Security Agency (CISA, 2021, párr. 1)(traducción propia), la ciberseguridad es el arte de proteger redes, dispositivos y datos contra accesos no autorizados o usos delictivos, y la práctica de garantizar la confidencialidad, integridad y disponibilidad de la información.*

Asimismo, Cains et al., p. (2022, p. 1644) presentan la definición de ciberseguridad como:

> *El Departamento de Seguridad Nacional indica que es una actividad o proceso que protege y/o defiende la información y los sistemas contra daños, uso o modificación no autorizados, o explotación. Aunque estas definiciones expresan la necesidad de proteger los activos, se centran en el hardware y el software y no tienen en cuenta los aspectos humanos de la ciberseguridad.*

Finalmente, Roșca, p. (2024, p. 378) en su trabajo expone tres definiciones luego de analizar diversas fuentes especializadas:

- Kemmerer (2003) define la ciberseguridad como el conjunto de métodos defensivos orientados a detectar posibles intrusos. Esta visión destaca el

papel esencial de la vigilancia y la capacidad de respuesta ante amenazas, subrayando la necesidad de mantener mecanismos de detección activos frente a los ataques que comprometan la seguridad de los sistemas de información.

- Por su parte, Amoroso (2006) amplía la perspectiva al señalar que la ciberseguridad busca reducir la probabilidad de que un ataque malicioso afecte a programas, computadoras o redes. Para ello, contempla la utilización de herramientas como sistemas de detección de intrusiones, antivirus, controles de acceso, mecanismos de autenticación, comunicaciones cifradas, entre otros. Esta definición resalta no solo la detección, sino también la prevención y mitigación de riesgos.

- La ITU (2009) aborda la ciberseguridad desde una perspectiva aún más amplia, considerándola como un conjunto de herramientas, normas, principios, salvaguardas, estrategias, medidas de gestión de riesgos, acciones formativas, controles de aseguramiento y tecnologías orientadas a proteger tanto el entorno cibernético como los activos de las organizaciones y usuarios.

Por consiguiente, Roșca (2024) de estas tres definiciones analizadas deduce una naturaleza dinámica y compleja de la ciberseguridad, donde estaca que el primer autor enfatiza en la necesidad de defensa y monitoreo, el segundo autor agrega la gestión proactiva y el uso de herramientas de protección y que el ultimo autor incorpora aspectos técnicos, estratégicos y formativos. De esto concluye que la ciberseguridad debe tener una gestión integral, donde combina aspectos de defensa, prevención, gestión de riesgos y de formación continua.

2.3.2. Principios fundamentales; confidencialidad, integridad y disponibilidad

Los principios fundamentales de la ciberseguridad están sustentados en un modelo conocido como la CIA:

- **Confidencialidad**: implica mantener restricciones autorizadas sobre el acceso y la divulgación de la información. La pérdida de confidencialidad se manifiesta como una divulgación no autorizada de datos.

- **Integridad**: consiste en proteger la información frente a modificaciones o pérdidas indebidas. También asegura la autenticidad y el no repudio de la información. Una pérdida de integridad ocurre cuando se modifica o elimina información sin autorización.

- **Disponibilidad**: se refiere a garantizar el acceso y uso oportuno y fiable de la información por parte de los usuarios autorizados. La pérdida de disponibilidad ocurre cuando se interrumpe el acceso o uso de la información o del sistema que la gestiona (Stalling, 2017).

Estos principios se encuentran sujetos y cubiertos desde normas internacionales como lo es la Organización Internacional de Normalización (ISO) en su norma ISO27000, el cual establece las directrices específicas para fortalecer la seguridad de información, promueve mejoras en la protección, eficiencia operativa y reducción de costos. La norma no está especificada para grandes o pequeñas organizaciones, es indiferente a ello, lo que hace posible su aplicación a cualquier sector y contexto (Babilonia, 2023).

2.4. Vulnerabilidades informáticas

Harkai (2024) confiesa que la ciberseguridad es un aspecto fundamental en la actualidad, derivada principalmente por la protección de dispositivos móviles. Aunque estos dispositivos ofrecen una serie de posibilidades como la portabilidad y accesibilidad, también exponen a los usuarios a diversos riesgos.

Por ello, es fundamental comprenden las vulnerabilidades informáticas asociadas no solo a los dispositivos móviles, si no, a toda la gama de posibilidades en donde

los atacantes observan oportunidades para comprometer la seguridad y privacidad de los usuarios.

Las vulnerabilidades se refieren a cualquier tipo de debilidad susceptible de ser explotada o utilizada de forma indebida, lo que puede resultar en consecuencias no deseadas. Por tanto, se podría entender una vulnerabilidad como:

> *Una debilidad que puede ser explotada por un ciberataque lanzado por un actor de amenaza. En otras palabras, la vulnerabilidad es un defecto, laguna, error, limitación, descuido o susceptibilidad en cualquier aspecto de la tecnología financiera, especialmente en el entorno informático. Si se explota una vulnerabilidad, puede causar graves pérdidas o daños a los activos (Harkai, 2024, p. 89).*

De este modo, si una debilidad se aprovecha, podría afectar negativamente un sistema o proceso (CyBOK, 2021). Para Kaur et al., (2021, p. 92) entre las principales vulnerabilidades asociadas a las tecnologías, plataformas y frameworks se encuentran las que se detallan en la Tabla 1:

Tabla 1. Vulnerabilidades generales de las tecnologías.

Nombre	Descripción
URL redirection	Es una vulnerabilidad sencilla que permite a un actor malicioso redirigir o reenviar una URL legítima (Localizador Uniforme de Recursos) para hacerla accesible bajo una o más direcciones URL diferentes. También se conoce como reenvío de URL. Cuando un navegador intenta abrir una página redireccionada, en su lugar se abre una página con una URL distinta.
Crafted URL redirection	Es una variante modificada de la redirección de URL en la que una dirección se crea o manipula intencionadamente para engañar a los usuarios y

	dirigirlos a páginas web diseñadas para realizar actividades ilegales.
Remote code execution	Se lleva a cabo mediante la ejecución remota de código a través de un script automatizado. El objetivo de explotar esta vulnerabilidad es otorgar privilegios administrativos de un sistema vulnerable a un usuario remoto. Una vez que el atacante obtiene esos privilegios, intenta ocultar su identidad y permanencia en el sistema comprometido, y lo usa para lanzar ataques de ejecución remota en otros equipos.
Microsoft exchange memory corruption	Es una vulnerabilidad de ejecución remota de código que afecta al software Microsoft Exchange. Se produce cuando el programa falla al gestionar un objeto en memoria. Al explotar esta vulnerabilidad, un atacante puede ejecutar código arbitrario en la memoria para realizar acciones como instalar programas, modificar permisos de archivos y carpetas o crear nuevas cuentas.
Information disclosure	Consiste en revelar información sensible, ya sea de manera intencional o accidental, a personas no autorizadas. Algunas organizaciones usan el término fuga de información, aunque la enumeración común de debilidades (CWE) desaconseja su uso, ya que el término “fuga” puede referirse también a otros problemas, como las fugas de memoria.
DLL hijacking	Es una vulnerabilidad en los sistemas operativos Windows que permite a los atacantes ejecutar código malicioso aprovechando una biblioteca de enlace dinámico (DLL) vulnerable. Las DLL son bibliotecas compartidas que contienen código, datos o recursos.
Ransomware	Es un tipo de malware que cifra archivos y directorios en un equipo objetivo, bloqueando el acceso autorizado y

	exigiendo un rescate económico para entregar la clave de descifrado. Ejemplos notorios de ataques de ransomware son WannaCry y CryptoWall, que han causado graves daños a nivel mundial.
Command injection	Permite la ejecución de comandos arbitrarios en el sistema operativo a través de una aplicación vulnerable. Esto ocurre cuando un usuario introduce datos no validados en un shell del sistema. Los atacantes aprovechan formularios, cookies o cabeceras HTTP para enviar comandos que se ejecutan con los privilegios de la aplicación vulnerable.
Out-of-bounds write:	Como su nombre lo indica, se produce cuando se escribe información fuera del límite asignado al búfer de una aplicación, ya sea antes de su inicio o después de su final. Puede prevenirse mediante la validación de entradas y verificación de los límites.
Cross-site Scripting (XSS)	Es una vulnerabilidad de inyección que permite al atacante insertar código malicioso en una página web legítima. Mediante aplicaciones web, los atacantes envían scripts que el usuario final ejecuta sin sospechar, ya que provienen de un sitio de confianza. Estos scripts pueden acceder a cookies, tokens de sesión u otros datos sensibles del navegador.
Microsoft Office SharePoint XSS	Ocurre cuando el servidor SharePoint de Microsoft no filtra adecuadamente las solicitudes web especialmente diseñadas. Si se explota, el atacante puede lanzar ataques XSS hacia otros sistemas, obteniendo acceso a contenido autorizado al que no debería tener acceso.
Elevated privileges	Un usuario normal no posee derechos administrativos. Sin embargo, tras explotar una vulnerabilidad, un atacante puede intentar elevar sus privilegios para

	obtener acceso administrativo y realizar actividades no autorizadas. Una vez logrados estos privilegios, el daño potencial puede llegar incluso al núcleo (kernel) del sistema operativo.
Brute-force authentication	En un ataque de fuerza bruta, el atacante prueba múltiples combinaciones de contraseñas o frases de paso hasta acertar. Se basa en una búsqueda exhaustiva para descubrir la clave correcta. El tiempo y el poder computacional necesarios aumentan exponencialmente con la longitud de la contraseña.
Execute a maliciously crafted file	Un archivo diseñado maliciosamente puede causar un desbordamiento de búfer, permitiendo al atacante inyectar y ejecutar código malicioso junto con el código legítimo.
Remote hijacking	Explota características legítimas del Protocolo de Escritorio Remoto (RDP) en Windows. Permite al atacante reanudar una sesión remota previamente desconectada, obteniendo privilegios elevados sin necesidad de credenciales.
DNS amplification	Es un ataque de denegación de servicio distribuido (DDoS) en el que el atacante utiliza un resolver DNS abierto para saturar un servidor objetivo con tráfico masivo de DNS, volviendo inaccesible al servidor para usuarios legítimos. Este ataque se potencia usando bots que generan grandes cantidades de solicitudes DNS falsificadas.
Directory traversal	Vulnerabilidad web que permite al atacante leer archivos arbitrarios en el servidor. En algunos casos, también puede escribir en ellos.
Arbitrary file overwrite	Permite al atacante sobrescribir archivos existentes o crear nuevos archivos en el servidor. También conocida

	como Zip-Slip, puede alterar el comportamiento de las aplicaciones o comprometer el servidor.
Money laundering	Muchas instituciones financieras son vulnerables al lavado de dinero, que consiste en legitimar fondos obtenidos ilícitamente. Este proceso busca ocultar el origen ilegal de los fondos para hacerlos parecer legítimos.
Phone verification without OTP	Esta vulnerabilidad permite omitir el proceso de autenticación mediante código de un solo uso (OTP) durante una transacción financiera.

Nota: La tabla muestra una serie de vulnerabilidades en tecnologías de información y su respectiva descripción. Elaboración propia a partir de información recolectada en Kaur et al., (2021, p. 92).

Luego de profundizar en las vulnerabilidades, estas podrían clasificarse en dos grandes categorías; tecnológicas y humanas.

2.4.1. Vulnerabilidades tecnológicas

Una vulnerabilidad tecnológica se considera técnica en consecuencia de una debilidad en hardware, software, redes o configuraciones de sistema que les permiten a los atacantes comprometer la confidencialidad, integridad o disponibilidad de un sistema (CyBOK, 2021). Un ejemplo es cuando la interfaz de una aplicación permite el ingreso de datos indebidos sin una validación adecuada, lo que podría ser aprovechado por un atacante para alterar el funcionamiento del sistema o acceder a información no autorizada.

Para Kaur et al. (2021) las vulnerabilidades tecnológicas más comunes son:

- Controles de seguridad obsoletos
- Antivirus desactualizado
- Sistemas operativos sin parches

- Instalación de aplicaciones de fuentes no confiables
- Dispositivos de seguridad de tipo endpoint débiles
- Vulnerabilidades en aplicaciones de teléfonos inteligentes
- Inyección de malware para robar credenciales
- Conexiones inseguras con el servidor
- Verificación de dispositivos sin OPT
- Sitios web
- Las vulnerabilidades más comunes son Cross-Site Scripting (XSS), exposición de datos sensibles y configuraciones de seguridad incorrectas, conforme a las categorías A3, A2 y A5 del (OWASP, 2025).

2.4.2. Vulnerabilidades humanas

Esta categoría hace referencia a errores que son cometidos por los usuarios finales, estas pueden ser por un descuido o por total desconocimiento. Incluso, se puede decir que este tipo de vulnerabilidades son de mayor peligro que las tecnológicas (Kaur et al., 2021).

Entre las vulnerabilidades más comunes se encuentran:

- Manejo de contraseñas
- Guardar contraseñas de forma automática
- Usar la misma contraseña en diferentes cuentas
- Frecuencia en el cambio de contraseñas
- Fortaleza y longitud en las contraseñas

- Compartir contraseñas con amistades
- Desechar documentos sensibles a la basura.
- Conciencia cibernética
- Hacer clic en correos sospechosos y compartir información en formularios
- Hacer clic en enlaces maliciosos relacionados con ofertas gratis
- Falta de educación en ciberseguridad
- Hábitos en el manejo de computadoras
- Dejar computadoras o estaciones de trabajo sin bloquear
- Confiar en empleados
- Uso de dispositivos personales
- Alfabetización digital

Las vulnerabilidades humanas son el factor clave que permite el éxito de los ataques de ingeniería social, ya que los atacantes buscan explotarlas mientras las víctimas intentan evitarlas o mitigarlas. Dichas vulnerabilidades abarcan la falta de conocimiento, los hábitos inseguros, la manipulación de emociones y diversos factores psicológicos, los cuales incluyen desde la naturaleza humana y los rasgos de personalidad hasta las características individuales, haciendo que las personas sean susceptibles a la manipulación y facilitando el accionar del atacante (Wang et al., 2021). Aksoy (2024) revela un informe de la compañía IBM el impacto potencial de estos tipos de errores, indica que si se pudieran mitigar los errores humanos se podría evitar hasta un 95% de las brechas de seguridad.

2.5. Herramientas y sistemas de evaluación de vulnerabilidades

La gestión de las vulnerabilidades en ciberseguridad requiere de una identificación, así como de una correcta clasificación y valoración del impacto potencial. Para lograrlo, se han desarrollado estándares y sistemas que permiten a las organizaciones analizar las amenazas detectadas y priorizar las acciones correctivas. Dentro de estos, destacan el Common Vulnerabilities and Exposures (CVE) y el Common Vulnerability Scoring System (CVSS**)**, las cuales son referencias internacionales en la industria de la ciberseguridad.

El sistema CVE, está gestionado por MITRE Corporation, proporciona un catálogo público de vulnerabilidades conocidas, asignándoles un identificador único y una descripción estandarizada. Esta práctica permite a los profesionales de seguridad y a las herramientas automatizadas consultar una base común al momento de reportar o mitigar vulnerabilidades (MITRE, 2025).Gracias al CVE, la industria puede hablar un "lenguaje común" sobre las fallas de seguridad, facilitando la coordinación de respuestas y la comparación de datos entre distintas plataformas (MITRE, 2024).

Sin embargo, el CVE por sí solo no determina la gravedad de la vulnerabilidad. Para ello, se utiliza el Common Vulnerability Scoring System (CVSS), desarrollado por el Forum of Incident Response and Security Teams (FIRST**)** (Chacón Luna, 2025). El CVSS ofrece un método para medir el nivel de riesgo de una vulnerabilidad mediante un puntaje numérico que va de 0.0 a 10.0, considerando factores como la complejidad del ataque, el nivel de privilegios requeridos y el impacto en la confidencialidad, integridad y disponibilidad de los sistemas (FIRTS, 2023).

2.6. Estándares internacionales

En un entorno digital cada vez más complejo, la adopción de estándares internacionales en ciberseguridad se ha convertido en una estrategia clave para fortalecer la resiliencia organizacional, garantizar el cumplimiento normativo y consolidar la confianza institucional. Estos marcos, como ISO/IEC 27001 o el NIST Cybersecurity Framework, no solo permiten estructurar sistemas de gestión

robustos, sino que también actúan como catalizadores de legitimidad y diferenciación competitiva en sectores altamente regulados (Choez-Calderón & Aldo-Patricio, 2025).

2.6.1. ISO/IEC 27001

La norma ISO/IEC 27001 tiene como objetivo principal salvaguardar la información y los sistemas que la gestionan frente a accesos no autorizados, divulgaciones indebidas o destrucción intencionada. Su implementación permite fortalecer la seguridad de los datos, reducir el riesgo de fraudes y prevenir pérdidas o filtraciones de información. Entre sus beneficios destacan la capacidad de identificar riesgos y aplicar controles adecuados para mitigarlos, garantizar la confidencialidad al restringir el acceso solo a personas autorizadas, y ofrecer flexibilidad para adaptar sus controles a toda la organización o a áreas específicas. Además, promueve la confianza de clientes y partes interesadas al demostrar un compromiso sólido con la protección de los datos, lo que puede posicionar a la empresa como proveedor preferente y facilitar el cumplimiento de expectativas regulatorias y comerciales (De la Rosa Martín, 2021).

En cuanto a sus componentes, la ISO/IEC 27001 abarca un conjunto interconectado de elementos. Estos incluyen la evaluación y gestión de riesgos, que orienta la identificación de vulnerabilidades y la definición de medidas de mitigación; la implementación de controles de seguridad, organizados en 93 prácticas distribuidas en cuatro categorías principales; el liderazgo de la alta dirección, indispensable para asignar recursos y consolidar una cultura de seguridad; la mejora continua, basada en el ciclo Planificar-Hacer-Verificar-Actuar, que garantiza la actualización constante frente a nuevas amenazas; la documentación y registros, que permiten dar trazabilidad a procesos y decisiones; y la concienciación y capacitación del personal, concebidas como estrategias para sostener un entorno seguro (Laghnimi et al., 2024).

En otros términos, La norma ISO/IEC 27001 se reconoce internacionalmente como un estándar fundamental para la gestión de la seguridad de la información. Su

implementación es vista por autoridades regulatorias y socios comerciales como una muestra clara del compromiso organizacional con las buenas prácticas y la responsabilidad en el manejo de datos sensibles (ISO, 2022).

2.6.2. NIST SP 800-50 Rev. 1

El reporte NIST SP 800-50 Rev. 1, de nombre Building a Cybersecurity and Privacy Learning Program, ofrece directrices para que las agencias y organizaciones diseñen, implementen y mantengan Programas de Aprendizaje en Ciberseguridad y Privacidad (CPLP) de forma integral. Esto incluye tanto a organizaciones grandes como pequeñas (Merritt et al., 2024).

El NIST SP 800-50 Rev tiene campañas y actividades de concienciación, entrenamientos de sensibilización, ejercicios prácticos, capacitaciones temáticas basadas en funciones específicas, así como programas educativos. También ofrece orientación sobre cómo elaborar un plan estratégico del programa, garantizando que existan los recursos adecuados para alcanzar los objetivos de aprendizaje de la organización.

La guía se encuentra organizada en cuatro secciones que reflejan un ciclo integral: el diseño del programa, orientado a identificar objetivos, audiencias y recursos; el desarrollo del material de capacitación, en el que se definen contenidos, métodos pedagógicos y herramientas de apoyo; la implementación del programa, que implica su puesta en marcha dentro de la organización; y finalmente, los procesos posteriores a la implementación, dedicados a la evaluación, retroalimentación y mejora continua de la iniciativa (Basha et al., 2024)

Por tanto, se destaca como un programa efectivo de concienciación y capacitación puede reducir significativamente las vulnerabilidades derivadas de errores humanos, al fortalecer las competencias de los usuarios, quienes son clave en la seguridad de la organización (Dupuis & Renaud, 2024).

2.6.3. ISO/IEC 31000:2018

La norma ISO 31000:2018 promueve un enfoque estructurado y continuo para gestionar riesgos, integrándolos en todos los procesos organizacionales con el fin de fortalecer la toma de decisiones y la resiliencia institucional (Botunac et al., 2024).

De acuerdo con Yonatan et al. (2025) la norma ISO 31000:2018 define el riesgo como la incertidumbre que afecta el logro de los objetivos. Bajo esta perspectiva, el riesgo se entiende a partir de tres dimensiones principales: los objetivos, que representan las metas estratégicas de una organización (como crecimiento, rentabilidad o innovación); la incertidumbre, asociada a la imposibilidad de prever con exactitud las condiciones y variabilidades del entorno; y los impactos, que corresponden a las consecuencias derivadas de eventos que desvían a la organización de sus resultados esperados.

Es aplicable a todas las organizaciones, independientemente de su tipo, tamaño, actividades y ubicación, y abarca todos los tipos de riesgo. Fue desarrollada por diversas partes interesadas y está destinada a cualquier persona que gestione riesgos, no solo a los gestores de riesgos profesionales (ISO, 2018b).

A partir de los hallazgos en la siguiente Tabla 2 se muestra un resumen de contenido de cada una de las normas descritas en los apartados anteriores.

Tabla 2. Resumen de normas.

Aspecto	ISO/IEC 27001:2022	ISO/IEC 31000:2018	NIST SP 800-50 Rev. 1
Enfoque principal	Estándar para la implementación de un Sistema de Gestión de Seguridad de la Información.	Directriz internacional para la gestión integral de riesgos.	Guía para establecer programas de concienciación y capacitación en ciberseguridad.
Objetivo	Proteger la confidencialidad,	Gestionar la incertidumbre que	Proporcionar un proceso estructurado para diseñar,

	integridad, disponibilidad y no repudio de la información.	impacta en el logro de objetivos estratégicos, considerando riesgos negativos y positivos.	desarrollar, implementar y evaluar programas de formación en seguridad.
Definición de riesgo	Riesgo como evento que compromete la seguridad de la información.	Riesgo como *incertidumbre* que afecta objetivos (incluye amenazas y oportunidades).	No define riesgo directamente, sino que lo aborda desde la perspectiva del factor humano y la reducción de incidentes por falta de conciencia.
Componentes principales	• Evaluación y gestión de riesgos. • 93 controles de seguridad. • Liderazgo y cultura de seguridad. • Ciclo de mejora continua. • Documentación y registros. • Capacitación del personal.	• Identificación, análisis, evaluación y tratamiento de riesgos. • Flexibilidad y adaptación. • Integración con otros marcos (COSO, ERM, COBIT, NIST, etc.). • Aplicación transversal a sectores.	• Diseño del programa: definición de objetivos, audiencias y recursos. • Desarrollo del material: contenidos y métodos. • Implementación: despliegue del programa en la organización. • Post-implementación: evaluación, retroalimentación y mejora.
Ámbito de aplicación	Seguridad de la información en cualquier organización.	Gestión integral de riesgos en diversos ámbitos (financiero, tecnológico, ambiental, etc.).	Concienciación y capacitación en ciberseguridad para empleados y directivos.
Carácter	Normativo y certificable.	Directriz de referencia, no certificable.	Documento técnico-guía, no certificable.
Aporte clave	Establece un marco de gestión certificable para la	Brinda un enfoque flexible y adaptable para gestionar la	Refuerza el factor humano como eje crítico de la ciberseguridad,

	seguridad de la información.	incertidumbre organizacional.	fomentando una cultura organizacional segura.

CAPÍTULO III. MARCO METODOLÓGICO

3.1. Introducción

El presente capítulo describe el enfoque metodológico para el desarrollo de la investigación, el cual permite garantizar la coherencia entre los objetivos formulados y los procedimientos utilizados para la recolección y análisis de datos. La metodología se establece como un conjunto de estrategias y técnicas que orientan el estudio hacia la obtención de información confiable y útil para la toma de decisiones fundamentadas.

Según Hernández et al. (2014) la metodología de investigación consiste en un proceso sistemático que guía la selección del tipo de estudio, el diseño, las técnicas e instrumentos, así como la interpretación de los resultados, en función de la naturaleza del problema planteado.

Este capítulo se estructura en dos apartados. En el primero, se establece el tipo de investigación, abarcando su finalidad, enfoque metodológico y naturaleza. En el segundo, se detallan los procedimientos administrativos y técnicos para el abordaje del estudio, incluyendo la definición de fuentes de información y la construcción de los instrumentos empleados para la recolección de datos.

3.2. Tipo de investigación

Desde una visión epistemológica, toda investigación se presenta su finalidad, enfoque, naturaleza metodológica y carácter investigativo. Esta investigación se enmarca bajo los siguientes supuestos:

3.2.1. Finalidad

La investigación puede ser teórica o aplicada. La investigación teórica se orienta a generar conocimientos abstractos sin pretender de forma inmediata la intervención, mientras que la investigación aplicada se enfoca en la solución de problemas concretos mediante la implementación de conocimientos existentes (Gómez, 2012). Por consiguiente, este trabajo se trata de una investigación aplicada, dado que se busca desarrollar una propuesta de evaluación de vulnerabilidades basada en

buenas prácticas de ciberseguridad, con aplicación directa en la empresa objeto de estudio.

3.2.2. Enfoque sistemático

El enfoque sistemático permite analizar los fenómenos organizacionales y sociales en distintos niveles interrelacionados. Según Narváez Castro et al. (2013) y Rodríguez Monroy & Fernández Chalé (2006), el nivel macro se refiere al contexto general en el que se desarrollan las organizaciones, abarcando factores económicos, políticos y administrativos de alcance nacional o internacional. El nivel meso comprende las políticas, instituciones y servicios de apoyo que facilitan la competitividad y fortalecen la interacción entre empresas y su entorno inmediato. El nivel meta, por su parte, se enfoca en las relaciones estratégicas entre actores sociales relevantes, considerando la cooperación, la visión compartida y la cultura organizacional como elementos claves para el desarrollo. Finalmente, el nivel micro corresponde a las empresas en particular, centrando el análisis en su estructura, procesos internos y estrategias para enfrentar los retos de competitividad y sostenibilidad.

En este proyecto, la investigación se enmarca en el nivel micro, ya que se centra exclusivamente en el estudio del Local 6 Inversiones Hamburgo, ubicado en el cantón central de Golfito. Este enfoque resulta adecuado porque permite realizar un diagnóstico detallado de su infraestructura digital, políticas internas y prácticas de ciberseguridad, con el fin de diseñar una propuesta ajustada a sus necesidades específicas y fortalecer su postura de seguridad digital.

3.2.3. Naturaleza

De acuerdo con Hernández et al. (2014), el enfoque cuantitativo es de carácter secuencial y probatorio, pues sigue un proceso estructurado en el que cada etapa antecede a la siguiente. Inicia con una idea delimitada, de la cual se derivan objetivos e hipótesis; posteriormente se establecen variables y se diseña un plan metodológico para medirlas, analizar los datos mediante métodos estadísticos y

extraer conclusiones. La lógica del proceso es lineal, rigurosa y orientada a la verificación de hipótesis.

En contraste, el enfoque cualitativo es flexible y circular, ya que no sigue necesariamente una secuencia rígida. Las preguntas e hipótesis pueden surgir antes, durante o después de la recolección de los datos, y su propósito principal es comprender los significados, percepciones y experiencias de los actores sociales en torno a un fenómeno. Este enfoque permite un análisis dinámico que va de los hechos a su interpretación y viceversa, otorgando profundidad en el estudio de contextos sociales y organizacionales (Hernández et al., 2014).

En este sentido, la presente investigación se enmarca en el enfoque cualitativo, pues busca comprender el fenómeno desde la perspectiva de los actores involucrados, particularmente en lo concerniente a la percepción, conocimientos y prácticas del personal respecto a la ciberseguridad y la gestión de vulnerabilidades. Esta aproximación resulta pertinente porque facilita captar la complejidad del contexto organizacional y social en el que se insertan los riesgos cibernéticos, permitiendo generar hallazgos que no se limitan a datos estadísticos, sino que profundizan en la experiencia y comprensión de los sujetos.

3.2.4. Carácter

La investigación adopta un carácter descriptivo y comprensivo, dado que se orienta, por un lado, a caracterizar las prácticas actuales en torno a la seguridad de la información, y por otro, a interpretar los factores humanos y organizativos que inciden en la existencia de vulnerabilidades. Esta doble perspectiva permite no solo identificar las condiciones actuales, sino también construir una base sólida para el diseño de estrategias de mejora.

3.3. Administración y abordaje del proyecto objeto

3.3.1. Descripción de supuestos

Este estudio parte del supuesto de que, durante el periodo de investigación, las condiciones actuales del Local 6 Inversiones Hamburgo se mantendrán sin cambios sustanciales en su infraestructura tecnológica, en sus procesos operativos y en la composición del personal involucrado. Se asume que la organización permitirá el acceso a la información necesaria mientras dichas características permanezcan vigentes y que los colaboradores mantendrán su disposición para participar en las encuestas y entrevistas contempladas. Asimismo, se presupone que no ocurrirán modificaciones abruptas como incidentes de ciberseguridad, migraciones tecnológicas, sustitución de personal clave o reestructuraciones internas que alteren el entorno digital evaluado. Bajo este marco de estabilidad temporal, se considera viable el diseño de la propuesta. En caso contrario, cualquier variación significativa en las condiciones de la organización podría exigir una revisión o ajuste de los resultados obtenidos.

3.3.2. Restricciones y riesgos

El presente estudio se desarrolla bajo ciertas restricciones que condicionan su alcance y ejecución. En primer lugar, la propuesta depende del acceso que la organización otorgue a su infraestructura tecnológica, documentación interna y al personal involucrado; cualquier limitación en la disponibilidad de esta información restringirá la profundidad del diagnóstico. Asimismo, el estudio se ve acotado a un periodo temporal específico, por lo que no contempla cambios posteriores que pudieran producirse una vez concluido el levantamiento de datos. Adicionalmente, se reconoce que los resultados estarán circunscritos al contexto particular del Local 6 Inversiones Hamburgo, por lo que no se busca generalización inmediata a otras empresas sin el debido ajuste contextual.

En cuanto a los riesgos, se identifica la posibilidad de que, durante el desarrollo del estudio, la organización experimente modificaciones estructurales, tecnológicas u operativas que alteren las condiciones iniciales, comprometiendo la validez de los insumos recolectados. Existe también el riesgo de sesgos en la información

proporcionada por los participantes por desconocimiento, resistencia al cambio o temor a implicaciones administrativas.

3.4. Sujetos y fuentes de información

Para llevar a cabo esta investigación, se definió un plan metodológico que comprende tanto la selección de fuentes como la construcción de instrumentos adecuados a los objetivos planteados.

3.4.1. Sujetos de información

Los sujetos de información del presente estudio corresponden al personal con rol activo en la gestión y operación del Local 6 Inversiones Hamburgo. La estructura organizacional está conformada por socios propietarios, dos encargados responsables de la logística y la administración, un contador externo y personal operativo compuesto por cajeros, bodegueros y vendedores. Dado que el objeto del estudio se orienta a la evaluación de vulnerabilidades y prácticas relacionadas con la gestión de activos digitales y toma de decisiones operativas, se considera pertinente priorizar como sujetos de información a los encargados administrativos y logísticos, así como al contador cuando su función involucre manejo de plataformas financieras o registros digitales, descartando la participación obligatoria del personal operativo cuyo rol no incide de forma directa en la gestión de ciberseguridad del negocio.

3.4.2. Fuentes de información

Esta investigación contempla fuentes primarias y secundarias. Las fuentes primarias incluyen los datos recolectados directamente mediante encuestas, entrevistas y listas de verificación aplicadas a encargados de la empresa.

Las fuentes secundarias comprenden documentación institucional, marcos normativos en ciberseguridad como ISO/IEC 27001, ISO/IEC 31000, NIST SP 800-50 y OWASP, así como literatura académica y técnica sobre evaluación de vulnerabilidades.

3.5. Diseño de técnicas e instrumentos para recolectar información

A continuación, se presenta las técnicas e instrumentos de recolección de información empleados en el Local 6.

3.5.1. Técnicas e instrumentos de recolección

Se diseñarán tres instrumentos principales:

- Encuesta estructurada, dirigida a los encargados de la empresa para identificar conocimientos, actitudes y prácticas relacionadas con la ciberseguridad. Este instrumento estará compuesto por preguntas cerradas y escala tipo Likert.

- Entrevista semiestructurada, aplicada a responsables de áreas técnicas o de gestión, con el fin de obtener información cualitativa sobre la implementación de controles de seguridad y la cultura organizacional en torno al riesgo cibernético.

- Lista de chequeo, basada en buenas prácticas internacionales (como el CIS Controls), con la finalidad de realizar una evaluación sistemática del entorno informático, las políticas existentes y las medidas de protección implementadas.

Cada instrumento será validado previamente a su aplicación, asegurando la pertinencia, coherencia y claridad de sus ítems, se utilizará la herramienta de Google Forms como medio para la creación y aplicación de los instrumentos. Los datos recolectados serán analizados mediante categorías emergentes y triangulación, garantizando la solidez del análisis y la confiabilidad de los hallazgos.

3.6. Determinación de variables

A continuación, en la Tabla 3 se expone la determinación de las variables de este proyecto.

Tabla 3. Descripción de variables del proyecto.

Objetivo específico	Variable	Conceptual	Operacional	Instrumental
Realizar un diagnóstico de la situación actual de la ciberseguridad en el Local 6 Inversiones Hamburgo, mediante una revisión de su infraestructura digital, prácticas operativas y políticas de seguridad existentes.	Estado de la ciberseguridad	Nivel de protección y control en la infraestructura digital, políticas y prácticas organizacionales frente a amenazas informáticas.	Evaluar la existencia y efectividad de políticas, procedimientos, infraestructura tecnológica y prácticas de seguridad del personal.	Entrevistas semiestructuradas a responsables y lista de chequeo basada en CIS Controls. Esto en Google Forms.
Identificar los riesgos existentes a través de la probabilidad y el impacto que puedan tener las vulnerabilidad	Riesgos cibernéticos	Posibilidad de que se materialicen amenazas que afecten la confidencialidad, integridad o disponibilidad	Clasificar los riesgos según su probabilidad e impacto, priorizando aquellos críticos para	Lista de chequeo de vulnerabilidades y análisis de datos recopilados mediante entrevistas y encuestas.

es informáticas presentes en el negocio, a través de una evaluación exploratoria basada en ISO/IEC 31000.		de los activos de información.	la organización.	Mediante un documento de Word.
Diseñar una herramienta práctica de evaluación de vulnerabilidades, adaptada a las características técnicas y operativas del Local 6 Inversiones Hamburgo, fundamentada en buenas prácticas internacionales de ciberseguridad.	Herramienta de evaluación	Instrumento que permite identificar, registrar y priorizar vulnerabilidades en la infraestructura digital y procesos de seguridad.	Elaborar una guía o instrumento de evaluación basado en las necesidades del Local 6 y buenas prácticas internacionales.	Documento de diseño de la herramienta, apoyado en información recopilada mediante encuestas, entrevistas y listas de chequeo. Mediante Google Forms.

Nota: Las variables están organizadas de acuerdo con la profundidad y alcance de cada uno de los objetivos específicos, presentando su explicación conceptual, su forma de operar y su instrumento.

3.6.1. Cronograma de actividades

La Tabla 4 presenta el cronograma de actividades planificadas para el desarrollo del proyecto, detallando las fases de diagnóstico, recolección de información, análisis de riesgos, diseño de la herramienta de evaluación y elaboración del informe final, distribuidas entre los meses de ejecución.

Tabla 4. Cronograma de actividades del proyecto.

Nombre de la tarea	Duración (días)	Inicio	Final
Trabajo de investigación final	134	20/7/2025	1/12/2025
Definición del título	1	20/7/2025	21/07/2025
Definición de objetivos	1	21/7/2025	22/07/2025
Creación del cronograma	1	22/7/2025	23/07/2025
Creación bitácora de trabajo	3	21/7/2025	24/07/2025
Revisión y entrega del plan de trabajo al tutor	19	25/07/2025	13/08/2025
Desarrollo Capítulo I			
Creación de estructura del TFG	1	01/09/2025	2/09/2025
Planteamiento del tema	1	03/09/2025	4/09/2025
Justificación del trabajo	1	05/09/2025	6/09/2025
Definición de alcances	1	06/09/2025	7/09/2025
Definición de limitaciones	0	07/09/2025	7/09/2025
Definición producto esperado	4	08/09/2025	12/09/2025
Envío Capítulo I al tutor	3	12/9/2025	15/09/2025
Desarrollo del Capítulo II			
Desarrollo de marco teórico	5	10/09/2025	15/09/2025
Envío Capítulo II al tutor	0	15/09/2025	15/09/2025
Desarrollo del Capítulo III			
Tipo de investigación	1	16/09/2025	17/09/2025
Administración y abordaje	1	18/09/2025	19/09/2025
Sujetos y fuentes	1	20/09/2025	21/09/2025
Diseño de técnicas e instrumentos	1	22/09/2025	23/09/2025
Revisión y envío Capítulo III al tutor	1	23/9/2025	24/09/2025
Desarrollo del Capítulo IV			
Introducción a la propuesta	4	25/09/2025	29/9/2025

Desarrollo de la propuesta	52	29/9/2025	20/11/2025
Envío Capítulo IV al tutor	1	21/11/2025	22/11/2025
Desarrollo del Capítulo V	0		
Desarrollo de conclusiones	9	22/11/2025	1/12/2025

Nota: La tabla contiene el cronograma de actividades generales del proyecto. Elaboración propia.

CAPÍTULO IV. ANÁLISIS DE RESULTADOS

4.1. Introducción

Este capítulo tiene como finalidad analizar los resultados obtenidos a partir de la aplicación de los instrumentos diseñados para el estudio, presentados en el capítulo del marco metodológico. Estos instrumentos permitieron analizar la infraestructura digital, las prácticas operativas, las percepciones del personal y el nivel de madurez en seguridad informática, así como identificar los riesgos más relevantes y los insumos para diseñar una herramienta de evaluación de vulnerabilidades ajustada al contexto operativo del negocio.

El análisis de resultado se desarrolla de acuerdo con los tres objetivos específicos de este proyecto. En primera instancia, se aborda un diagnóstico del estado actual de la ciberseguridad del negocio, seguido, se analizan los riesgos identificados según su probabilidad e impacto mediante ISO/IEC 31000, y finalmente, se integran los hallazgos para sustentar el diseño de una herramienta práctica de evaluación de vulnerabilidades basada en buenas prácticas internacionales.

4.2. Análisis del diagnóstico de la situación actual de la ciberseguridad

Con el fin de dar respuesta al primer objetivo específico, se realizó un diagnóstico general del estado de la seguridad en el negocio. Para ello se generó una triangulación de los tres instrumentos. Esta estrategia establece un mejor panorama de la madurez de la ciberseguridad del negocio y evidenciar la percepción interna del estado con una realidad operativa.

Estos instrumentos permitieron evaluar tanto la existencia de controles reales como la efectividad percibida, esto se alinea con la variable estado de la ciberseguridad.

4.2.1. Entrevista

En esta sección se recuperan los resultados de la entrevista (**ver Anexo 1. Entrevista**), en este caso se obtuvo acceso al administrador y contador de la

organización. Primero se presentan las preguntas abordadas para posteriormente analizar las respuestas.

1. ¿Qué sistemas/servicios son críticos para operar (facturación, inventario, banca, correo, nube)? ¿Qué pasaría si fallan 24–48 h?

   Las dos personas entrevistadas coinciden en que los sistemas o servicios críticos para la operación de la empresa es la facturación y la banca. Por ejemplo, un entrevistado indicó "*facturación por dependencia de factor externo (hacienda)*"

2. ¿Quién **decide** sobre compras TI/seguridad? ¿Cómo priorizan?

   Ambos entrevistados indicaron que las decisiones de compra corresponden a gerencia. Uno de los entrevistados indicó que "*no hay tanto énfasis en seguridad más que en el sistema que opere el eje central que es facturar*".

3. ¿Qué **controles** aplican hoy? (Actualizaciones, antivirus/EDR, MFA, respaldos, restricciones de software). ¿Qué funciona y qué no?

   Los entrevistados coindicen que los controles que más aplican es el uso de antivirus y la generación de respaldos. Por ejemplo "*antivirus, respaldos. Todo funciona*"

4. **Incidentes** vividos (phishing, fraude, malware, caídas): ¿qué hicieron? ¿qué aprendieron?

   Los entrevistados no manifiestan haber sufrido consecuencias directas de un incidente más que caídas del sistema. Principalmente el vivido por hacienda en años anteriores que indirectamente les afecto por el tema de la facturación. Por ejemplo "*caídas, Intentos de fraudes, intentos de phishing.*

Se reportaron las caídas al proveedor. Se elevó el intento de fraude al poder judicial".

5. ¿Cómo se gestionan los accesos y cuentas? creación/baja, privilegios,
   Los entrevistados indican que son ellos mismos los que dan acceso a los sistemas, principalmente al de facturación al módulo de cajas. Por lo general generar usuario y contraseña, y el privilegio de acceso. Por ejemplo "*Contraseñas, privilegios*". Lo anterior debido a que el software es obtenido mediante licencia e instalado en un servidor propio.

6. **Respaldos y recuperación:** frecuencia, ubicación, prueba de restauración, tiempos/riesgos.

   Ambos entrevistados manifiestan que realizan un respaldo semanal. Por ejemplo "*respaldo semanal de la información. No hay pruebas de restauración ni se han medido los tiempos*"

7. **Correo y web:** filtros, dominios propios, sitios falsos suplantadores, monitoreo de presencia en línea.
   En cuanto al correo, se cuenta con un dominio propio. Además, en el pasado un sitio web y ahora no lo tienen habilitado. Por ejemplo "*No se han implementado filtros, el dominio es propio. no hay monitoreo en línea*".

8. **Capacitación y cultura:** qué ha recibido el personal, materiales internos, señales rojas que ya reconocen.
   En cuanto a capacitación los entrevistados indicaron que no han recibido ni impartido al personal. Han existido conversaciones esporádicas sobre algunos pequeño posibles acontecimientos que no han pasado a mayor. Por ejemplo "*No se han recibido capacitaciones. El conocimiento ha sido sobre la marcha y algunas recomendaciones externas, no más que eso*".

9. **Terceros/proveedores:** bancos, pasarelas, nube, soporte técnico. ¿Exigen MFA/controles?

   En cuanto a controles de autenticación multifactorial con terceros o proveedores se desconoce un poco de parte de los entrevistados. Sin embargo, un entrevistado determina *"los bancos, luego no hay o se identifica ese tipo de control".*

10. **Planes y métricas:** ¿miden algo (p. ej., tasa de parches, pruebas de restauración)?

    Los entrevistados indican que no llevan métricas ni planes. Por ejemplo "*No, no se mide.*

11. **Barreras** (presupuesto, tiempo, conocimiento) y apoyos que facilitarían avanzar.

    De acuerdo con lo manifestado, se considera que el presupuesto, no obstante, se deja abierta la posibilidad de que el desconocimiento sea también una causa. Por ejemplo *"El presupuesto es considerado en temas de seguridad. Sin embargo, al ser un sistema interno y con acceso limitado al espacio donde se ubica el almacenamiento de información se considera seguro".*

12. **Cierre:** si pudieras implementar **tres** mejoras de bajo costo en 30 días, ¿Cuáles serían?

    Los entrevistados manifiestan que después de tener un poco más de contexto creen oportuno *"capacitación de los colaboradores, generar políticas, mejorar los controles de acceso a los sistemas que utilizamos", "ciberseguridad, fraudes".*

La entrevista reveló que la empresa opera únicamente con dos controles básicos: *uso de antivirus y realización de respaldos semanales*.

4.2.2. Encuesta

A continuación, en la Tabla 5 se muestran las respuestas de las encuestas (**ver Anexo 2. Encuesta)** aplicadas en relación con 7 categorías. Las declaraciones corresponden a una escala tipo Likert: 1 Muy en desacuerdo hasta 5 totalmente de acuerdo.

Tabla 5. Resultados de la encuesta

ITEMS	1	2	3	4	5	MEDIA	SD
Gobernanza y políticas							
Existe una persona responsable (formal/informal) de ti/seguridad.	0	0	0	2	0	4,00	0,000
Tenemos políticas básicas (contraseñas, uso aceptable, respaldo, byod).	0	0	0	2	0	4,00	0,000
Las políticas se comunican y están disponibles al personal.	0	0	0	1	1	4,50	0,707
Revisamos políticas al menos 1 vez al año.	1	1	0	0	0	1,50	0,707
Gestión de activos y configuración segura							
Mantenemos inventario de equipos y cuentas.	0	0	0	1	1	4,50	0,707
Actualizamos so/aplicaciones con parches de seguridad regularmente.	0	0	0	0	2	5,00	0,000
Usamos antivirus/EDR vigente en todos los equipos.	0	0	0	0	2	5,00	0,000
Restringimos la instalación de software no autorizado.	0	0	0	0	2	5,00	0,000
Control de accesos y autenticación							
Se exige contraseñas fuertes y cambio periódico.	0	0	1	0	1	4,00	1,414
Usamos MFA en correo, banca, nube u otros sistemas críticos.	0	0	1	0	1	4,00	1,414
Las cuentas se desactivan al egreso del personal.	0	0	0	0	2	5,00	0,000
Se aplica menor privilegio según función.	0	0	0	1	1	4,50	0,707
Protección de datos y respaldos							
Realizamos copias de seguridad regulares.	0	0	0	0	2	5,00	0,000
Probamos la restauración de respaldos.	1	1	0	0	0	1,50	0,707
Limitamos quién puede ver/exportar datos sensibles.	0	0	0	1	1	4,50	0,707
Usamos almacenamiento en nube con control de acceso.	1	1	0	0	0	1,50	0,707

ITEMS	1	2	3	4	5	MEDIA	SD
Correo, web y concienciación							
Hay filtros anti-phishing/antimalware en correo.	1	1	0	0	0	1,50	0,707
El personal recibió capacitaciones básicas de ciberseguridad en los últimos 12 meses.	1	1	0	0	0	1,50	0,707
Sabemos reportar correos/enlaces sospechosos.	1	0	0	1	0	2,50	2,121
Se evita el uso de usb desconocidos o sitios no confiables.	0	0	0	2	0	4,00	0,000
Detección, respuesta y continuidad							
Se registran incidentes; existe un punto de contacto.	0	1	0	1	0	3,00	1,414
Contamos con pasos básicos para responder a incidentes (aislar equipo, cambiar claves, avisar).	0	0	2	0	0	3,00	0,000
Existe noción de continuidad/recuperación (qué hacer si un sistema cae).	0	0	0	1	1	4,50	0,707
Percepción de riesgo y mejora							
Percibo riesgo de phishing/ransomware en los próximos 12 meses.	0	0	0	0	2	5,00	0,000
La empresa está dispuesta a adoptar controles de bajo costo (MFA, parches, copias).	0	0	0	1	1	4,50	0,707

Nota: La tabla contiene los resultados sistematizados de la encuesta aplicada a los actores de la empresa en estudio. Elaboración propia.

A partir de la encuesta aplicada se puede indicar que no existe un responsable formal de TI, no se aplican parches periódicos normalizados, no hay políticas documentadas formalmente, no se gestionan cuentas de acceso formalizadas ni normadas, no hay controles estrictos de correo electrónico ni prácticas de capacitación, y no hay ningún mecanismo de monitoreo o respuesta a incidentes.

Además, como pregunta abierta en el cuestionario ¿Qué te preocupa más y qué te facilitaría mejorar? Los entrevistados consideran el "*Desconocimiento avances en materia de sistemas y seguridad digital*" y "*Respuesta a incidentes del personal, falta de capacitación*".

No obstante, en los resultados de la encuesta se mostraron resultados que se consideran sobreestimadas del complimiento de controles básicos. Los colaboradores consideraron estar *de acuerdo o totalmente* de acuerdo en preguntas de políticas básicas, contraseñas fuertes, actualizaciones periódicas y restricciones

de software, esto aun cuando en la entrevista no se considera que estos están totalmente implementados. Esta brecha evidencia que la percepción no refleja la operatividad, esto es un hallazgo crítico para el diagnóstico.

4.2.3. Lista de chequeo

A continuación, se muestran las respuestas de obtenidas de la lista de chequeo (**ver Anexo 3. Lista de chequeo)** basada en los CIS Controls, esta lista fue completada por medio de observación y entrevista al encargado de comercio al momento de realizarla.

- Identify (Inventario y contexto)
- Inventario actualizado de equipos (PC, POS, routers/AP, móviles).
- Inventario de cuentas y roles (correo, nube, banca, sistemas).
- Lista de proveedores críticos (banca, nube, soporte TI).
- Dueño responsable para cada sistema.
- Protect (Controles preventivos)
- Parches del SO y Apps dentro de 30 días.
- Antivirus/EDR activo y administrado.
- Políticas de contraseñas robustas y bloqueo por intentos.
- Respaldo regular y prueba de restauración.
- Filtrado de correo (anti-spam/anti-phishing) y bloqueo de adjuntos peligrosos.
- Configuración segura de Wi-Fi (WPA2/3, contraseña fuerte, red de invitados separada).

- Mínimo privilegio y separación de cuentas admin/usuario.
- Política BYOD básica (si usan celulares personales para cuentas de trabajo).
- Señalización y controles físicos mínimos (acceso a caja/PC, cierre de oficina).
- Detect (Monitoreo básico)
- Revisiones mensuales de alertas de antivirus/EDR y de correo.
- Conservación de registros mínimos (eventos de acceso, inicios de sesión).
- Procedimiento para revisar pagos/transferencias inusuales.
- Respond (Respuesta a incidentes)
- Persona contacto de incidentes definida.
- Pasos operativos documentados (aislar equipo, cambiar claves, informar a banco/proveedor, registrar).
- Canal de reporte interno (correo/teléfono) conocido por todos.
- Recover (Continuidad)
- Procedimiento de recuperación (qué restaurar primero, cuentas de emergencia).
- Lecciones aprendidas / mejora tras incidentes o simulacros.

La lista de chequeo basada en los CIS Controls, presentó un buen cumplimiento en todos los dominios identify, protect, detect, respond y recover. Sin embargo, estos resultados discrepan de evidencia obtenida de los instrumentos anteriores, lo que demuestra que el personal interpreta controles mínimos como equivalencias a

prácticas avanzadas de ciberseguridad. Por ejemplo, indicar "*Sí*" en "*Control de contraseñas robustas*" cuando en realidad no hay una política formal ni una rotación periódica.

El estado de la seguridad en la empresa se considera que contiene una madurez baja, controles informales, ausencia de políticas, falta de monitoreo y una marcada brecha entre la percepción del personal y la verdadera postura de seguridad. Este diagnóstico considera la existencia de posibles vulnerabilidades críticas y valida la necesidad de una evaluación formal.

4.3. Identificar riesgos existentes a través de la probabilidad y el impacto

Con base en el diagnóstico del estado actual, se procedió a identificar, analizar y evaluar los riesgos mediante el marco ISO/IEC 31000. Se evalúa cada vulnerabilidad por su probabilidad de ocurrencia y su impacto potencial sobre la continuidad del negocio.

La identificación se fundamenta en la triangulación de los tres instrumentos aplicados: entrevista semiestructurada, encuesta estructurada tipo Likert, y lista de chequeo basada en los CIS Controls. Esto permitió identificar debilidades técnicas, procedimentales y humanas, así como incidentes previos que condiciona e incrementa la probabilidad de materializar amenazas como fraude, phishing y ransomware.

El siguiente apartado expone los riesgos detectados:

4.3.1. Lista de riesgos identificados.

Del análisis del diagnóstico emergen nueve riesgos principales, resultantes de la ausencia de controles, la falta de gobernanza y las brechas entre percepción y práctica operativa.

- R1. Ausencia de autenticación multifactor (MFA): facilita accesos no autorizados en banca, servicios en la nube y correos corporativos.

- R2. Uso de contraseñas débiles y falta de política de gestión de credenciales: no existe rotación, no hay políticas documentadas, y los privilegios no se gestionan formalmente.

- R3. Respaldos incompletos y sin pruebas de restauración: la empresa realiza copias semanales, pero nunca ha probado la recuperación, lo que incrementa riesgo operacional.

- R4. Ausencia total de monitoreo, registros y alertas: no se revisan logs, no se monitorean eventos ni alertas de antivirus/EDR, aumentando la probabilidad de ataques silenciosos.

- R5. Falta de filtros antiphishing y control del correo electrónico: no existe protección avanzada contra phishing ni validación de dominios suplantadores.

- R6. Falta de capacitación en ciberseguridad del personal: la organización nunca ha brindado formación, lo que aumenta riesgos humanos (errores, apertura de enlaces, ingeniería social).

- R7. Brecha crítica entre percepción interna y realidad operativa: el personal cree que existen políticas y controles que en realidad no están implementados; esto inhibe acciones correctivas.

- R8. Inexistencia de políticas formales de seguridad: no hay documentos normativos, lo que dificulta establecer estándares, roles y responsabilidades.

- R9. Dependencia operativa de servicios externos (Hacienda, banca) sin plan de continuidad: las caídas de Hacienda han paralizado medianamente el negocio y no existe plan alterno más que manual.

4.3.2. Criterios de análisis de riesgos

Para clasificar los riesgos se utilizó una escala de 1 a 3, tanto para probabilidad como para impacto, conforme a ISO/IEC 31000.

La Tabla 6 contiene los valores y descriptores de la probabilidad del riesgo.

Tabla 6. Probabilidad del riesgo

Valor	Descripción
3 (Alta)	No existen controles; incidentes previos; exposición constante
2 (Media)	Controles mínimos o informales; predisposición evidente
1 (Baja)	Controles robustos y efectivos (no aplica en este caso)

Nota: La tabla contiene los valores y descriptores de la probabilidad de riesgos utilizados en el estudio. Elaboración propia.

Los instrumentos demostraron que la mayoría de los controles no existen o son informales, por lo que hay un predominio de probabilidad **alta**.

La Tabla 7 muestra los valores y descriptores del impacto de los riesgos.

Tabla 7. Impacto de los riesgos

Valor	Descripción
3 (Alto)	Afecta directamente la continuidad del negocio, facturación, banca
2 (Medio)	Afecta procesos relevantes, pero no detiene totalmente la operación
1 (Bajo)	Impacto acotado y de rápida recuperación

Nota: La tabla contiene los valores y descriptores del impacto de los riesgos utilizados en el estudio. Elaboración propia.

De acuerdo con la criticidad del sistema de facturación y el historial de caídas, varios riesgos tienen impacto **alto**.

La Tabla 8 presenta el nivel del riesgo, esto se determina de acuerdo con ISO/IEC 31000 como Riesgo = Probabilidad × Impacto.

Tabla 8. Nivel del riesgo

Resultado	Nivel
8–9	Crítico
5–7	Alto
3–4	Medio
1–2	Bajo

Nota: La tabla contiene los resultados y niveles de riesgos utilizados en el estudio. Elaboración propia.

4.3.3. Matriz de riesgos

La Tabla 9 contiene los resultados de la aplicación de matriz de riesgos de la empresa en cuestión. Para ello se le otorga un ID a cada uno de los riesgos establecidos en apartados anteriores, se indica el riesgo, se establece la probabilidad, se le agrega el impacto y finalmente se multiplica esa probabilidad por el impacto. Con ello se logra establecer un nivel de clasificación.

Tabla 9. Resultado de la matriz de riesgos.

ID	Riesgo	Prob.	Impacto	Nivel	Clasificación
R1	Sin MFA	3	3	**9**	Crítico

ID	Riesgo	Prob.	Impacto	Nivel	Clasificación
R2	Contraseñas débiles y sin política	3	3	**9**	Crítico
R3	Respaldos sin prueba	3	3	**9**	Crítico
R4	Sin monitoreo ni registros	3	3	**9**	Crítico
R5	Sin filtros antiphishing	3	3	**9**	Crítico
R6	Sin capacitación	3	2	**6**	Alto
R7	Percepción inflada	3	2	**6**	Alto
R8	Sin políticas	2	2	**4**	Medio
R9	Dependencia (Hacienda, bancos)	2	3	**6**	Alto

Nota: La tabla contiene descriptores resultantes de la matriz de riesgos del estudio. Elaboración propia.

El proceso de identificación y análisis de riesgos, basado en ISO/IEC 31000, permitió identificar un conjunto de vulnerabilidades críticas que afectan directamente los activos de información de la empresa. La ausencia de controles esenciales como MFA, políticas de contraseñas, monitoreo y capacitación incrementa la probabilidad de ataques y fallos operativos.

La matriz evidencia que cinco riesgos alcanzan un nivel crítico, principalmente asociados a debilidades en autenticación, respaldo, correo y monitoreo. Otros riesgos de nivel alto se relacionan con la falta de capacitación y la dependencia operativa del sistema de facturación.

La presencia de una brecha significativa entre la percepción del personal y la postura de seguridad real constituye un riesgo transversal que agrava los demás.

Estos resultados demuestran la necesidad urgente de establecer controles mínimos alineados con buenas prácticas internacionales (ISO/IEC 27001, CIS Controls, NIST), así como de desarrollar una herramienta sistemática que permita monitorear y evaluar periódicamente estas vulnerabilidades.

4.4. Diseñar una herramienta práctica de evaluación de vulnerabilidades

La herramienta diseñada constituye un instrumento metodológico que permite evaluar de forma sistemática y estructurada el nivel de ciberseguridad del Local 6 Inversiones Hamburgo. Su diseño se fundamenta en marcos normativos reconocidos internacionalmente, tales como ISO/IEC 27001 (Seguridad de la Información), ISO/IEC 31000 (Gestión de Riesgos), NIST CSF (Cybersecurity Framework), NIST SP 800-50 (Awareness & Training) y CIS Controls.

La herramienta propuesta se apoya en tres pilares: evaluación de controles, análisis de madurez y gestión de riesgos. Cada uno se vincula de forma directa con las normas internacionales.

4.4.1. Evaluación de controles

El primer componente consiste en un checklist estructurado que agrupa 23 controles esenciales repartidos entre los cinco dominios del NIST Cybersecurity Framework: Identify, Protect, Detect, Respond, Recover.

La Tabla 10 muestra la lista de controles seleccionados para la elaboración de la herramienta de evaluación, presenta sus descriptores basados en los marcos normativos.

Tabla 10. Lista de controles basados en los dominios del NIST

ID	Dominio NIST CSF	Control	Descripción operativa	Marco normativo relacionado
C1	Identify	Inventario de activos	Registro actualizado de equipos (PC, POS, routers, móviles).	CIS 1; ISO 27001 A.5.9; NIST ID.AM
C2	Identify	Inventario de cuentas	Registro de cuentas y roles: correo, nube, banca, sistemas.	CIS 2; ISO 27001 A.5.17; NIST ID.AM
C3	Identify	Proveedores críticos	Lista de servicios externos esenciales (banca, nube, soporte TI).	CIS 15; ISO 27001 A.5.22; NIST ID.SC
C4	Identify	Responsables por sistema	Asignación formal de responsables por sistema crítico.	ISO 27001 A.5.9; NIST ID.GV
C5	Protect	Parches del SO y apps	Actualización de sistemas dentro de 30 días.	CIS 7; ISO 27001 A.8.8; NIST PR.IP
C6	Protect	Antivirus/EDR	Protección antimalware activa y gestionada.	CIS 10; ISO 27001 A.8.7; NIST PR.DS
C7	Protect	Políticas de contraseñas	Complejidad, longitud, bloqueo por intentos.	CIS 5; ISO 27001 A.5.16; NIST PR.AC
C8	Protect	Respaldos	Realización periódica de copias de seguridad.	CIS 11; ISO 27001 A.8.13; NIST PR.IP
C9	Protect	Prueba de restauración	Ensayo documentado de recuperación de información.	CIS 11.3; ISO 27001 A.8.14; NIST PR.IP
C10	Protect	Filtrado de correo	Protección antiphishing, anti-spam y bloqueo de adjuntos peligrosos.	CIS 9; ISO 27001 A.8.7; NIST PR.DS

ID	Dominio NIST CSF	Control	Descripción operativa	Marco normativo relacionado
C11	Protect	Wi-Fi seguro	WPA2/3, contraseñas fuertes y red de invitados.	CIS 4/12; ISO 27001 A.7.10; NIST PR.AC
C12	Protect	Privilegio mínimo	Separación de cuentas admin/usuario.	CIS 6; ISO 27001 A.5.15; NIST PR.AC
C13	Protect	Política BYOD	Lineamientos mínimos para uso de celulares personales.	CIS 15; ISO 27001 A.5.23; NIST PR.AC
C14	Protect	Controles físicos mínimos	Cierre de oficina, acceso restringido a PCs y cajas.	CIS 4; ISO 27001 A.7.4; NIST PR.PT
C15	Protect	Restricción de software	Control sobre instalación de software no autorizado.	CIS 10; ISO 27001 A.5.20; NIST PR.IP
C16	Detect	Revisión de alertas	Revisión mensual de antivirus, correo y accesos.	CIS 8; ISO 27001 A.8.15; NIST DE.CM
C17	Detect	Conservación de registros	Registro de accesos, inicios de sesión y actividades relevantes.	CIS 8; ISO 27001 A.5.35; NIST DE.CM
C18	Detect	Pagos inusuales	Procedimiento para identificar transacciones anómalas.	CIS 3/14; ISO 27001 A.5.28; NIST DE.CM
C19	Respond	Responsable de incidentes	Punto de contacto formal para gestionar incidentes.	CIS 17; ISO 27001 A.5.31; NIST RS.CO
C20	Respond	Procedimiento de respuesta	Pasos operativos para actuar ante incidentes.	CIS 17; ISO 27001 A.5.30; NIST RS.RP

ID	Dominio NIST CSF	Control	Descripción operativa	Marco normativo relacionado
C21	Respond	Canal de reporte	Medio oficial para reportar incidentes (teléfono/correo).	CIS 17; ISO 27001 A.6.4; NIST RS.CO
C22	Recover	Plan de recuperación	Priorización de restauración y cuentas de emergencia.	CIS 11; ISO 27001 A.17.1; NIST RC.IM
C23	Recover	Lecciones aprendidas	Documentación y mejora tras incidentes.	CIS 17.5; ISO 27001 A.10.1; NIST RC.IM

Nota: La tabla contiene la lista de controles basados en los dominios del NIST. Elaboración propia.

Este enfoque es consistente con:

- CIS Controls.

  Los CIS constituyen un conjunto priorizado de controles altamente prácticos. Ejemplos aplicados en la herramienta:

  - “Inventario de equipos y cuentas” (CIS Control 1) → C1, C2
  - “Configuración segura de Wi-Fi” → C12
  - “Gestión de privilegios” → C13
  - “Control de software no autorizado” → C9
  - “Antivirus/EDR activo” → C8

  Cada control se califica en escala:

  - 0 = No implementado
  - 1 = Parcial

- 2 = Completamente implementado

- ISO/IEC 27001 — Anexo A

Varios controles del checklist están directamente alineados con el Anexo A de ISO/IEC 27001, por ejemplo:

- A.5 Políticas de seguridad → C6, C14
- A.8 Gestión de activos → C1-C3
- A.9 Control de acceso → C13
- A.12 Protección contra malware → C8
- A.17 Continuidad del negocio → C22

Ejemplo práctico aplicado al Local 6

El control C10 (Respaldos regulares) evalúa si el Local 6 implementa copias semanales. C11 evalúa si realmente se han probado las restauraciones; ISO/IEC 27001 establece que la restauración debe verificarse periódicamente. Este tipo de contraste permite detectar brechas entre la práctica declarada y la implementación real.

4.4.2. Análisis de madurez por dominios

La segunda sección del instrumento ilustra el análisis de madurez bajo el enfoque del NIST Cybersecurity Framework. Cada control asignado a un dominio suma a su nivel de madurez.

La herramienta busca calcular automáticamente el puntaje obtenido, puntaje máximo posible y porcentaje de madurez.

Por ejemplo, si el dominio Protect tiene 7 controles y solo 2 están correctamente implementados: Puntaje obtenido = 4, Puntaje máximo = 14, Nivel de madurez = 28.5%

Este resultado evidencia que, aunque existan antivirus o respaldos, faltan controles fundamentales como: MFA, privilegios mínimos, gestión de parches, políticas formales. Este déficit impacta directamente la exposición a riesgos.

4.4.3. Matriz de riesgos

La tercera sección implementa un modelo de gestión de riesgos conforme a ISO/IEC 31000, que establece: identificación del riesgo, análisis de probabilidad, evaluación de impacto, priorización del riesgo y tratamiento sugerido

El propósito de esta herramienta es proveer un mecanismo práctico, reproducible y adaptado a las características técnicas y operativas del negocio, facilitando la identificación de vulnerabilidades, la priorización de riesgos y la toma de decisiones fundamentadas para fortalecer la postura de seguridad digital.

Para cada riesgo identificado, se asignaron valores base, probabilidad de 1 a 3 e impacto de 1 a 3. La herramienta busca calcular la probabilidad ajustada, impacto ajustado, Nivel (probabilidad por impacto) y establecer una clasificación: crítico de 8 a 9, alto de 5 a 7, medio, de 3 a 4 y bajo de 1 a 2.

Por ejemplo, Riesgo R4: Respaldos sin prueba de restauración:

- Probabilidad = 2
- Impacto = 3
- Nivel = 6
- Nivel = 6 = Alto

Del resultado Alto para ese riesgo podría significar que, si hace respaldos, pero nunca se ha probado si realmente funcional. La restauración fallida durante un

incidente podría provocar pérdida de facturas, datos contables incompletos y retraso en las operaciones. Se podría determinar que la ISO 31000 recomienda priorizar riesgos de nivel alto y crítico.

4.4.4. Funcionamiento de la herramienta

Los valores ingresados provienen de las entrevistas, observación directa, evidencias operativas, resultados de encuesta y lista de chequeo técnica. La herramienta automatiza los análisis una vez ingresados los valores de cumplimiento (0–2).

Una vez ingresados los datos, los controles suman al dominio correspondiente, los promedios se convierten en porcentajes de madurez, los riesgos se clasifican automáticamente y la matriz de riesgos se actualiza en tiempo real.

La herramienta permite generar el estado real de los controles implementados, madurez por dominio (Identify, Protect, Detect, Respond, Recover), mapa de riesgos con clasificación crítica.

4.4.5. Relación entre la herramienta y normas

La Tabla 11 contiene una descripción de la correspondencia asociación entre la herramienta de evaluación con las normas.

Tabla 11. Relación entre la herramienta propuesta y las normas

Componente	Norma asociada	Aplicación en el proyecto
Checklist de controles	CIS v8, ISO/IEC 27001	Lista de controles esenciales adaptados al entorno del Local 6
Madurez por dominios	NIST CSF	Evaluación estructurada Identify-Protect-Detect-Respond-Recover
Matriz de riesgos	ISO 31000	Probabilidad, impacto, nivel, priorización
Cultura y capacitación	NIST SP 800-50	Identificación de brechas formativas y ausencia de programas
Continuidad del negocio	ISO/IEC 27001 A.17	Evaluación de resiliencia ante fallos de sistemas

Nota: La tabla contiene la relación entre los componentes de la herramienta y normas para la aplicación en el estudio. Elaboración propia.

Considerando la evidencia recopilada, se diseña una herramienta de evaluación de vulnerabilidades conformada

4.4.6. Ejemplo de uso

Paso 1

En la Tabla 12 se muestra el resultado de selección el cual el encargado completa el cumplimiento, y se obtienen 0–2 puntos por control.

Tabla 12. Ejemplo de checklist de control de la herramienta de evaluación.

ID	Dominio	Control	Descripción	Cumplimiento (0–2)	Riesgo asociado
C1	Identify	Inventario de activos	Lista actualizada de equipos y cuentas	1	R5
C2	Identify	Inventario de cuentas y roles	Cuentas de correo, facturación, banca	1	R5
C3	Identify	Lista de proveedores críticos	Banca, soporte, sistema de facturación	2	R10
C4	Identify	Responsable por sistema	Persona encargada de banca, facturación, respaldos	0	R8
C5	Protect	MFA en banca/correo	Autenticación multifactor en accesos críticos	1	R1
C6	Protect	Política de contraseñas	Reglas de complejidad y rotación periódica	1	R2
C7	Protect	Actualización de sistemas	Parches de SO y apps < 30 días	0	R5
C8	Protect	Antivirus/EDR activo	Protección activa y actualizada	1	R5
C9	Protect	Restricción de software	Bloqueo de instalación no autorizada	2	R5
C10	Protect	Respaldos regulares	Copias de seguridad semanales	0	R4
C11	Protect	Pruebas de restauración	Ensayo de recuperación de respaldos	0	R4
C12	Protect	Wi-Fi seguro	WPA2/3, contraseña fuerte, red invitados	2	R5
C13	Protect	Privilegios mínimos	Accesos según rol y función	1	R3
C14	Protect	Política BYOD	Uso de dispositivos personales con control	0	R7
C15	Detect	Revisión de alertas	Revisión mensual de antivirus/EDR/correo	2	R5

ID	Dominio	Control	Descripción	Cumplimiento (0–2)	Riesgo asociado
C16	Detect	Registros (logs) mínimos	Registro de accesos e inicios de sesión	1	R5
C17	Detect	Revisión pagos inusuales	Control de transferencias o pagos sospechosos	1	R6
C18	Respond	Responsable de incidentes	Persona contacto para incidentes	1	R6
C19	Respond	Procedimiento de incidentes	Pasos básicos documentados ante incidentes	0	R6
C20	Respond	Canal interno de reporte	Correo/teléfono conocido por el personal	0	R6
C21	Recover	Plan de continuidad	Plan básico ante caída de servicios críticos	1	R10
C22	Recover	Lecciones aprendidas	Registro de incidentes y mejoras	1	R7

Nota: La tabla contiene la lista de checklist de controles de la herramienta propuesta en el estudio. Elaboración propia.

Paso 2

El Excel calcula automáticamente el nivel de madurez por dominio. Por ejemplo, en la Tabla 13 se puede observar que Identify alcanza el 50% y Protect 40%.

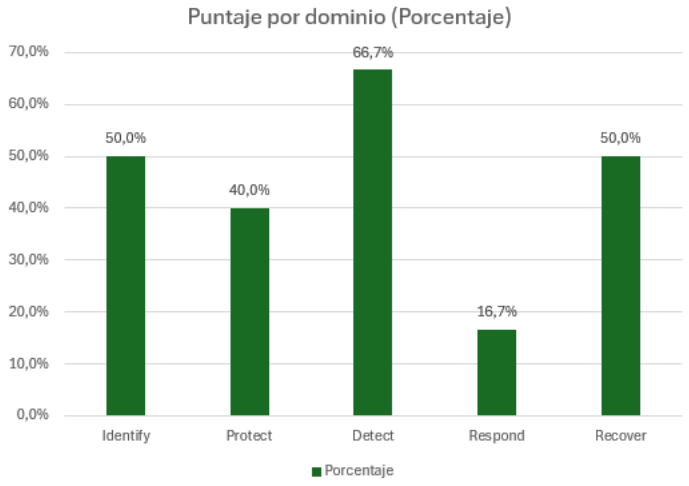
Tabla 13. Ejemplo de nivel de madurez por dominio de la herramienta de evaluación

Dominio	Puntaje obtenido	Puntaje máximo	Porcentaje
Identify	4	8	50,0%
Protect	8	20	40,0%
Detect	4	6	66,7%
Respond	1	6	16,7%
Recover	2	4	50,0%

Nota: La tabla contiene descriptores de madurez por dominio de la herramienta propuesta en el estudio. Elaboración propia.

A continuación, en la se puede observar gráficamente la distribución de madurez de los dominios.

Imagen 2. Ejemplo de madurez de dominio en la herramienta de evaluación.



Nota: La imagen presenta el grado de madurez alcanzado en cada uno de los dominios del NIST. Elaboración propia.

Paso 3

La Tabla 14 ejemplifica lo que se muestra en la tabla de matriz de riesgos. La columna de clasificación indica la categoría expuesta de acuerdo con la probabilidad por el impacto, esto ajustado al cumplimiento de controles del checklist.

Tabla 14. Ejemplo Matriz de riesgo y clasificación de la herramienta de evaluación.

ID	Riesgo	Prob. base	Impacto base	Prob. ajustada	Impacto ajustado	Nivel	Clasificación
R1	Ausencia de MFA en accesos críticos	3	2	3	2	6	Alto
R2	Contraseñas débiles y sin política	3	2	3	2	6	Alto
R3	Gestión deficiente de cuentas de usuario	3	2	3	2	6	Alto
R4	Respaldos sin prueba de restauración	3	3	3	3	9	Crítico
R5	Ausencia de monitoreo y controles técnicos básicos	3	2	3	2	6	Alto

ID	Riesgo	Prob. base	Impacto base	Prob. ajustada	Impacto ajustado	Nivel	Clasificación
R6	Respuesta a incidentes limitada o inexistente	3	3	3	3	9	Crítico
R7	Falta de capacitación del personal en ciberseguridad	3	2	3	2	6	Alto
R8	Brecha entre percepción y realidad de seguridad	3	2	3	2	6	Alto
R9	Ausencia de políticas formales de seguridad	2	1	2	1	2	Bajo
R10	Dependencia de servicios externos sin plan de continuidad	3	1	2	1	2	Bajo

Nota: La tabla los descriptores resultantes de la matriz de riesgos y su clasificación de la herramienta. Elaboración propia.

Paso 5

Analizar el contexto que indica la herramienta, qué riesgo se reduce si se implementa determinado control. Por ejemplo, R4 “Respaldos sin prueba de restauración” se reduce si se implementa el C10 “Respaldos regulares”, “Copias de seguridad semanales” y C11 “Pruebas de restauración”, “Ensayo de recuperación de respaldos”.

Por consiguiente, la integración de los instrumentos aplicados permitió abordar cada variable del proyecto en coherencia con sus dimensiones conceptual, operacional e instrumental. La herramienta diseñada representa un aporte práctico para fortalecer la seguridad del negocio y apoyar decisiones informadas en materia de protección de activos digitales.

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

Luego de aplicar y analizar los instrumentos de recolección de información; entrevista semiestructurada, encuesta estructurada y lista de chequeo técnica, así como de construir la matriz de riesgos y la herramienta de evaluación, se presentan las conclusiones principales del Trabajo Final de Graduación, articuladas con los objetivos específicos planteados.

Respecto al objetivo específico 1 “diagnóstico del estado de la ciberseguridad”, el diagnóstico evidenció que el Local 6 Inversiones Hamburgo presenta un nivel de madurez bajo en ciberseguridad, con controles implementados de forma principalmente informal. La empresa se apoya casi exclusivamente en el uso de antivirus y en la realización de respaldos semanales, sin contar con políticas documentadas, monitoreo sistemático ni métricas de seguridad.

Aunque en la encuesta los participantes manifestaron estar “de acuerdo” o “totalmente de acuerdo” con la existencia de políticas básicas, contraseñas robustas, actualización de sistemas y restricciones de software (promedios cercanos a 4 y 5 en varios ítems), las entrevistas y la observación directa muestran que estos controles no se encuentran formalizados ni gestionados bajo un sistema de gestión de seguridad.

Esta brecha entre percepción declarada y realidad operativa constituye un hallazgo central, la organización cree estar mejor protegida de lo que realmente está, lo que aumenta su exposición a incidentes.

Respecto al objetivo específico 2 “identificación de riesgos según ISO/IEC 31000”, a partir del diagnóstico y siguiendo el enfoque de ISO/IEC 31000, se identificó un conjunto de riesgos críticos y altos que afectan activos clave como el sistema de facturación, la banca en línea y la información contable. La matriz de riesgos muestra que cinco riesgos alcanzan un nivel crítico (por ejemplo, ausencia de autenticación multifactor, contraseñas débiles sin política, respaldos sin prueba de restauración, falta de monitoreo y ausencia de filtros antiphishing), mientras que

otros riesgos se clasifican como altos (falta de capacitación, percepción inflada, dependencia de servicios externos como Hacienda y la banca).

Estos resultados confirman que el negocio está expuesto a amenazas que pueden comprometer la confidencialidad, integridad y disponibilidad de la información, especialmente en procesos críticos como la facturación electrónica y las operaciones financieras, y que la falta de formalización de controles incrementa la probabilidad de materialización de incidentes. De tal forma, se genera un resumen de informe para presentar a la empresa en cuestión (**ver Anexo 4. Informe diagnóstico**).

Respecto al objetivo específico 3 “diseño de la herramienta de evaluación” la herramienta de evaluación (**ver Anexo 5. Herramienta de evaluación**) de vulnerabilidades diseñada basada en un checklist de 23 controles esenciales, un análisis de madurez por dominios del NIST CSF y una matriz de riesgos según ISO/IEC 31000 constituye un instrumento práctico y adaptado al contexto del Local 6. Su estructura permite:

- Evaluar el cumplimiento de controles alineados con CIS Controls e ISO/IEC 27001.
- Medir el nivel de madurez en los dominios Identify, Protect, Detect, Respond y Recover del NIST CSF.
- Priorizar riesgos en función de probabilidad e impacto, facilitando la toma de decisiones.

Esta herramienta responde al vacío detectado en la organización. No existía un mecanismo sistemático para diagnosticar y priorizar vulnerabilidades. Además, el diseño podría ser replicable y adaptable a otras pymes con características similares, lo que amplía la contribución práctica del trabajo.

Además, desde una dimensión organizacional, el estudio mostró que el Local 6 carece de un responsable formal de TI o de seguridad, algo común en Pymes de acuerdo con estudio previos según sus capacidades, no cuenta con un programa

estructurado de capacitación ni con métricas o planes de mejora continua en ciberseguridad.

No obstante, la encuesta refleja una alta percepción de riesgo frente a amenazas como phishing o ransomware y una disposición a adoptar controles de bajo costo (MFA, parches, copias de seguridad), lo que constituye un factor habilitador para futuras iniciativas. Este contraste sugiere que la principal limitación no es la falta de conciencia del riesgo, sino la ausencia de guía metodológica y recursos organizativos para transformar esa conciencia en acciones sistemáticas.

Finalmente, el proyecto demuestra que es posible trasladar marcos internacionales de ciberseguridad (ISO/IEC 27001, ISO/IEC 31000, NIST CSF, NIST SP 800-50 y CIS Controls) a un contexto pyme local, como el del Local 6 en Golfito, mediante instrumentos simples (encuesta, entrevista, lista de chequeo) integrados en una herramienta de evaluación comprensible para actores no especialistas.

En este sentido, este trabajo no solo caracteriza el nivel de madurez y los riesgos del negocio, sino que propone una ruta metodológica para que pymes con recursos limitados puedan iniciar procesos de mejora en su postura de seguridad digital sin depender de soluciones costosas o complejas.

5.2. Recomendaciones

A partir de las conclusiones expuestas y considerando los marcos de referencia utilizados, se formulan las siguientes recomendaciones, que buscan ser concretas, graduales y viables para el contexto del Local 6 Inversiones Hamburgo.

Se recomienda que el Local 6 designe formalmente designar en un plazo no mayor a 6 meses un responsable de TI y/o ciberseguridad, aunque sea a tiempo parcial o como función adicional de una persona existente (por ejemplo, uno de los encargados o el contador cuando su rol lo permita). Esta figura debería coordinar la aplicación de la herramienta propuesta, consolidar evidencias y dar seguimiento a las acciones de mejora.

Asimismo, se sugiere elaborar y aprobar al menos un conjunto mínimo de políticas formales, alineadas con ISO/IEC 27001:

- Política de contraseñas y accesos.
- Política de uso aceptable de equipos, redes e internet.
- Política básica de respaldos y retención de información.

Estas políticas deben documentarse, comunicarse al personal, revisarse al menos una vez al año y vincularse a los hallazgos de la herramienta de evaluación.

También, en coherencia con ISO/IEC 31000, se recomienda priorizar en un plazo de 3 meses el tratamiento de los riesgos clasificados como críticos y altos en la matriz: ausencia de MFA, contraseñas débiles sin política, respaldos sin prueba de restauración, falta de filtros antiphishing, falta de monitoreo y ausencia de capacitación, así como la alta dependencia de sistemas externos como Hacienda y la banca.

Acciones sugeridas de bajo costo:

- Habilitar MFA en correo y banca en línea donde esté disponible.
- Implementar políticas de cambio periódico de contraseñas, con longitud y complejidad mínimas.
- Programar pruebas trimestrales de restauración de respaldos, documentando resultados.
- Configurar filtro antispam/antiphishing básico (por ejemplo, a través del proveedor de correo) y revisar alertas al menos una vez al mes.
- Definir un registro sencillo de incidentes (archivo o bitácora) donde se documenten eventos, acciones y lecciones aprendidas.

Tomando como referencia el NIST SP 800-50, se recomienda que en un plazo de 6 meses la empresa establezca un programa básico de concienciación y capacitación, adaptado a su tamaño y recursos, que incluya:

- Una sesión introductoria anual sobre riesgos más frecuentes (phishing, ransomware, uso de USB, manejo de contraseñas).
- Microcapacitaciones breves (15–20 minutos) cuando se detecten incidentes o nuevas campañas de fraude.
- Materiales simples (afiches, recordatorios por WhatsApp o correo) con “buenas prácticas” concretas.

Asimismo, se recomienda institucionalizar el uso de la herramienta de evaluación de vulnerabilidades como parte de la gestión rutinaria del negocio y estarla aplicando al menos 1 vez cada 6 meses. En particular:

- Aplicar el checklist y el análisis de madurez al menos una vez al año, o tras cambios relevantes en sistemas o procesos.
- Actualizar la matriz de riesgos después de cada evaluación, registrando evoluciones (riesgos que bajan de nivel, nuevos riesgos identificados).
- Utilizar los resultados del instrumento como insumo para la toma de decisiones de inversión en tecnología (por ejemplo, priorizar la compra de soluciones que mitiguen los riesgos críticos).

De esta forma, la herramienta deja de ser solo un producto del TFG y se convierte en un mecanismo permanente de seguimiento, alineado con la lógica de mejora continua de ISO/IEC 27001.

Finalmente, desde una perspectiva académica, se recomienda explorar en un plazo de 1 año la aplicación de la herramienta en otras pymes del cantón de Golfito o de la región, con el fin de validar y ajustar el instrumento en contextos similares, generar datos comparativos sobre el nivel de madurez en ciberseguridad de pymes

regionales y alimentar futuras líneas de investigación relacionadas con transformación digital y gestión de riesgos en pequeñas y medianas empresas.

BIBLIOGRAFÍA

Aksoy, C. (2024). BUILDING A CYBER SECURITY CULTURE FOR RESILIENT ORGANIZATIONS AGAINST CYBER ATTACKS. *İşletme Ekonomi ve Yönetim Araştırmaları Dergisi*, *7*(1), 96-110. https://doi.org/10.33416/baybem.1374001

Amoroso, E. (2006). *Cyber Security* (1.ª ed.). Silicon Press.

Babilonia, G. (2023). BENEFICIOS DE LAS NORMAS ISO 27000. *HIGH TECH-ENGINEERING JOURNAL*, *3*(2). https://doi.org/10.46363/high-tech.v3i2.4

Basha, S., Taherdoost, H., & Zanchettin, C. (2024). Exploring Cybersecurity Training and Awareness Approaches. En *Exploring Cybersecurity Training and Awareness Approaches* (1.ª ed., pp. 1-12). Springer. https://doi.org/10.1007/978-981-97-5791-6_1

Botunac, I., Parlov, N., & Bosna, J. (2024). Opportunities of Gen AI in the Banking Industry with regards to the AI Act, GDPR, Data Act and DORA. *2024 13th Mediterranean Conference on Embedded Computing, MECO 2024*. https://doi.org/10.1109/MECO62516.2024.10577936

Bustillos Ortega, O., & Rojas Segura, J. (2022). Protocolo básico de ciberseguridad para pymes. *Interfases*, *016*, 168-186. https://doi.org/10.26439/interfases2022.n016.6021

Bustillos Ortega, O., & Rojas Segura, J. (2023). Cómo promueven los Estados la ciberseguridad de las pymes. *Interfases*, *017*, 21-37. https://doi.org/10.26439/interfases2023.n017.6246

Cains, M. G., Flora, L., Taber, D., King, Z., & Henshel, D. S. (2022). Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Context using Expert Elicitation. *Risk Analysis*, *42*(8), 1643-1669. https://doi.org/10.1111/risa.13687

Calle Herencia, C. A. (2022). transformación digital y su importancia en las pymes. *Iberoamerican Business Journal*, *5*(2), 64-81. https://doi.org/10.22451/5817.ibj2022.vol5.2.11059

Calvo, K., & Sánchez, R. (2015). *Propuesta de incorporación de un estándar de cifrado a las bases de datos de la UTN según lo establecido en la legislación vigente*. Universidad Técnica Nacional.

Cardozo, E., Velásquez de Naime, Y., & Monroy, C. R. (2012). Revisión de la definición de PYME en América Latina. *10th Latin American and Caribbean Conference for Engineering and Technology*, 1-10. https://oa.upm.es/19446/

Centro de Informática, U. (2025, mayo 24). *Recursos de ciberseguridad*. Centro de Informática.

Chacón Luna, A. (2025). *Principales vulnerabilidades y acciones de mitigación recomendadas en la administración del active directory de Microsoft.* [Universidad Estatal Península de Santa Elena]. https://repositorio.upse.edu.ec/handle/46000/12531

Choez-Calderón, C. J., & Aldo-Patricio, M. O. (2025). La ciberseguridad como prioridad empresarial dentro de marcos los regulatorios y normativos internacionales. *Revista Científica Ciencia y Método*, *03*(3). https://doi.org/10.55813/gaea/rcym/v3/n

CISA. (2021, febrero 1). *What is Cybersecurity?* America´s Cyber Defense Agency.

CyBOK. (2021). *The Cyber Security Body of Knowledge*. https://www.nationalarchives.gov.uk/

De la Rosa, J. (2019). *CIBERSEGURIDAD PARA PYMES*. https://uvadoc.uva.es/handle/10324/38735

De la Rosa Martín, T. (2021). AUTOMATIZACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC

27001. *Revista Científica de la Universidad de Cienfuegos*, *13*(5). https://rus.ucf.edu.cu/index.php/rus/article/view/2260

Dupuis, M., & Renaud, K. (2024). Risk Assessment & Mitigation for Core Security Capabilities. *eCrime Researchers Summit, eCrime*, 43-57. https://doi.org/10.1109/eCrime66200.2024.00010

FIRTS. (2023). *Common Vulnerability Scoring System version 4.0 Specification*. https://www.first.org/cvss/

Gómez, S. (2012). *Metodología de la investigación* (1.ª ed.). Red Tercer Milenio.

González-Díaz, R., & Becerra-Pérez, L. (2021). PYMES en América Latina: clasificación, productividad laboral, retos y perspectivas. *CiiD Journal*, *01*. https://orcid.org/0000-0002-7529-8847

Harkai, A. (2024). Main Characteristics and Cybersecurity Vulnerabilities of IoT Mobile Devices. En *Smart Innovation, Systems and Technologies* (Vol. 367, pp. 219-230). Springer. https://doi.org/10.1007/978-981-99-6529-8_19

Hernández, R., Fernández, C., & Baptista, P. (2014). *Metododología de la Investigación* (6.ª ed.). McGRAW-HILL.

Inoguchi Rojas, A., & Macha Moreno, E. L. (2017). *Gestión de la ciberseguridad y prevención de los ataques cibernéticos en las PYMES del Perú, 2016*. https://doi.org/https://hdl.handle.net/20.500.14005/2810

ISO. (2018a). *Information technology – Security techniques – Information security management systems – Overview and vocabulary (ISO/IEC Standard No. 27000:2018*.

ISO. (2018b). *ISO 31000 Risk management ISO 31000*. https://www.iso.org/standard/65694.html

ISO. (2022). *ISO/IEC 27001 Information security, cybersecurity and privacy protection — Information security management systems — Requirements*.

ITU. (2009). *Overview of Cybersecurity.*

Junior, C. R., Becker, I., & Johnson, S. (2023). *Unaware, Unfunded and Uneducated: A Systematic Review of SME Cybersecurity*. http://arxiv.org/abs/2309.17186

Kaur, G., Lashkari, Z., & Lashkari, A. (2021). *Understanding Cybersecurity Management in FinTech Challenges, Strategies, and Trends*. Springer. http://www.springer.com/series/16360

Kemmerer, R. A. (2003). Cybersecurity. *25th International Conference on Software Engineering, 2003. Proceedings.*, 705-715. https://doi.org/10.1109/ICSE.2003.1201257

Kraus, S., Durst, S., Ferreira, J. J., Veiga, P., Kailer, N., & Weinmann, A. (2022). Digital transformation in business and management research: An overview of the current status quo. *International Journal of Information Management*, *63*. https://doi.org/10.1016/j.ijinfomgt.2021.102466

Laghnimi, J., Moumane, K., Ahmed, Z., Lamkimel, M., Kacimi, Z., & Wahi, Y. (2024). ISO/IEC 27001 Certification in Moroccan Companies: Trends and Future Recommendations. *Proceedings - 2024 World Conference on Complex Systems, WCCS 2024*. https://doi.org/10.1109/WCCS62745.2024.10765551

May-Grosser, S. (2025, mayo 26). *El Depósito Libre Comercial de Golfito no cuenta con sistema de compras en línea*. Delfino.

Merritt, M., Hansche, S., Ellis, B., Sanchez-Cherry, K., Snyder, J. N., & Walden, D. (2024). *Building a cybersecurity and privacy learning program*. https://doi.org/10.6028/NIST.SP.800-50r1

MICITT. (2023). *Estrategia Nacional de Ciberseguridad, Costa Rica 2023-2027*.

MITRE. (2025). *CVE - Common Vulnerabilities and Exposures.* MITRE Corporation. https://www.cve.org

Municipalidad de Golfito. (2020, mayo 27). *Suplantación de correos electrónicos*.

Narváez Castro, M., Fernández De Hurtado, G., & Henríquez Barraez, A. (2013). COMPETITIVIDAD DE EMPRESAS TURÍSTICAS: UN ANÁLISIS DESDE EL ENFOQUE SISTÉMICO *. *Revista Facultad de Ciencias Económicas: Investigación y Reflexión*, *XXI*(1), 243-260. http://www.scielo.org.co/scielo.php?pid=S0121-68052013000100014&script=sci_arttext

National Institute of Standards and Technology. (2022). *Framework for Improving Critical Infrastructure Cybersecurity*.

Orlandi, P. (2006). Las Pymes y su rol en el Comercio Internacional. En *White Paper Series del Centro de Estudios para el Desarrollo Exportador–CEDEX*. https://www.palermo.edu/economicas/pdf_economicas/cbrs/cbrs_viejos/las_pyme_y_su_rol_en_el_comercio_internacional.pdf

OWASP. (2025). *OWASP Top Ten*. The OWASP® Foundation.

Paula Yugsi, A. E., Toapanta Tulcan, E. A., & Flores Lagla, G. A. (2024). Tecnologías emergentes para las PYMES en los cantones Sigchos y Latacunga. *Visionario Digital*, *8*(3), 118-137. https://doi.org/10.33262/visionariodigital.v8i3.3133

Pozo-Benites, K. B., Guadalupe-Sánchez, K. W., Peñarreta-Barrera, E. E., & Meza-Salvatierra, J. K. (2025). Transformación digital de las PYMES en América Latina: barreras, oportunidades y estrategias para la competitividad. *Multidisciplinary Latin American Journal (MLAJ)*, *3*(2), 236-255. https://doi.org/10.62131/mlaj-v3-n2-015

Rodríguez Monroy, C., & Fernández Chalé, L. (2006). Revista venezolana de gerencia. *Revista Venezolana de Gerencia*, *11*(35), 335-351.

http://ve.scielo.org/scielo.php?script=sci_arttext&pid=S1315-99842006000300002&lng=es&nrm=iso&tlng=es

Roșca, S.-T. (2024). *CYBERSECURITY WITHIN CRITICAL INFRASTRUCTURES*.

Sánchez-Sánchez, P. A., García-González, J. R., Triana, A., & Perez-Coronell, L. (2021). Medida del nivel de seguridad informática de las pequeñas y medianas empresas (PYMEs) en Colombia. *Información tecnológica*, *32*(5), 121-128. https://doi.org/10.4067/s0718-07642021000500121

Stalling, W. (2017). *Cryptography and network security principles and practice* (Seven).

UK National Cyber Security Strategy. (2016). *National Cyber Security Strategy 2016-2021*.

Valero Bueno, G. G., & Haz López, L. V. (2022). Ciberseguridad post covid-19 y su impacto en las pymes del Ecuador. *Pro Sciences: Revista de Producción, Ciencias e Investigación*, *6*(46). https://doi.org/10.29018/issn.2588-1000vol6iss46

Wang, Z., Zhu, H., & Sun, L. (2021). Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods. *IEEE Access*, *9*, 11895-11910. https://doi.org/10.1109/ACCESS.2021.3051633

Yonatan, A. Z., Susanto, S., Sukapto, P., Zagloel, T. Y. M., & Timotius, E. (2025). NAVIGATING RISKS WITH ISO 31000 FOR A SUSTAINABLE FUTURE: A STRATEGIC APPROACH IN THE INDONESIA TEXTILE INDUSTRY. *Management Systems in Production Engineering*, *33*(2), 82-92. https://doi.org/10.2478/mspe-2025-0009

ANEXOS

Anexo 1. Entrevista

Guía de entrevista semiestructurada para los responsables del Local 6 Inversiones Hamburgo

Este instrumento cualitativo tiene como finalidad obtener información más profunda sobre la forma en que el Local 6 gestiona la seguridad digital de sus operaciones, sistemas y procesos administrativos.

A través de entrevistas semiestructuradas con los socios, encargados de logística, administración y contabilidad, se pretende identificar las estrategias actuales de protección de la información, experiencias con incidentes cibernéticos (por ejemplo, correos fraudulentos o ataques a puntos de venta), y percepciones sobre las limitaciones técnicas o presupuestarias que enfrenta la empresa.

La información cualitativa recolectada complementará los resultados de la encuesta y permitirá generar una visión integral del estado de la ciberseguridad en el Local 6.

¿Qué **sistemas/servicios** son críticos para operar (facturación, inventario, banca, correo, nube)? ¿Qué pasaría si fallan 24–48 h?

¿Quién **decide** sobre compras TI/seguridad? ¿Cómo priorizan?

¿Qué **controles** aplican hoy? (Actualizaciones, antivirus/EDR, MFA, respaldos, restricciones de software). ¿Qué funciona y qué no?

Incidentes vividos (phishing, fraude, malware, caídas): ¿qué hicieron, ¿qué aprendieron?

Accesos y cuentas: creación/baja, privilegios, contraseñas, proveedores externos.

Respaldos y recuperación: frecuencia, ubicación, prueba de restauración, tiempos/riesgos.

Correo y web: filtros, dominios propios, sitios falsos suplantadores, monitoreo de presencia en línea.

Capacitación y cultura: qué ha recibido el personal, materiales internos, señales rojas que ya reconocen.

Terceros/proveedores: bancos, pasarelas, nube, soporte técnico. ¿Exigen MFA/controles?

Planes y métricas: ¿miden algo (p. ej., tasa de parches, pruebas de restauración)? Próximas mejoras de “impacto rápido”.

Barreras (presupuesto, tiempo, conocimiento) y apoyos que facilitarían avanzar.

Cierre: si pudieras implementar **tres** mejoras de bajo costo en 30 días, ¿Cuáles serían?

Anexo 2. Encuesta

Encuesta estructurada sobre conocimientos y prácticas de ciberseguridad en el Local 6 Inversiones Hamburgo

Este instrumento tiene como propósito recopilar información cuantitativa sobre el nivel de conocimiento, percepción del riesgo y aplicación de medidas básicas de ciberseguridad por parte del personal administrativo y técnico del Local 6 Inversiones Hamburgo.

A través de una serie de preguntas cerradas tipo Likert, la encuesta permitirá identificar brechas formativas, debilidades operativas y el grado de cumplimiento de buenas prácticas relacionadas con contraseñas seguras, respaldo de información, actualizaciones de software, autenticación multifactor, y manejo de incidentes.
Los resultados servirán para medir el nivel de madurez en ciberseguridad de la organización y orientar futuras acciones de fortalecimiento interno.

Sección A. Perfil organizacional

Descripción (opcional)

Rol en la empresa

Socio / Encargado / Contador

Antigüedad en el rol

Menos de 1 año / 1 a 3 años / 4 a 6 años / más de 6 años

Tamaño del personal

1 a 5 / 6 a 10 / 11 a 25 / Más de 25

Sistemas clave que usa su área

Cajas – Facturación / Inventario / Bancos / Correo / Mensajería / Nube. Otro___

Sección B. Gobernanza y políticas

Descripción (opcional)

Existe una persona responsable (formal/informal) de TI/seguridad.

Desacuerdo 1 2 3 4 5 Totalmente de acuerdo

Tenemos **políticas** básicas (contraseñas, uso aceptable, respaldo, BYOD).

Desacuerdo 1 2 3 4 5 Totalmente de acuerdo

Las políticas se **comunican** y están disponibles al personal.

Desacuerdo 1 2 3 4 5 Totalmente de acuerdo

Revisamos políticas al menos **1 vez al año**.

Desacuerdo 1 2 3 4 5 Totalmente de acuerdo

Sección C. Gestión de activos y configuración segura

Descripción (opcional)

Mantenemos **inventario** de equipos y cuentas.

Desacuerdo 1 2 3 4 5 Totalmente de acuerdo

Actualizamos **SO/aplicaciones** con parches de seguridad regularmente.

Desacuerdo 1 2 3 4 5 Totalmente de acuerdo

Usamos antivirus/EDR **vigente** en todos los equipos.

Desacuerdo 1 2 3 4 5 Totalmente de acuerdo

Restringimos la instalación de software no autorizado.

Desacuerdo 1 2 3 4 5 Totalmente de acuerdo

Sección D. Control de accesos y autenticación

Descripción (opcional)

Se exige **contraseñas fuertes** y cambio periódico.

Desacuerdo 1 2 3 4 5 Totalmente de acuerdo

Usamos **MFA** en correo, banca, nube u otros sistemas críticos.

Desacuerdo 1 2 3 4 5 Totalmente de acuerdo

Las cuentas se **desactivan** al egreso del personal.

Desacuerdo 1 2 3 4 5 Totalmente de acuerdo

Se aplica **menor privilegio** según función.

Desacuerdo 1 2 3 4 5 Totalmente de acuerdo

Sección E. Protección de datos y respaldos

Descripción (opcional)

Realizamos **copias de seguridad** regulares.

Desacuerdo 1 2 3 4 5 Totalmente de acuerdo

Probamos la **restauración** de respaldos.

Desacuerdo 1 2 3 4 5 Totalmente de acuerdo

Limitamos quién puede **ver/exportar** datos sensibles.

Desacuerdo 1 2 3 4 5 Totalmente de acuerdo

Usamos almacenamiento en nube **con control de acceso**.

Desacuerdo 1 2 3 4 5 Totalmente de acuerdo

Sección F. Correo, web y concienciación

Descripción (opcional)

Hay **filtros** anti-phishing/antimalware en correo.

Desacuerdo 1 2 3 4 5 Totalmente de acuerdo

El personal recibió **capacitaciones** básicas de ciberseguridad en los últimos 12 meses.

Desacuerdo 1 2 3 4 5 Totalmente de acuerdo

Sabemos **reportar** correos/enlaces sospechosos.

Desacuerdo 1 2 3 4 5 Totalmente de acuerdo

Se evita el uso de **USB** desconocidos o sitios no confiables.

Desacuerdo 1 2 3 4 5 Totalmente de acuerdo

Sección G. Detección, respuesta y continuidad

Descripción (opcional)

Se **registran** incidentes; existe un **punto de contacto**.

Desacuerdo 1 2 3 4 5 Totalmente de acuerdo

Contamos con pasos básicos para **responder** a incidentes (aislar equipo, cambiar claves, avisar).

Desacuerdo 1 2 3 4 5 Totalmente de acuerdo

Existe noción de **continuidad/recuperación** (qué hacer si un sistema cae).

Desacuerdo 1 2 3 4 5 Totalmente de acuerdo

Sección H. Percepción de riesgo y mejora

Descripción (opcional)

Percibo **riesgo** de phishing/ransomware en los próximos 12 meses.

Desacuerdo 1 2 3 4 5 Totalmente de acuerdo

La empresa está **dispuesta** a adoptar controles de bajo costo (MFA, parches, copias).

Desacuerdo 1 2 3 4 5 Totalmente de acuerdo

Principal **barrera**:. (opción múltiple)

Desconocimiento / Presupuesto / Tiempo / Falta de responsable / Otra

¿Qué te preocupa más y qué te facilitaría mejorar?

Anexo 3. Lista de Chequeo

Lista de chequeo técnica para la evaluación de vulnerabilidades en el Local 6 Inversiones Hamburgo

Este instrumento tiene como propósito evaluar el cumplimiento de controles básicos de ciberseguridad en las infraestructuras tecnológicas, redes y sistemas utilizados en el Local 6 Inversiones Hamburgo.

Se centra en verificar la existencia de medidas de protección tales como inventario de activos tecnológicos, configuraciones seguras de routers y equipos, mecanismos de respaldo de información, autenticación multifactor, y políticas de contraseñas.

La lista de chequeo se aplicará durante la visita técnica al local, permitiendo identificar vulnerabilidades críticas y registrar evidencia observable, lo que servirá para elaborar el informe diagnóstico final y las recomendaciones de mitigación personalizadas para la empresa.

Identify (Inventario y contexto)

- Inventario actualizado de equipos (PC, POS, routers/AP, móviles).
- Inventario de cuentas y roles (correo, nube, banca, sistemas).
- Identificación de datos sensibles (clientes, finanzas, catálogos, claves).
- Lista de proveedores críticos (banca, nube, soporte TI). Dueño responsable para cada sistema

Protect (Controles preventivos)

- Parches del SO y Apps dentro de 30 días. Antivirus/EDR activo y administrado.
- MFA habilitado en correo, banca, nube y paneles críticos.
- Políticas de contraseñas robustas y bloqueo por intentos.
- Respaldo regular y prueba de restauración. Filtrado de correo (anti-spam/anti-phishing) y bloqueo de adjuntos peligrosos.
- Navegación segura (bloqueo de sitios maliciosos, lista blanca si es posible).
- Configuración segura de Wi-Fi (WPA2/3, contraseña fuerte, red de invitados separada). Mínimo privilegio y separación de cuentas admin/usuario.
- Cifrado de discos portátiles (si hay laptops).
- Política BYOD básica (si usan celulares personales para cuentas de trabajo).
- Señalización y controles físicos mínimos (acceso a caja/PC, cierre de oficina).

Detect (Monitoreo básico)

- Revisiones mensuales de alertas de antivirus/EDR y de correo.
- Conservación de registros mínimos (eventos de acceso, inicios de sesión).
- Procedimiento para revisar pagos/transferencias inusuales.

Respond (Respuesta a incidentes)

- Persona contacto de incidentes definida.
- Pasos operativos documentados (aislar equipo, cambiar claves, informar a banco/proveedor, registrar).
- Canal de reporte interno (correo/teléfono) conocido por todos.

Recover (Continuidad)

- Procedimiento de recuperación (qué restaurar primero, cuentas de emergencia).
- Prueba de restauración realizada los últimos 6–12 meses.
- Lecciones aprendidas / mejora tras incidentes o simulacros.

Anexo 4. Informe diagnóstico

MAESTRÍA EN CIBERSEGURIDAD

Informe diagnóstico y recomendaciones

AUTOR

Mainor Cruz Alvarado

Pérez Zeledón, Costa Rica

diciembre, 2025

1.Introducción y contexto

El presente documento expone los resultados del diagnóstico de ciberseguridad realizado en el Local 6 Inversiones Hamburgo, ubicado en el cantón central de Golfito. El propósito general del diagnóstico fue evaluar el estado actual de la seguridad digital del negocio, identificar las principales vulnerabilidades y riesgos asociados a sus sistemas críticos, y proponer acciones estratégicas para fortalecer su postura de seguridad, tomando como referencia buenas prácticas internacionales en ciberseguridad.

El análisis se centra en los sistemas y servicios que dan soporte a la operación del local, particularmente en los procesos de facturación, inventario, banca en línea y comunicación por correo electrónico, sin incluir pruebas de intrusión ni análisis de código fuente.

2.Metodología de evaluación

Para el desarrollo del diagnóstico se aplicó una estrategia de triangulación de instrumentos, con el fin de obtener una visión integral del estado de la ciberseguridad en el Local 6. Los instrumentos utilizados fueron:

a) Entrevista semiestructurada a personas clave (administrador y contador), con el objetivo de comprender la percepción de la ciberseguridad, los sistemas críticos, los controles actualmente aplicados y la experiencia previa frente a incidentes.

b) Encuesta estructurada con escala tipo Likert (1 a 5), dirigida a personal clave, para valorar la existencia y efectividad percibida de controles básicos de ciberseguridad, tales como políticas, gestión de accesos, respaldos, capacitación y percepción de riesgo.

c) Lista de chequeo técnica basada en buenas prácticas y marcos de referencia como NIST Cybersecurity Framework (Identify, Protect, Detect, Respond, Recover)

y CIS Controls, aplicada mediante observación y validación con el encargado, con el fin de constatar la implementación real de controles técnicos y organizativos.

Con la información obtenida se elaboró una matriz de riesgos siguiendo los lineamientos de ISO/IEC 31000, considerando probabilidad e impacto sobre los activos y procesos críticos del negocio. Posteriormente, se diseñó una herramienta práctica de evaluación de vulnerabilidades que consolida los hallazgos en forma estructurada.

3.Resultados del diagnóstico de ciberseguridad

3.1 Gobernanza y políticas

El diagnóstico evidenció que el Local 6 no cuenta con un responsable formal de tecnologías de información o de ciberseguridad. Las decisiones relacionadas con compras tecnológicas y aspectos de seguridad se toman directamente desde la gerencia, con apoyo operativo de los encargados, sin una estructura formal de roles ni de responsabilidades en materia de seguridad digital.

Asimismo, no se identificaron políticas documentadas de contraseñas, uso aceptable de equipos y recursos tecnológicos, BYOD (Bring Your Own Device), gestión de respaldos o control de accesos. Si bien el personal entrevistado manifestó la existencia de “prácticas” o “acuerdos” internos, estas se encuentran en un nivel informal y no siguen un ciclo de aprobación, difusión, revisión y actualización periódica.

Este escenario refleja una gobernanza de la ciberseguridad incipiente, en la cual no hay un marco normativo interno que oriente de manera sistemática la gestión de riesgos ni la implementación de controles.

3.2 Infraestructura y controles técnicos (función Protect)

En el ámbito técnico se identificaron algunos controles básicos que constituyen fortalezas iniciales. Entre ellos destacan el uso de soluciones antivirus en los equipos principales y la realización de respaldos semanales de información

relevante. Estas prácticas proporcionan un nivel mínimo de protección frente a amenazas conocidas y ante eventuales pérdidas de datos.

No obstante, se observaron múltiples debilidades relevantes:

a) No se aplica un esquema formal de gestión de parches y actualizaciones. La instalación de actualizaciones del sistema operativo y aplicaciones se realiza de forma reactiva y no bajo un calendario definido o un procedimiento normalizado.

b) No se utiliza autenticación multifactor (MFA) en servicios críticos, como la banca en línea, el correo electrónico corporativo o las posibles plataformas en la nube.

c) Los respaldos, aunque se ejecutan, no se someten a pruebas periódicas de restauración, por lo que se desconoce con certeza la capacidad real de recuperación y los tiempos de restablecimiento.

d) No existe una política formal de contraseñas robustas que establezca requisitos mínimos de longitud, complejidad y periodicidad de cambio, ni mecanismos claros de bloqueo por intentos fallidos.

e) No se encuentran reguladas de manera formal la instalación de software ni el uso de dispositivos personales para fines laborales (BYOD), lo que aumenta la superficie de exposición a software no autorizado o potencialmente malicioso.

En conjunto, estas debilidades evidencian que el negocio descansa en controles técnicos básicos, insuficientes frente al panorama actual de amenazas para pequeñas y medianas empresas.

3.3 Monitoreo y detección (función Detect)

En relación con la función de detección, se observó que el Local 6 no cuenta con un esquema formal de monitoreo de seguridad. No se revisan de forma sistemática los registros (logs) de accesos, inicios de sesión, eventos de sistemas o alertas generadas por soluciones antivirus o por el correo electrónico.

Tampoco existe un procedimiento documentado para la identificación y revisión de pagos o transferencias inusuales, a pesar de que el negocio mantiene operaciones financieras recurrentes. Las verificaciones, cuando se realizan, dependen de la experiencia y criterio del personal, y no de un protocolo establecido.

Esta ausencia de monitoreo estructurado dificulta la detección temprana de actividades sospechosas o incidentes en desarrollo, y limita la capacidad de reconstruir lo sucedido en caso de un evento de seguridad.

3.4 Respuesta a incidentes (función Respond)

El diagnóstico reveló que el Local 6 no dispone de un procedimiento formal de respuesta a incidentes de ciberseguridad. No se identificaron documentos que describan pasos a seguir ante un incidente, tales como aislar equipos, cambiar contraseñas, notificar a bancos o proveedores, ni mecanismos formalizados para registrar y analizar lo sucedido.

Si bien los entrevistados reconocen haber enfrentado caídas de sistemas e intentos de fraude o phishing, la respuesta a estos eventos ha sido eminentemente reactiva, basada en la experiencia y el criterio individual, sin generar lecciones aprendidas documentadas ni acciones preventivas sistemáticas.

La inexistencia de un proceso estructurado de respuesta aumenta la dependencia de la reacción improvisada y reduce la capacidad de contener el impacto de incidentes futuros.

3.5 Continuidad del negocio y recuperación (función Recover)

En lo relativo a continuidad, el Local 6 realiza respaldos semanales de información crítica; sin embargo, no cuenta con un plan de recuperación que establezca prioridades de restauración, tiempos máximos de indisponibilidad aceptables o procedimientos específicos ante la caída de sistemas clave.

El negocio presenta una alta dependencia de servicios externos, especialmente de los sistemas de Hacienda para la facturación electrónica y de la banca en línea para

la gestión financiera. No se han analizado escenarios de contingencia ante la indisponibilidad prolongada de estos servicios ni se han definido alternativas operativas.

En estas condiciones, un incidente de seguridad o una interrupción en servicios externos podría traducirse en una imposibilidad temporal de facturar o de ejecutar transacciones críticas, con impacto directo en la continuidad del negocio.

3.6 Cultura de seguridad y capacitación

El diagnóstico permitió constatar la ausencia de un programa formal de capacitación o concienciación en ciberseguridad. El personal no ha recibido formaciones estructuradas en temas como phishing, ransomware, manejo seguro de contraseñas, uso de dispositivos extraíbles o navegación segura.

No obstante, la encuesta aplicada revela que las personas colaboradoras perciben que existen riesgos asociados a la seguridad digital y manifiestan preocupación por la falta de capacitación y de claridad en la respuesta ante incidentes. Esta situación indica que el factor humano constituye a la vez una fuente potencial de vulnerabilidad y una oportunidad para la implementación de estrategias formativas que fortalezcan la postura de seguridad del negocio.

4.Panorama de riesgos

A partir de los hallazgos anteriores se construyó una matriz de riesgos siguiendo los principios de ISO/IEC 31000, considerando la probabilidad de ocurrencia y el impacto sobre los procesos críticos. Entre los riesgos identificados como más relevantes se encuentran los siguientes:

a) Ausencia de autenticación multifactor en accesos críticos, aumentando el riesgo de compromisos de cuentas de correo y de banca en línea.

b) Debilidad en la gestión de contraseñas, al no existir una política formal ni mecanismos de control de complejidad y rotación, lo que facilita accesos no autorizados.

c) Respaldos sin prueba de restauración, que pueden derivar en pérdida efectiva de información o en tiempos prolongados de recuperación ante incidentes.

d) Falta de monitoreo y conservación de registros de seguridad, lo que dificulta detectar actividades inusuales y analizar incidentes a posteriori.

e) Ausencia de capacitación estructurada en ciberseguridad, que incrementa la probabilidad de que campañas de phishing o esquemas de fraude tengan éxito.

f) Dependencia de servicios externos sin un análisis formal de continuidad, exponiendo al negocio a interrupciones que afecten directamente la facturación y las operaciones financieras.

Estos riesgos fueron clasificados en niveles crítico, alto, medio o bajo, de acuerdo con su probabilidad e impacto, y evidencian un nivel de exposición significativo en áreas claves de la operación del local.

5.Recomendaciones estratégicas para fortalecer la postura de seguridad digital

Con base en los resultados del diagnóstico y considerando la realidad operativa del Local 6, se proponen las siguientes recomendaciones estratégicas:

5.1 Gobernanza y formalización de políticas

Designar formalmente una persona responsable de coordinar los aspectos de tecnologías de información y ciberseguridad, aunque sea en condición de responsabilidad parcial.

Elaborar, aprobar y difundir un conjunto mínimo de políticas de seguridad, que incluya, al menos:

a) Política de contraseñas y control de accesos.

b) Política de uso aceptable de equipos, internet, correo electrónico y dispositivos personales.

c) Política de respaldos y retención de información.

Establecer la revisión periódica de estas políticas, idealmente con frecuencia anual, ajustándolas a cambios tecnológicos y organizativos.

5.2 Fortalecimiento de controles técnicos esenciales

Implementar autenticación multifactor en los servicios donde esté disponible, priorizando banca en línea, correo corporativo y otros sistemas crítico–operativos.

Definir un procedimiento de gestión de parches y actualizaciones que establezca una frecuencia mínima (por ejemplo, mensual) para la revisión e instalación de actualizaciones de sistemas y aplicaciones.

Formalizar la estrategia de respaldos, definiendo:

a) Frecuencia y alcance de las copias de seguridad.

b) Ubicación de las copias (incluyendo al menos una copia separada del equipo principal).

c) Responsable de la ejecución y verificación de los respaldos.

Realizar pruebas de restauración de respaldos en intervalos regulares (por ejemplo, cada tres o seis meses), documentando resultados, tiempos de recuperación y ajustes necesarios.

Configurar mecanismos de filtrado de correo electrónico (antispam, antiphishing) para reducir el volumen de mensajes maliciosos que llegan a las bandejas de entrada.

5.3 Monitoreo, registros y respuesta a incidentes

Establecer un registro mínimo de incidentes y eventos de seguridad, donde se consigne fecha, sistema afectado, descripción del evento, impacto percibido y acciones correctivas.

Revisar de manera periódica (por ejemplo, mensual) las alertas de soluciones antivirus, los reportes de correo (mensajes marcados como sospechosos) y cualquier registro disponible de accesos o cambios relevantes.

Documentar un procedimiento básico de respuesta a incidentes que indique acciones claras ante eventos de seguridad, tales como aislar equipos sospechosos, modificar credenciales, notificar a bancos y proveedores, y registrar lo sucedido.

5.4 Continuidad de negocio y recuperación

1. Desarrollar un plan de recuperación ante incidentes que considere los procesos de facturación, gestión bancaria, inventario y contabilidad, definiendo:

a) Orden de prioridad en la restauración de sistemas y datos.

b) Tiempos máximos de interrupción aceptables para cada servicio.

c) Responsables de ejecutar y supervisar las acciones de recuperación.

2. Revisar la dependencia de servicios externos y, en la medida de lo posible, definir medidas de contingencia para escenarios de indisponibilidad prolongada de plataformas críticas.

5.5 Capacitación y cultura de ciberseguridad

1. Implementar un programa básico de concienciación en ciberseguridad para el personal, que incluya, al menos, una sesión anual sobre temas como phishing, contraseñas seguras, uso responsable de dispositivos y reconocimiento de señales de alerta.

2. Incorporar contenidos de ciberseguridad en los procesos de inducción de nuevo personal, de modo que desde el ingreso se conozcan las políticas internas y las prácticas esperadas.

3. Utilizar medios sencillos, como afiches, recordatorios impresos o mensajes internos, para reforzar periódicamente buenas prácticas y pautas de comportamiento seguro.

El diagnóstico realizado permite concluir que el Local 6 Inversiones Hamburgo se encuentra en una etapa inicial de madurez en ciberseguridad, con algunos controles técnicos básicos presentes, pero sin una estructura formal de gobernanza, monitoreo, respuesta a incidentes ni continuidad del negocio.

A pesar de ello, se identifican elementos favorables, como la existencia de respaldos, la percepción de riesgo por parte del personal y la disposición a mejorar. La implementación gradual y priorizada de las recomendaciones planteadas, especialmente en lo referente a formalización de políticas, adopción de autenticación multifactor, pruebas de restauración de respaldos y establecimiento de un programa básico de capacitación, permitirá fortalecer de manera significativa la postura de seguridad digital del negocio, reduciendo su exposición a incidentes y contribuyendo a la sostenibilidad de sus operaciones en el entorno digital actual.

Anexo 5. Herramienta de evaluación

En el siguiente enlace se deja disponible la herramienta de evaluación. Consiste en un documento de tipo Excel.

https://www.dropbox.com/scl/fo/y9zpmemvdt47h7vyg1mn5/AEmwzn1Big64cNR52fGcvgw?rlkey=3sacrzjm3onwie1go8jo1wd9z&st=jh426fea&dl=0