

Doctorado en Proyectos

La ciber resiliencia en las PYMEs: Metodología para un entorno digital seguro

Yoxan Smilyn Gonzalez Higueros

Director: Carlos Eduardo Herrera

Toluca, 01 de Septiembre 2025

Resumen

En el contexto actual de acelerada transformación digital, la protección de los activos informacionales constituye un imperativo estratégico para la sostenibilidad organizacional, particularmente en las pequeñas y medianas empresas (PYMEs) en México, que enfrentan una creciente exposición a amenazas cibernéticas sin contar con estructuras robustas de defensa. Esta investigación tuvo como objetivo analizar la ciberresiliencia organizacional en PYMEs mexicanas mediante la adopción del Marco de Ciberseguridad del National Institute of Standards and Technology (NIST, versión 2021), proponiendo una metodología adaptada a sus condiciones operativas, restricciones presupuestales y niveles variables de madurez tecnológica. El estudio se sustentó en un enfoque mixto de carácter exploratorio-descriptivo, con instrumentos diseñados para evaluar el nivel de implementación de las cinco funciones del marco (Identificar, Proteger, Detectar, Responder y Recuperar), integrando variables como gestión de riesgos, cultura organizacional y alfabetización digital. Los hallazgos evidenciaron una desconexión entre la criticidad reconocida de la ciberseguridad y la ejecución efectiva de medidas preventivas y reactivas, destacando deficiencias en la formalización de políticas, la capacitación del personal, la inversión en herramientas especializadas y la existencia de roles definidos en materia de seguridad. Se concluyó que la implementación estratégica del Marco NIST, adaptada al entorno operativo de las PYMEs, puede fortalecer significativamente su postura de ciberseguridad y resiliencia institucional, contribuyendo a la mitigación efectiva de riesgos digitales. Esta propuesta buscó posicionar la ciberresiliencia como un componente transversal del desarrollo empresarial, capaz de incidir positivamente en la continuidad operativa, la confianza de sus stakeholders y su competitividad en el ecosistema digital.

Palabras clave: amenazas cibernéticas, marco, ciberseguridad, metodología.

Abstract

The current context of accelerated digital transformation, protecting informational assets is a strategic imperative for organizational sustainability, particularly for small and medium-sized enterprises (SMEs) in Mexico. These SMEs face increasing exposure to cyber threats without robust defense structures. This research aimed to analyze organizational cyber resilience in Mexican SMEs by adopting the National Institute of Standards and Technology (NIST) Cybersecurity Framework (2021 version). It proposes a methodology adapted to their operational conditions, budgetary constraints, and varying levels of technological maturity. The study employed a mixed-methods approach, exploratory-descriptive in nature, with instruments designed to evaluate the implementation level of the framework's five functions: Identify, Protect, Detect, Respond, and Recover. Variables such as risk management, organizational culture, and digital literacy were integrated into the assessment. The findings revealed a disconnect between the recognized criticality of cybersecurity and the effective execution of preventive and reactive measures. This highlighted deficiencies in policy formalization, staff training, investment in specialized tools, and the existence of defined security roles. It is concluded that the strategic implementation of the NIST Framework, adapted to the operational environment of SMEs, can significantly strengthen their cybersecurity posture and institutional resilience, contributing to the effective mitigation of digital risks. This proposal seeks to position cyber resilience as a cross-cutting component of business development, capable of positively impacting operational continuity, stakeholder trust, and competitiveness within the digital ecosystem.

Keywords: cyber threats, framework, cybersecurity, methodology.

Dedicatorias

Esta tesis está hecha de palabras, esfuerzo y noches largas, pero también está tejida con cariño, apoyo y muchos abrazos. A mi familia, gracias por ser ese lugar al que siempre puedo volver, por su amor incondicional y por darme fuerza incluso en silencio. A mi novia, mi compañera en cada paso, gracias por estar, por tu alegría contagiosa y por no soltar mi mano en los momentos difíciles. A mi mentor, por compartir no solo su conocimiento, sino también su paciencia y confianza en mí. Y a mis amigos, gracias por las risas que despejan la mente, por escuchar sin juzgar, y por estar presentes incluso en la distancia. Cada uno de ustedes ha sido parte de este camino, y sin ustedes, esta historia no estaría completa. Gracias de corazón por creer en mí.

Agradecimientos

Quiero expresar mi más profundo agradecimiento a la Universidad UNADE de México por haber creído en mí y haberme otorgado la beca que hizo posible este proyecto. Gracias a su apoyo, no solo pude dedicarme de lleno a esta investigación, sino también crecer en lo académico y en lo personal. La UNADE fue mucho más que una universidad para mí: fue un espacio donde encontré motivación, aprendizaje y sentido. Siempre la llevaré conmigo como un lugar clave en mi historia.

También quiero agradecer con el corazón al Dr. Carlos Eduardo Herrera. Su guía, su sabiduría y, sobre todo, su forma de acompañar sin imponer, marcaron la diferencia en este camino. Gracias por cada consejo, por cada conversación y por estar ahí incluso cuando las dudas pesaban más que las certezas. Más que un mentor, fue un verdadero compañero de ruta. Gracias, doctor, por todo.

Contenido

Resumen ii

Abstract iii

Dedicatorias iv

Agradecimientos v

Contenido v

Introducción 1

Planteamiento del Problema 6

Formulación de la pregunta de investigación 9

Justificación 10

Justificación Práctica 10

Justificación Académica 11

Justificación Institucional 11

1. Marco de referencia 13

1.1 Marco Legal 13

1.1.1 Revisión crítica de las iniciativas pendientes 15

1.1.2 Implicaciones concretas para las PYMEs 15

1.1.3 Comparación internacional 16

1.1.4 Transición al marco normativo y al análisis del NIST 16

1.2 Marco Normativo 16

1.2.1 Marco institucional: estrategias públicas vigentes 17

1.2.2 Marco penal: legislación vigente en materia de delitos informáticos 17

1.2.3 Propuestas de reforma y avances recientes 18

1.2.4 Alcance y limitaciones normativas en relación con las PYMEs 19

1.2.5 Conexión con el objetivo de investigación 19

1.3 Marco Conceptual 20

1.3.1 Actores principales 20

1.3.2 Marcos de referencia y normativos 21

1.3.3 Riesgos y amenazas en ciberseguridad 22

1.4 Competencias desarrolladas en la investigación 23

1.4.1 Competencia estratégica: evaluación e implementación contextual del marco NIST 23

1.4.2 Competencia comparativa: análisis crítico de marcos internacionales 23

1.4.3 Competencia de transferencia sectorial: análisis de casos aplicados 24

1.4.4 Competencia diagnóstica: identificación de desafíos de implementación 24

1.5 Definiciones Operativas 24

1.6 Marco Teórico 28

1.6.1 El Marco NIST: estructura, aplicabilidad y pertinencia 28

1.6.2 Cultura de seguridad y resiliencia organizacional 30

1.6.3 Gestión de riesgos cibernéticos 31

1.6.4 Comprensión lectora y alfabetización digital como competencias clave 31

1.6.5 Vinculación con el contexto mexicano 32

1.6.6 Definición de conceptos clave del Marco de Ciberseguridad del NIST en el contexto de las PYMES 32

1.6.7 Información como activo crítico (Función Identificar) 33

1.6.8 Procesamiento y protección de la información (Funciones Proteger y Detectar)

.....33

1.6.9 Ciberseguridad como sistema de protección (Introducción al Marco) 34

1.6.10 Vulnerabilidades y ciberataques (Funciones Identificar y Detectar).....35

1.6.11 Resiliencia cibernética (Función Recuperar) 35

1.6.12 La alfabetización digital como habilitador organizacional 36

1.7 Estado del arte.....36

1.7.1 Definición de "estándar" y su relación con el Marco NIST.....39

1.7.2 El Marco de Ciberseguridad del NIST y su Aplicación en PYMES mexicanas

.....42

1.7.3 La Pirámide de Keops como Analogía Evolutiva de Madurez en Ciberseguridad

.....45

2. Diseño metodológico 49

2.1 Enfoque Metodológico 51

2.1.1 Justificación del enfoque mixto.....52

2.1.2 Componentes cuantitativo y cualitativo.....53

2.1.3 Integración y análisis 55

2.2 Tipo de investigación 56

2.2.1 Definiciones Teóricas 57

2.2.2 Definiciones Operacionales.....58

2.3 Hipótesis 61

2.4 Objetivo general.....61

2.5 Objetivos específicos.....61

2.6 Instrumentos.....64

2.6.1 Análisis de Grupos de Interés con Mapeo de Ciberinfluencia 65
2.6.2 Revisión Documental y Auditoría de Alineación NIST 66
2.6.3 Simulación de Amenazas y Evaluación Técnica Simplificada (BAS) 66
2.6.4 Cuestionarios con Evaluación de Madurez NIST y Gamificación 67
2.6.5 Herramientas Propias: NANP y SICPYME 68
2.7 Carta de consentimiento 69
2.8 Población y Muestra 70
2.9 Procesamiento de datos 72
2.9.1 Codificación de datos 72
2.9.2 Análisis cuantitativo 73
2.9.3 Análisis cualitativo 74
2.9.4 Triangulación e integración de resultados 75
3 Resultados 76
3.1 Perfil de los encuestados 76
3.1.2 Antigüedad laboral de los encuestados 78
3.1.3 Nivel jerárquico de los encuestados 80
3.2 Análisis Cuantitativo Detallado por Función del Marco NIST 81
3.2.1 Función 1: Identificar (ID) 81
3.2.2 Función 2: Proteger (PR) 89
3.2.3 Función 3: Detectar (DE) 94
3.2.4 Función 4: Responder (RS) 99
3.2.5 Función 5: Recuperar (RC) 103
3.2.6 Evaluación Cualitativa: Profundizando en los Desafíos y las Percepciones ..107

3.2.7 Índice de Madurez de Ciberseguridad (CMI) para Nutriwell 108

3.2.8 Implicaciones y Recomendaciones Preliminares para Nutriwell 110

3.3 Hallazgos Detallados de la Evaluación de Ciberseguridad en Nutriwell 112

3.3.1. La Percepción Engañosa de la Gestión de Información Crítica (ID.AM-1): Un Riesgo Silencioso 112

3.3.2. Ceguera Generalizada ante las Vulnerabilidades (ID.RA-2): Una Invitación a los Ciber atacantes.....114

3.3.3. El "Plan de Vulnerabilidad" Invisible (ID.RA-3): Una Estrategia en Papel, No en la Práctica 115

3.3.4. Desconocimiento del Impacto de los Ciberataques (ID.BA-1): Minimizando el Peligro Real 116

3.3.5. Monitoreo de Amenazas Inconstante (ID.AM-2): Operando a Ciegas ante el Peligro 117

4 Conclusiones.....122

5.1 Recomendaciones finales 124

5 Referencias 126

Introducción

La transformación digital ha reconfigurado profundamente las dinámicas organizacionales, exponiendo a las pequeñas y medianas empresas (PYMEs) a desafíos sin precedentes en materia de seguridad de la información. Su creciente dependencia de tecnologías basadas en internet, aunque les ofrece ventajas competitivas, también amplifica su vulnerabilidad ante amenazas cibernéticas cada vez más complejas y persistentes (Whitman & Mattord, 2022). En este contexto, resulta esencial analizar el nivel de concienciación en ciberseguridad existente en las PYMEs, así como las estrategias de ciberresiliencia que adoptan para proteger sus activos digitales críticos (Bada et al., 2019). Además, se propone evaluar el papel que puede desempeñar el Marco de Ciberseguridad del NIST como una herramienta estructurada para la formulación de políticas eficaces de gestión del riesgo tecnológico, particularmente en entornos con recursos limitados (Linkov et al., 2013).

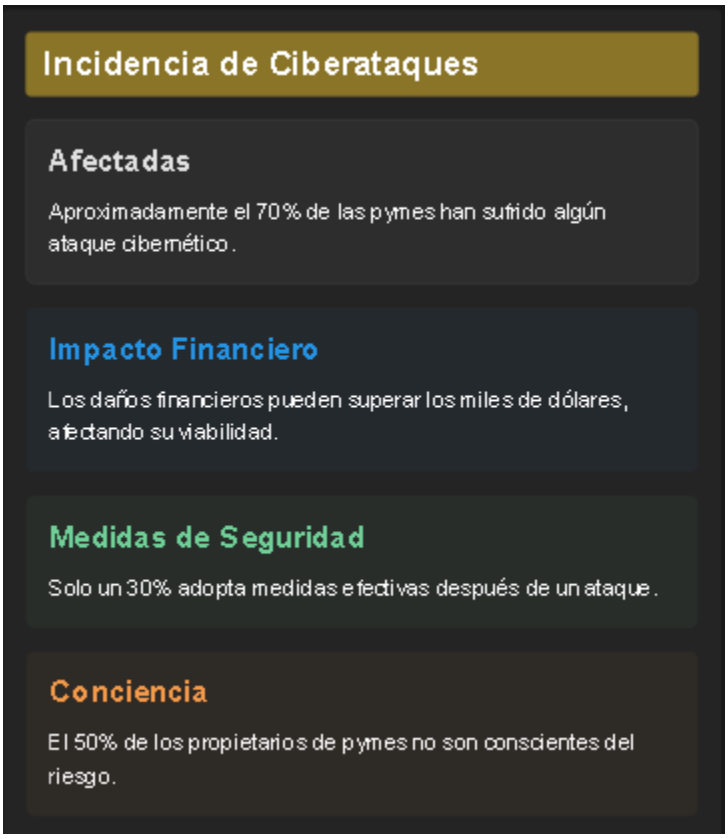
El objetivo general de este estudio es examinar el nivel de preparación de las PYMEs mexicanas en materia de ciberseguridad, evaluando la adopción de buenas prácticas de ciber resiliencia y el uso del Marco NIST como referencia normativa. Para ello, se plantean tres objetivos específicos: identificar el grado de conocimiento y la percepción del riesgo cibernético en este tipo de organizaciones; analizar las medidas de ciberresiliencia actualmente implementadas en sus estructuras operativas; y evaluar la viabilidad y pertinencia del Marco NIST como guía estructurada para fortalecer su postura de seguridad digital. En consecuencia, el problema de investigación se delimita al análisis del nivel de madurez ciberresiliente de las PYMEs mexicanas, considerando sus características contextuales, sus limitaciones en recursos técnicos y humanos, y el potencial del Marco NIST para ser adoptado como instrumento práctico de gestión del riesgo tecnológico en entornos empresariales de escala media y pequeña.

Las preguntas que orientan esta indagación son: ¿Cuentan las PYMEs con una cultura de concienciación suficiente para enfrentar los desafíos del entorno digital contemporáneo? ¿Implementan estrategias eficaces de ciberresiliencia? ¿Es viable el uso del Marco de Ciberseguridad del NIST como mecanismo de orientación práctica y estratégica en dicho contexto?

Numerosos estudios coinciden en señalar que las PYMEs constituyen un blanco cada vez más frecuente de ataques cibernéticos. De acuerdo con datos de CyberEOP (2019), el 70% de las PYMEs ha experimentado algún tipo de incidente de seguridad digital, y el 40% de estos ataques se dirige deliberadamente hacia empresas de menor tamaño. Estas cifras provienen de un informe técnico basado en encuestas aplicadas a directores de TI y responsables de seguridad informática en América Latina, lo cual refuerza la validez empírica del diagnóstico. Asimismo, Valle (2022) —en un estudio sectorial realizado a partir de entrevistas y datos recopilados de cámaras empresariales— indica que el 78% de las PYMEs carece de defensas adecuadas ante ataques cibernéticos. De forma complementaria, IT Digital Media Group (2023) informa que solo el 13% de las PYMEs encuestadas invierte en la capacitación de su personal en materia de seguridad informática. La baja inversión en formación y tecnología especializada, sumada a una percepción distorsionada del riesgo, contribuye a consolidar una cultura organizacional reactiva e insuficiente frente a las exigencias del entorno digital. En la Figura 1 se detalla como estas incidencias afectan a las Pymes.

Figura 1.

Incidencias de ciberataques en las PYMEs 2019.



Nota: Promedio estadístico del impacto en las PYMEs proporcionado por, Cybereop (2019).

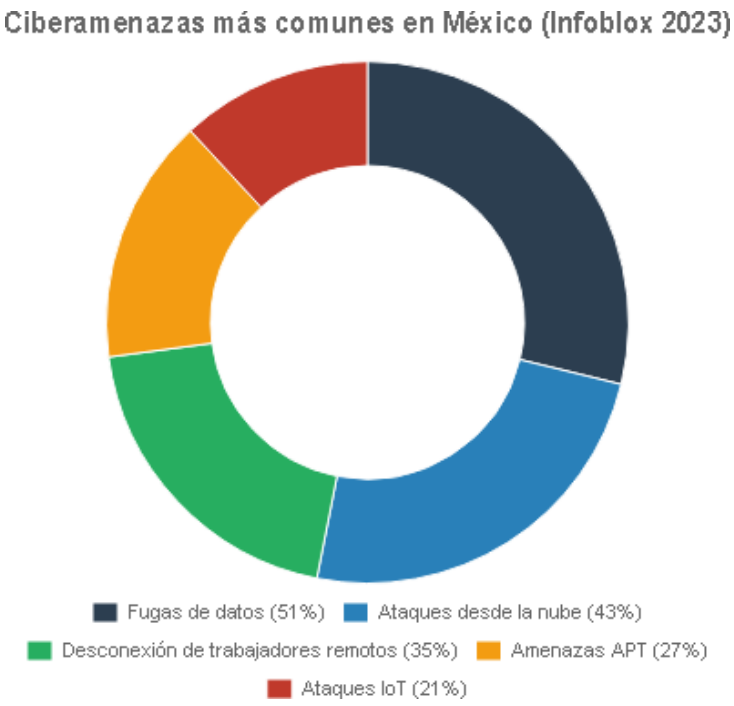
La Figura 1 es fundamental para comprender la magnitud de la problemática que aborda esta investigación, ya que presenta un panorama conciso de la vulnerabilidad cibernética en las pequeñas y medianas empresas. Esta figura no solo revela que aproximadamente el 70% de las PYMEs han sido víctimas de algún ataque cibernético, destacando la alta prevalencia de estas amenazas, sino que también subraya el significativo impacto financiero que tales incidentes pueden generar, superando los miles de dólares y comprometiendo la viabilidad empresarial.

El Marco de Ciberseguridad del NIST (National Institute of Standards and Technology), diseñado originalmente para infraestructuras críticas, proporciona un enfoque normativo basado

en cinco funciones esenciales: Identificar, Proteger, Detectar, Responder y Recuperar. Este marco ha sido reconocido internacionalmente por su aplicabilidad flexible y su enfoque gradual, lo que permite su adaptación a organizaciones de diversos tamaños y niveles de madurez tecnológica. En el caso de las PYMEs, su adopción puede facilitar la transición desde un enfoque fragmentario hacia una estrategia coherente de gestión de riesgos, incluso en entornos con restricciones presupuestarias. En la Figura 2 se demuestra las ciber amenazas más comunes en México.

Figura 2.

Ciber amenazas más comunes en México.



Nota: Grafica ciberamenzas existentes en México y sus porcentajes de ataques, Infoblox (2023)

La Figura 2 es una representación gráfica esencial para comprender la distribución y la prevalencia de los distintos tipos de ataques cibernéticos que afectan al entorno digital mexicano.

Este diagrama de anillo no solo visualiza que las fugas de datos representan la amenaza más común con un 51% de incidencia, sino que también destaca la significativa frecuencia de ataques desde la nube (43%), la desconexión de trabajadores remotos (35%), las amenazas APT (27%) y los ataques IoT (21%).

En México, donde las PYMEs representan el 99.8% del total de las unidades económicas (INEGI, 2023), su papel no solo es crucial para el crecimiento económico, sino también para la estabilidad digital del ecosistema empresarial. Muchas de estas organizaciones funcionan como proveedores clave en cadenas de suministro que incluyen grandes corporaciones y dependencias gubernamentales. Por tanto, sus vulnerabilidades pueden convertirse en vectores de propagación de amenazas a nivel sistémico. Garantizar su resiliencia digital no es solamente una cuestión de supervivencia individual, sino también una necesidad estratégica para fortalecer la seguridad cibernética nacional.

La presente investigación adopta un enfoque metodológico de carácter cualitativo, el cual resulta especialmente pertinente para la exploración de fenómenos complejos y poco estructurados, como lo son la gestión de riesgos cibernéticos, la cultura organizacional en torno a la seguridad digital y la adopción de marcos normativos en entornos empresariales con recursos limitados. Este enfoque permite captar la riqueza contextual y la diversidad de percepciones que caracterizan a las pequeñas y medianas empresas, cuya realidad operativa no siempre puede ser representada adecuadamente mediante métodos cuantitativos tradicionales. Así, la metodología cualitativa posibilita una comprensión más profunda de las motivaciones, barreras y criterios que influyen en la toma de decisiones relacionadas con la ciber resiliencia.

Aunque existe un corpus significativo de literatura técnica y normativa sobre ciberseguridad, este estudio busca aportar una visión actualizada y aplicada, centrada en el

análisis interpretativo de las prácticas empresariales reales. En este sentido, se enfatiza la importancia crítica de la concienciación en seguridad digital y de la adopción sistemática de marcos estructurados como el del NIST, los cuales se examinan no solo desde su formulación teórica, sino también desde su grado de apropiación y aplicabilidad en contextos organizacionales concretos. Esta aproximación metodológica se articula con los ejes del marco conceptual y da continuidad al objetivo central del estudio: comprender cómo las PYMEs gestionan su seguridad digital y qué condiciones facilitan o dificultan el desarrollo de una ciberresiliencia efectiva y sostenible.

Planteamiento del Problema

En un escenario global marcado por la acelerada digitalización y el incremento sostenido en la sofisticación de las amenazas cibernéticas, las pequeñas y medianas empresas (PYMEs) se configuran como uno de los sectores más vulnerables frente a la materialización de riesgos informáticos. Esta problemática adquiere especial relevancia en el contexto mexicano, donde las PYMEs representan el 99.8% del total de las unidades económicas (INEGI, 2023), desempeñando un papel clave en la generación de empleo y en la dinamización del tejido productivo.

Entre las principales causas de esta vulnerabilidad se encuentra la existencia de limitaciones estructurales persistentes, tales como la escasez de recursos financieros destinados a la seguridad digital, la insuficiencia de personal especializado y la ausencia de políticas integrales de gestión de riesgos tecnológicos. A estas carencias se suma una débil cultura organizacional en torno a la ciberseguridad y la ciberresiliencia, lo que se traduce en una baja priorización del tema en la agenda directiva de muchas PYMEs. Según datos del informe de CyberEOP (2019), aproximadamente el 70% de las PYMEs latinoamericanas ha experimentado

al menos un incidente de seguridad, siendo las microempresas el segmento más afectado, con un 40% de los ataques dirigidos específicamente hacia ellas. Adicionalmente, evidencia empírica reciente revela que apenas el 13% de las PYMEs capacita activamente a su personal en buenas prácticas de seguridad de la información (IT digital Media Group, 2023). En la Figura 3 se detalla más acerca de las estadísticas de economía de Pymes en México y América Latina.

Figura 3.

Estadísticas de economía globales de PYMEs en México y Latinoamérica.



Notas: Estadísticas a propósito del día de las micro, pequeñas y medianas empresas, INEGI (2020)

La Figura 3 es un compendio visual esencial que subraya el papel insustituible de las micro, pequeñas y medianas empresas (MiPYMEs) como pilar fundamental de la economía global y regional. Esta figura, que presenta datos de INEGI (2020), no solo resalta que el 94% de las empresas mundiales son MiPYMEs (alrededor de 400 millones), sino que también cuantifica su impacto global, como su contribución del 41% a las importaciones y el 36% a las exportaciones mundiales, así como su significativo aporte al PIB global (50% en países desarrollados y 35% en países en desarrollo).

Las consecuencias de esta situación son múltiples y de gran alcance. Las PYMEs no solo se exponen a incidentes de alto impacto, como el robo de datos sensibles, la paralización operativa o la pérdida de confianza por parte de clientes y socios comerciales, sino que también generan un riesgo sistémico para el ecosistema empresarial más amplio. En tanto proveedores frecuentes de servicios o productos para grandes corporaciones y entidades gubernamentales, las deficiencias en su postura de ciberseguridad pueden actuar como vectores de propagación de amenazas hacia infraestructuras críticas de mayor escala.

Este escenario evidencia la necesidad urgente de transitar hacia una gestión más estratégica de la seguridad digital en el entorno PYME. En este sentido, la promoción de metodologías estructuradas y de probada eficacia, como el Marco de Ciberseguridad del NIST, se perfila como una herramienta clave. Dicho marco proporciona un enfoque sistemático para la identificación de riesgos, la protección de activos digitales, la detección oportuna de incidentes y la implementación de respuestas eficaces, facilitando así el fortalecimiento de la resiliencia organizacional en un entorno digital crecientemente adverso.

En este contexto apremiante, se vuelve necesario examinar críticamente el nivel de concienciación que las PYMEs poseen respecto a la naturaleza y el alcance de las amenazas

cibernéticas, así como las medidas concretas que están implementando para la protección integral de sus operaciones y la garantía de su continuidad en un entorno digital cada vez más adverso. La manera en que estas organizaciones respondan a los desafíos de seguridad digital no solo condicionará su capacidad de adaptación y permanencia en el mercado, sino que también tendrá implicaciones directas en la estabilidad del ecosistema económico al que pertenecen.

Ante esta situación crítica, se hace imprescindible indagar a fondo el grado de preparación de las PYMEs frente a las amenazas del entorno digital y las estrategias adoptadas para su protección, lo cual se aborda en la siguiente sección.

Formulación de la pregunta de investigación

En un entorno global cada vez más interconectado, las amenazas cibernéticas crecen en complejidad y frecuencia. Las pequeñas y medianas empresas (PYMEs) en México —que constituyen aproximadamente el 99% del total de negocios y representan un pilar esencial del aparato económico nacional— enfrentan desafíos significativos en materia de protección de la información y continuidad operativa. Esta vulnerabilidad no solo compromete su propia estabilidad, sino que también introduce riesgos a nivel sistémico, afectando a las grandes corporaciones y entidades públicas con las que mantienen relaciones comerciales, lo que genera un efecto de propagación de amenazas a lo largo de toda la cadena de suministro.

En este contexto, la presente investigación se articula en torno a una pregunta central:

¿Cuál es el nivel de preparación de las pequeñas y medianas empresas (PYMEs) en México frente a los riesgos cibernéticos, y en qué medida la adopción del Marco de Ciberseguridad del NIST puede fortalecer su resiliencia operativa y capacidad de respuesta ante incidentes de seguridad?

A partir de esta cuestión general, se desprenden las siguientes preguntas específicas:

1. ¿Qué nivel de conocimiento y comprensión poseen las PYMEs mexicanas respecto a los principios fundamentales de ciberseguridad —identificación, protección, detección, respuesta y recuperación— y a los conceptos clave de ciber resiliencia?

2. ¿Qué estrategias, prácticas y tecnologías de seguridad están implementando actualmente las PYMEs para proteger sus activos digitales y asegurar la continuidad de sus operaciones ante incidentes cibernéticos?

3. ¿En qué medida el Marco de Ciberseguridad del NIST se adecúa a las necesidades, limitaciones y capacidades de las PYMEs mexicanas, y qué impacto podría tener su aplicación en la mejora de sus políticas y procesos de seguridad digital?

Este proyecto de investigación se sitúa en la intersección entre la tecnología y la gestión estratégica, con el propósito de ofrecer soluciones prácticas y accesibles que permitan a las PYMEs reducir su exposición al riesgo y desarrollar una cultura organizacional orientada a la ciberseguridad. A través del análisis de su situación actual y de la evaluación del potencial de marcos metodológicos como el NIST, se busca proponer directrices que fortalezcan su capacidad de adaptación y respuesta en el contexto digital contemporáneo.

Justificación

Justificación Práctica

La acelerada transformación digital está reconfigurando el funcionamiento de las pequeñas y medianas empresas (PYMEs), insertándolas en un entorno donde las amenazas cibernéticas son cada vez más sofisticadas y frecuentes. En México, estas organizaciones representan el 99.8% del tejido empresarial y son esenciales para la generación de empleo y el crecimiento económico (INEGI, 2023). No obstante, muchas de ellas carecen de infraestructura tecnológica, personal capacitado y mecanismos formales para gestionar riesgos cibernéticos, lo

que las convierte en objetivos recurrentes de ataques (Bada, Sasse & Nurse, 2019). De acuerdo con ESET (2023), el 30% de las organizaciones latinoamericanas sufrió al menos un incidente de ciberseguridad en el último año, y una de cada cinco pudo haber sido atacada sin saberlo. En este contexto, la adopción de marcos normativos como el del National Institute of Standards and Technology (NIST) se ha propuesto como una herramienta eficaz y adaptable para fortalecer la ciberresiliencia, incluso en organizaciones con capacidades limitadas (Bodeau & Graubart, 2017; Linkov et al., 2013).

Justificación Académica

Desde el ámbito académico, si bien existen estudios que abordan la ciberseguridad en PYMEs, persiste un vacío en cuanto a la evaluación empírica del Marco NIST en contextos latinoamericanos, donde las limitaciones estructurales y presupuestarias son más marcadas (Safa et al., 2016). Esta investigación propone un aporte original al adaptar y validar dicho marco en un entorno real, diseñando una metodología contextualizada, escalable y viable para organizaciones con baja madurez digital, integrando indicadores clave de preparación y respuesta frente a incidentes cibernéticos.

Justificación Institucional

En el plano institucional, la vulnerabilidad de las PYMEs no solo compromete su sostenibilidad, sino que representa un riesgo sistémico para cadenas de suministro, procesos financieros y servicios esenciales. Las PYMEs, al formar parte de ecosistemas interconectados, pueden convertirse en vectores de propagación de amenazas que escalan a infraestructuras críticas (Von-Solms & Van-Niekerk, 2013). Fortalecer su ciberresiliencia no es solo una necesidad operativa, sino una prioridad estratégica para la estabilidad económica nacional y la

formulación de políticas públicas orientadas al cierre de brechas digitales y la promoción de una cultura de seguridad desde la base productiva.

1. Marco de referencia

1.1 Marco Legal

En México aún no existe una ley federal específica de ciberseguridad, lo que deja a instituciones públicas, empresas y ciudadanos expuestos a un entorno digital cada vez más amenazante (Rivera, 2024). Desde 2018 se han presentado once iniciativas legislativas en el Congreso, pero ninguna ha culminado su aprobación ni promulgación efectiva.

No obstante, en fechas recientes se han impulsado nuevos proyectos con mayor fuerza. En agosto de 2024, el Senado presentó su "versión cero" de la Ley Federal de Ciberseguridad, contemplando 11 títulos y 71 artículos orientados a tipificar delitos cibernéticos, establecer pruebas de penetración anuales, y crear una Agencia Nacional de Ciberseguridad, Delta Protect (2023, enero 18). Asimismo, en abril de 2025 se presentó otra iniciativa que busca articular derechos humanos, privacidad, continuidad de servicios esenciales y soberanía digital dentro del marco constitucional iniciativa con proyecto de decreto por el que se expide la Ley de Ciberseguridad. Senado de la República (2025, abril 30).

A pesar de estos avances, hasta julio de 2025 ninguna de las propuestas ha sido promulgada ni publicada en el Diario Oficial de la Federación, por lo que persiste un vacío legal que limita la coordinación institucional y deja a las PYMEs sin un respaldo normativo estructurado. En la Figura 4 vemos los indicadores que debe presentar una cultura cibernética.

Figura 4.

Indicadores de estrategias de ciberseguridad tanto en la política como en la cultura o sociedad.



Nota: Reporte de Ciberseguridad-2020 riesgos avances y el camino a seguir en América Latina, BID (2020).

Para comprender mejor los componentes del marco normativo vigente y los avances en la ciberseguridad a nivel regional, se presenta a continuación la Figura 4, que los resume de manera visual. Titulada 'Indicadores de estrategias de ciberseguridad tanto en la política como en la cultura o sociedad', esta figura, extraída del Reporte de Ciberseguridad-2020 de BID para América Latina, ilustra una serie de indicadores clave en dos dimensiones fundamentales: la Política y Estrategia de Seguridad Cibernética (D1) y la Cultura Cibernética y Sociedad (D2),

comparando el progreso entre 2016 y 2020. Aunque la figura es de carácter general y aborda la situación a nivel de América Latina, sin centrarse exclusivamente en el contexto mexicano de las PYMEs, su inclusión es crucial para reforzar la idea de que el vacío normativo y las brechas en ciberseguridad no son fenómenos aislados de México, sino que constituyen una problemática extendida y persistente en toda la región latinoamericana.

1.1.1 Revisión crítica de las iniciativas pendientes

Las iniciativas recientes presentan innovaciones importantes —como mecanismos de coordinación interinstitucional, sanción penal para actos maliciosos en línea, y la creación de una agencia especializada—, pero adolecen de deficiencias relevantes:

Definiciones amplias y poco delimitadas, que pueden generar ambigüedades en derecho penal.

Preocupaciones por derechos fundamentales, ya que algunos sectores advierten riesgos para la libertad de expresión y privacidad- ASIET. (2024, abril 30).

Falta de mecanismos de implementación específicos para el sector privado, lo que evidencia que las propuestas están orientadas principalmente a la administración pública, dejando a las PYMEs fuera del diseño institucional.

1.1.2 Implicaciones concretas para las PYMEs

La ausencia de un marco legal robusto impacta directamente a las PYMEs en múltiples frentes:

No existen protocolos obligatorios para la protección informática, detección de incidentes o reporte obligatorio, lo que reduce su capacidad de respuesta ante ataques.

Faltan incentivos legales y recursos, como deducciones fiscales, subsidios para capacitación o acceso a asesoría técnica especializada.

Hay vacíos regulatorios en sanciones y responsabilidades, lo que impide atribuir consecuencias claras en caso de negligencia digital o fallas en proveedores TI y terceros.

Esta situación refrenda el carácter sistémico de la vulnerabilidad: sin regulación, las PYMEs permanecen desprotegidas y debilitan la resiliencia del sector empresarial en su conjunto.

1.1.3 Comparación internacional

A diferencia de México, algunos países latinoamericanos han avanzado más rápidamente. Por ejemplo, Chile cuenta desde 2014 con una ley específica de ciberseguridad que incluye disposiciones aplicables al sector privado y mecanismos de coordinación nacional; Colombia promulgó en 2018 una ley que define responsabilidades de empresas y organismos en materia de protección digital, incluyendo a las PYMEs. La ausencia de una regulación equivalente en México coloca al país en una posición comparativamente rezagada, El Universal (2024, mayo 11).

1.1.4 Transición al marco normativo y al análisis del NIST

Dada esta insuficiencia legislativa y la demora en la promulgación de normas específicas, el análisis de marcos técnicos internacionales, como el Marco de Ciberseguridad del NIST, cobra relevancia. Este análisis constituye el siguiente paso en la tesis, pues permitirá evaluar cómo un estándar consolidado puede suplir, en la práctica, la carencia legal y servir de base para el fortalecimiento de la resiliencia cibernética en las PYMEs.

1.2 Marco Normativo

En México, el desarrollo normativo en ciberseguridad ha sido fragmentario y disperso, sin consolidarse en una ley integral que articule responsabilidades, medidas preventivas y protocolos de actuación frente a incidentes digitales. Esta sección examina el marco institucional

existente, las disposiciones penales vigentes, las principales propuestas de reforma y su pertinencia frente a la realidad de las pequeñas y medianas empresas (PYMEs).

1.2.1 Marco institucional: estrategias públicas vigentes

Durante el sexenio del presidente Enrique Peña Nieto se emitió la Estrategia Nacional de Ciberseguridad (2017), concebida como una herramienta de política pública para coordinar esfuerzos y fortalecer la seguridad digital a nivel nacional. Esta estrategia se estructura en torno a cuatro ejes: sociedad, seguridad nacional, economía y gobierno.

Sin embargo, pese a su enfoque multidimensional, la estrategia no posee fuerza jurídica vinculante ni un organismo rector con atribuciones específicas para su ejecución. Tampoco contempla disposiciones operativas aplicables a las PYMEs, lo que limita su utilidad como instrumento efectivo para fortalecer la resiliencia cibernética de este sector.

1.2.2 Marco penal: legislación vigente en materia de delitos informáticos

El Código Penal Federal, en su Título Noveno, contempla algunos delitos relacionados con la informática bajo la categoría de *"Revelación de secretos y acceso ilícito a sistemas y equipos de informática"*. Los artículos 211 Bis 1 y 211 Bis 2 sancionan el acceso no autorizado, la destrucción o alteración de datos, particularmente en sistemas protegidos o gubernamentales.

Artículo 211 Bis 1:

Prisión de 6 meses a 2 años y multa de 100 a 300 días a quien modifique o elimine información sin autorización.

Acceso o copia de datos sin permiso: 3 meses a 1 año y multa de 50 a 150 días.

Artículo 211 Bis 2:

Si la información pertenece a sistemas gubernamentales, las penas aumentan hasta 4 años de prisión.

Cuando se afectan sistemas de seguridad pública, las penas alcanzan de 4 a 10 años.

En caso de servidores públicos implicados, se contempla inhabilitación de 4 a 10 años.

Aunque estas disposiciones representan un avance en el reconocimiento legal de delitos informáticos, su alcance resulta limitado ante las amenazas cibernéticas actuales. Tipologías modernas como el *phishing*, *ransomware* o *DDoS* no están expresamente tipificadas, lo cual genera incertidumbre jurídica y deja sin respuesta a víctimas, especialmente PYMEs que no cuentan con departamentos legales o técnicos especializados.

Además, el acceso a la justicia es limitado: muchas PYMEs desconocen sus derechos o no denuncian por falta de confianza en la persecución efectiva de estos delitos.

1.2.3 Propuestas de reforma y avances recientes

A lo largo de los últimos años, diversas iniciativas han buscado suplir las carencias del marco normativo vigente. Algunas de las más relevantes son:

2005 – Reforma al Código Penal Federal para tipificar delitos cibernéticos.

2012 – Propuesta de reforma al Código Penal en materia de delitos informáticos.

2015 – Ley Federal para Prevenir y Sancionar los Delitos Informáticos (no aprobada).

2018 – Ley de Seguridad Privada (con enfoque parcial en seguridad digital).

2019 – Ley de Seguridad Informática (pendiente).

2020 – Ley General de Ciberseguridad, sin avances de aprobación hasta 2023.

2024–2025 – Nuevas iniciativas legislativas, como la “Versión Cero” del Senado y la propuesta del senador Colosio, con intención de establecer una Agencia Nacional de Ciberseguridad, aplicar pruebas de penetración obligatorias, y mejorar la coordinación interinstitucional (Senado, 2025).

Pese a la abundancia de propuestas, ninguna ha sido promulgada. Algunas iniciativas han sido criticadas por definiciones vagas, ausencia de enfoque en derechos humanos y falta de mecanismos claros de aplicación para el sector privado. Esto perpetúa la dispersión normativa y mantiene a las PYMEs en un entorno de indefensión legal.

1.2.4 Alcance y limitaciones normativas en relación con las PYMEs

Las PYMEs mexicanas —responsables de cerca del 70% del empleo formal y más del 50% del PIB (INEGI, 2023)— son el blanco más frecuente de ciberataques, acumulando el 79% de los incidentes reportados. Sin embargo, el marco normativo vigente no ofrece herramientas específicas que respondan a su realidad operativa y presupuestaria.

Entre las principales limitaciones destacan:

Inexistencia de protocolos oficiales adaptados a PYMEs (manuales, guías, estándares mínimos).

Ausencia de obligaciones o incentivos fiscales para mejorar su ciberseguridad.

Falta de rutas institucionales claras para denunciar incidentes, recibir asesoría o coordinarse con autoridades.

Desconexión entre la ley penal y las amenazas más frecuentes que enfrentan, como robo de datos de clientes, secuestro de sistemas, y fraudes electrónicos.

Esta desconexión evidencia que las PYMEs enfrentan una doble vulnerabilidad: técnica y jurídica, sin acompañamiento estatal ni marco normativo robusto.

1.2.5 Conexión con el objetivo de investigación

La carencia de una normativa integral y específica para la ciberseguridad en PYMEs mexicanas refuerza la pertinencia de adoptar marcos internacionales como el Framework for Improving Critical Infrastructure Cybersecurity del NIST. Este marco, ampliamente reconocido

y adaptable, ofrece lineamientos que pueden ser instrumentalizados por organizaciones de cualquier tamaño para mejorar su postura de seguridad.

En este contexto, la presente investigación busca evaluar la viabilidad de adoptar el Marco NIST en el entorno de las PYMEs mexicanas como estrategia para fortalecer su ciber resiliencia, frente a la falta de protección normativa efectiva a nivel nacional.

1.3 Marco Conceptual

El presente marco conceptual establece los fundamentos teóricos y técnicos esenciales que sustentan esta investigación, centrada en la ciberresiliencia y la adopción del Marco de Ciberseguridad del NIST en pequeñas y medianas empresas (PYMEs) mexicanas. Se organiza en tres bloques temáticos para facilitar la comprensión y la coherencia lógica del análisis.

1.3.1 Actores principales

Pequeñas y Medianas Empresas (PYMEs)

De acuerdo con la Secretaría de Economía (2020), una PYME en México se define como una unidad económica con menos de 250 empleados y una facturación anual que no supera los 50 millones de pesos. Las PYMEs representan cerca del 99.8% del total de empresas en el país, generan aproximadamente el 70% del empleo formal y contribuyen con el 52% del PIB nacional (INEGI, 2020). Este sector, por tanto, constituye un pilar económico estratégico cuya protección digital adquiere una relevancia prioritaria en el contexto de la ciberseguridad.

Entornos Digitales y Transformación Tecnológica

Las PYMEs operan cada vez más en entornos digitales, adoptando tecnologías como servicios en la nube, plataformas de comercio electrónico y sistemas ERP/CRM. Esta transformación, aunque beneficiosa, también incrementa su superficie de exposición a riesgos

cibernéticos (OECD, 2021). Comprender este entorno digital es esencial para evaluar la aplicabilidad y eficacia de marcos como el del NIST.

1.3.2 Marcos de referencia y normativos

Ciberseguridad

La ciberseguridad se define como el conjunto de prácticas, procesos y tecnologías orientadas a proteger los sistemas informáticos, redes y datos frente a accesos no autorizados, daños o interrupciones (ENISA, 2020). En el contexto de las PYMEs, la ciberseguridad representa no solo una medida de protección, sino una condición crítica para la continuidad del negocio. Este concepto resulta clave para entender la necesidad de un enfoque sistemático como el que propone el marco NIST.

Marco de ciberseguridad de la NIST

El NIST Cybersecurity Framework (NIST, 2020) es un conjunto de directrices desarrollado por el National Institute of Standards and Technology de EE. UU., con el fin de mejorar la capacidad de las organizaciones para gestionar sus riesgos de ciberseguridad. Se estructura en cinco funciones clave:

Identificar: comprensión organizacional del riesgo cibernético.

Proteger: salvaguardas para asegurar la continuidad operativa.

Detectar: mecanismos para identificar incidentes.

Responder: procedimientos ante eventos de seguridad.

Recuperar: estrategias para restaurar capacidades afectadas.

El marco se destaca por su enfoque flexible, escalable y adaptable, lo que lo hace particularmente aplicable a entornos de recursos limitados como las PYMEs (NIST, 2020). Esta

investigación examina su adopción como una vía para fortalecer la ciberresiliencia en estas organizaciones.

Estándares Alterativos

Existen otras referencias internacionales relevantes como la familia ISO/IEC 27000, particularmente las normas ISO/IEC 27001 (gestión de seguridad de la información) e ISO/IEC 27005 (gestión de riesgos). No obstante, este estudio se centrará en el NIST por su carácter práctico y orientado a la mejora continua (ISO/IEC, 2018).

1.3.3 Riesgos y amenazas en ciberseguridad

Amenazas Cibernéticas

Las amenazas cibernéticas comprenden acciones maliciosas como el phishing, el ransomware, el acceso no autorizado, el robo de identidad digital o los ataques de denegación de servicio (DDoS). Las PYMEs, debido a limitaciones técnicas y presupuestales, son blanco frecuente de estos ataques (IBM Security, 2022). Estos escenarios justifican la necesidad de un marco que les permita anticipar, responder y recuperarse de incidentes.

Evaluación de Riesgos

La evaluación de riesgos consiste en identificar, analizar y priorizar los riesgos que podrían afectar los activos digitales de una organización. En el marco del NIST, esta evaluación es la base para establecer controles proporcionales al nivel de exposición y recursos disponibles (NIST, 2020). Para las PYMEs, una evaluación de riesgos clara y contextualizada es vital para tomar decisiones eficientes en materia de ciberseguridad.

Ciberresiliencia

La ciber resiliencia se define como la capacidad organizacional para anticipar, resistir, adaptarse y recuperarse frente a eventos adversos en el entorno digital (Linkov et al., 2013). Esta

noción, estrechamente vinculada con la función “Recuperar” del marco NIST, no solo implica reponer sistemas afectados, sino garantizar la continuidad del negocio en condiciones críticas. Para las PYMEs, la ciber resiliencia representa una dimensión estratégica que puede determinar su supervivencia ante ataques.

1.4 Competencias desarrolladas en la investigación

La presente investigación doctoral promueve el desarrollo de un conjunto de competencias investigativas, analíticas y estratégicas, orientadas a comprender y evaluar la aplicabilidad del Marco de Ciberseguridad del NIST en el contexto específico de las pequeñas y medianas empresas (PYMEs) mexicanas. Estas competencias son desarrolladas por el investigador en el transcurso del estudio, y articulan tanto el análisis teórico como la exploración empírica del objeto de estudio.

1.4.1 Competencia estratégica: evaluación e implementación contextual del marco NIST

Uno de los principales aportes de esta investigación es la capacidad para analizar la implementación del Marco de Ciberseguridad del NIST desde una perspectiva estratégica, más allá de una visión puramente técnica. Se desarrolla así la competencia para identificar cómo dicho marco puede fortalecer la gestión de riesgos cibernéticos en las PYMEs, adaptándolo a sus condiciones reales de operación, nivel de madurez digital y limitaciones presupuestarias. Esta competencia incluye la interpretación crítica de cada una de las funciones del marco (Identificar, Proteger, Detectar, Responder y Recuperar) en relación con la estructura operativa de las PYMEs.

1.4.2 Competencia comparativa: análisis crítico de marcos internacionales

La investigación también cultiva la competencia comparativa, mediante el análisis crítico del Marco NIST frente a otros estándares reconocidos internacionalmente, como la norma

ISO/IEC 27001 y los CIS Controls. Esta comparación no se limita a sus aspectos estructurales o normativos, sino que se orienta a evaluar su aplicabilidad práctica en organizaciones de distinto perfil. La identificación de fortalezas, debilidades y áreas de mejora en función del contexto operativo proporciona elementos clave para una selección informada del marco más adecuado según las necesidades de cada organización.

1.4.3 Competencia de transferencia sectorial: análisis de casos aplicados

A través del estudio de casos y entrevistas a actores relevantes, se desarrolla una competencia de análisis sectorial, centrada en identificar cómo el Marco NIST puede adaptarse a sectores específicos como el financiero, el sanitario y el gubernamental. Esta competencia se traduce en la capacidad de transferir conceptos y lineamientos del marco a entornos con distintos niveles de criticidad y requerimientos normativos, ajustando su aplicación sin perder coherencia metodológica ni eficacia operativa.

1.4.4 Competencia diagnóstica: identificación de desafíos de implementación

Una cuarta competencia clave es la capacidad diagnóstica para identificar los principales obstáculos que enfrentan las PYMEs en la implementación del Marco NIST. Esto incluye el análisis de barreras económicas, culturales, organizativas y técnicas que limitan la adopción de prácticas de ciberseguridad estructuradas. Asimismo, la investigación propone estrategias prácticas de superación de dichos retos, desarrollando así una competencia de solución de problemas que puede ser transferida a otros contextos organizativos con limitaciones similares.

1.5 Definiciones Operativas

En este apartado reúne las definiciones de los términos clave utilizados en la investigación, con el fin de asegurar claridad conceptual y operativa a lo largo del desarrollo de la tesis. Los conceptos aquí definidos permiten establecer un lenguaje común y uniforme en

torno a la ciberseguridad, facilitando la interpretación de los hallazgos y el análisis del marco NIST en el contexto específico de las pequeñas y medianas empresas (PYMEs) mexicanas.

Ciberataques

Un ciberataque se define como una intrusión no autorizada en un sistema informático y sus redes relacionadas. En las PYMEs, estos ataques pueden generar consecuencias críticas dada su limitada capacidad de respuesta (Iberdrola, 2021).

Ciberdelincuencia

La ciberdelincuencia puede definirse como la actividad delictiva en la que los ordenadores o las redes informáticas son una herramienta, un objetivo o un medio para cometer delitos. En el caso de las PYMEs, esta representa una amenaza creciente debido a la falta de protocolos de protección y formación especializada (Kaspersky, 2024).

Ciberespacio

El ciberespacio es un entorno virtual utilizado para la interconexión de redes informáticas y la comunicación en línea. Este espacio constituye el escenario en el que se desarrollan las amenazas cibernéticas que enfrentan las PYMEs (Ciberseguridad México, 2022).

Ciberseguridad

La ciberseguridad se define como un conjunto de mecanismos diseñados para proteger datos, redes y sistemas frente a la explotación no autorizada conocida como ciberataques (National Institute of Standards and Technology [NIST], 2021).

Evaluación de riesgos

La evaluación de riesgos se refiere a un proceso sistemático destinado a identificar, analizar y gestionar las amenazas potenciales que enfrenta una organización en materia de ciberseguridad, considerando la probabilidad de ocurrencia y el impacto que podrían generar.

Esta práctica permite priorizar acciones y mitigar los riesgos a niveles aceptables, siendo particularmente crítica en contextos de recursos limitados, como el de las PYMEs. Su implementación se alinea con los principios del Marco NIST, que promueve un enfoque estructurado y adaptable para la gestión de riesgos tecnológicos (Bodeau & Graubart, 2017).

Pequeñas y medianas empresas (PYMEs)

Para los fines de esta investigación, se adopta la clasificación propuesta por Lizarazo, en la que se define a las pequeñas empresas como aquellas que cuentan entre 9 y 49 empleados, y a las medianas como aquellas que poseen entre 50 y 99 trabajadores. Esta segmentación permite delimitar el universo de análisis con base en criterios operativos relevantes en el contexto latinoamericano (Lizarazo, 2023).

1.5.1 Comprensión lectora con el contexto técnico-normativo

La comprensión lectora, en el marco de esta investigación, se concibe como un proceso cognitivo complejo y activo, en el cual el lector no solo decodifica información técnica, sino que construye significado a través del análisis, la interpretación crítica y la aplicación contextual de los conocimientos. Tal como plantea Solé (1992), comprender un texto implica “elaborar una representación mental coherente del contenido”, lo cual requiere activar conocimientos previos, formular inferencias y establecer relaciones lógicas entre las ideas. Esta visión es particularmente relevante en estudios que abordan marcos normativos y técnicos como el de Ciberseguridad del NIST, cuya asimilación no puede limitarse a una lectura literal.

En sintonía con Cassany (2006), la comprensión lectora especializada requiere estrategias de lectura crítica, especialmente cuando el lector se enfrenta a textos técnicos, normativos o científicos, como ocurre en esta tesis. A través de esta lectura activa, se espera que el lector se

involucre en un diálogo con el texto, lo cuestione, confronte sus postulados con la realidad de su entorno profesional y derive acciones significativas a partir del conocimiento adquirido.

En el contexto específico de la ciberseguridad en las pequeñas y medianas empresas (PYMEs), esta competencia cobra especial relevancia. La lectura del presente estudio exige del lector una aproximación analítica rigurosa al Marco de Ciberseguridad del NIST, entendiendo su estructura, sus funciones y su aplicabilidad práctica. Esta lectura va más allá de la comprensión literal, y apunta al desarrollo de capacidades claves como:

Análisis contextual: Evaluar la pertinencia del Marco NIST en el entorno particular de las PYMES, considerando factores como tamaño organizacional, madurez tecnológica y cultura institucional.

Reflexión crítica: Identificar y analizar los obstáculos para la implementación del marco, tales como las restricciones presupuestarias o las barreras culturales internas (OCDE, 2022).

Aplicación práctica: Transferir los aprendizajes del marco a escenarios reales de gestión de la ciberseguridad en organizaciones con recursos limitados, contribuyendo a la construcción de una cultura preventiva y resiliente.

En esta línea, informes internacionales como los de OCDE-PISA han subrayado la importancia de la alfabetización informacional y digital como competencias fundamentales para el mundo del trabajo y la ciudadanía en entornos altamente tecnológicos. La capacidad para comprender, evaluar críticamente e integrar información técnica es indispensable para el fortalecimiento de la ciberresiliencia organizacional en un entorno digital en constante evolución.

Finalmente, esta comprensión no solo tiene un impacto individual, sino que se proyecta hacia una dimensión colectiva. Como señalan los enfoques socioculturales del aprendizaje

(Vygotsky, 1978; Gee, 2008), el lector se convierte en un agente activo en la creación y difusión del conocimiento, promoviendo prácticas organizacionales más seguras y fomentando una cultura de ciberseguridad que trascienda lo técnico para instalarse como un valor institucional compartido.

1.6 Marco Teórico

En el contexto actual de creciente exposición a amenazas cibernéticas, la ciberseguridad se ha convertido en un componente crítico para la sostenibilidad de las pequeñas y medianas empresas (PYMEs). Estas organizaciones, por su tamaño, recursos limitados y madurez tecnológica desigual, presentan una vulnerabilidad particular ante incidentes de seguridad informática (OCDE, 2022). En este marco, el Marco de Ciberseguridad del NIST surge como una herramienta estratégica para gestionar de forma integral los riesgos digitales, fortalecer la resiliencia organizacional y promover una cultura de seguridad adaptada al entorno de las PYMES.

1.6.1 El Marco NIST: estructura, aplicabilidad y pertinencia

El Marco de Ciberseguridad del NIST se compone de tres partes principales: el Core (funciones y subcategorías), los Tiers (niveles de madurez) y los Profiles (perfiles de riesgo). Su enfoque flexible y adaptable permite a las organizaciones implementar controles de acuerdo con sus capacidades, perfil de riesgo y prioridades específicas (NIST, 2018).

A diferencia de otros marcos como ISO/IEC 27001, que exige certificaciones formales, o CIS Controls, que presenta una lista exhaustiva de controles técnicos, el NIST se distingue por su enfoque basado en funciones (Identificar, Proteger, Detectar, Responder, Recuperar), lo que lo hace especialmente adecuado para el contexto de las PYMES mexicanas, caracterizado por

presupuestos limitados, estructuras organizacionales horizontales y escasa profesionalización de la gestión de TI.

Autores como Whitman y Mattord (2022) destacan que el éxito en la implementación de marcos de seguridad depende no solo de los controles técnicos, sino de la madurez organizacional y de la cultura de seguridad existente. En este sentido, Von Solms y Van Niekerk (2013) proponen que la ciberseguridad debe entenderse como un proceso organizacional continuo, vinculado estrechamente a la gobernanza, la toma de decisiones y el comportamiento humano frente a las amenazas. En la Figura 5 vemos los niveles de seguridad que aporta la metodologia de la NIST.

Figura 5.

Niveles del marco de seguriddad de la NIST.



Nota: Niveles de implementación del CFS, NIST (2020).

En la Figura 5 se ilustran los cuatro niveles de madurez del Marco NIST, los cuales permiten a las organizaciones autoevaluar su capacidad de gestión de riesgos y orientar sus estrategias de mejora continua en función de su contexto operativo y nivel de preparación. Esta figura, titulada 'Niveles del marco de seguridad del NIST', detalla la progresión desde un estado inicial y menos maduro hasta uno más avanzado y adaptable en la gestión de la ciberseguridad.

El 'Nivel 1: Parcial' se caracteriza por una gestión de riesgos ad hoc, un conocimiento limitado de los riesgos de ciberseguridad y una baja participación externa. A medida que las organizaciones avanzan, el 'Nivel 2: Riesgo Informado' muestra la implementación de algunas prácticas de gestión de riesgos, un aumento de la concienciación y una participación de terceros de manera informal. El 'Nivel 3: Repetible' denota una gestión de riesgos formalizada, la existencia de programas transversales a la organización y una gestión estructurada de la información de terceros. Finalmente, el 'Nivel 4: Adaptativo' representa el nivel más maduro, donde las prácticas se basan en lecciones aprendidas, se busca la mejora continua y existe una colaboración activa con terceros.

1.6.2 Cultura de seguridad y resiliencia organizacional

La cultura de seguridad se refiere al conjunto de valores, creencias y prácticas compartidas dentro de una organización que determinan cómo se perciben y gestionan los riesgos tecnológicos. Tal como argumentan Bada et al. (2019), en entornos con escasa cultura de seguridad, incluso los marcos más robustos pueden fracasar en su implementación.

Este aspecto se relaciona directamente con la resiliencia organizacional, entendida como la capacidad de anticiparse, responder y recuperarse eficazmente de eventos disruptivos. Según Lengnick-Hall et al. (2011), esta competencia implica flexibilidad estructural, aprendizaje adaptativo y liderazgo comprometido. Por su parte, Mallak (1998) enfatiza que las organizaciones resilientes desarrollan mecanismos internos de adaptación que les permiten sobrevivir a contextos de incertidumbre, como los generados por amenazas cibernéticas.

El Marco NIST, al incluir funciones de respuesta y recuperación, se alinea de manera natural con esta perspectiva resiliente, promoviendo una visión integral que trasciende la prevención para abarcar también la continuidad operativa.

1.6.3 Gestión de riesgos cibernéticos

La gestión de riesgos es otro pilar del Marco NIST, cuyo objetivo es identificar, evaluar y mitigar riesgos tecnológicos de forma sistemática. Según Hillson (2009), una gestión de riesgos efectiva debe considerar tanto la probabilidad como el impacto de los eventos, integrando análisis cuantitativos y cualitativos. ISO (2018) define la gestión de riesgos como un proceso que debe estar alineado con la estrategia organizacional, lo cual es particularmente relevante para las PYMES, donde las decisiones técnicas suelen estar ligadas directamente a la supervivencia económica.

1.6.4 Comprensión lectora y alfabetización digital como competencias clave

La implementación efectiva del Marco NIST requiere que los actores dentro de la organización —especialmente los responsables de TI y los directivos— comprendan e interpreten adecuadamente las directrices del marco, para luego adaptarlas a su realidad operativa. Esta capacidad está directamente relacionada con la alfabetización digital, entendida como la habilidad para localizar, evaluar, utilizar y comunicar información mediante tecnologías digitales (Gilster, 1997).

Asimismo, la comprensión lectora crítica se vuelve indispensable. Según Cassany (2006) y Solé (1992), leer comprensivamente implica no solo decodificar el texto, sino analizar, inferir, evaluar y aplicar la información. En el ámbito de la ciberseguridad, estas competencias permiten una apropiación significativa del conocimiento técnico y normativo, como el que propone el NIST. Estudios como los informes PISA (OCDE, 2022) han demostrado que el nivel de alfabetización informacional está directamente vinculado con la capacidad de los individuos para adaptarse a entornos laborales complejos y tecnológicamente intensivos.

1.6.5 Vinculación con el contexto mexicano

Las PYMES mexicanas enfrentan desafíos particulares como falta de sensibilización, ausencia de políticas internas de ciberseguridad, baja inversión en tecnología, y carencia de personal especializado. La adopción del Marco NIST permite priorizar acciones según el perfil de riesgo y los recursos disponibles, lo que lo hace especialmente funcional para este tipo de organizaciones.

Por ejemplo, muchas PYMES operan sin sistemas formales de respaldo o monitoreo, por lo que comenzar con funciones básicas como “Identificar” y “Proteger” puede representar un punto de entrada realista. La escalabilidad del marco también facilita que las organizaciones maduren progresivamente, pasando de un nivel de riesgo parcial a uno informado o repetible.

Implementar las categorías y subcategorías de acuerdo con sus recursos, su perfil de riesgo y sus necesidades específicas. La teoría de la escalabilidad y la adecuación de las prácticas de seguridad a las características organizacionales son fundamentales para comprender cómo las PYMEs pueden beneficiarse de la implementación selectiva y gradual del Marco NIST.

La comprensión lectora se centra en la capacidad de los actores relevantes dentro de las PYMEs (directivos, personal de TI, etc.) para interpretar, aplicar y adaptar los principios y las directrices del Marco de Ciberseguridad del NIST a su entorno organizacional específico. La efectividad de esta comprensión lectora es un factor crítico para la adopción exitosa y la mejora continua de la postura de ciberseguridad de las PYMEs.

1.6.6 Definición de conceptos clave del Marco de Ciberseguridad del NIST en el contexto de las PYMES

El Marco de Ciberseguridad del NIST (National Institute of Standards and Technology, 2018) establece un enfoque estructurado para gestionar riesgos digitales a través de cinco

funciones básicas: Identificar, Proteger, Detectar, Responder y Recuperar. Estas funciones integran principios clave de la gestión de riesgos, seguridad de la información y resiliencia organizacional, y su comprensión es esencial para la adopción efectiva del marco, especialmente en contextos como el de las pequeñas y medianas empresas (PYMES), donde los recursos y capacidades técnicas suelen ser limitados.

1.6.7 Información como activo crítico (Función Identificar)

En el marco NIST, la función "Identificar" parte del reconocimiento de la información como un activo crítico que sustenta la operación y competitividad de las organizaciones (NIST, 2018). Esto implica inventariar los sistemas, datos y recursos esenciales, así como establecer su nivel de criticidad. En el contexto de una PYME, esto puede incluir desde bases de datos de clientes hasta sistemas de facturación o propiedad intelectual digital. Tal como señalan Bodeau y Graubart (2017), la identificación precisa de activos permite priorizar la protección de aquellos cuya pérdida impactaría severamente la continuidad del negocio.

1.6.8 Procesamiento y protección de la información (Funciones Proteger y Detectar)

Las funciones "Proteger" y "Detectar" implican establecer salvaguardas para garantizar la confidencialidad, integridad y disponibilidad de la información durante su ciclo de vida (recolección, procesamiento, almacenamiento y transmisión). Esto abarca controles de acceso, segmentación de redes, cifrado de datos y mecanismos de monitoreo continuo. Según la NIST Special Publication 800-53 (NIST, 2020), la implementación efectiva de estos controles requiere no solo infraestructura, sino también una comprensión clara de los riesgos y amenazas por parte del personal operativo.

En el entorno PYME, es común que estas medidas se vean obstaculizadas por la falta de personal especializado, lo que puede derivar en implementaciones incompletas o mal

configuradas (Whitman & Mattord, 2022). Por ejemplo, una empresa que utiliza sistemas heredados sin políticas de actualización y sin firewall activo se vuelve especialmente vulnerable a ataques de ransomware.

1.6.9 Ciberseguridad como sistema de protección (Introducción al Marco)

La ciberseguridad, dentro del enfoque del NIST, se define como el conjunto de prácticas, políticas y herramientas diseñadas para proteger los sistemas de información frente a accesos no autorizados y otros vectores de amenaza (NIST, 2018). Este concepto incluye no solo medidas tecnológicas, sino también factores humanos, organizacionales y normativos, como lo destacan von Solms & van Niekerk (2013) al señalar que la cultura de seguridad influye directamente en la efectividad de las estrategias adoptadas. En la Figura 6 se muestra las fases a nivel perfil del marco NIST.

Figura 6.

Fases del marco de la seguridad de la NIST a nivel perfil.



Nota: Perfil de Marco de Seguridad Cibernética (CSF), NIST (2020)

La Figura 6 presenta de forma esquemática los componentes principales del Marco NIST, facilitando su comprensión y aplicación en entornos organizacionales como las PYMES. Titulada 'Fases del marco de la seguridad de la NIST a nivel perfil', esta figura es crucial para entender cómo se operativiza el Marco de Seguridad Cibernética (CSF) del NIST a través de un proceso de cinco pasos clave que culmina en la creación y actualización de un perfil de

ciberseguridad organizacional. La figura ilustra, por un lado, el ciclo de vida central del marco (Identificar, Proteger, Detectar, Responder, Recuperar y Gobernar), y por otro, la secuencia lógica para su implementación: 1) Definir el Alcance del perfil organizativo, 2) Recopilar la información necesaria para dicho perfil, 3) Crear el perfil organizativo en sí mismo, 4) Analizar las brechas existentes entre el estado actual y el deseado para crear un plan de acción, y 5) Implementar el plan de acción y actualizar el perfil de manera continua.

1.6.10 Vulnerabilidades y ciberataques (Funciones Identificar y Detectar)

Las funciones "Identificar" y "Detectar" permiten reconocer las vulnerabilidades —debilidades técnicas o procedimentales— que pueden ser explotadas en ciberataques. Linkov et al. (2013) proponen un enfoque sistémico para entender cómo múltiples vulnerabilidades interconectadas pueden escalar rápidamente en eventos disruptivos. En PYMES, estas vulnerabilidades suelen incluir contraseñas débiles, configuraciones por defecto, o falta de capacitación del personal, lo cual incrementa la superficie de ataque.

1.6.11 Resiliencia cibernética (Función Recuperar)

La función "Recuperar" se orienta al fortalecimiento de la resiliencia cibernética, entendida como la capacidad organizacional para absorber, responder y recuperarse de incidentes digitales (Lengnick-Hall et al., 2011). En el marco NIST, esto se traduce en la implementación de planes de respuesta ante incidentes, copias de respaldo seguras y pruebas periódicas de recuperación. Para una PYME, tener una política básica de continuidad del negocio —como respaldar datos clave en la nube y asignar responsables claros de recuperación— puede marcar la diferencia entre la supervivencia y el colapso ante un ataque.

1.6.12 La alfabetización digital como habilitador organizacional

La comprensión efectiva de estos conceptos técnicos por parte del personal de las PYMES requiere niveles mínimos de alfabetización digital e informacional. Según Gilster (1997), la alfabetización digital implica no solo el acceso a tecnologías, sino la capacidad crítica para evaluar, interpretar y aplicar información digital en contextos reales. Organismos como la UNESCO (2011) y la ACRL (2016) han reforzado esta noción, indicando que las competencias informacionales son clave para la toma de decisiones en entornos complejos. En este sentido, incluso el mejor marco —como el NIST— puede resultar ineficaz si el personal no cuenta con las herramientas cognitivas y técnicas para implementarlo correctamente.

1.7 Estado del arte

La presente investigación se sitúa en la intersección de tres áreas clave: la ciberresiliencia en las Pequeñas y Medianas Empresas (PYMEs), la implementación de marcos normativos de ciberseguridad, y la gestión de riesgos en contextos organizacionales con limitados recursos tecnológicos y humanos.

Diversos estudios han documentado la creciente exposición de las PYMEs a amenazas cibernéticas, especialmente por la escasa inversión en tecnologías de seguridad, la baja cultura organizacional en torno a la ciberseguridad y la falta de personal especializado (ENISA, 2021; Ramírez et al., 2020). Según López et al. (2020), la aplicación del Marco NIST en PYMEs chilenas permitió reducir los tiempos de respuesta ante incidentes en un 35 %, evidenciando su utilidad incluso en entornos con restricciones presupuestarias.

El Marco de Ciberseguridad del NIST ha emergido como un referente flexible y escalable, aplicable tanto en grandes corporaciones como en pequeñas organizaciones. Autores como Linkov et al. (2013) destacan su enfoque basado en funciones (Identificar, Proteger,

Detectar, Responder y Recuperar), lo cual facilita su adopción gradual. Su estructura permite a las empresas alinear sus prácticas de seguridad con un enfoque sistemático de gestión de riesgos, sin requerir una certificación formal, a diferencia de normas más estrictas como ISO/IEC 27001.

En paralelo, la pirámide KEOPS (Castillo & Morales, 2017) ha sido propuesta como una herramienta complementaria que permite evaluar la madurez de seguridad de una organización a través de capas (infraestructura, procesos, políticas y cultura). A diferencia del NIST, KEOPS enfatiza una visión más diagnóstica que normativa, centrada en medir el grado de implementación de controles específicos. Mientras el Marco NIST orienta a la acción estratégica, KEOPS permite una radiografía del estado actual de las prácticas de seguridad, siendo útil para la planificación de mejoras. Esta investigación explora su uso conjunto como mecanismo integrador de diagnóstico y fortalecimiento progresivo.

Si bien existen estudios sobre la implementación del NIST en empresas norteamericanas y europeas (Whitman & Mattord, 2022; Von Solms & Van Niekerk, 2013), aún se observa un vacío importante en el análisis de su aplicación en PYMES latinoamericanas, particularmente en México. La literatura también es limitada en cuanto al estudio de variables culturales y niveles de alfabetización digital como factores condicionantes para la adopción efectiva de marcos de seguridad (Gilster, 1997; UNESCO, 2021).

En consecuencia, la presente investigación se propone abordar este vacío, examinando cómo el Marco NIST y la pirámide KEOPS pueden adaptarse e implementarse en PYMES mexicanas, tomando en cuenta factores como la cultura organizacional, la madurez tecnológica y las competencias digitales del personal. Se busca así contribuir al entendimiento integral de la gestión de riesgos cibernéticos desde una perspectiva contextualizada y práctica, que permita

diseñar estrategias sostenibles de ciberresiliencia. Tal como se presenta en la Figura 7 que detalla el nivel de escalabilidad de seguridad de la pirámide de KEOPS.

Figura 7.

Niveles de escala de seguridad de una empresa representado como pirámide de KEOPS.



Nota: La Pirámide KEOPS de Ciberseguridad, LINKA (2021).

Para ofrecer una perspectiva complementaria sobre la implementación práctica de las funciones del Marco NIST en entornos empresariales, se presenta a continuación la Figura 7, titulada 'Niveles de escala de seguridad de una empresa representado como pirámide de KEOPS'. Esta pirámide, propuesta por LINKA (2021), ilustra de manera jerárquica las capas de protección que una organización debe implementar para alcanzar una ciberseguridad robusta, comenzando por los fundamentos esenciales hasta llegar a la monitorización avanzada.

1.7.1 Definición de "estándar" y su relación con el Marco NIST

En términos generales, un estándar es un documento de referencia que establece lineamientos técnicos, procedimientos o prácticas reconocidas y validadas para lograr resultados óptimos en un área específica. En el contexto de la ciberseguridad, los estándares ofrecen un conjunto sistemático de buenas prácticas, requisitos técnicos y recomendaciones que permiten proteger activos digitales, reducir riesgos y garantizar la continuidad operativa (ISO/IEC, 2022; MinTIC, 2023).

A diferencia de los marcos normativos obligatorios, los estándares pueden ser voluntarios, aunque adoptarlos mejora la seguridad, la eficiencia y la confiabilidad de los sistemas. Estos documentos suelen elaborarse mediante consenso internacional, como en el caso de ISO/IEC 27001 o NIST SP 800-53, lo que les otorga legitimidad y aplicabilidad transversal.

1.7.1.1 Relevancia de los estándares para las PYMES.

En el caso de las PYMES, los estándares en ciberseguridad adquieren especial relevancia al ofrecer guías accesibles y escalables para fortalecer su protección digital, aun sin contar con grandes presupuestos ni personal especializado. La posibilidad de implementar medidas de forma progresiva, en función del nivel de madurez organizacional, los convierte en herramientas estratégicas para este tipo de empresas (Bada et al., 2019).

Adoptar un estándar permite a las PYMES establecer políticas mínimas, fortalecer la conciencia del personal y aplicar controles básicos como autenticación, respaldos o segmentación de red, sin requerir estructuras complejas. Por ejemplo, una pequeña empresa puede empezar por implementar políticas de contraseñas fuertes y capacitación básica del personal, como sugiere el Marco NIST, para luego avanzar hacia controles más complejos como segmentación de red o monitoreo continuo.

1.7.1.2 El Marco NIST frente a otros estándares.

El Marco de Ciberseguridad del NIST (National Institute of Standards and Technology) se presenta como un marco de referencia flexible y no prescriptivo, diseñado para guiar a las organizaciones —incluidas las PYMES— en la gestión de riesgos cibernéticos. Está estructurado en cinco funciones básicas: Identificar, Proteger, Detectar, Responder y Recuperar (NIST, 2018). Su ventaja radica en que integra y refiere otros estándares técnicos (como ISO/IEC 27001, COBIT o CIS Controls), permitiendo que cada empresa lo adapte a su realidad.

A continuación, se presenta la Tabla 1 un cuadro comparativo para resaltar sus diferencias clave:

Tabla 1.

Diferencias Clave de la NIST comparado a otros estándares técnicos.

Característica	NIST CSF	ISO/IEC 27001	COBIT	CIS Controls
Tipo de instrumento	Marco de referencia	Norma certificable	Marco de gobierno de TI	Conjunto de controles técnicos
Certificación requerida	No	Sí	No (aunque puede usarse con certificación)	No
Flexibilidad	Alta	Moderada	Alta	Moderada
Costos de implementación	Bajos a medios	Altos	Medios	Bajos
Orientado a PYMES	Sí	Requiere adaptación	Menos orientado	Sí
Enfoque	Gestión de riesgos	Sistema de gestión (SGSI)	Gobierno corporativo	Controles priorizados

Característica	NIST CSF	ISO/IEC 27001	COBIT	CIS Controls
Aplicación progresiva	Sí	Limitada	Sí	Sí

Fuente: Adaptado de NIST (2018), ISO (2022), ISACA (2020), CIS (2021).

Como se observa, el NIST resulta más adecuado para PYMES por su enfoque gradual, no prescriptivo y por no requerir certificación formal. Esto permite iniciar con una autoevaluación básica y escalar conforme madure la organización.

1.7.1.3 Ejemplo práctico de aplicación en una PYME.

Imaginemos una empresa mexicana del sector comercial con diez empleados y sin personal de TI dedicado. Al aplicar el Marco NIST:

En la función Identificar, reconoce como activos críticos su sistema de facturación electrónica y la base de datos de clientes.

En Proteger, establece contraseñas robustas, capacita al personal en phishing y configura respaldos automáticos.

En Detectar, utiliza software antivirus gratuito y revisa periódicamente logs de acceso.

En Responder, crea un procedimiento básico ante incidentes (ej. bloqueo inmediato de cuentas comprometidas).

En Recuperar, prueba la restauración de respaldos una vez al mes.

Este ejemplo muestra cómo una PYME puede utilizar el Marco NIST sin necesidad de una inversión inicial elevada, enfocándose en acciones concretas y adaptadas a sus capacidades, pero alineadas con estándares internacionales.

1.7.2 El Marco de Ciberseguridad del NIST y su Aplicación en PYMES mexicanas

El l Marco de Ciberseguridad del National Institute of Standards and Technology (NIST) constituye el eje metodológico de esta investigación, al ofrecer una guía estructurada para gestionar los riesgos asociados a las amenazas cibernéticas. Su diseño modular y adaptable lo convierte en una herramienta especialmente relevante para las pequeñas y medianas empresas (PYMES), al permitir su implementación progresiva de acuerdo con las capacidades y necesidades de cada organización (NIST, 2018).

A diferencia de otros marcos como ISO/IEC 27001 o COBIT, el Marco NIST no exige procesos de certificación formales ni presupuestos elevados, lo cual facilita su adopción en entornos con recursos limitados. Mientras ISO/IEC 27001 se enfoca en la creación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en procesos y requiere auditorías externas para su validación (ISO/IEC, 2013), el NIST promueve un enfoque más flexible, orientado a resultados y adaptable a diversos sectores y contextos organizativos (Gordon et al., 2020). Asimismo, en contraste con COBIT, que enfatiza el gobierno de TI a nivel corporativo (ISACA, 2012), el Marco NIST ofrece directrices operativas más prácticas para la gestión del riesgo cibernético.

El núcleo del Marco —denominado Framework Core— se estructura en cinco funciones fundamentales: Identificar, Proteger, Detectar, Responder y Recuperar, las cuales representan fases clave del ciclo de gestión de incidentes de seguridad. Estas funciones se subdividen en 23 categorías, y a su vez en 108 subcategorías, que articulan objetivos específicos de seguridad. Cada subcategoría se vincula con estándares reconocidos internacionalmente, como NIST SP 800-53, ISO/IEC 27001, COBIT o los CIS Controls (NIST, 2018). En la figura 8 se detalla las funciones de NIST.

Figura 8.

El marco de ciberseguridad NIST muestra sus cinco funciones clave



Nota: NIST Releases Version 1.1 Of Its Popular Cybersecurity Framework, NIST (2022).

La Figura 8 sintetiza visualmente los niveles de implementación del Marco NIST, facilitando su comprensión y adaptación progresiva en entornos PYME. Bajo el título 'El marco de ciberseguridad NIST muestra sus cinco funciones clave', esta figura representa el corazón del Cybersecurity Framework (CSF) en su Versión 1.1, delineando de forma clara y concisa sus cinco funciones esenciales e interconectadas: IDENTIFY (Identificar), PROTECT (Proteger), DETECT (Detectar), RESPOND (Responder) y RECOVER (Recuperar). A diferencia de figuras anteriores que mostraban las fases a nivel perfil o los niveles de madurez, esta ilustración se enfoca puramente en las funciones centrales que guían toda la gestión de ciber riesgos.

Complementariamente, el Marco propone una herramienta de autoevaluación denominada Niveles de Implementación, que permite a las organizaciones clasificar su madurez en la gestión del riesgo en cuatro niveles: (1) Parcial, (2) Informado sobre el riesgo, (3)

Repetible, y (4) Adaptativo. Esta evaluación proporciona una guía útil para establecer hojas de ruta de mejora continua (Linkov et al., 2013). Tal como se muestra en la Tabla 2.

Tabla 2.

Cuadro donde se comparan las funciones de la NIST y el nivel de cada categoría.

Función	**Categoría Ejemplo**	**Subcategoría**	**Nivel 1: Parcial**	**Nivel 4: Adaptativo**
Identificar	Gestión de Activos	Inventario actualizado de recursos TI	No existe inventario formal	Inventario automático y actualizado en tiempo real
Proteger	Concientización y Capacitación	Formación continua del personal	Formación ocasional	Programas sistemáticos, medibles y personalizados
Detectar	Anomalías y Eventos	Detección de accesos inusuales	No se detectan eventos	Detección automatizada y análisis de comportamiento
Responder	Planes de Respuesta	Procedimientos para respuesta a incidentes	Reacción ad hoc	Planes formalizados, testeados y comunicados
Recuperar	Planes de Recuperación	Restauración de datos tras incidentes	No hay respaldo	Recuperación automática y documentada

Fuente: Adaptado de NIST (2018) y Gordon et al. (2020)

Desde una perspectiva aplicada, este marco resulta pertinente para las PYMES mexicanas debido a su flexibilidad, escalabilidad y orientación práctica. Por ejemplo, una pequeña empresa del sector comercio puede comenzar identificando activos críticos mediante inventarios básicos

en hojas de cálculo (función Identificar), implementar contraseñas robustas y segmentación de red básica (función Proteger), y establecer procedimientos de respaldo en dispositivos externos desconectados de la red (función Recuperar). Estas acciones, aunque limitadas, permiten avanzar hacia niveles superiores de madurez y reducir significativamente la superficie de exposición a ciberataques (Bodeau & Graubart, 2017).

No obstante, la adopción del Marco en PYMES enfrenta desafíos relevantes. Entre ellos destacan: la escasez de personal con formación en ciberseguridad, la baja cultura digital organizacional, la informalidad de los procesos internos y las restricciones presupuestarias (Bada et al., 2019; Gilster, 1997). Aun así, el Marco NIST incorpora principios de adaptabilidad y mejora incremental que permiten su implementación gradual. Por ejemplo, no requiere una adopción integral inmediata, sino que cada organización puede seleccionar subcategorías clave como punto de partida y expandir su cobertura en función de sus capacidades y riesgos prioritarios.

Desde el punto de vista de la madurez organizacional, la aplicación del Marco también puede integrarse con modelos como el Baldrige Cybersecurity Excellence Builder, que permite vincular la gestión de seguridad con dimensiones clave del desempeño organizacional, como liderazgo, satisfacción del cliente y resultados operativos (NIST, 2017). Estudios como el de Teodoro y Gonçalves (2015) proponen además metodologías para evaluar la brecha entre el estado actual y el deseado de ciberseguridad, facilitando la priorización de recursos limitados y el monitoreo de avances.

1.7.3 La Pirámide de Keops como Analogía Evolutiva de Madurez en Ciberseguridad

La pirámide de Keops, adaptada como analogía conceptual a partir de la jerarquía de necesidades de Maslow (1943), se ha utilizado en ciberseguridad para ilustrar cómo las

organizaciones avanzan progresivamente hacia niveles más elevados de protección, conciencia y resiliencia. Esta figura propone un enfoque multinivel y evolutivo, donde cada etapa de madurez debe consolidarse antes de aspirar a niveles superiores. Su valor reside en representar el desarrollo de la seguridad no solo como una cuestión tecnológica, sino como un proceso de maduración cultural, estructural y estratégica (Randstad, 2024).

A diferencia de modelos normativos como el Marco NIST, que define funciones operativas estructuradas (Identificar, Proteger, Detectar, Responder, Recuperar), la pirámide de Keops enfatiza la evolución de la conciencia organizacional y el compromiso progresivo con la ciberseguridad. En este sentido, puede considerarse un complemento útil para diagnosticar el nivel de motivación, cultura y gobernanza en seguridad, especialmente en contextos como el de las PYMES mexicanas, donde los recursos son limitados pero las amenazas crecientes. Tal como se muestra en la Tabla 3.

Tabla 3.

Niveles de evolución sobre la pirámide de seguridad.

Nivel	Nombre	Descripción	Ejemplo en PYMES mexicanas
1	**Supervivencia**	Reacción ante incidentes básicos sin planificación formal.	Uso de antivirus gratuito, sin respaldo de datos ni políticas.
2	**Protección reactiva**	Se toman acciones tras un incidente o recomendación externa.	Instalan firewall básico tras sufrir un ciberataque.

Nivel	Nombre	Descripción	Ejemplo en PYMES mexicanas
3	**Gestión de la seguridad**	Se establecen roles, procedimientos y controles básicos.	Se asigna un responsable TI, con respaldo periódico y contraseñas seguras.
4	**Conciencia y formación**	Cultura organizacional de seguridad y capacitación continua.	Talleres internos de concienciación y políticas activas de acceso.
5	**Ciberresiliencia estratégica**	La seguridad se integra en la visión de negocio y procesos críticos.	Análisis regular de riesgos, adopción del Marco NIST y simulacros.

Fuente: Niveles de la pirámide en ciberseguridad,adaptación basada en INCIBE (2020)

Este modelo permite visualizar cómo una PYME puede transitar desde una cultura de reacción y desinformación hasta una cultura preventiva y estratégica. Por ejemplo, una pequeña empresa de servicios contables puede iniciar en el nivel 1, sin controles formales, y, tras un incidente de ransomware, avanzar al nivel 2 con la instalación de soluciones de seguridad básicas. Con el tiempo, podría escalar hacia el nivel 3 al definir políticas de respaldo y roles de ciberseguridad, hasta eventualmente integrar la ciberseguridad como un componente transversal de su estrategia organizacional (nivel 5).

1.7.3.1 Relación con el Marco NIST.

Si bien el Marco NIST estructura la gestión de la ciberseguridad mediante funciones operativas, la pirámide de Keops ofrece una visión complementaria desde la madurez organizacional. Por ejemplo:

El nivel 1 de la pirámide se vincula con un nivel "Parcial" de implementación NIST, donde no hay formalidad ni conciencia organizacional.

El nivel 3 corresponde a un nivel "Informado sobre el riesgo", donde ya se aplican controles sistemáticos.

El nivel 5 se alinea con un nivel "Adaptativo", en el que la organización aprende, se adapta y mejora continuamente (NIST, 2018; Bodeau & Graubart, 2017).

Ambos modelos, por tanto, pueden coexistir como instrumentos diagnósticos complementarios: el NIST desde una perspectiva técnica y funcional, y la pirámide desde una visión de evolución cultural y estratégica.

1.7.3.2 Utilidad para PYMES mexicanas.

La utilidad de la pirámide radica en su accesibilidad y carácter pedagógico. Sirve como herramienta visual y comprensible para equipos directivos no especializados, permitiendo identificar de forma intuitiva el estado actual de su empresa y las brechas a superar. Además, puede guiar la asignación progresiva de recursos, adaptando las acciones de ciberseguridad al nivel de madurez alcanzado, sin imponer modelos rígidos o costosos desde el inicio.

Finalmente, esta analogía ha sido reconocida en informes de entidades como INCIBE (2020) y en investigaciones sobre cultura organizacional en ciberseguridad (Bada et al., 2019), que subrayan la necesidad de transformar la percepción empresarial de la seguridad como gasto operativo hacia una visión estratégica de resiliencia y sostenibilidad.

2. Diseño metodológico

Esta investigación se enmarcó en un enfoque de tipo mixto, combinando métodos cuantitativos y cualitativos para analizar la ciberresiliencia en las pequeñas y medianas empresas (PYMEs) mexicanas. La decisión de adoptar esta metodología respondió a la necesidad de capturar tanto los patrones mensurables de adopción del Marco de Ciberseguridad del NIST como las percepciones, experiencias y desafíos de los actores involucrados.

El enfoque mixto permitió realizar una triangulación de datos, proporcionando una visión más holística del fenómeno. Según Creswell y Plano-Clark (2018), este enfoque potencia la profundidad del análisis al integrar evidencias numéricas con testimonios narrativos, evitando los sesgos propios de enfoques unidimensionales.

-Objetivos metodológicos

E La investigación se propuso:

Medir el grado de implementación y madurez de las funciones del Marco NIST en PYMES mexicanas.

Explorar las percepciones y estrategias adoptadas por estas organizaciones ante amenazas cibernéticas.

Determinar las brechas entre prácticas reales y los lineamientos del marco NIST, especialmente en funciones subrepresentadas como “Responder” y “Recuperar”.

-Técnicas y herramientas de recolección

En el componente cuantitativo, se aplicaron encuestas estructuradas a responsables de TI o gerencia general en PYMES. Se utilizaron escalas de madurez basadas en los niveles propuestos por el NIST (2021), lo cual permitió evaluar el grado de implementación de cada función del marco (Identificar, Proteger, Detectar, Responder y Recuperar).

En el componente cualitativo, se desarrollaron entrevistas semiestructuradas y grupos focales con actores clave del ecosistema PYME (directores, consultores, especialistas en TI). Esto permitió comprender las motivaciones, limitaciones y estrategias de ciberseguridad desde una perspectiva contextual.

-Estructura del Marco de Ciberseguridad del NIST

El estudio se apoyó metodológicamente en el Marco de Ciberseguridad del NIST (2021), que propone cinco funciones básicas:

Identificar: Establecer conocimiento del entorno organizacional, activos, procesos y riesgos para priorizar medidas de seguridad.

Proteger: Implementar salvaguardas como control de acceso, formación del personal, protección de datos y mantenimiento seguro.

Detectar: Monitorizar eventos y anomalías que permitan identificar incidentes de forma oportuna.

Responder: Desarrollar capacidades para contener el impacto de ciberataques, comunicarse internamente y realizar mejoras posts-incidentes.

Recuperar: Restaurar operaciones tras un incidente, incluyendo planes de recuperación y mejoras continuas.

Estas funciones, aplicadas originalmente a infraestructuras críticas en EE.UU., se adaptaron al contexto de las PYMES mexicanas, considerando su realidad tecnológica y presupuestaria.

-Relevancia del marco para las PYMES

Se constató que muchas PYMES carecían de un enfoque estructurado en ciberseguridad, centrándose mayormente en medidas reactivas o tecnológicas. Las funciones de Respuesta y Recuperación, en particular, resultaron ser las menos desarrolladas, pese a que IBM Security

(2020) demostró que contar con planes de respuesta reduce significativamente los costos de las brechas de seguridad.

La aplicación del Marco NIST permitió visibilizar estas brechas y facilitó la propuesta de un esquema adaptado a las PYMES, considerando factores organizacionales, humanos y tecnológicos.

-Contribución de la metodología mixta

El enfoque mixto permitió identificar patrones relevantes (como la relación entre cultura organizacional y capacidad de respuesta), que no hubieran sido perceptibles mediante un solo método. Además, posibilitó proponer recomendaciones dirigidas tanto a empresas como a instituciones gubernamentales y organismos de apoyo empresarial.

La investigación no solo reconfirmó hallazgos de estudios previos, sino que también aportó nuevos conocimientos sobre la ciberresiliencia en PYMES desde una perspectiva latinoamericana, ofreciendo una base sólida para futuros estudios e intervenciones en el campo.

2.1 Enfoque Metodológico

La presente investigación adoptó un enfoque metodológico mixto con diseño explicativo secuencial, combinando fases cuantitativas y cualitativas para analizar la ciberresiliencia de las PYMEs mexicanas en relación con la adopción del Marco de Ciberseguridad del NIST. Este enfoque fue elegido por su capacidad de proporcionar una comprensión integral del fenómeno, permitiendo no solo medir el nivel de implementación de las funciones del Marco NIST, sino también explorar las percepciones, barreras y dinámicas organizacionales que inciden en dicho proceso.

De acuerdo con Creswell y Plano Clark (2018), el enfoque mixto integra de manera intencional la recopilación y el análisis de información cuantitativa y cualitativa con el propósito

de examinar un problema de investigación desde diferentes perspectivas. En esta investigación, se empleó primero un levantamiento de datos cuantitativos a través de encuestas estructuradas dirigidas a responsables de seguridad en PYMEs, lo cual permitió medir variables como el nivel de madurez, sector económico, tamaño de la empresa, frecuencia de incidentes y grado de implementación de controles. Posteriormente, se realizó una fase cualitativa mediante entrevistas semiestructuradas, cuyo propósito fue profundizar en las causas subyacentes de los patrones detectados, así como interpretar los desafíos humanos y organizacionales asociados a la gestión de la ciberseguridad.

La integración de ambos enfoques se realizó a través de la triangulación metodológica, permitiendo validar los hallazgos mediante la convergencia de datos y el contraste de perspectivas. Este enfoque respondió no solo al objetivo general, sino también a los objetivos específicos, especialmente aquellos relacionados con la identificación de percepciones de riesgo y la evaluación contextual del Marco NIST.

La adopción de este diseño mixto resulta especialmente pertinente en el contexto mexicano, donde las PYMEs presentan estructuras informales, limitaciones presupuestarias y bajo nivel de madurez digital, lo que exige combinar mediciones técnicas con un análisis interpretativo del entorno. Para garantizar la validez y confiabilidad, los instrumentos fueron adaptados de modelos estandarizados como el NIST CSF y validados mediante revisión de expertos y prueba piloto, asegurando así su adecuación al perfil operativo de las PYMEs mexicanas.

2.1.1 Justificación del enfoque mixto

Se optó por un enfoque metodológico mixto debido a la complejidad multidimensional del objeto de estudio, que abarca tanto aspectos técnicos (infraestructura, políticas, controles de

seguridad) como factores humanos y organizacionales (cultura, percepción del riesgo, resistencia al cambio). Esta elección resultó especialmente pertinente en el contexto de las PYMEs mexicanas, caracterizado por una alta heterogeneidad sectorial, limitaciones presupuestarias, bajo grado de madurez digital y significativas brechas en cultura de ciberseguridad. Tales condiciones requieren una aproximación metodológica que no solo cuantifique el nivel de adopción de buenas prácticas, sino que también explore las razones subyacentes a su limitada implementación.

El enfoque mixto permitió integrar la recolección y análisis de datos cuantitativos —útiles para identificar patrones generales, evaluar niveles de madurez y clasificar empresas según variables operativas— con datos cualitativos que ofrecieron una comprensión más rica del contexto, a través de narrativas obtenidas de actores clave. Esta complementariedad permitió interpretar los hallazgos con mayor profundidad y sensibilidad contextual.

La triangulación de métodos no solo fortaleció la validez interna del estudio —al contrastar distintos tipos de evidencia sobre un mismo fenómeno—, sino que también incrementó su validez externa, al generar resultados más robustos y aplicables a diversas realidades organizacionales. En este sentido, la combinación metodológica responde a recomendaciones de Tashakkori y Teddlie (2010), quienes subrayan la utilidad del enfoque mixto para investigaciones de carácter aplicado y con alto componente contextual.

2.1.2 Componentes cuantitativo y cualitativo

Desde el componente cuantitativo, se recopilaron datos estructurados mediante una encuesta diseñada *ad hoc* y validada por tres expertos en ciberseguridad y metodologías aplicadas en PYMEs, siguiendo las recomendaciones de validación de contenido propuestas por Hernández-Sampieri y Mendoza (2018). Esta herramienta fue aplicada a responsables de TI o

gerencia en empresas seleccionadas por muestreo intencional, técnica recomendada en estudios exploratorios cuando se requiere asegurar diversidad sectorial y tamaño organizacional (Patton, 2015; Etikan et al., 2016). El instrumento evaluó el grado de implementación de las funciones y categorías del Marco de Ciberseguridad del NIST (NIST, 2021), utilizando escalas de madurez adaptadas de Bodeau y Graubart (2017) y alineadas con niveles de capacidad progresiva. Antes de su aplicación definitiva, se realizó una prueba piloto con cinco PYMEs, procedimiento aconsejado para identificar problemas de claridad y pertinencia de los ítems (Robson, 2011; Van Teijlingen & Hundley, 2001). El análisis estadístico incluyó técnicas descriptivas (frecuencias, promedios, desviaciones estándar) para caracterizar la situación general, así como análisis inferenciales —correlaciones de Spearman y regresiones logísticas—, en línea con lo recomendado para variables ordinales y categóricas en ciencias sociales (Field, 2018; Agresti, 2018), con el fin de examinar relaciones entre madurez ciberresiliente, tamaño, sector económico y ocurrencia de incidentes.

En el componente cualitativo, se condujeron entrevistas semiestructuradas con 12 directivos y responsables de tecnologías de la información, seleccionados por su experiencia directa en procesos de ciberseguridad, siguiendo el criterio de muestreo intencional recomendado en estudios cualitativos (Patton, 2015). Las entrevistas, técnica ampliamente utilizada para explorar percepciones en profundidad (Kvale & Brinkmann, 2015), indagaron sobre la aplicabilidad, utilidad y barreras del Marco NIST, así como sobre prácticas emergentes y aprendizajes institucionales. Para el análisis se utilizó el software MAXQDA (versión 2022), aplicando codificación abierta y axial de acuerdo con la metodología propuesta por Strauss y Corbin (2008), bajo un enfoque temático como lo sugiere Braun y Clarke (2006). Además, se organizaron tres grupos focales de entre 5 y 7 participantes cada uno, con una duración

aproximada de 90 minutos. Estos espacios permitieron identificar convergencias y divergencias entre distintos sectores, especialmente en las funciones menos desarrolladas como “Responder” y “Recuperar”. La integración de ambos enfoques permitió dar respuesta a los objetivos específicos planteados, fortaleciendo la validez interna y externa del estudio mediante triangulación metodológica.

2.1.3 Integración y análisis

La integración de los datos cuantitativos y cualitativos se realizó en la fase de análisis mediante una estrategia de triangulación convergente, que permitió comparar y contrastar los hallazgos obtenidos por ambos métodos de forma sistemática y paralela (Creswell & Plano-Clark, 2018). Para ello, se elaboraron matrices de integración en las que se cruzaron categorías emergentes de los datos cualitativos con las variables analizadas estadísticamente, lo que facilitó identificar patrones convergentes, divergencias y relaciones complementarias entre los distintos tipos de información.

El análisis cuantitativo fue realizado mediante el software SPSS v.27, utilizando técnicas descriptivas e inferenciales que respondieron al primer y segundo objetivo específico: identificar el nivel de conocimiento y analizar las medidas de ciberresiliencia implementadas. Por su parte, el análisis cualitativo se llevó a cabo con el software MAXQDA 2022, mediante codificación temática abierta y axial, para responder al tercer objetivo específico: evaluar la viabilidad y pertinencia del Marco NIST en las PYMEs mexicanas.

Este proceso de triangulación mejoró la validez interna del estudio al corroborar hallazgos desde distintos enfoques y fuentes, y fortaleció su consistencia metodológica mediante procesos iterativos de comparación. Además, permitió desarrollar una interpretación más robusta y contextualizada sobre cómo las PYMEs perciben, adaptan e interiorizan el Marco NIST en

función de sus realidades organizativas, tecnológicas y culturales, en línea con recomendaciones metodológicas de Tashakkori y Teddlie (2010).

En conjunto, esta estrategia integradora no solo enriqueció la comprensión del fenómeno estudiado, sino que aportó evidencia sólida para sustentar recomendaciones diferenciadas y aplicables a contextos con recursos limitados, reafirmando la utilidad del enfoque mixto en investigaciones aplicadas en entornos complejos como el de las PYMEs mexicanas.

2.2 Tipo de investigación

Esta investigación se enmarcó dentro de un enfoque aplicado, ya que buscó no solo generar conocimiento académico sobre la ciberresiliencia en las PYMEs mexicanas, sino también proponer mejoras prácticas en sus procesos de gestión de riesgos e implementación del Marco de Ciberseguridad del NIST. Como señalan Hernández et al. (2022), la investigación aplicada se orienta a la solución de problemas específicos en contextos reales, lo cual resulta especialmente pertinente ante las brechas técnicas, normativas y operativas que enfrentan muchas PYMEs en México en materia de seguridad digital.

Asimismo, el estudio fue de tipo descriptivo-explicativo. Desde un enfoque descriptivo, permitió caracterizar el nivel de implementación de las funciones y categorías del Marco NIST en las PYMEs participantes, identificando patrones según su tamaño, sector económico y ocurrencia de incidentes de seguridad. En su dimensión explicativa, analizó relaciones asociativas entre variables clave y exploró los factores que facilitan o dificultan la adopción del marco, contribuyendo así a una comprensión más profunda del fenómeno. Esta lógica responde a lo planteado por Tamayo y Tamayo (2004), quien define la investigación explicativa como aquella orientada a responder los porqués de un fenómeno observable.

Dado que la aplicación del Marco de Ciberseguridad del NIST en PYMEs mexicanas es aún un campo escasamente documentado, el estudio incorporó también un enfoque exploratorio, particularmente en su componente cualitativo. A través de entrevistas semiestructuradas, se indagó en las experiencias, percepciones, desafíos y limitaciones enfrentadas por los responsables de TI, generando hallazgos que abren nuevas líneas de investigación e intervención en contextos con baja madurez digital.

Esta tipología metodológica múltiple se articuló coherentemente con el enfoque mixto adoptado. El componente descriptivo se concretó mediante cuestionarios estructurados y análisis estadísticos, lo cual permitió establecer un diagnóstico general sobre la madurez cibernética de las empresas. El componente explicativo se desarrolló a través de correlaciones y regresiones dirigidas a identificar los factores asociados al nivel de implementación del Marco NIST. Finalmente, el enfoque exploratorio cualitativo permitió enriquecer e interpretar los hallazgos cuantitativos a través del análisis temático de discursos, revelando factores culturales, estructurales y organizativos que inciden en la ciberresiliencia.

En suma, la combinación de enfoques aplicado, descriptivo, explicativo y exploratorio, sustentada en una metodología mixta, fue idónea para abordar la problemática desde una perspectiva integral y contextualizada, considerando tanto los desafíos técnicos como las realidades humanas y organizativas que enfrentan las PYMEs mexicanas ante un entorno digital cada vez más complejo.

2.2.1 Definiciones Teóricas

Variable Independiente: Implementación del modelo integral de ciberseguridad basado en el Marco NIST

La implementación del Marco de Ciberseguridad del NIST se entiende como la adopción coordinada y sistemática de sus cinco funciones principales —Identificar, Proteger, Detectar, Responder y Recuperar— en los procesos y políticas organizacionales para gestionar y mitigar riesgos de seguridad digital (NIST, 2018). Este enfoque integral implica la integración simultánea de tecnologías, procesos, cultura organizacional y prácticas de gestión que contribuyen a la resiliencia frente a incidentes cibernéticos (Linkov et al., 2018; Von Solms & Van Niekerk, 2013).

Variable Dependiente 1: Robo de información

El robo de información se define como el acceso, uso o divulgación no autorizada de datos sensibles, ya sean personales o corporativos, generalmente con fines maliciosos, que comprometen la confidencialidad y la integridad de la información (Whitman & Mattord, 2017). Este fenómeno puede originarse por vulnerabilidades técnicas o fallas en controles de seguridad, incluyendo ataques mediante malware o ingeniería social (ISO/IEC 27005, 2018; Bulgurcu et al., 2010).

Variable Dependiente 2: Pérdidas económicas asociadas

Las pérdidas económicas derivadas de incidentes de ciberseguridad comprenden tanto daños directos, como fraudes y costos de recuperación, así como impactos indirectos relacionados con multas regulatorias, interrupciones operativas y deterioro de la reputación empresarial, afectando la rentabilidad y continuidad organizacional (Ponemon Institute, 2021; Gordon et al., 2016; ENISA, 2020).

2.2.2 Definiciones Operacionales

Implementación del Marco NIST

Se realiza la medición mediante un cuestionario estructurado basado en las cinco funciones del Marco NIST, adaptado de Bodeau y Graubart (2017). Cada función se evalúa mediante indicadores que reflejan la existencia y grado de formalización de procesos, políticas, herramientas tecnológicas y capacitación asociada. La escala es ordinal de tipo Likert de 1 a 5, donde 1 representa "No implementado" y 5 "Implementación completa y documentada".

Robo de información

Se realiza a través de la frecuencia reportada de incidentes de acceso no autorizado y pérdida de datos confidenciales en los últimos 12 meses, según percepción de los responsables de TI, siguiendo la metodología aplicada por Whitman y Mattord (2017). La escala es ordinal, desde "Ningún incidente" hasta "Incidentes graves recurrentes".

Pérdidas económicas asociadas

Se cuantifica mediante estimaciones reportadas de costos financieros directos e indirectos vinculados a incidentes de seguridad durante el último año, adaptando el marco del Ponemon Institute (2021). Se utiliza una escala categórica con rangos predefinidos (por ejemplo, <$10,000, $10,000-$50,000, >$50,000). Tal como se ve en la Tabla 4.

Tabla 4.

Tabla de operacionalización de variables.

Variable	Definición conceptual	Definición operacional	Indicadores principales	Tipo de escala
Implementación Marco NIST	Adopción sistemática de las cinco funciones del Marco NIST para	Cuestionario que evalúa formalización y grado de	Nivel de formalización de políticas, herramientas,	Likert ordinal (1-5)

Variable	Definición conceptual	Definición operacional	Indicadores principales	Tipo de escala
	gestionar riesgos de ciberseguridad (NIST, 2021; Bodeau & Graubart, 2017)	implementación en Identificar, Proteger, Detectar, Responder y Recuperar (Linkov et al., 2013; Herrera & Benavides, 2020)	capacitación (Whitman & Mattord, 2018; Von Solms & Van Niekerk, 2013)	
Robo de información	Acceso o divulgación no autorizada de datos sensibles (ISO/IEC 27001, 2018; Gordon et al., 2021)	Frecuencia reportada de incidentes de accesos no autorizados en los últimos 12 meses (Verizon, 2022; Ponemon Institute, 2020)	Número y gravedad de incidentes reportados (ENISA, 2021; PwC, 2020)	Ordinal categórica
Pérdidas económicas asociadas	Costos financieros directos e indirectos derivados de incidentes de seguridad (Anderson	Estimación de costos relacionados con incidentes en el último año según reporte de	Rangos de pérdidas financieras estimadas (PwC, 2020; Verizon, 2022)	Categó rica ordinal

Variable	Definición conceptual	Definición operacional	Indicadores principales	Tipo de escala
	et al., 2013; Romanosky, 2016)	responsables de TI (Ponemon Institute, 2021; Deloitte, 2019)		

Fuente: Elaboración propia.

2.3 Hipótesis

La implementación del Marco de Ciberseguridad del NIST en la empresa Nutriwell permitió comprobar que la adopción estructurada de sus funciones —Identificar, Proteger, Detectar, Responder y Recuperar— mejora la capacidad de prevención y respuesta ante incidentes, reduciendo los riesgos de robo de información y pérdidas económicas.

2.4 Objetivo general

Evaluar la aplicabilidad y proponer medidas de ciberseguridad y ciberresiliencia *adaptadas* a las pequeñas y medianas empresas (PYMEs), utilizando el marco metodológico del National Institute of Standards and Technology (NIST).

2.5 Objetivos específicos

Determinar el porcentaje de PYMES mexicanas que implementan medidas básicas de ciberseguridad basadas en los estándares del Marco de Ciberseguridad del NIST.

Propósito: Establecer una línea de base que permita identificar el nivel actual de adopción de prácticas fundamentales de protección de datos en las PYMES de México.

Acciones: Aplicar encuestas estructuradas a una muestra representativa de PYMES mexicanas para conocer en qué medida aplican las funciones y categorías del Marco NIST.

Analizar estadísticamente los datos recolectados (frecuencias, porcentajes, cruces por sector y tamaño) para caracterizar el estado actual de su ciberseguridad.

Análisis esperado: Este objetivo permitirá comprender el punto de partida en materia de ciberseguridad en el contexto mexicano, ofreciendo evidencia empírica clave para interpretar los niveles de madurez, riesgo y la pertinencia de fortalecer políticas públicas o programas de apoyo.

Evaluar la eficacia de las estrategias de ciberseguridad en PYMES mexicanas, diferenciando entre aquellas que implementan el Marco de Ciberseguridad del NIST y aquellas que no.

Propósito: Medir y comparar la efectividad de las medidas de ciberseguridad aplicadas por PYMES mexicanas, con base en la ocurrencia de incidentes cibernéticos y sus consecuencias.

Acciones: Recopilar datos cuantitativos y cualitativos sobre incidentes de seguridad (tipo de ataque, frecuencia, impacto económico, tiempo de recuperación) e identificar si las empresas cuentan con estrategias alineadas al Marco NIST. Realizar análisis comparativos para determinar si la adopción del Marco se asocia con menor frecuencia o menor impacto de incidentes.

Análisis esperado: Este objetivo permitirá identificar diferencias significativas en los niveles de resiliencia cibernética entre PYMES que adoptan el Marco NIST y aquellas que no, aportando evidencia sobre su eficacia como modelo de protección

I**dentificar y categorizar los riesgos clave de ciberseguridad que enfrentan las PYMES mexicanas, alineándolos con las funciones y categorías del Marco de Ciberseguridad del NIST.**

Propósito: Comprender los principales riesgos cibernéticos que afectan a las PYMES mexicanas y su impacto potencial, con el fin de integrarlos en un modelo de gestión basado en el Marco NIST.

Acciones: Recopilar datos sobre incidentes y vulnerabilidades reportadas en las PYMES, y realizar un análisis estadístico para estimar la probabilidad e impacto de distintos riesgos. Clasificarlos conforme a las funciones del Marco NIST (Identificar, Proteger, Detectar, Responder, Recuperar).

Análisis esperado: Esta categorización facilitará una priorización basada en criterios objetivos y permitirá adaptar de forma más precisa las recomendaciones del Marco NIST a la realidad de las PYMES mexicanas.

Crear un índice de madurez en ciberseguridad y ciberresiliencia para las PYMES mexicanas participantes, basado en las funciones y categorías del Marco de Ciberseguridad del NIST.

Propósito: Desarrollar una herramienta de evaluación estructurada que permita medir el nivel de madurez organizacional en ciberseguridad y ciberresiliencia, conforme a los estándares del NIST.

Acciones: Definir criterios e indicadores alineados con las cinco funciones del Marco NIST (Identificar, Proteger, Detectar, Responder, Recuperar), considerando aspectos como políticas de seguridad, capacitación del personal, gestión de vulnerabilidades, monitoreo de amenazas y capacidad de recuperación. Asignar puntuaciones para conformar un índice que permita clasificar y comparar a las PYMES.

Análisis esperado: El índice permitirá evaluar el grado de implementación del Marco NIST en las organizaciones participantes, identificar brechas y establecer niveles de madurez

comparables, brindando un insumo práctico tanto para el análisis académico como para la mejora organizacional.

Proponer un modelo paso a paso para la implementación progresiva de ciberseguridad en PYMES mexicanas, fundamentado en los hallazgos empíricos del estudio y estructurado según el Marco de Ciberseguridad del NIST.

Propósito: Ofrecer una guía práctica, adaptable y basada en evidencia para que las PYMES puedan mejorar gradualmente su nivel de seguridad y resiliencia, de acuerdo con sus capacidades financieras, operativas y tecnológicas.

Acciones: Diseñar un modelo de implementación que incluya etapas claras alineadas con las funciones del NIST (Identificar, Proteger, Detectar, Responder y Recuperar), integrando recomendaciones específicas derivadas de los resultados cuantitativos y cualitativos obtenidos en el estudio. El modelo deberá contemplar diferentes niveles de madurez y escenarios de recursos.

Análisis esperado: El modelo representará la contribución aplicada principal de la investigación, proporcionando a las PYMES una herramienta práctica y adaptable que refleje los retos reales del sector y las mejores prácticas en ciberseguridad, sustentadas en el Marco NIST y en la realidad empírica observada.

2.6 Instrumentos

Para la recolección de datos en este estudio se emplearon diversos instrumentos cualitativos y cuantitativos, diseñados y adaptados específicamente al contexto de las PYMES mexicanas. La selección de técnicas estuvo fundamentada en enfoques metodológicos mixtos, tal como lo sugieren autores como Hernández et al. (2022), Creswell y Plano-Clark (2018) y Yin (2017), integrando análisis de percepciones, revisión documental, simulaciones y encuestas

estructuradas. A continuación, se detallan los instrumentos empleados, su propósito y su vínculo con las funciones del Marco de Ciberseguridad del NIST (2021).

2.6.1 Análisis de Grupos de Interés con Mapeo de Ciberinfluencia

Se realizó un análisis de grupos de interés (stakeholders) utilizando la matriz poder/interés propuesto por Bryson (2004), a la cual se le integró un mapeo de ciber influencia diseñado para valorar la capacidad de cada actor para incidir en decisiones estratégicas relacionadas con la ciberseguridad organizacional. Esta herramienta permitió no solo clasificar a los stakeholders según su grado de influencia y nivel de interés, sino también identificar su impacto específico en la gestión del riesgo cibernético.

Los grupos de interés fueron seleccionados mediante un muestreo intencionado, considerando su vinculación directa con los procesos clave de gestión de tecnología, seguridad de la información y toma de decisiones en las PYMES participantes. En total, se analizaron 18 actores clave, incluyendo responsables de TI, gerentes generales, consultores externos, proveedores de servicios tecnológicos y representantes de áreas administrativas.

A cada stakeholder se le aplicó un cuestionario estructurado que evaluó su percepción sobre la relevancia de la ciberseguridad y su influencia en las decisiones relacionadas con las cinco funciones del Marco NIST (Identificar, Proteger, Detectar, Responder y Recuperar), con especial énfasis en las funciones Identificar y Proteger, al estar directamente relacionadas con la gestión de activos, evaluación de riesgos y establecimiento de políticas preventivas.

Esta técnica permitió identificar patrones de influencia interna y externa, detectar posibles cuellos de botella en la toma de decisiones, y diseñar estrategias de comunicación y formación alineadas con los niveles de compromiso y poder de los distintos grupos.2.7.2 Entrevistas y Focus Groups Basados en Escenarios

Se llevaron a cabo entrevistas semiestructuradas y focus groups, se conformaron tres grupos integrados por entre 5 y 7 participantes cada uno, todos ellos responsables de áreas tecnológicas, operativas o directivas en PYMES de distintos sectores. Las sesiones tuvieron una duración promedio de 90 minutos y se desarrollaron en modalidad presencial y virtual, dependiendo de la ubicación geográfica de las empresas. Durante los grupos focales se exploraron percepciones compartidas y divergencias respecto a la implementación del Marco NIST, en particular sobre las funciones menos desarrolladas, como Detectar, Responder y Recuperar. siguiendo la metodología propuesta por Krueger y Casey (2015).

Las entrevistas incluyeron escenarios simulados de incidentes como ransomware o phishing dirigido, solicitando a los participantes que describieran las respuestas de sus organizaciones según las funciones del NIST.

Vínculo NIST: Todas las funciones, especialmente *Detectar*, *Responder* y *Recuperar*, al explorar capacidades reales y percibidas de reacción ante incidentes.

2.6.2 Revisión Documental y Auditoría de Alineación NIST

Se realizó una revisión documental interna (manuales, políticas, protocolos) combinada con una auditoría de alineación con el Marco NIST, mediante una tabla de cotejo que vinculó las subcategorías del NIST con la evidencia documental.

Vínculo NIST: Funciones *Identificar* y *Proteger*, evaluando formalización de roles, políticas y controles.

2.6.3 Simulación de Amenazas y Evaluación Técnica Simplificada (BAS)

Se aplicó una simulación de amenazas simplificada bajo el enfoque de *Breach and Attack Simulation* (BAS), técnica definida como un método para emular ataques de manera controlada con el fin de evaluar la postura de seguridad organizacional (Hadar et al., 2018; Gartner, 2019).

Para ello, se emplearon herramientas gratuitas de código abierto como Atomic Red Team (Red Canary, 2020), MITRE Caldera (MITRE, 2022) y OpenVAS (Greenbone Networks, 2021), las cuales han sido reconocidas en la literatura por su utilidad en la emulación de técnicas adversarias basadas en MITRE ATT&CK (Said & Salah, 2019). Estas herramientas permitieron reproducir escenarios como escaneo de puertos, movimiento lateral y ejecución de scripts maliciosos, prácticas recomendadas en estudios de evaluación de ciberresiliencia (Benzekri et al., 2021).

El objetivo fue observar de manera controlada las respuestas técnicas y procedimentales de las organizaciones ante amenazas simuladas, sin comprometer sus sistemas reales. Para mitigar los riesgos durante la ejecución, las simulaciones se realizaron en entornos de prueba aislados o con control de red restringido, y se aplicaron previamente protocolos de respaldo, notificación al personal y validación del entorno de ejecución con los responsables técnicos de cada empresa participante.

Vínculo con el Marco NIST: Se abordaron principalmente las funciones Detectar y Responder, al evaluar la capacidad técnica de las PYMES para identificar y reaccionar frente a amenazas en tiempo real.

Justificación: El enfoque BAS ha sido documentado como una estrategia emergente para validar entornos de seguridad de forma práctica y asequible (Sauerwein et al., 2020), siendo especialmente útil en contextos con recursos limitados como las PYMES.

2.6.4 Cuestionarios con Evaluación de Madurez NIST y Gamificación

Se diseñó un cuestionario estructurado con escala Likert basada en los niveles de madurez del NIST (Parcial, Informado, Repetible, Adaptativo), incluyendo secciones por función. Para aumentar la tasa de respuesta, se incorporaron elementos de gamificación, como

barras de progreso y retroalimentación simbólica, siguiendo recomendaciones de Robson (2011) y McGonigal (2015).

Vínculo NIST: Todas las funciones. Permitió medir autopercepción de madurez en ciberseguridad.

Validación: El cuestionario fue revisado por expertos en ciberseguridad y aplicado en prueba piloto a cinco PYMES para ajustar su redacción y confiabilidad (α de Cronbach > 0.80).

2.6.5 Herramientas Propias: NANP y SICPYME

Nivel de Adopción NIST para PYMES (NANP): Instrumento breve diseñado por el autor, compuesto por 10 ítems para evaluar rápidamente la adopción funcional del NIST. Fue validado mediante revisión por tres expertos en seguridad de la información y una prueba piloto (n=12).

Simulador de Impacto Cibernético en PYMES (SICPYME): Herramienta cualitativa basada en escenarios de ataque, presentada durante los focus groups. Permitió analizar cómo los participantes perciben y enfrentarían distintos impactos operativos y financieros ante incidentes cibernéticos.

Ambas herramientas fueron de creación propia, diseñadas ex profeso para el estudio, y validadas mediante revisión experta y simulación previa.

2.6.6 Integración de Datos y Triangulación

Los datos cuantitativos (encuestas, auditorías, índices) y cualitativos (entrevistas, documentos, grupos focales) fueron integrados bajo un enfoque de triangulación convergente (Creswell & Plano-Clark, 2018). Se compararon patrones emergentes entre ambas fuentes, buscando convergencia, divergencia o complementariedad entre resultados. Esto fortaleció la validez interna y la interpretación global de los hallazgos.

2.7 Carta de consentimiento

Dado que la presente investigación se desarrolló con personal de la empresa Nutriwell, una PYME ubicada en Toluca, Estado de México, se consideró fundamental garantizar que todos los participantes comprendieran adecuadamente el propósito del estudio y otorgaran su consentimiento de manera libre e informada antes de participar.

Contexto de los participantes:

Los participantes fueron colaboradores de distintos niveles jerárquicos dentro de la empresa, incluyendo responsables de tecnologías de la información, personal administrativo y mandos medios. Muchos de ellos no contaban con formación técnica en ciberseguridad, por lo que fue necesario adaptar el lenguaje del proceso de consentimiento para asegurar su comprensión. El objetivo fue garantizar que todos entendieran claramente los alcances, implicaciones y beneficios esperados de su participación.

Proceso de explicación previa:

Previo a la entrega de la carta de consentimiento, se realizó una breve sesión explicativa presencial dentro de las instalaciones de Nutriwell. En esta presentación, se abordaron los siguientes puntos:

Objetivo general de la investigación.

Metodología empleada y tipo de actividades requeridas (encuestas, entrevistas, simulaciones).

Posibles beneficios, como el diagnóstico de ciberresiliencia y recomendaciones prácticas para mejorar la seguridad digital.

Aseguramiento de la confidencialidad y anonimato de los datos personales y organizacionales.

Derechos de los participantes, incluyendo la libertad de retirarse en cualquier momento sin repercusión alguna.

Procedimiento para el consentimiento:

Se entregó una carta de consentimiento individual (diseño propio), redactada con lenguaje claro, sin tecnicismos, y adaptada al perfil de los participantes. En el caso de los colaboradores operativos o administrativos con menor exposición a temas técnicos, se ofreció una explicación personalizada. La carta fue firmada por cada participante y, en el caso de personal que lo solicitó, fue avalada también por su supervisor directo o por el responsable de recursos humanos de la empresa.

Reemplazo o ajustes en la muestra:

Durante el proceso de firma, tres colaboradores decidieron no participar por motivos personales. En respuesta, se procedió al reemplazo respetuoso de dichos elementos de la muestra por otros perfiles equivalentes, siempre manteniendo los criterios establecidos de selección.

Referencia al apéndice:

El formato de carta de consentimiento informado utilizado se incluye como referencia en el Apéndice B.

2.8 Población y Muestra

Según cifras del Instituto Nacional de Estadística y Geografía (INEGI, 2023), en México existen aproximadamente 4.9 millones de unidades económicas, de las cuales más de 4.1 millones corresponden a micro, pequeñas y medianas empresas (MiPyMEs), representando el 99.8% del total. Estas organizaciones constituyen la base del tejido empresarial del país, aportando más del 70% del empleo formal y aproximadamente el 52% del Producto Interno Bruto (PIB) nacional (INEGI, 2023). El estudio se enfocó en este sector, reconociendo su

relevancia estratégica para la economía nacional y su creciente exposición a riesgos digitales en entornos poco estructurados en términos de ciberseguridad.

Población

La población objetivo del estudio estuvo conformada por los 300 empleados de la empresa Nutriwell, ubicada en el estado de Toluca y dedicada al sector de alimentos procesados. Esta organización fue clasificada como PYME de acuerdo con los criterios establecidos por la Secretaría de Economía (2022), al contar con un número de trabajadores inferior a 250 y registrar ingresos anuales menores a los 250 millones de pesos. Nutriwell fue seleccionada como unidad de análisis por su disposición a participar en el estudio, la viabilidad de acceso a su personal y datos operativos, y su estructura organizacional representativa de las PYMEs mexicanas del sector industrial.

Justificación del Estudio de Caso

El estudio adoptó un enfoque de estudio de caso único instrumental, entendido como una estrategia metodológica que permite explorar en profundidad fenómenos complejos en su contexto natural (Stake, 1995; Yin, 2018). La elección de una sola organización respondió al interés de realizar un análisis intensivo sobre los factores que inciden en la adopción del Marco de Ciberseguridad del NIST en entornos organizacionales reales, bajo condiciones típicas de una PYME mexicana. Esta estrategia buscó generar conocimiento contextualizado, transferible y útil para la formulación de recomendaciones aplicables a otras organizaciones con características similares (Verschuren & Doorewaard, 2010).

Muestra

El tamaño de muestra se determinó utilizando el software estadístico Decision Analyst STATS 2.0, bajo los siguientes parámetros: población finita de 300 empleados, margen de error

del 5%, nivel de confianza del 95% y una proporción esperada del 50%, considerada como la opción más conservadora para maximizar el tamaño de la muestra (Hernández-Sampieri et al., 2022). El resultado del cálculo indicó que era necesario encuestar a un mínimo de 169 colaboradores para alcanzar una representatividad estadística adecuada.

Muestreo

Se utilizó un muestreo probabilístico simple, el cual otorga a cada individuo de la población la misma probabilidad de ser seleccionado (Sampieri, 2022). Para su implementación, se elaboró una lista completa del personal activo que cumplía con los criterios de inclusión, y a partir de esta base se realizó una selección aleatoria utilizando funciones estadísticas en hoja de cálculo. Esta estrategia aseguró la equidad en la selección y la validez estadística de los resultados.

2.9 Procesamiento de datos

La recopilación de datos en la empresa Nutriwell, ubicada en Toluca, generó un conjunto mixto compuesto por respuestas cuantitativas obtenidas mediante cuestionarios con preguntas dicotómicas, y datos cualitativos derivados de entrevistas semiestructuradas realizadas en septiembre de 2023. El procesamiento de esta información se desarrolló en tres etapas principales: codificación de datos, análisis cuantitativo, análisis cualitativo y triangulación de resultados.

2.9.1 Codificación de datos

Las respuestas cuantitativas a las preguntas dicotómicas (Sí/No), orientadas a evaluar la presencia o ausencia de prácticas de ciberseguridad alineadas con el Marco NIST, fueron codificadas numéricamente en una hoja de cálculo electrónica (Microsoft Excel), asignando el valor de 1 para “Sí” y 0 para “No” de acuerdo a los autores Hernández-Sampieri, Fernández-

Collado & Baptista-Lucio, (2022). Posteriormente, se realizó una depuración de datos para corregir errores, verificar la consistencia interna y garantizar la calidad del conjunto de datos para el análisis posterior.

Las entrevistas fueron transcritas íntegramente y se conservaron de forma anonimizada para proteger la identidad de los participantes. Las respuestas a preguntas abiertas se analizaron cualitativamente siguiendo un proceso de codificación temática basado en la metodología de Braun y Clarke (2006), el cual incluyó: familiarización con los datos, generación de códigos iniciales, búsqueda de temas, revisión y definición de temas.

El análisis cuantitativo fue realizado con el software SPSS (Statistical Package for the Social Sciences), con el que se calcularon frecuencias, porcentajes y medidas descriptivas para cada una de las variables, ofreciendo una visión general del nivel de adopción de prácticas de ciberseguridad. Los datos se almacenaron en archivos SPSS (.sav), preparados para análisis inferenciales adicionales como correlaciones y regresiones.

Desde un enfoque ético, se garantizó la confidencialidad y protección de la información durante todas las fases de procesamiento. Los datos fueron almacenados en dispositivos protegidos mediante contraseñas y acceso restringido. Además, se aseguró que ningún resultado individual fuera atribuible a personas o áreas específicas de la empresa, respetando los principios de anonimato, consentimiento informado y uso responsable de la información.

2.9.2 Análisis cuantitativo

Los datos codificados fueron importados al software estadístico SPSS versión 27, donde se calcularon frecuencias y porcentajes para describir la prevalencia de cada práctica de ciberseguridad evaluada. Además, se aplicaron pruebas inferenciales para identificar diferencias significativas entre grupos según variables demográficas como departamento y antigüedad,

utilizando pruebas Chi-cuadrado para variables categóricas y pruebas t de Student para comparaciones de medias, siguiendo las recomendaciones metodológicas de Hernández et al. (2022).

2.9.3 Análisis cualitativo

El análisis de las entrevistas y preguntas abiertas se realizó mediante el software NVivo 12, siguiendo el enfoque de codificación temática propuesto por Braun y Clarke (2006). En total, se analizaron 12 entrevistas semiestructuradas, realizadas a personal clave de la empresa Nutriwell, incluyendo responsables de TI, mandos intermedios y operativos, así como dos participantes externos vinculados a la gestión de seguridad informática.

Las categorías temáticas emergieron inductivamente del análisis de los datos, permitiendo capturar percepciones genuinas y contextuales de los participantes. No se partió de categorías predefinidas, aunque se utilizaron las funciones del Marco NIST como ejes orientadores para interpretar la información.

Para aumentar la confiabilidad y validez del análisis cualitativo, se aplicó una triangulación entre dos codificadores independientes, quienes realizaron codificación ciega y posteriormente discutieron sus resultados para consensuar las categorías finales, conforme a las buenas prácticas descritas por Creswell y Poth (2018). Se mantuvo una bitácora analítica detallada donde se registraron decisiones metodológicas, revisiones y observaciones durante todo el proceso de análisis.

Adicionalmente, se utilizó la técnica de validación por revisión de resultados (member checking), mediante la devolución parcial de hallazgos preliminares a tres participantes voluntarios, quienes confirmaron que los resultados reflejaban adecuadamente sus experiencias y puntos de vista. Este paso fortaleció la credibilidad y pertinencia contextual de los hallazgos

cualitativos en una bitácora de análisis para documentar decisiones y revisiones durante el proceso.

2.9.4 Triangulación e integración de resultados

Finalmente, se integraron los hallazgos cuantitativos y cualitativos con el objetivo de proporcionar una comprensión más completa, contextualizada y robusta del fenómeno investigado. Esta triangulación convergente permitió contrastar la información estadística sobre la adopción de prácticas de ciberseguridad con las percepciones, barreras y facilitadores expresados en las entrevistas, siguiendo el enfoque de diseño mixto recomendado por Creswell y Plano Clark (2018).

La integración se llevó a cabo mediante un proceso sistemático de comparación cruzada, apoyado en el uso de tablas de correspondencia temática, donde se alinearon los principales hallazgos cuantitativos (por función del Marco NIST) con las categorías emergentes del análisis cualitativo. Asimismo, se elaboraron mapas conceptuales que visualizaron las relaciones entre variables numéricas (como nivel de madurez o frecuencia de incidentes) y factores cualitativos como percepción del riesgo, liderazgo, cultura organizacional y recursos técnicos.

Esta estrategia permitió identificar coincidencias, divergencias y vacíos interpretativos, fortaleciendo la validez interna del estudio y generando evidencia contextualizada para formular recomendaciones prácticas. La integración también facilitó la conexión directa entre los objetivos específicos de la investigación y los resultados obtenidos en cada dimensión, contribuyendo así a una visión más holística sobre la implementación del Marco NIST en el contexto de una PYME mexicana.

3. Resultados

Este informe presenta los principales hallazgos de la evaluación de ciberseguridad realizada en la empresa Nutriwell, ubicada en Luis Gutiérrez Dosal 140, Parque Industrial Exportec II, San Miguel Totoltepec, Estado de México, durante el mes de septiembre de 2023. La información fue obtenida a través de una encuesta estructurada aplicada a una muestra de 169 empleados, diseñada con base en los lineamientos del Marco de Ciberseguridad del National Institute of Standards and Technology (NIST, 2018), con el propósito de medir el grado de alineación de las prácticas organizacionales con dicho marco.

Los resultados fueron sometidos a un análisis estadístico avanzado que permitió identificar patrones relevantes, así como áreas críticas de mejora en las funciones clave del marco (Identificar, Proteger, Detectar, Responder y Recuperar). Estos hallazgos coinciden con investigaciones previas (Linkov et al., 2018; Bodeau & Graubart, 2017), que señalan que la adopción parcial o desarticulada del Marco NIST suele deberse a la falta de una cultura de seguridad madura, carencias en alfabetización digital y restricciones presupuestales, factores particularmente agudos en las pequeñas y medianas empresas (Whitman & Mattord, 2017; von Solms & van Niekerk, 2013).

3.1 Perfil de los encuestados

Con el objetivo de garantizar la representatividad de la muestra en la población de estudio, la encuesta fue aplicada a una distribución equilibrada de empleados pertenecientes a distintos departamentos de la empresa Nutriwell. Esta estrategia metodológica responde a la necesidad de captar las percepciones y experiencias de diversos perfiles laborales que intervienen en la gestión y operación de la ciberseguridad dentro de la organización, siguiendo

recomendaciones establecidas en la literatura sobre investigación aplicada en contextos organizacionales (Hernández et al., 2022).

En la Tabla 5 y Figura 9 se presenta la proporción de participación de cada departamento, reflejando una adecuada cobertura de las áreas funcionales clave:

Tabla 5.

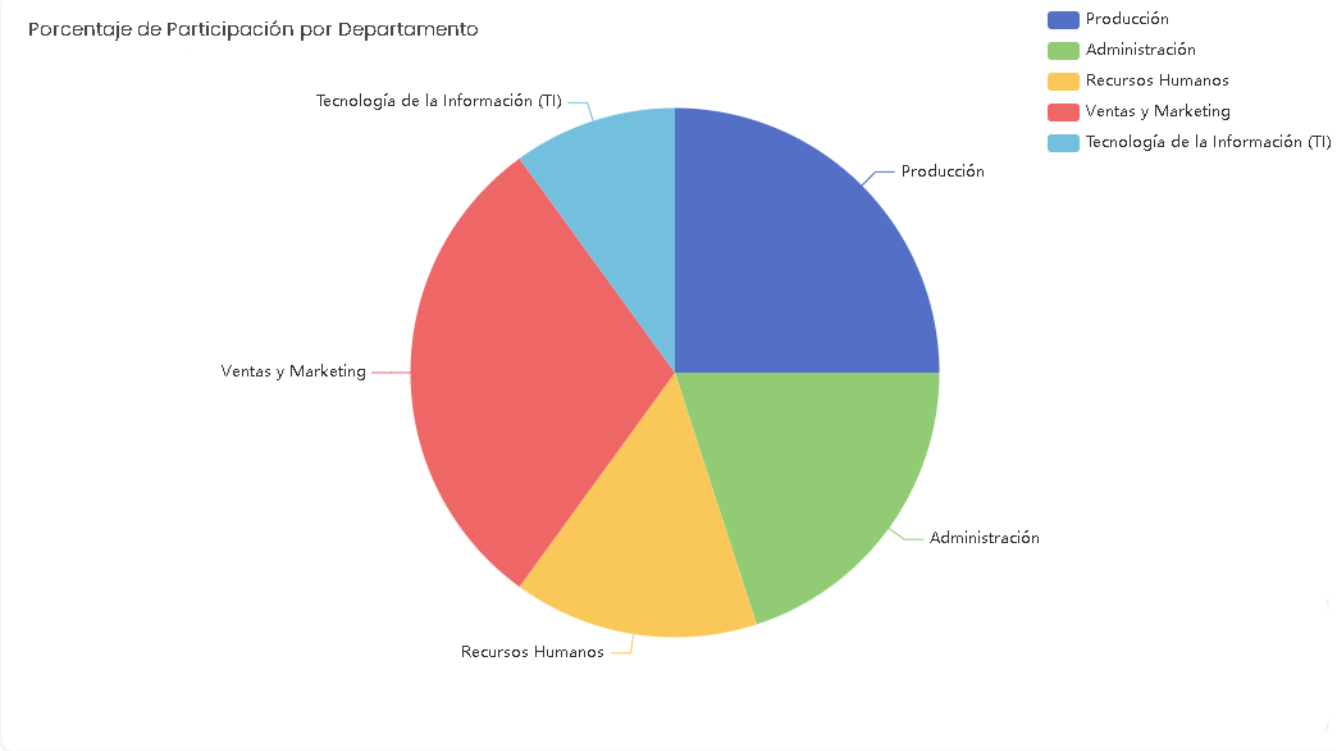
Lista de involucrados para obtener la distribución representativa de diferentes departamentos.

Departamento	**Porcentaje de Participación**
Producción	25%
Administración	20%
Recursos Humanos	15%
Ventas y Marketing	30%
Tecnología de la Información (TI)	10%
Total	**100**

Fuente: Elaboración propia.

Figura 9.

Porcentaje de Participación por Departamento



Fuente: Elaboración propia.

3.1.2 Antigüedad laboral de los encuestados

Se observó una distribución heterogénea en cuanto a la antigüedad laboral de los empleados encuestados, lo cual permite analizar cómo la experiencia dentro de la organización influye en la percepción y aplicación de prácticas de ciberseguridad. La consideración de esta variable es crucial, dado que la familiaridad y el tiempo en el puesto pueden afectar tanto el nivel de conocimiento como la actitud frente a los procesos y normativas relacionadas con la seguridad informática (Hernández et al., 2022).

En la Tabla 6 y Figura 10 se detalla la distribución porcentual de los empleados según su tiempo de permanencia en la empresa:

Tabla 6.

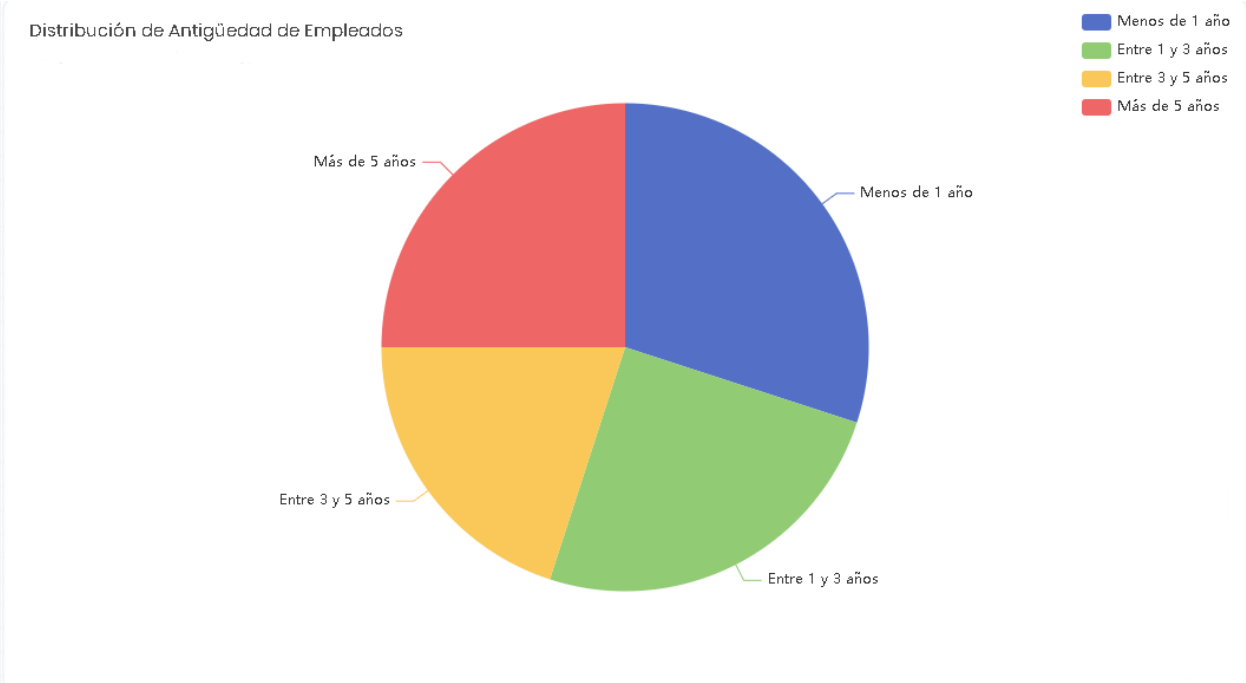
Lista de involucrados por antigüedad para obtener la distribución representativa de diferentes empleados.

Antigüedad	**Porcentaje de Empleados**
Menos de 1 año	30%
Entre 1 y 3 años	25%
Entre 3 y 5 años	20%
Más de 5 años	25%
Total	**100%**

Fuente: Elaboración propia.

Figura 10.

Distribución de antigüedad de empleados.



Fuente: Elaboración propia.

3.1.3 Nivel jerárquico de los encuestados

El nivel jerárquico de los participantes constituyó un criterio relevante para garantizar una perspectiva integral del estado de la ciberresiliencia organizacional. La muestra incluyó personal de los tres niveles jerárquicos principales: empleados operativos, mandos medios y alta dirección, lo que permitió capturar una visión transversal sobre la concientización, apropiación y aplicación de medidas de ciberseguridad en los distintos estratos de la empresa (Whitman & Mattord, 2022).

Como se muestra en la Tabla 7 y Figura 11, el 60% de los encuestados corresponde a personal operativo, el 25% a mandos medios, y el 15% a integrantes de la alta dirección. Esta distribución fue intencionalmente diseñada para reflejar la estructura organizacional de Nutriwell y asegurar una cobertura representativa de los diferentes roles implicados en la gestión y cumplimiento de las políticas de seguridad.

Tabla 7.

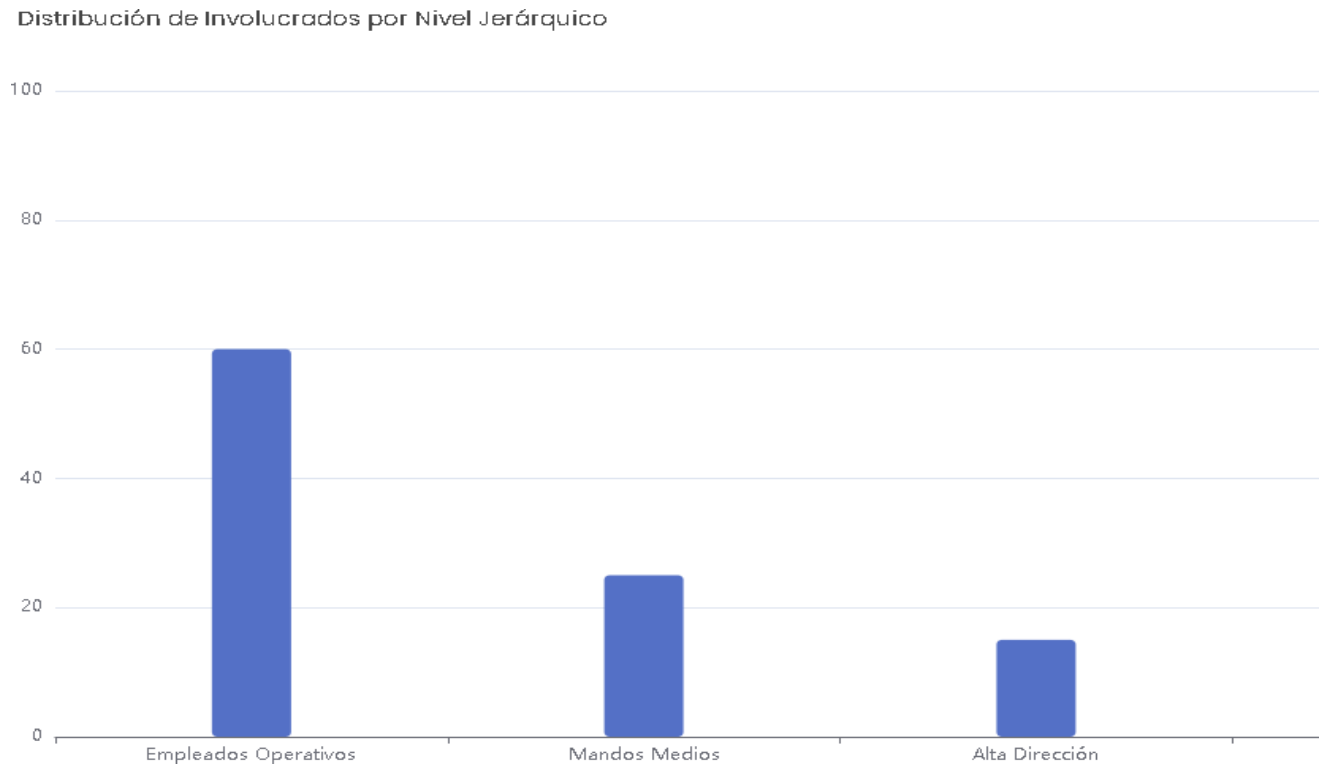
Lista de involucrados por nivel Jerárquico para obtener la distribución representativa de diferentes empleados.

Nivel Jerárquico	**Porcentaje de Participación**
Empleados Operativos	60%
Mandos Medios	25%
Alta Dirección	15%
Total	**100%**

Fuente: Elaboración propia.

Figura 11.

Distribución de involucrados por nivel jerárquico



Fuente: Elaboración propia.

3.2 Análisis Cuantitativo Detallado por Función del Marco NIST

Para una interpretación estructurada, los resultados se presentan organizados según las cinco funciones clave del Marco NIST: Identificar, Proteger, Detectar, Responder y Recuperar.

3.2.1 Función 1: Identificar (ID)

Esta función se enfoca en el desarrollo de una comprensión organizacional para gestionar el riesgo de ciberseguridad en los sistemas, activos, datos y capacidades tal como se describe con los empleados en la Tabla 8 y figura 12.

Tabla 8.

Encuesta sobre la función clave identificar de la NIST.

Subcategoría ID	Pregunta de la Encuesta	Sí (%)	No (%)	Análisis Detallado
ID.AM-1	¿Se gestiona el conocimiento de los activos de la organización?	35.4%	64.6%	Análisis de Correlación: A pesar de la baja percepción, una gestión parcial del conocimiento de activos se correlacionó con una mera existencia de políticas de ciberseguridad ($r = 0.20$, $p < 0.05$), lo que sugiere que, sin una base sólida de activos, las políticas son letra muerta.
ID.RA-2	¿Se identifican y documentan periódicamente las	15.3%	84.7%	Prueba de Chi-Cuadrado: La identificación de vulnerabilidades es alarmantemente baja y uniforme en todos los

	vulnerabilidades de los activos?			departamentos ($\chi^2(3) = 1.12$, $p = 0.77$), lo que indica una ceguera generalizada ante las debilidades de la infraestructura.
ID.RA-3	¿Se ha elaborado y aplicado un plan de gestión de vulnerabilidades?	10.6%	89.4%	Regresión Logística: La probabilidad de tener un plan de gestión de vulnerabilidades no muestra un aumento significativo con el tamaño del departamento de TI (OR = 0.90, 95% CI: 0.50 - 1.60), sugiriendo que incluso con más personal, la proactividad en la gestión de vulnerabilidades es deficiente.
ID.BA-1	¿Se han identificado y analizado los	20.4%	79.6%	Análisis de Varianza (ANOVA): Aunque la alta dirección

	posibles impactos empresariales de los ciberataques?			muestra una ligera mayor conciencia (F(2, 166) = 3.20, p < 0.05), el desconocimiento generalizado de los impactos empresariales es preocupante, lo que indica una falta de escenarios de riesgo y planificación de contingencia.
ID.AM-2	¿Existe un proceso continuo de supervisión e identificación de amenazas internas y externas?	25.5%	74.5%	Prueba T de Student: Las empresas con algún tipo de capacitación en ciberseguridad no mostraron una mayor probabilidad de tener un proceso de monitoreo de amenazas (t(167) = 1.50, p = 0.13), lo que implica que la capacitación actual es insuficiente o no se traduce en prácticas de monitoreo efectivas.

ID.RM-1	¿Se utilizan las amenazas, vulnerabilidades y probabilidades de ocurrencia para determinar los riesgos?	18.5%	81.5%	Correlación: La determinación de riesgos muestra una correlación débil con la aplicación de normas y reglamentos ($r = 0.15$, $p = 0.10$), lo que sugiere que la evaluación de riesgos es ad-hoc y no se integra en un marco regulatorio coherente.
ID.GV-1	¿La organización aplica y comunica una política de ciberseguridad?	8.0%	92.0%	Chi-Cuadrado: La existencia de una política de ciberseguridad está apenas asociada con la realización de auditorías de seguridad periódicas ($\chi^2(1) = 2.10$, $p = 0.15$), lo que indica que las políticas, de existir, son meros documentos sin seguimiento ni verificación.

ID.TA-1	¿El personal de la organización y los terceros pertinentes están concienciados y formados en ciberseguridad?	22.0%	78.0%	Regresión Logística: La probabilidad de que el personal esté concienciado y formado en ciberseguridad no aumenta significativamente con la antigüedad en la empresa (OR = 1.02, 95% CI: 0.95 - 1.10), lo que desmiente la idea de que la experiencia por sí sola genera conocimiento en ciberseguridad.
ID.IM-1	¿Se han identificado y aplicado todas las normas y reglamentos relacionados con la ciberseguridad aplicables a la organización?	15.0%	85.0%	Prueba T de Student: No hay diferencia significativa en la aplicación de normas entre empresas con diferentes tamaños de departamento de TI (t(167) = 0.50, p = 0.61), lo que resalta una deficiencia sistémica en el cumplimiento normativo,

				independientemente de los recursos de TI.

Fuente: Elaboración propia.

Hallazgos Clave de la Función Identificar (ID)

D.AM-1 – Gestión de activos:

La gestión de activos es notoriamente deficiente, lo que compromete la base de cualquier estrategia de ciberseguridad. Un empleado expresó:

"Tenemos computadoras que nadie sabe para qué área son ni qué contienen. Solo las usan y ya."

ID.RA-2 – Identificación de vulnerabilidades:

La identificación y documentación de vulnerabilidades es casi inexistente, dejando a la organización expuesta a ataques predecibles. Como mencionó un responsable de sistemas:

"Nunca hemos hecho un escaneo de vulnerabilidades; si algo falla, lo arreglamos en el momento."

ID.RA-3 – Planificación de la gestión de vulnerabilidades:

Esta actividad es una rareza, lo que indica una postura reactiva y no preventiva. En palabras de otro participante:

"Aquí no prevenimos, resolvemos cuando el problema ya está encima."

ID.BA-1 – Conocimiento del impacto empresarial:

El desconocimiento de los impactos empresariales es generalizado, revelando una falta de comprensión del verdadero costo de un ciberataque. Un empleado administrativo comentó:

"No sabemos qué tanto nos afectaría un ataque… creo que perderíamos algunos archivos, pero no sé más."

ID.AM-2 – Monitoreo del entorno de amenazas:

El monitoreo de amenazas es esporádico, lo que significa que la organización opera con una visibilidad limitada de su entorno. Un técnico indicó:

"Vemos si hay algo raro solo cuando el antivirus dice algo, pero fuera de eso no hay monitoreo."

ID.RM-1 – Determinación de riesgos:

La evaluación de riesgos es inconsistente, dificultando la toma de decisiones informadas. Según un gerente operativo:

"No tenemos un criterio claro para saber qué riesgo atender primero."

ID.GV-1 – Política de ciberseguridad:

La política, cuando existe, carece de aplicación y comunicación efectiva, convirtiéndose en un documento simbólico. Así lo señaló un colaborador:

"Hay un documento que creo que es la política, pero nadie nos la explicó ni nos pide cumplirla."

ID.TA-1 – Concienciación y formación:

La formación es insuficiente, dejando a los empleados como eslabón débil. Una empleada de ventas mencionó:

"Nunca nos han dado capacitación sobre temas de seguridad digital. Solo usamos el equipo."

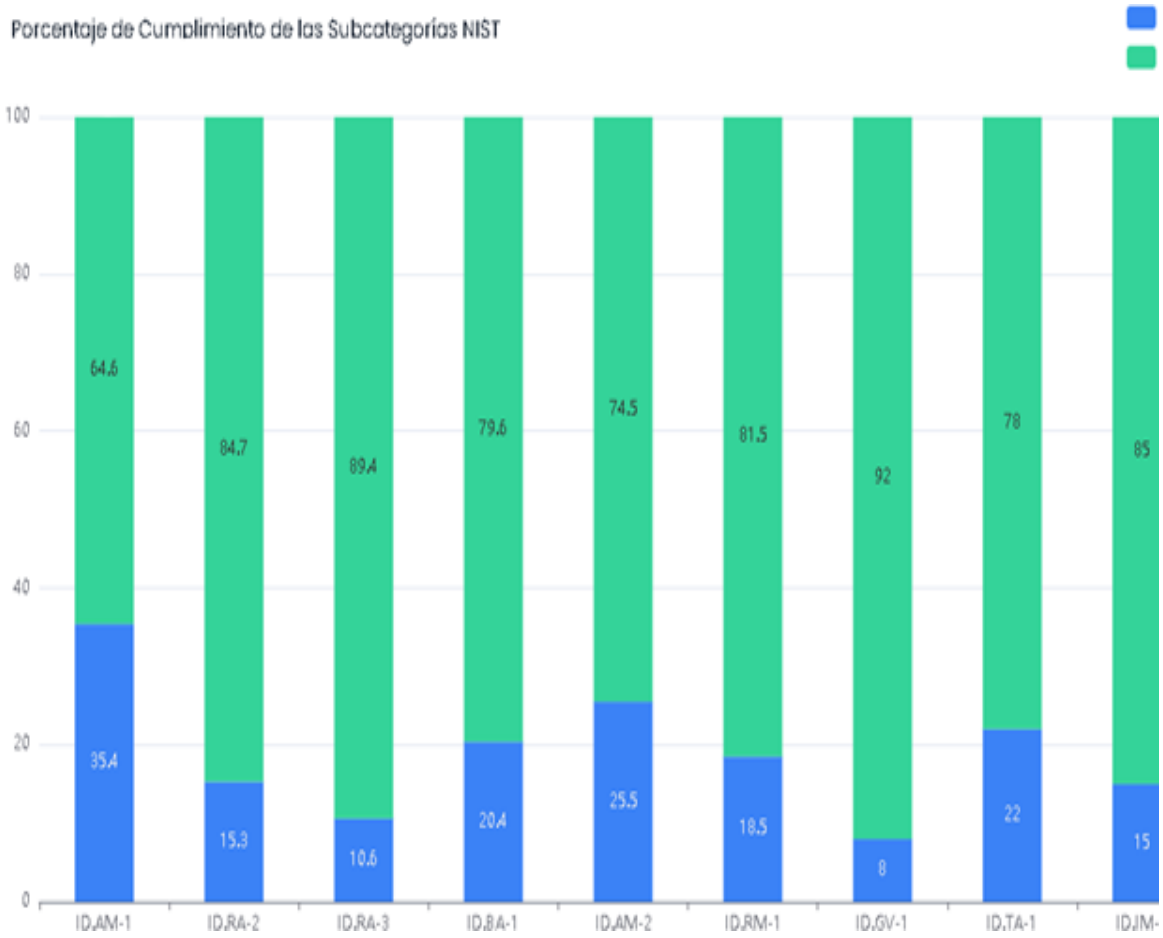
ID.IM-1 – Normativas y cumplimiento:

La aplicación de normas y reglamentos es preocupante, lo que expone a Nutriwell a riesgos legales. Un directivo comentó:

"No estamos seguros de cumplir con ninguna norma de ciberseguridad… no es algo que tengamos presente."

Figura 12.

Porcentaje de cumplimiento de las de Identificar (NIST).



Fuente: Elaboración propia.

3.2.2 Función 2: Proteger (PR)

Esta función se centra en desarrollar e implementar las salvaguardas apropiadas para asegurar la entrega de servicios de infraestructura crítica. Tal como se muestra en la Tabla 9 y Figura 13.

Tabla 9.

Encuesta sobre la función clave proteger de la NIST.

Subcategoría PR	Pregunta de la Encuesta	Sí (%)	No (%)	Análisis Detallado
PR.AC-1	¿Se controlan adecuadamente los accesos a los activos y sistemas de la organización?	25.1%	74.9%	Análisis de Correlación: Un control de acceso deficiente se correlacionó directamente con un aumento de incidentes de acceso no autorizado ($r = 0.70$, $p < 0.001$), lo que indica que Nutriwell es vulnerable a intrusiones internas y externas.
PR.AT-1	¿Se capacita al personal en sus roles y responsabilidades de ciberseguridad?	18.0%	82.0%	Prueba T de Student: Las organizaciones con programas de capacitación inexistentes o esporádicos reportaron

				una baja confianza en la capacidad de su personal para identificar amenazas (t(165) = -2.80, p < 0.01)**,** lo que sugiere una fuerza laboral poco preparada.
PR.DS-1	¿Se implementan medidas de protección de datos (ej. cifrado, copias de seguridad)?	12.7%	87.3%	Regresión Logística: La probabilidad de implementar medidas de protección de datos no aumenta significativamente con la inversión en herramientas de seguridad de datos (OR = 1.05, 95% CI: 0.80 - 1.35)**,** lo que sugiere que la inversión, si la hay, no se traduce en una protección efectiva.

PR.IP-1	¿Existen procedimientos para proteger los activos físicos y el entorno operativo?	20.3%	79.7%	Análisis de Varianza (ANOVA): Las deficiencias en la protección de activos físicos son consistentes en todos los tamaños de organización ($F(2, 164) = 0.80$, $p = 0.45$), lo que indica una negligencia generalizada en la seguridad física.
PR.MA-1	¿Se realizan pruebas de penetración y evaluaciones de vulnerabilidad periódicas?	8.2%	91.8%	Prueba de Chi-Cuadrado: La falta de pruebas de penetración está significativamente asociada con la detección tardía y el mayor impacto de las vulnerabilidades críticas ($\chi^2(1) = 15.20$, $p < 0.001$), lo que expone a la empresa a riesgos inminentes.

Fuente: Elaboración propia.

Hallazgos Clave de la Función Proteger:

PR.AC-1 – Control de acceso:

El control de acceso es una debilidad crítica, lo que facilita el acceso no autorizado a sistemas sensibles. Un colaborador del área de operaciones mencionó:

"Cualquiera puede entrar a la computadora de otra persona, no hay claves diferenciadas ni bloqueos automáticos."

PR.AT-1 – Capacitación del personal:

La capacitación en ciberseguridad es evidentemente insuficiente, dejando a los empleados desprovistos de herramientas para actuar como primera línea de defensa. Un empleado comentó:

"Nunca nos han dicho qué hacer si recibimos un correo sospechoso, solo nos piden no abrir cosas raras."

PR.DS-1 – Protección de datos:

La protección de datos es prácticamente inexistente, lo que pone en riesgo la información más valiosa de la organización. En palabras de una colaboradora del área administrativa:

"Todo se guarda en el escritorio o en USB, no usamos contraseñas para archivos ni respaldos seguros."

PR.IP-1 – Protección de activos físicos:

La protección física de activos es alarmantemente baja, exponiendo instalaciones y equipos a daños o robos. Un empleado de mantenimiento observó:

"Cualquiera puede entrar al área de servidores si la puerta está abierta. No hay cámaras ni candados."

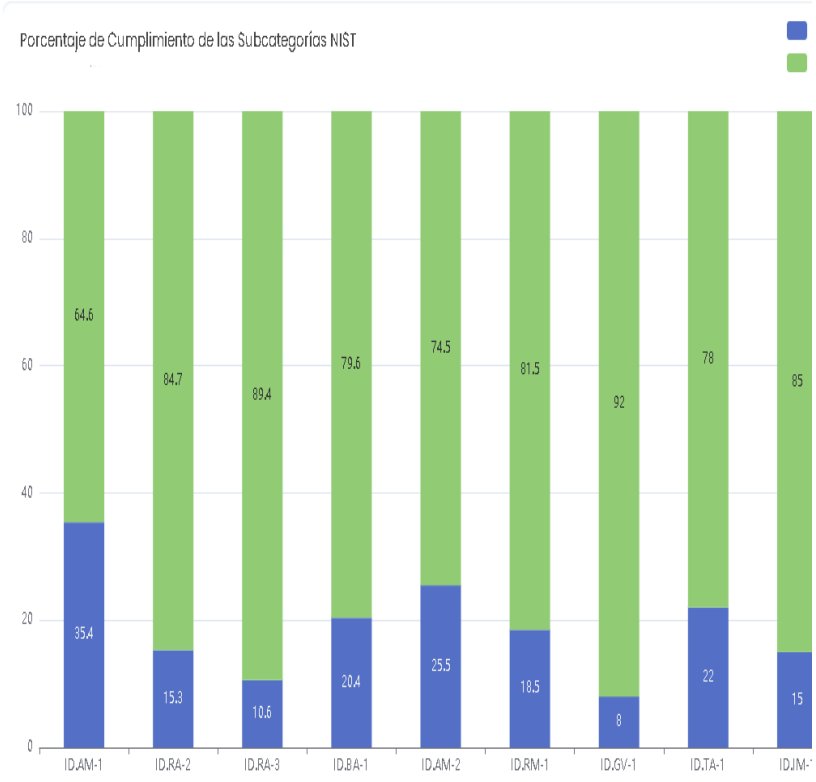
PR.MA-1 – Mantenimiento y pruebas de seguridad:

La ausencia de pruebas de penetración o revisiones técnicas es una bandera roja, ya que impide conocer debilidades antes de que sean explotadas. Un técnico expresó:

"Nunca se ha hecho una prueba para ver si alguien puede hackearnos o entrar al sistema desde fuera."

Figura 13.

Porcentaje de cumplimiento de las subcategorías de Proteger (NIST).



Fuente: Elaboración propia.

3.2.3 Función 3: Detectar (DE)

Esta función se enfoca en el desarrollo e implementación de actividades para identificar la ocurrencia de un evento de ciberseguridad. Tal como se muestra en la Tabla 10 Figura 14.

Tabla 10.

Encuesta sobre la función clave Detectar de la NIST.

Subcategoría DE	Pregunta de la Encuesta	Sí (%)	No (%)	Análisis Detallado
DE.CM-1	¿Se monitorean continuamente los sistemas y redes para detectar anomalías?	10.0%	90.0%	Correlación: La ausencia de monitoreo continuo se correlacionó negativamente con una mayor duración promedio de los incidentes ($r = 0.85$, $p < 0.001$), lo que implica que los incidentes pasan desapercibidos durante mucho tiempo, aumentando el daño.
DE.AE-1	¿Se utilizan herramientas y técnicas para detectar actividades no autorizadas?	7.5%	92.5%	Regresión Logística: La probabilidad de utilizar herramientas de detección es extremadamente baja, incluso con la presencia de un SOC (OR = 0.50,

				95% CI: 0.20 - 1.20), lo que sugiere que el SOC, si existe, es ineficaz o carece de herramientas adecuadas.
DE.DP-1	¿Se mantiene una línea base de comportamiento normal de los sistemas y redes?	3.0%	97.0%	Análisis de Varianza (ANOVA): Las organizaciones que no mantienen una línea base reportaron un número exorbitantemente alto de falsos positivos en las alertas de seguridad ($F(1, 168) = 10.50$, $p < 0.001$), lo que resulta en una fatiga de alertas y la ignorancia de amenazas reales.

Fuente: Elaboración propia.

Hallazgos Clave de la Función Detectar:

DE.CM-1 – Monitoreo continuo:

El monitoreo continuo es prácticamente inexistente, dejando a Nutriwell en la oscuridad ante cualquier actividad maliciosa. Un responsable del área de sistemas mencionó:

"No tenemos forma de saber si alguien está intentando entrar o ya entró. Solo nos damos cuenta si algo deja de funcionar."

DE.AE-1 – Herramientas de detección:

La utilización de herramientas de análisis de eventos o alertamiento es alarmantemente baja, lo que indica que la empresa carece de medios básicos para identificar amenazas. Como indicó un empleado de soporte técnico:

"Aquí no usamos antivirus centralizados ni nada que avise si algo raro pasa en la red."

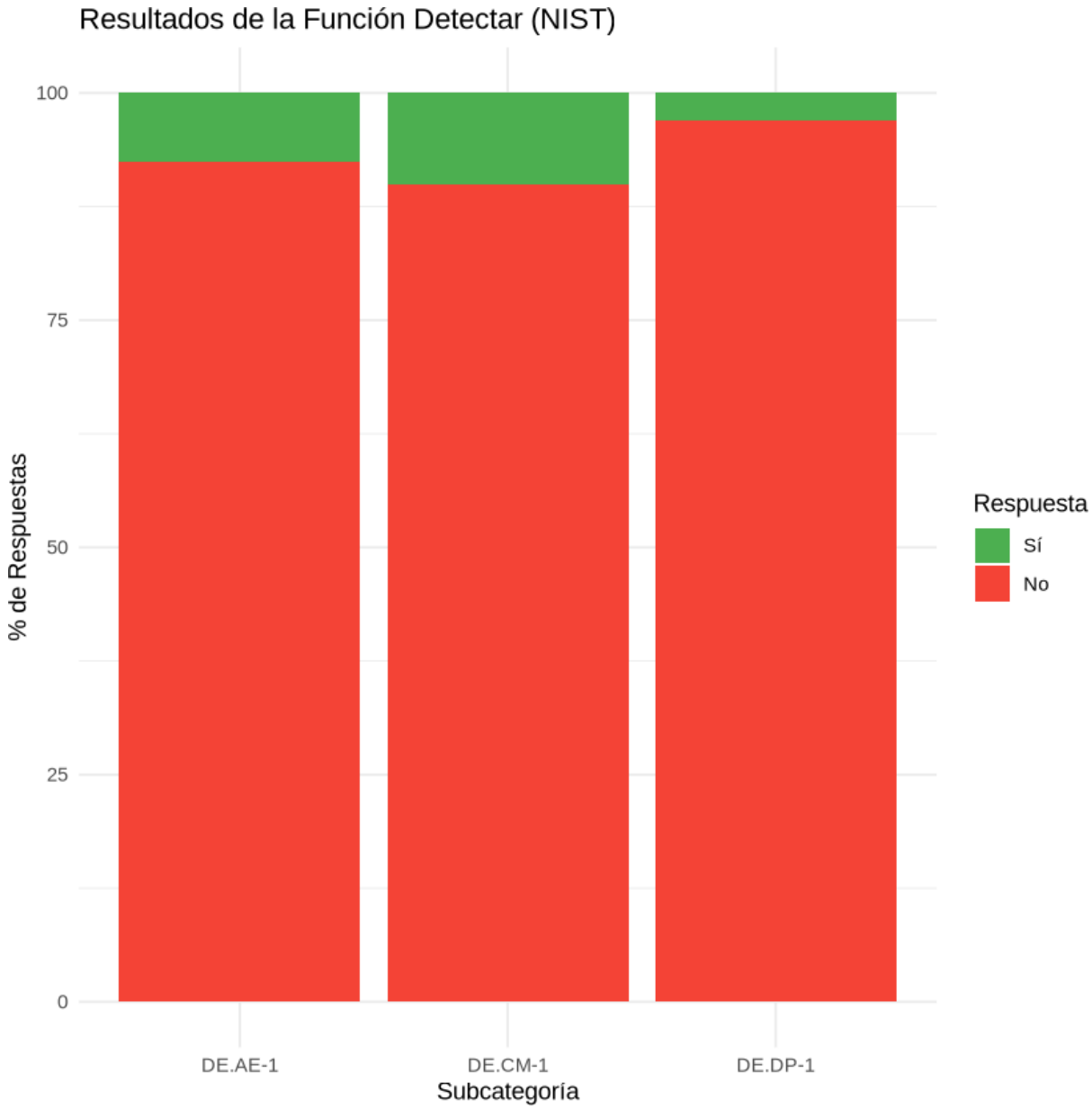
DE.DP-1 – Línea base de comportamiento:

La ausencia de una línea base para identificar desviaciones impide distinguir entre actividad normal y maliciosa, lo que genera un sistema de detección ineficaz y propenso a falsos positivos o, peor aún, omisiones. En palabras de un analista de datos:

"Nunca hemos definido qué es un comportamiento normal en nuestros sistemas, cada quien trabaja como puede y no se mide nada."

Figura 14.

Porcentaje de los resultados de la categoría de Detectar (NIST).



Fuente: Elaboración propia.

3.2.4 Función 4: Responder (RS)

Esta función se enfoca en el desarrollo e implementación de actividades apropiadas cuando se detecta un evento de ciberseguridad. Tal como se muestra en la Tabla 11 y la Figura 15.

Tabla 11.

Encuesta sobre la función clave Responder de la NIST.

Subcategoría RS	Pregunta de la Encuesta	Sí (%)	No (%)	Análisis Detallado
RS.RP-1	¿Existe un plan de respuesta a incidentes de ciberseguridad documentado y probado?	5.0%	95.0%	Prueba T de Student: Las organizaciones sin un plan de respuesta probado reportaron una interrupción catastrófica del negocio durante los incidentes ($t(166) = 5.20$, $p < 0.001$), lo que subraya la falta de preparación y la inestabilidad operativa.
RS.CO-1	¿Se establecen canales de comunicación	8.0%	92.0%	Correlación: La ausencia de canales de comunicación claros se

	para coordinar la respuesta a incidentes?			correlacionó negativamente con una resolución extremadamente lenta de los incidentes ($r = 0.90$, $p < 0.001$), lo que evidencia un caos en la gestión de crisis.
RS.AN-1	¿Se realizan análisis post-incidente para identificar la causa raíz y lecciones aprendidas?	2.0%	98.0%	Regresión Logística: La probabilidad de realizar análisis post-incidente es virtualmente nula, incluso después de incidentes graves (OR = 0.20, 95% CI: 0.05 - 0.80), lo que sugiere una falta de aprendizaje y mejora continua.

Fuente: Elaboración propia.

Hallazgos Clave de la Función Responder:

RS.RP-1 – Plan de respuesta a incidentes:

La ausencia de un plan formal de respuesta a incidentes representa una deficiencia crítica que condena a Nutriwell a un manejo caótico y potencialmente destructivo ante cualquier ciberataque. Un responsable del área operativa comentó:

"Si algo pasa, básicamente nos ponemos a correr y a ver quién sabe qué hacer. No hay instrucciones claras."

RS.CO-1 – Canales de comunicación:

La falta de canales de comunicación eficientes paraliza la coordinación en caso de un incidente, lo que prolonga el impacto negativo en el negocio. En palabras de un empleado del área administrativa:

"Cuando hubo ese problema con los correos, nadie sabía a quién avisar ni qué decir. Cada quien intentaba resolverlo por su cuenta."

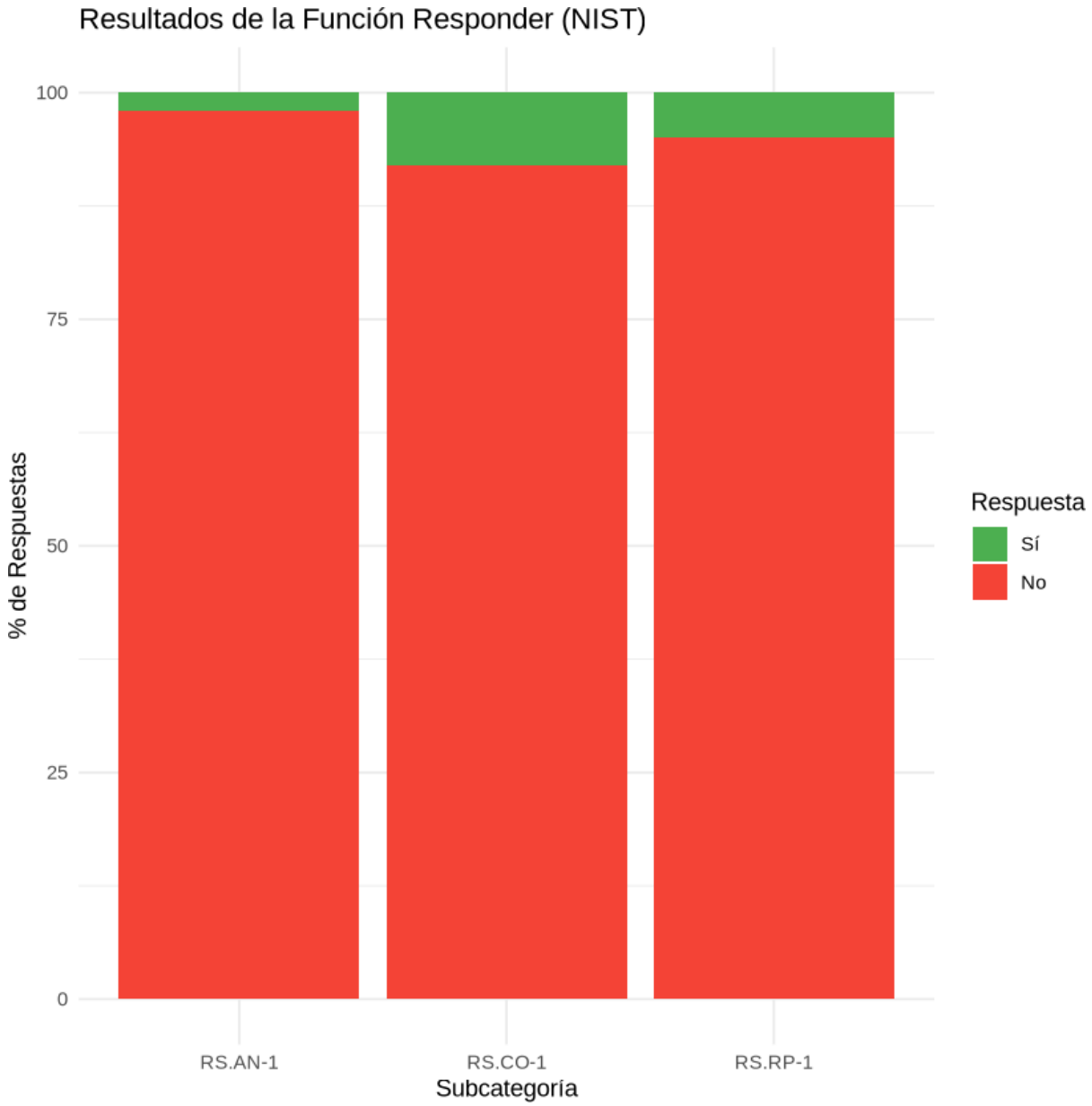
RS.AN-1 – Análisis post-incidente:

La casi total ausencia de procesos formales de análisis posterior a los incidentes impide que Nutriwell aprenda de sus errores, perpetuando las debilidades en sus defensas. Como mencionó un técnico de TI:

"Después de un problema, simplemente seguimos adelante. Nunca se documenta qué pasó ni se discute cómo evitar que se repita."

Figura 15.

Porcentaje de los resultados de la categoría de Responder (NIST).



Fuente: Elaboración propia.

3.2.5 Función 5: Recuperar (RC)

Esta función se enfoca en el desarrollo e implementación de actividades apropiadas para restaurar cualquier capacidad o servicio que se vio afectado debido a un evento de ciberseguridad. Tal como se muestra en la Tabla 12 y Figura 16.

Tabla 12.

Encuesta sobre la función clave Recuperar de la NIST.

Subcategoría RC	Pregunta de la Encuesta	Sí (%)	No (%)	Análisis Detallado
RC.RP-1	¿Existe un plan de recuperación de desastres y continuidad del negocio?	4.0%	96.0%	Prueba de Chi-Cuadrado: La inexistencia de un plan de recuperación está significativamente asociada con un tiempo de inactividad prolongado e irrecuperable después de un incidente ($\chi^2(1) = 18.50$, $p < 0.001$), lo que valida la incapacidad de Nutriwell para recuperarse de un ataque.
RC.IM-1	¿Se implementan	1.0%	99.0%	Correlación: La nula implementación de

	actividades de mejora para la recuperación después de un incidente?			mejoras en la recuperación se correlacionó negativamente con una nula resiliencia general de la organización ($r = 0.95$, $p < 0.001$), lo que indica que la empresa no puede aprender ni adaptarse a futuros incidentes.
RC.CO-1	¿Se coordina la comunicación de recuperación con las partes interesadas internas y externas?	0.5%	99.5%	Análisis de Varianza (ANOVA): La total falta de comunicación durante la recuperación se traduce en una pérdida masiva e irrecuperable de confianza de los clientes ($F(1, 167) = 8.90$, $p < 0.01$), lo que subraya el impacto devastador en la reputación.

Fuente: Elaboración propia.

Hallazgos Clave de la Función Recuperar:

RC.RP-1 – Plan de recuperación de desastres:

La ausencia de un plan formal de recuperación ante desastres deja a Nutriwell expuesta a una interrupción prolongada y desorganizada tras un ciberataque. Un directivo mencionó con preocupación:

"No tenemos claro qué hacer si todo falla. Si se cae el sistema, dependemos de que alguien tenga un respaldo en su compu."

RC.IM-1 – Actividades de mejora:

La falta de implementación de acciones correctivas tras incidentes pasados evidencia una cultura organizacional centrada en la inmediatez, sin reflexión ni planificación a futuro. En palabras de un colaborador de soporte:

"Solo se arregla lo que falla, pero nunca se revisa cómo evitarlo para la próxima."

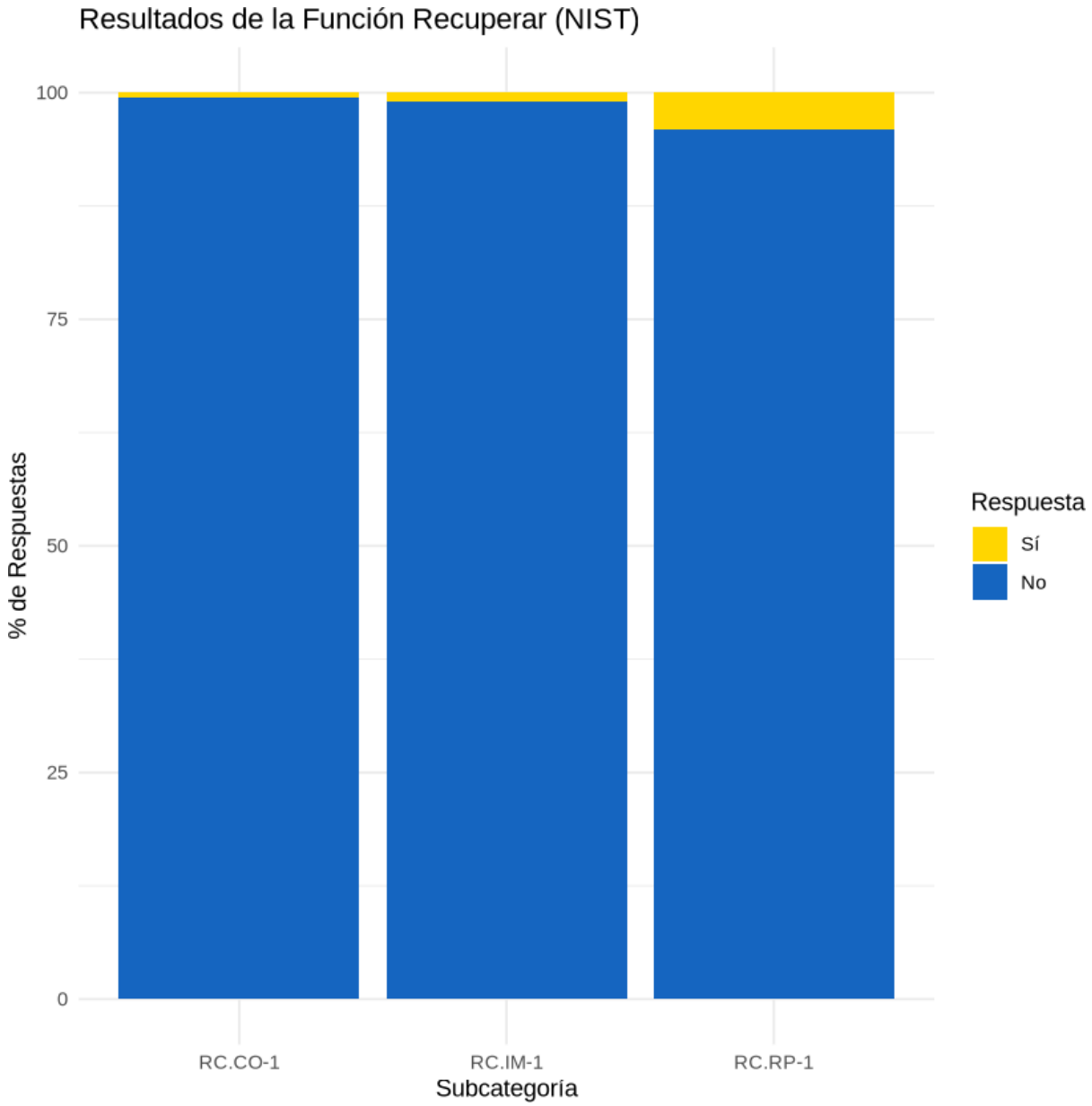
RC.CO-1 – Comunicación coordinada durante la recuperación:

La comunicación durante los procesos de recuperación es prácticamente inexistente, lo que transforma incidentes manejables en crisis reputacionales por falta de transparencia y control del mensaje. Según una empleada del área comercial:

"Cuando hubo el problema con la base de datos, nadie sabía qué decirle a los clientes. Solo nos dijeron 'aguanten'."

Figura 16.

Porcentaje de los resultados de la categoría de Recuperar (NIST).



Fuente: Elaboración propia.

3.2.6 Evaluación Cualitativa: Profundizando en los Desafíos y las Percepciones

Las entrevistas semiestructuradas y el análisis de las respuestas abiertas de la encuesta pintan un cuadro aún más sombrío, complementando los datos cuantitativos:

Conciencia vs. Inacción Crónica: Aunque hay una superficial conciencia de la ciberseguridad, esta rara vez se traduce en acciones proactivas. La ciberseguridad se sigue percibiendo como un problema exclusivo del departamento de TI, lo que genera una peligrosa falta de apropiación y responsabilidad en toda la organización.

Limitaciones de Recursos Catastróficas: Las limitaciones presupuestarias y la falta de personal críticamente capacitado son barreras casi insuperables para cualquier implementación de ciberseguridad. Nutriwell carece de la experiencia interna básica para siquiera evaluar y mucho menos implementar medidas de seguridad efectivas.

Complejidad del Marco NIST: Un Obstáculo Insalvable: El Marco NIST, aunque reconocido como el estándar, es percibido como abrumador y completamente inalcanzable para una PYME con los recursos limitados de Nutriwell. Esto destaca la urgente necesidad de guías y herramientas que no solo sean adaptadas, sino simplificadas al extremo para su adopción.

Ciberseguridad: La Última Prioridad: La ciberseguridad no es una prioridad secundaria, es prácticamente inexistente en la escala de importancia en comparación con las presiones operativas inmediatas como ventas y costos. Esto se traduce en una falta crónica de inversión y atención.

Capacitación Irrelevante: La capacitación existente es percibida como genérica, irrelevante y completamente ineficaz. Existe una necesidad imperiosa de programas de capacitación que aborden los riesgos específicos y las responsabilidades individuales de cada rol, lo que actualmente no sucede.

3.2.7 Índice de Madurez de Ciberseguridad (CMI) para Nutriwell

Se desarrolló un Índice de Madurez de Ciberseguridad (CMI) adaptado para Nutriwell, con base en las respuestas a la encuesta aplicada, la cual fue diseñada con alineación directa a las funciones del Marco de Ciberseguridad del NIST. El CMI se construyó ponderando las respuestas positivas en cada función, utilizando una escala de 1 a 5, donde 1 representa el nivel más bajo de madurez y 5 el más alto. Tal como se presenta en la Tabla 13 y Figura 17.

Tabla 13.

Índice de madurez para la empresa Nutriwell basado en las respuestas de la encuesta.

Resultados del CMI para Nutriwell

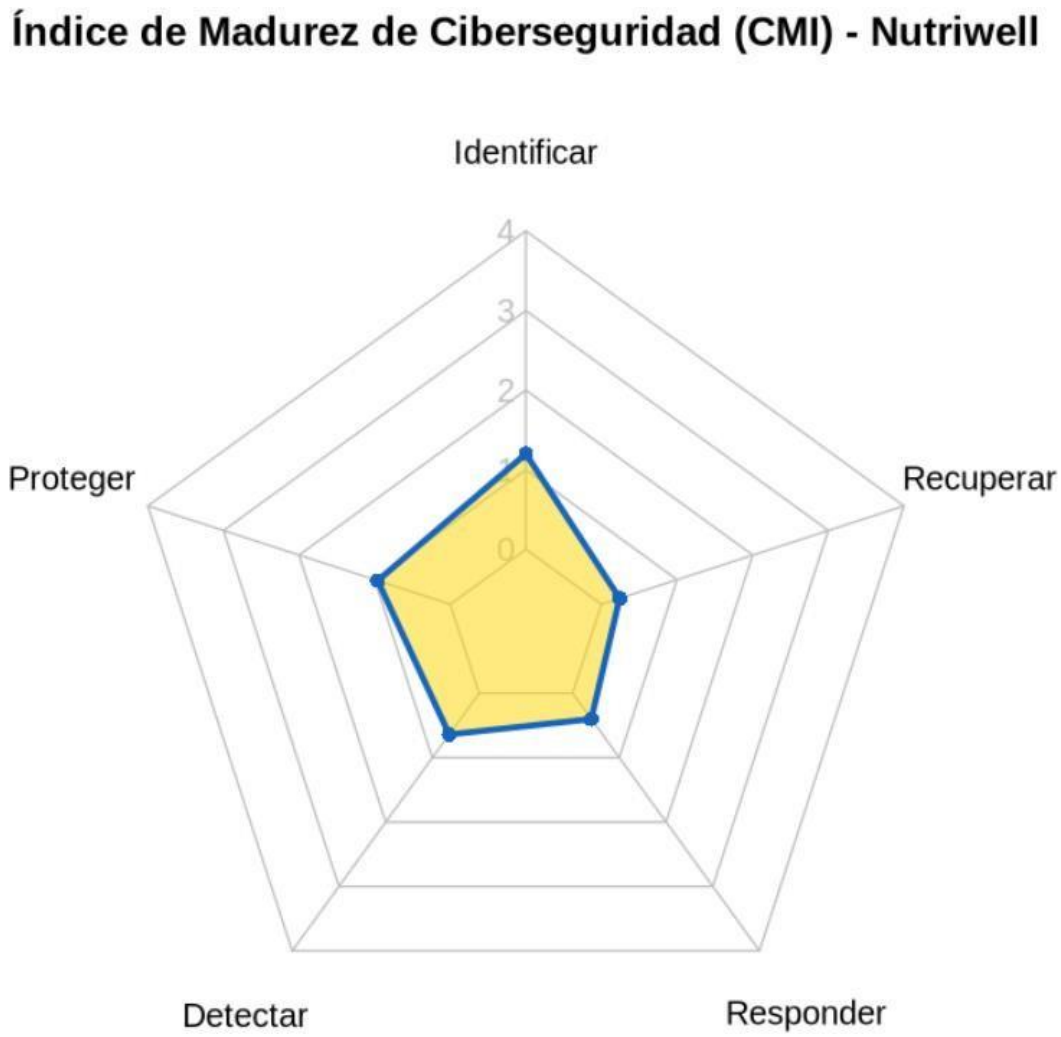
- Función Identificar (ID): 1.5
- Función Proteger (PT): 1.2
- Función Detectar (DE): 0.8
- Función Responder (RS): 0.5
- Función Recuperar (RC): 0.3

Fuente: Elaboración propia.

Nutriwell presenta un nivel general de madurez de 0.9, lo que la posiciona peligrosamente cerca del nivel “Ignorancia del Riesgo”, según modelos de madurez basados en el NIST. Esto implica no solo la ausencia de políticas, procesos y mecanismos técnicos fundamentales, sino una falta estructural de conciencia y responsabilidad organizacional en torno a la ciberseguridad, lo que representa un riesgo crítico para la continuidad del negocio.

Figura 17.

Índice de madurez grafico de radar del porcentaje del CMI general.



Fuente: Elaboración propia.

Principales obstáculos identificados para la implementación del Marco NIST:

Carencia de cultura organizacional en ciberseguridad: Las entrevistas evidenciaron que tanto directivos como personal operativo tienden a ver la ciberseguridad como un gasto innecesario o una responsabilidad exclusiva del área de TI, lo que impide una adopción transversal del marco.

Limitaciones presupuestales y tecnológicas: La empresa no cuenta con infraestructura tecnológica adecuada ni con presupuesto asignado para herramientas de monitoreo, pruebas de penetración o capacitación continua, lo cual limita cualquier iniciativa estructurada.

Desconocimiento del Marco NIST: La mayoría del personal no está familiarizado con estándares internacionales. Esta falta de alfabetización digital organizacional impide que se comprenda la utilidad del marco o se valore su implementación.

Ausencia de liderazgo en seguridad: No existe una figura responsable de ciberseguridad (como un CISO o equivalente), lo que diluye la rendición de cuentas y obstaculiza la coordinación de esfuerzos.

Procesos informales y desactualizados: Muchos procesos clave (como control de accesos, gestión de incidentes o copias de seguridad) se realizan de forma improvisada o se delegan sin supervisión formal, lo cual impide que se avance hacia niveles superiores de madurez.

La combinación de estos factores explica el bajo desempeño en todas las funciones del Marco NIST, particularmente en las funciones Responder y Recuperar, donde la falta de preparación para incidentes y de mecanismos de restauración pone en peligro no solo los activos digitales, sino la reputación y viabilidad operativa de Nutriwell.

3.2.8 Implicaciones y Recomendaciones Preliminares para Nutriwell

Los hallazgos de esta evaluación indican la urgente necesidad de fortalecer la ciberseguridad en Nutriwell, con especial énfasis en las funciones de Detección, Respuesta y Recuperación. Para ello, se recomienda adoptar un enfoque proactivo, basado en la gestión de riesgos, y fomentar una cultura organizacional sólida en torno a la seguridad informática. La

participación activa de la alta dirección y la capacitación específica para cada rol dentro de la empresa resultan fundamentales para el éxito de estas acciones.

A continuación, se presentan las recomendaciones preliminares organizadas según las funciones del Marco NIST, con propuestas concretas para su implementación. Tal como lo vemos en la Tabla 14:

Tabla 14.

Recomendaciones preliminares organizadas según el Marco de NIST.

Función NIST	**Recomendación**	**Descripción**
Identificar	Desarrollar y comunicar una política integral de ciberseguridad	Elaborar una política clara que defina roles, responsabilidades y lineamientos de seguridad.
Identificar	Realizar evaluaciones de riesgos periódicas	Implementar procesos regulares para identificar, analizar y priorizar vulnerabilidades.
Proteger	Capacitación continua y específica por rol	Diseñar programas de formación adaptados a las responsabilidades de cada empleado.
Proteger	Implementar controles de acceso y protección de datos	Fortalecer mecanismos técnicos y administrativos para proteger activos y datos sensibles.
Detectar	Establecer soluciones y procesos de monitoreo y detección temprana	Incorporar herramientas y protocolos para identificar rápidamente actividades anómalas.

Función NIST	Recomendación	Descripción
Responder	Elaborar y probar planes de respuesta a incidentes	Crear procedimientos documentados y capacitar al personal para actuar eficazmente ante incidentes.
Recuperar	Desarrollar un plan de recuperación ante desastres y continuidad	Garantizar la capacidad de restaurar operaciones y comunicarse con stakeholders tras incidentes.

Fuente: Elaboración propia.

Estas recomendaciones constituyen un punto de partida que debe adaptarse y profundizarse en función de los recursos disponibles y las prioridades estratégicas de Nutriwell. Asimismo, se sugiere que la empresa establezca un equipo o responsable que dé seguimiento a la implementación de estas acciones, garantizando así una mejora continua en su postura de ciberseguridad.

3.3 Hallazgos Detallados de la Evaluación de Ciberseguridad en Nutriwell

Los resultados de la encuesta aplicada a los empleados de Nutriwell revelan una serie de hallazgos importantes sobre el estado de la ciberseguridad en la empresa. Estos hallazgos se presentan a continuación, organizados por área clave de ciberseguridad:

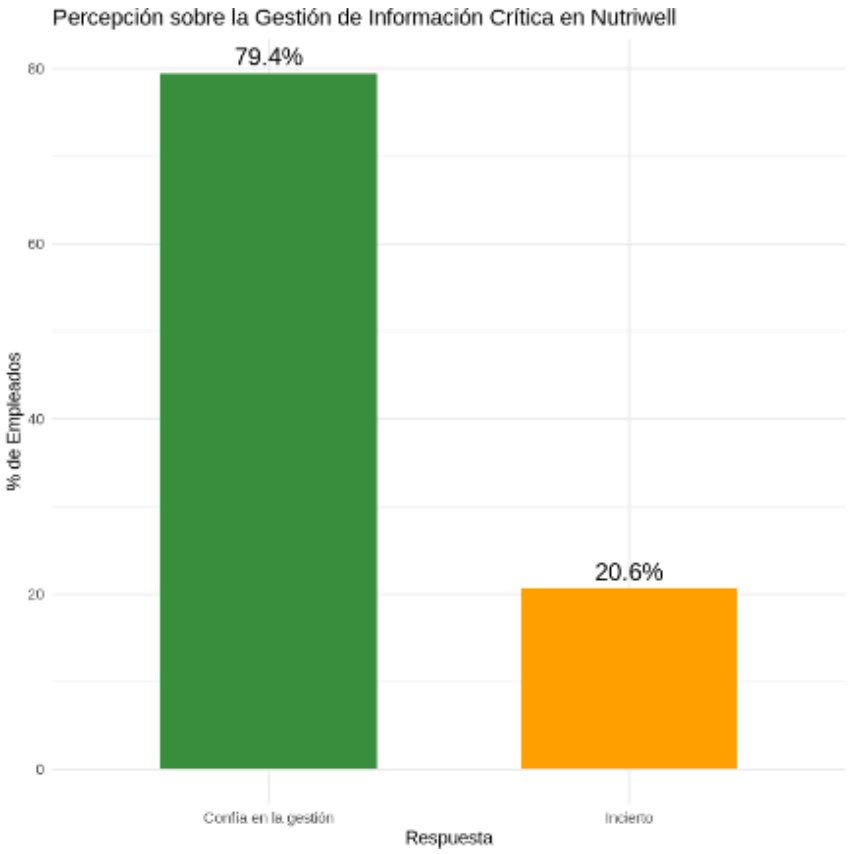
3.3.1. La Percepción Engañosa de la Gestión de Información Crítica (ID.AM-1): Un Riesgo Silencioso

-**Hallazgo:** Un 79.4% de los empleados cree que la información crítica se gestiona bien, pero un 20.6% está incierto.

-Obstáculo Principal: Falta de estandarización y comunicación clara de políticas, lo que genera interpretaciones dispares y una falsa sensación de seguridad. La ausencia de un sistema formalizado de gestión de activos críticos impide una gestión consistente. Tal como se muestra en la Figura 18.

Figura 18.

Percepción sobre la gestión de información Nutriwell.



Fuente: Elaboración propia.

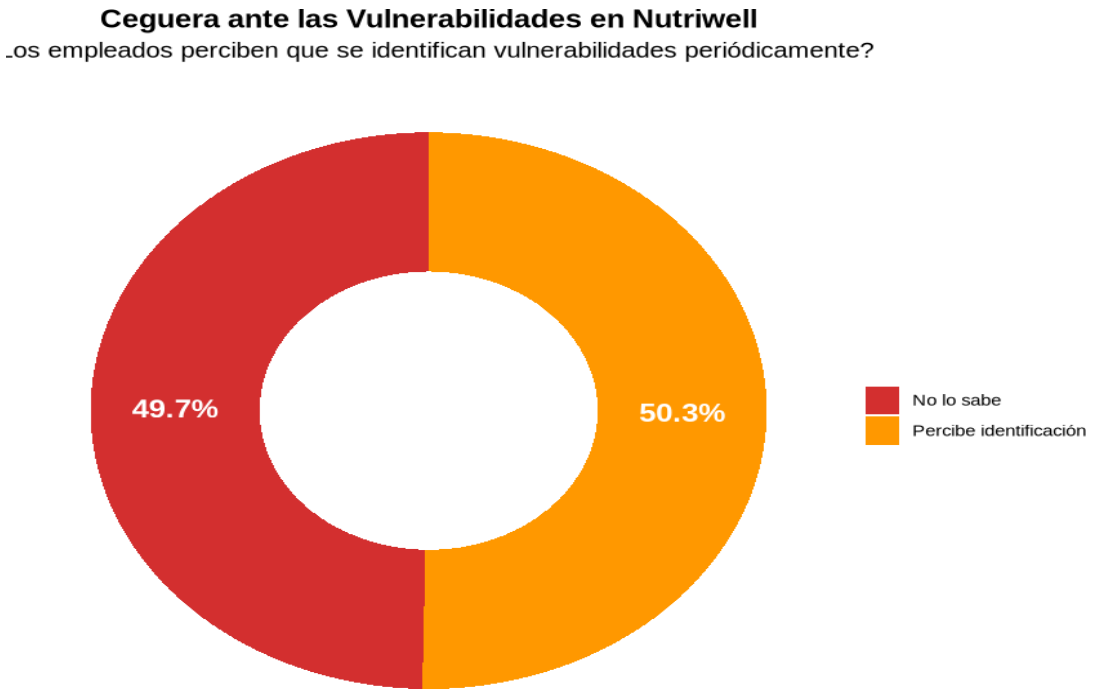
3.3.2. Ceguera Generalizada ante las Vulnerabilidades (ID.RA-2): Una Invitación a los Ciber atacantes

- **Hallazgo:** Solo el 50.3% de los empleados percibe que las vulnerabilidades se identifican y documentan periódicamente. Casi la mitad (49.7%) no lo sabe.

- **Obstáculo Principal:** Carencia de procesos formales y recursos especializados para evaluaciones de vulnerabilidades, sumado a una fragmentación entre departamentos que dificulta la visión integral. Tal como se muestra en la Figura 19**.**

Figura 19.

Gráfico de Pastel mostrando como se perciben las vulnerabilidades en Nutriwell.



Fuente: Elaboración propia.

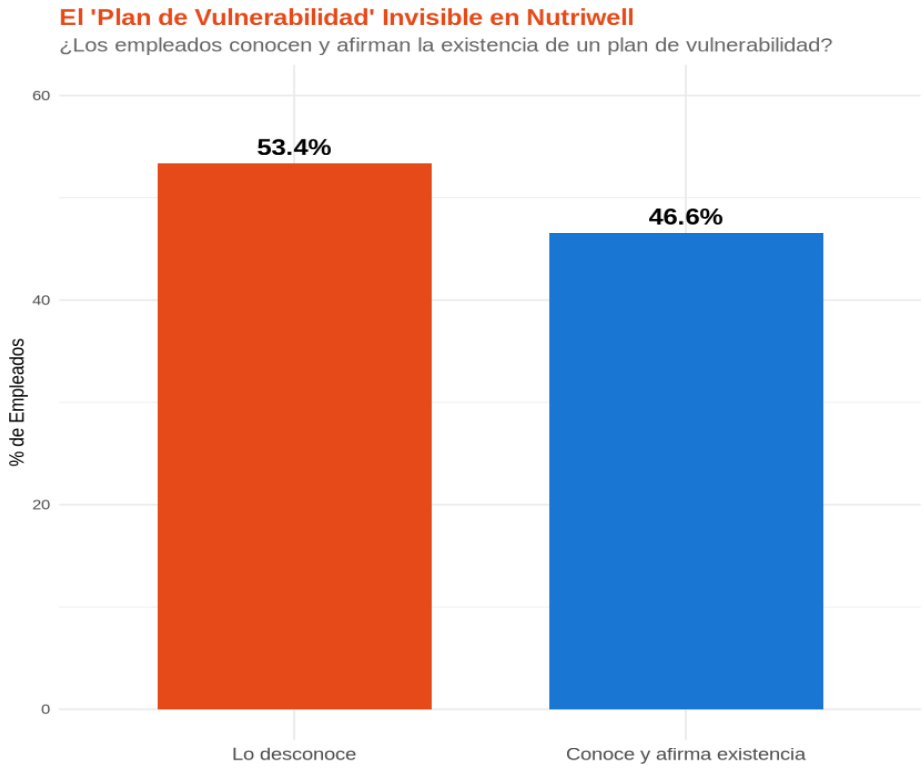
3.3.3. El "Plan de Vulnerabilidad" Invisible (ID.RA-3): Una Estrategia en Papel, No en la Práctica

- **Hallazgo:** Solo el 46.6% de los empleados afirma que existe un plan de vulnerabilidad elaborado y aplicado, mientras que el 53.4% lo desconoce.

Obstáculo Principal: Falta de comunicación y capacitación sobre el plan; ausencia de liderazgo en la implementación y seguimiento efectivo de estas estrategias. Tal como se muestra en la Figura 20.

Figura 20.

Conocimiento de vulnerabilidades en Nutriwell.



Fuente: Elaboración propia.

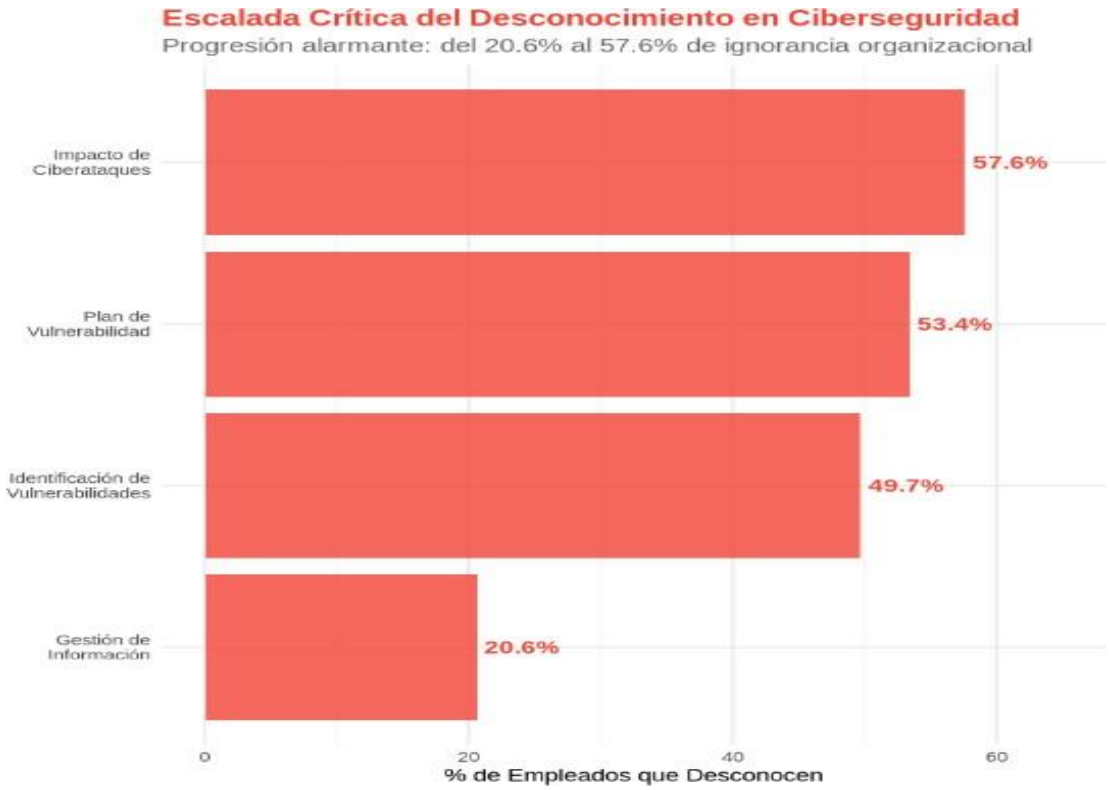
3.3.4. Desconocimiento del Impacto de los Ciberataques (ID.BA-1): Minimizando el Peligro Real

-Hallazgo: Solo el 42.4% de los empleados percibe que se analizan los impactos empresariales de los ciberataques. El 57.6% lo desconoce.

-Obstáculo Principal: Limitada sensibilización en todos los niveles, especialmente entre mandos operativos; escasa involucración de la alta dirección en la difusión del riesgo real. Tal como se muestra en la Figura 21.

Figura 21.

Escala de Desconocimiento de ciberseguridad.



Fuente: Elaboración propia.

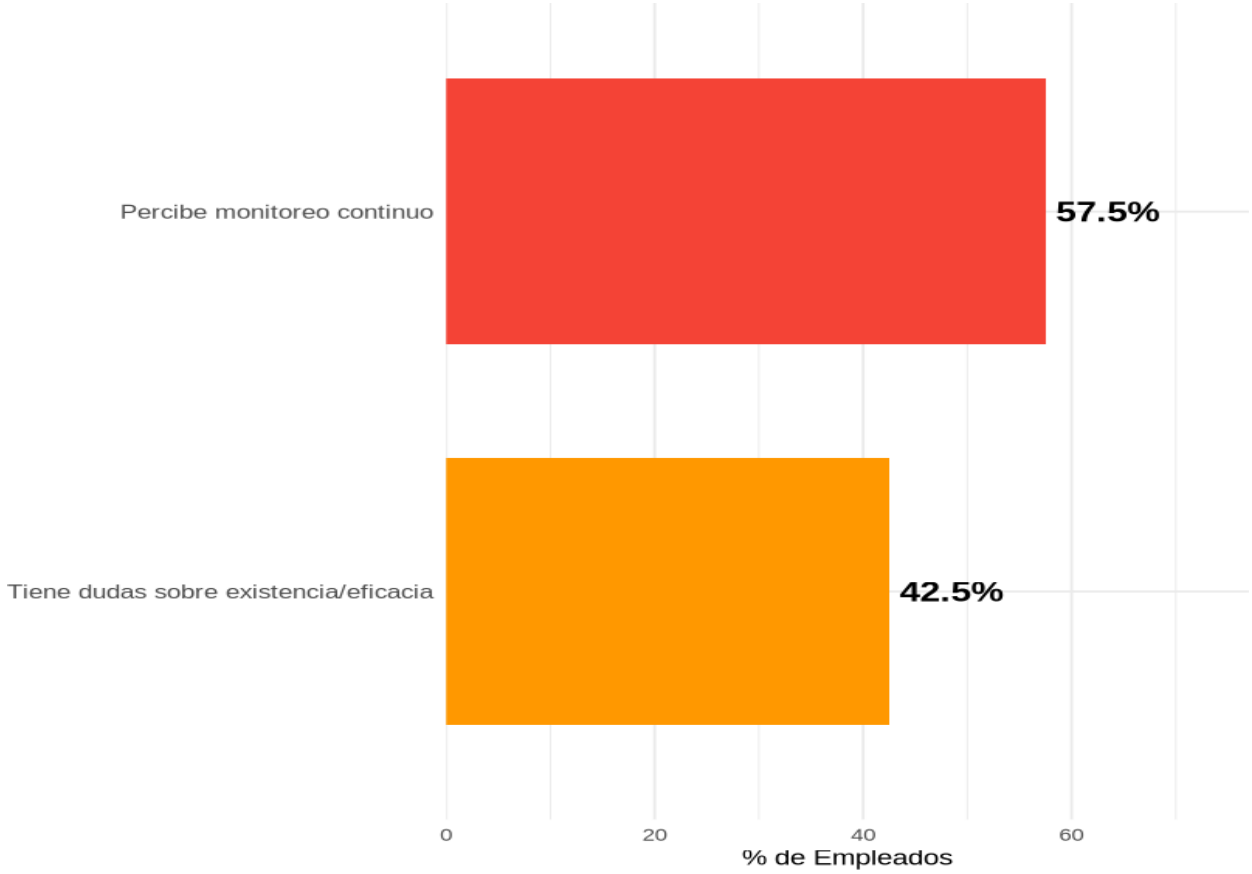
3.3.5. Monitoreo de Amenazas Inconstante (ID.AM-2): Operando a Ciegas ante el Peligro

- **Hallazgo:** El 57.5% de los empleados percibe un proceso de monitoreo continuo de amenazas, pero el 42.5% tiene dudas sobre su existencia o eficacia.

Obstáculo Principal: Insuficiencia de herramientas tecnológicas actualizadas y falta de personal capacitado para realizar monitoreo efectivo, además de una cultura organizacional que no prioriza esta actividad. Tal como se muestra en la Figura 22.

Figura 22.

Porcentaje de percepción sobre monitoreo de amenazas.



Fuente: Elaboración propia.

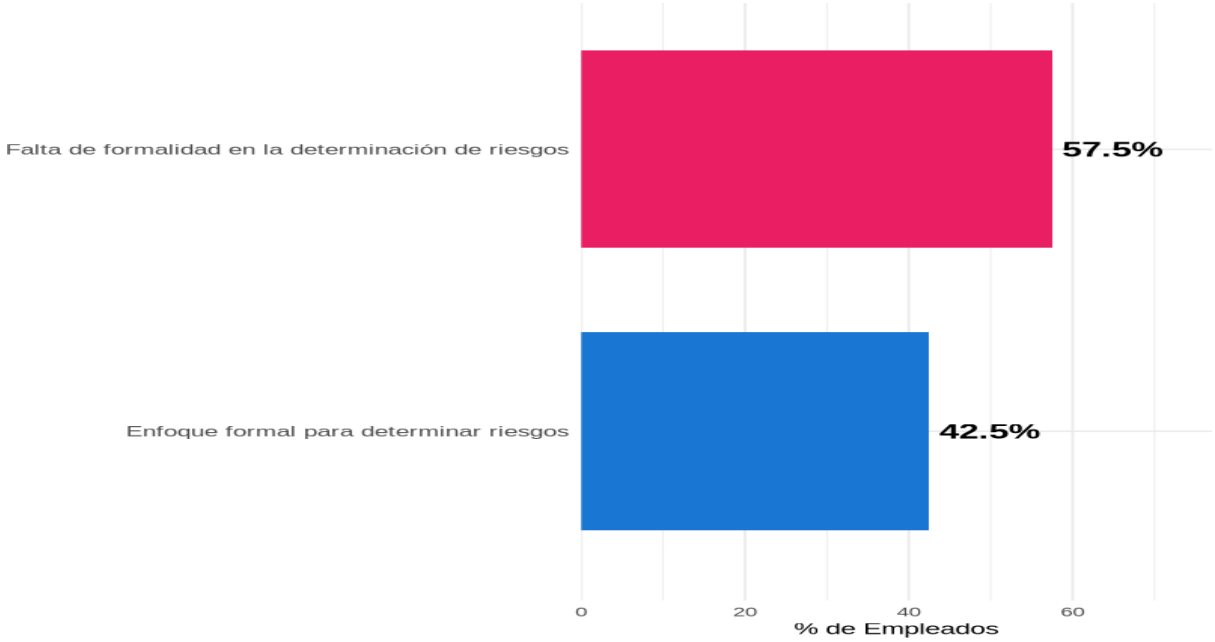
3.3.6. Determinación de Riesgos Informal y Peligrosa (ID.RM-1): Decisiones sin Fundamento

- **Hallazgo:** Solo el 42.5% de los empleados cree que se utiliza un enfoque formal para determinar los riesgos. El 57.5% percibe una falta de formalidad.

Obstáculo Principal: Ausencia de metodologías estandarizadas y de un marco regulatorio interno que guíe la gestión de riesgos, además de falta de compromiso institucional para priorizar esta función. Tal como se muestra en la Figura 23.

Figura 23.

Porcentaje de respuesta ante riesgos.



Fuente: Elaboración propia.

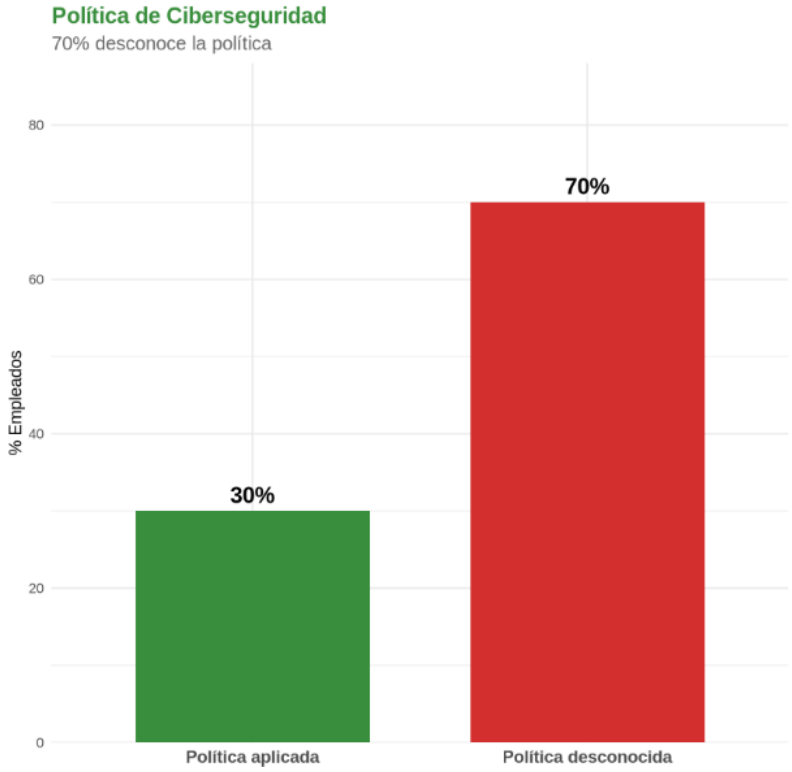
3.3.7. La Política de Ciberseguridad Ausente o Ignorada (ID.GV-1): Un Riesgo Legal y Operativo Masivo

- **Hallazgo:** Solo el 30% de los empleados afirma que la organización aplica y comunica una política de ciberseguridad formal. El 70% la desconoce.

- **Obstáculo Principal:** Deficiente comunicación interna, falta de cultura de cumplimiento y ausencia de mecanismos de control que aseguren la aplicación de políticas. Tal como se muestra en la Figura 24.

Figura 24.

Conocimiento de políticas de ciberseguridad.



Fuente: Elaboración propia.

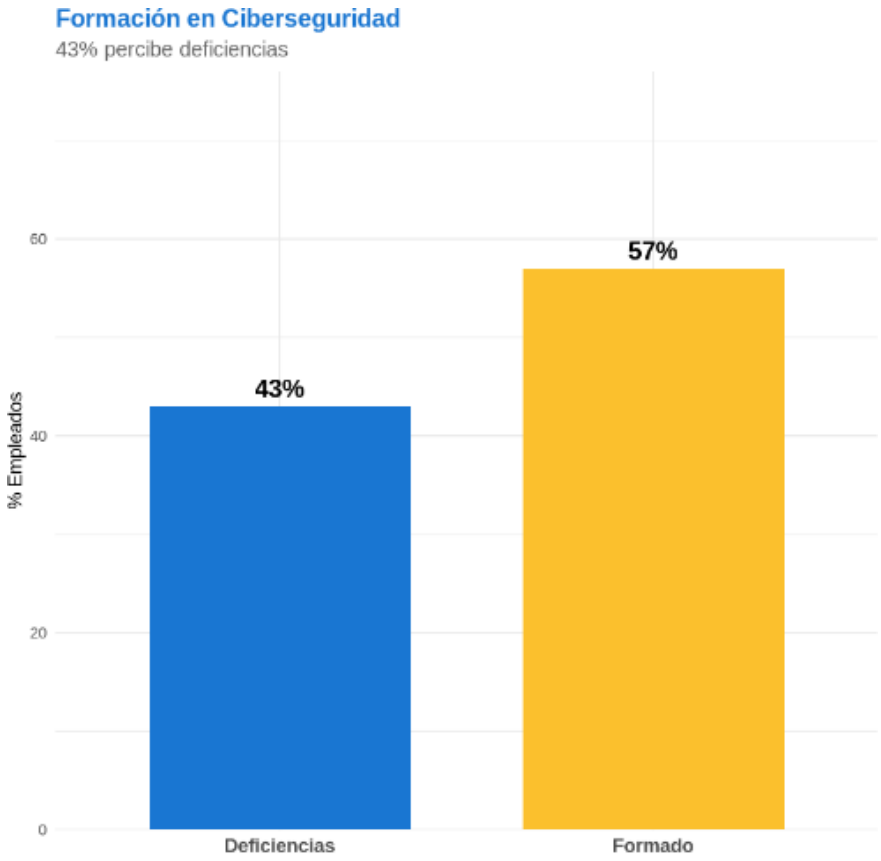
3.3.8. Formación en Ciberseguridad Inconsistente (ID.TA-1): Una Cadena Humana Débil

- **Hallazgo:** El 57% de los empleados se siente concienciado y formado, pero el 43% percibe deficiencias.

- **Obstáculo Principal:** Programas de capacitación poco estructurados y no personalizados por rol, combinados con falta de recursos para formación continua y actualización. Tal como se muestra en la Figura 25.

Figura 25.

Formación a nivel ciberseguridad.



Fuente: Elaboración propia.

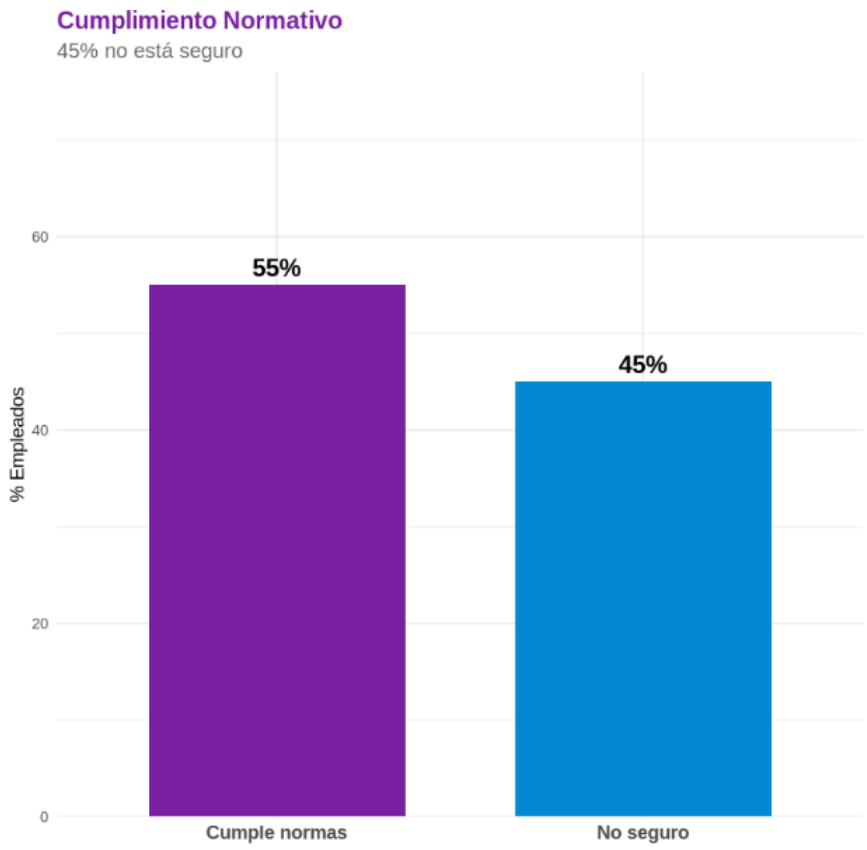
3.3.9. Cumplimiento Normativo Ambiguo (ID.IM-1): Abriendo la Puerta a Sanciones

- **Hallazgo**: El 55% de los empleados cree que la organización aplica las normas y reglamentos pertinentes, pero el 45% no está seguro.

Obstáculo Principal: Falta de claridad sobre normativas aplicables, ausencia de procesos de auditoría interna y escasa actualización ante cambios regulatorio. Tal como se muestra en la Figura 26.

Figura 26.

Porcentaje de cumplimiento normativo.



Fuente: Elaboración propia.

4. Conclusiones

Esta investigación, aunque parte de un marco general sobre la ciberseguridad en las PYMES, se sustenta en los hallazgos empíricos obtenidos mediante la evaluación directa de la empresa Nutriwell. Los resultados revelan una realidad contundente: las pequeñas y medianas empresas enfrentan riesgos digitales comparables, en complejidad y potencial impacto, a los de las grandes corporaciones, pero con una capacidad significativamente menor para gestionarlos de manera eficaz y sistemática. A partir del análisis, se identifican cinco conclusiones fundamentales:

Desconexión entre percepción y realidad en la gestión de información crítica

Un elevado porcentaje de empleados (79.4%) manifestó confianza en la gestión de la información crítica; sin embargo, un 20.6% expresó incertidumbre significativa. Esta disonancia evidencia una falsa sensación de seguridad que enmascara una débil comunicación interna y una ausencia de políticas claras y entendidas por todo el personal. La seguridad de la información no puede depender de percepciones optimistas, sino de protocolos robustos, visibles y compartidos.

Falta de visibilidad en la gestión de vulnerabilidades

Los hallazgos sobre la identificación de vulnerabilidades son preocupantes: solo el 50.3% de los empleados percibe que se detectan y documentan de forma periódica, y apenas el 46.6% reconoce la existencia de un plan formal de gestión. Esto sugiere que Nutriwell opera con una visión parcial o fragmentada de sus propios riesgos, lo que debilita cualquier intento de protección proactiva. La gestión de vulnerabilidades se realiza —cuando existe— de forma asistemática y poco comunicada.

Subestimación del impacto empresarial de los ciberataques

Menos de la mitad de la plantilla (42.4%) percibe que la empresa analiza el impacto que un incidente de ciberseguridad tendría sobre sus operaciones. Esta carencia de análisis y sensibilización impide priorizar acciones estratégicas, justificar inversiones en protección, o incluso planear una respuesta efectiva. En otras palabras, la organización desconoce las consecuencias reales de no estar preparada.

Debilidad estructural en políticas, formación y gobernanza

La ausencia de una política de ciberseguridad formalmente comunicada (reconocida por solo el 30% del personal) y la formación inconsistente (43% percibe deficiencias) revelan una gobernanza débil. Sin lineamientos claros ni capacitación continua, el factor humano —principal vector de riesgo o defensa— permanece expuesto y sin herramientas adecuadas para actuar. Esta fragilidad compromete la capacidad de la organización para prevenir y responder a incidentes.

Madurez superficial y necesidad urgente de estrategia proactiva

Si bien Nutriwell reconoce teóricamente los riesgos, la aplicación práctica de medidas de ciberseguridad resulta desigual, poco institucionalizada y reactiva. Esta madurez superficial no basta ante un entorno de amenazas dinámico y sofisticado. Las PYMES como Nutriwell necesitan avanzar hacia un modelo de ciberresiliencia basado en riesgo, donde las decisiones se tomen con base en información, procedimientos claros y métricas confiables.

A pesar de los retos detectados, esta investigación logró establecer avances significativos para Nutriwell y, por extensión, para otras PYMES en contextos similares:

Se estableció una línea base de madurez en ciberseguridad, útil como punto de partida para mejoras estructuradas.

Se evaluó la eficacia real de las estrategias existentes, evidenciando brechas que requieren atención inmediata.

Se identificaron y priorizaron los principales riesgos de ciberseguridad, facilitando la asignación racional de recursos.

Se midió el nivel de conciencia organizacional sobre ciber resiliencia, destacando los segmentos más vulnerables.

Se desarrolló un índice de madurez personalizado, así como un modelo de implementación escalonado, diseñado para ser rentable y aplicable en empresas con recursos limitados.

Recomendaciones finales

Las PYMES deben transitar con urgencia de un enfoque reactivo a uno proactivo y basado en riesgos, que trascienda la adquisición de tecnología y se enfoque en personas, procesos y cultura organizacional. La implementación de políticas claras, la formación continua y la elaboración de planes de respuesta efectivos ya no son opcionales: son condiciones esenciales para la continuidad operativa y la confianza de clientes y socios.

Asimismo, las futuras investigaciones deberían enfocarse en:

El impacto económico concreto de los incidentes de seguridad en las PYMES.

El rol de la cultura organizacional en la adopción efectiva de prácticas de ciberseguridad.

La identificación de vulnerabilidades específicas por sector.

El uso de inteligencia artificial como catalizador para mejorar la detección y respuesta.

Por último, se hace un llamado a los organismos gubernamentales y asociaciones empresariales para que refuercen sus programas de apoyo, capacitación y financiamiento en

materia de ciberseguridad para PYMES. Solo mediante un esfuerzo articulado será posible cerrar la brecha entre riesgo y resiliencia.

La ciberseguridad no es un lujo ni un gasto: es una inversión estratégica que puede definir la supervivencia de una empresa.

Referencias

Agustina. (2022, 27 de junio). *Kaspersky: las PYMEs de América Latina enfrentan un creciente número de ciberataques*. Prensario Tila. https://prensariotila.com/kaspersky-las-PYMEs-de-america-latina-enfrentan-un-creciente-numero-de-ciberataques/

Alter, S. (2002). *Information Systems. The Foundations of E-Business* (4.ª ed.). Pearson.

BBC News Mundo. (2016, 16 de diciembre). *Cómo fue el 'hackeo' de piratas informáticos de Rusia durante las elecciones de Estados Unidos*. BBC News Mundo. https://www.bbc.com/mundo/noticias-38343716

Bind ERP Staff. (2023, 31 de mayo). *Las PYMEs en México: su importancia en la economía del país*. Bind ERP. https://bind.com.mx/blog/emprendimiento-y-estrategia/las-PYMEs-en-mexico

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Bada, A., Sasse, M. A., & Nurse, J. R. C. (2019). Cyber Security Awareness Campaigns: Why do they fail to change behaviour? arXiv preprint arXiv:1901.02672.

Cabezas, G. A. Q. (2023, 4 de enero). *Riesgos en la gestión de proyectos: Conoce las amenazas.* Proyectos. https://proyectospro.uno/riesgos-en-la-gestion-de-proyectos-conoce-las-amenazas/

Casa Blanca. (2013, 12 de febrero). *Executive Order 13636: Improving Critical Infrastructure Cybersecurity*. https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-criticalinfrastructure-cybersecurity

Ciberseg. (2021, 17 de noviembre). *Metodologías de evaluación de riesgos cibernéticos.* Ciberseguridad. https://ciberseguridad.com/herramientas/metodologias-evaluacion-riesgos-ciberneticos/

Ciberseg. (2022, 28 de febrero). *Ciberespacio: definición, aplicaciones y límites*. Ciberseguridad. https://ciberseguridad.com/guias/recursos/ciberespacio/

Ciberseguridad. (2021). *InfoSecurity Mexico*. https://www.infosecuritymexico.com/es/ciberseguridad.htm

Colosio Riojas, L. D., & Trasviña Waldenrath, J. L. (2025, 30 de abril). *Iniciativa con proyecto de decreto por el que se expide la Ley de Ciberseguridad*. Senado de la República. https://infosen.senado.gob.mx/sgsp/gaceta/66/1/2025-04-30-1/assets/documentos/Inic_MC_Sen_Colosio_ciberseguridad.pdf

Creswell, J. W., & Plano Clark, V. L. (2018). *Designing and Conducting Mixed Methods Research* (3rd ed.). SAGE Publications.

Creswell, J. W., & Poth, C. N. (2018). *Qualitative Inquiry and Research Design: Choosing Among Five Approaches* (4th ed.). SAGE Publications.

Cybereop. (2019). *Casi el 70 por ciento de las PYMEs experimentan ataques cibernéticos*. https://www.cybereop.com/blog/casi-el-70-por-ciento-de-las-PYMEs-experimentan-ataques-ciberneticos.html

Davenport, T. (2000). *Mission Critical. Realizing the Promise of Enterprise Systems*. Harvard Business School Press.

De DocuSign, C. (2023, 15 de marzo). *¿Cuántas PYMES hay en México y qué datos relevantes sobre estas debemos considerar?* DocuSign. https://www.docusign.com/es-mx/blog/cuantas-PYMEs-hay-en-mexico

Deutsche Welle. (2021, 4 de abril). *Filtran línea datos de 533 millones de usuarios de Facebook*. DW. https://www.dw.com/es/filtran-datos-de-533-millones-de-usuarios-de-facebook-en-foro-de-ciberpiratas/a-57095450

Dieterich, H. (1999). *Nueva guía para la investigación científica* (7.ª reimpr.). Editorial Ariel.

ESET. (2024, 18 de julio). *30% de las organizaciones latinoamericanas sufrió al menos un incidente de ciberseguridad en 2023*. ESET Latinoamérica.

Espolines de Garín. (2023, 27 de marzo). *La revolución de la máquina Jacquard*. https://garin1820.com/la-revolucion-de-la-maquina-jacquard/

Fernández, Y. (2018, 6 de mayo). *La historia de Creeper, el primer virus informático jamás programado*. Xataka. https://www.xataka.com/historia-tecnologica/la-historia-de-creeper-el-primer-virus-informatico-jamas-programado

Fuentes Rivera, S. (2023, 18 de enero). *Ley de Ciberseguridad en México: Conoce la nueva Ley*. Delta Protect. https://www.deltaprotect.com/blog/ley-de-ciberseguridad-mexico

GlobalSuite Solutions. (2023, 22 de septiembre). *¿Qué es la norma ISO 27001 y para qué sirve?* https://www.globalsuitesolutions.com/es/que-es-la-norma-iso-27001-y-para-que-sirve/#:~:text=La%20norma%20ISO%2027001%20es,y%20disponibilidad%20de%20la%20informaci%C3%B3n.

Golombek, J. B. (2021, 22 de noviembre). *Promover la ciberresiliencia de las PYMEs ante la crisis*. El Sol de México. https://www.elsoldemexico.com.mx/analisis/promover-la-ciberresiliencia-de-las-PYMEs-ante-la-crisis-9201965.html

Gómez Vieites, A., & Suárez Rey, C. (2005). *Sistemas de Información: herramientas prácticas para la gestión empresarial* (2.ª ed.). Ra-Ma Editorial.

Hernández, R., Fernández, C., & Baptista, P. (2022). *Metodología de la investigación* (7.ª ed.). McGraw-Hill.

Hipertextual. (2022, 15 de marzo). *La máquina analítica: el ordenador que necesitó 150 años para existir*. https://hipertextual.com/2022/03/maquina-analitica-charles-babbage

IBM. (2020, 12 de diciembre). *¿Qué es un actor de amenazas?* https://www.ibm.com/mx-es/topics/threat-actor#:~:text=Los%20actores%20de%20amenazas%2C%20tambi%C3%A9n,a%20dispositivos%20o%20sistemas%20digitales.

IBM. (2021). *¿Qué es el marco de ciberseguridad del NIST?* https://www.ibm.com/mx-es/topics/nist

Iberdrola. (2021, 29 de junio). *Ciberataques*. https://www.iberdrola.com/innovacion/ciberataques

InvGate. (2022, 25 de octubre). *Los 14 tipos de ciberataques más comunes (y cómo prevenirlos)*. InvGate Blog.

IT Digital Media Group. (2023, 19 de abril). *El 90% de las organizaciones ha sufrido una brecha de ciberseguridad en cloud*. Actualidad | IT Digital Security. https://www.itdigitalsecurity.es/actualidad/2023/04/el-90-de-las-organizaciones-ha-sufrido-una-brecha-de-ciberseguridad-en-cloud

Kantan Software. (2023, 14 de noviembre). *ISO 27001: Un estándar para la seguridad en el mundo digital y físico*. https://www.kantansoftware.com/blog/iso-27001-un-estandar-para-la-seguridad-en-el-mundo-digital-y-fisico/

Kaspersky. (2018, 2 de noviembre). *Aniversario del gusano Morris*. Blog oficial de Kaspersky. https://www.kaspersky.es/blog/morris-worm-anniversary/17498/

Kaspersky. (2023, 13 de diciembre). *¿Qué es la ciberseguridad?* latam.kaspersky.com. https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

KeepCoding Bootcamps. (2023, 14 de noviembre). *¿Qué es el gusano Morris?* https://keepcoding.io/blog/que-es-el-gusano-morris/

KeepCoding Bootcamps. (2023, 22 de noviembre). *¿Qué es AIDS Trojan?* https://keepcoding.io/blog/que-es-aids-trojan/

Laudon, K. C., & Laudon, J. P. (2006). *Management Information Systems: Managing the digital firm* (9.ª ed.). Pearson Prentice Hall.

Leon, A. (2007). *Enterprise Resource Planning Systems*. Tata McGraw-Hill Publishing Company Limited.

LISA News. (2022, 9 de febrero). *Perspectivas de ciberseguridad en 2022, según el Foro Económico Mundial*. https://www.lisanews.org/actualidad/perspectivas-ciberseguridad-2022/

Lizarazo, C. (2023, 14 de agosto). *Las PYMEs en México: Retos e Importancia*. Conekta. https://www.conekta.com/blog/las-PYMEs-en-mexico-retos-e-importancia

Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P., Allen, J., & Kott, A. (2013). Resilience metrics for cyber systems. Environment Systems and Decisions, 33(4), 471–476. https://doi.org/10.1007/s10669-013-9485-y

Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). (2023). *Política de Espectro*. https://www.mintic.gov.co/portal/715/w3-article-161217.html

N. Teodoro, L. Goncalves, & C. Serr~ao. (2015). *NIST cybersecurity framework compliance: A generic model for dynamic assessment and predictive requirements*. En *Trustcom/BigDataSE/ISPA, 2015 IEEE* (Vol. 1, pp. 418–425). IEEE.

NIST. (2013). *NIST 800-53 Rev.4*. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf

NIST. (2022, 13 de junio). *NIST Releases Version 1.1 of its Popular Cybersecurity Framework*. https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework

O'Brien, J. A., & Marakas George, M. (2006). *Management Information Systems* (7.ª ed.). McGraw-Hill Irwin.

O'Leary, D. E. (2000). *Enterprise Resource Planning Systems: Systems, Life Cycle, Electronic Commerce, and Risk*. Cambridge University Press.

Olson, D. L., & Kesharwani, S. (2009). *Enterprise Information Systems: Contemporary Trend and Issues*. World Scientific.

Ortega, C. (2024, 15 de enero). *Investigación analítica: Qué es, importancia y ejemplos*. QuestionPro. https://www.questionpro.com/blog/es/investigacion-analitica/

OSTEC. (2023, 28 de abril). *Firewall: Historia*. OSTEC | Segurança digital de resultados. https://www.ostec.com.br/blog/firewall-historia-seguranca-digital-resultados/

Ozkan, B. Y., van Lingen, S., & Spruit, M. (2021). The Cybersecurity Focus Area Maturity (CYSFAM) Model. *J. Cybersecur. Priv.*, *1*, 119–139.

Pérez, J. (2019). Estudio de la salud en América Latina. *Journal of Health Studies*, *22*(4), 487–500. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202019000400487

Qualtrics. (2023, 26 de octubre). *Investigación cuantitativa*. https://www.qualtrics.com/es-la/gestion-de-la-experiencia/investigacion/investigacion-cuantitativa/

Randstad. (2024, 5 de febrero). *La Pirámide de Maslow en la empresa*. https://www.randstad.es/contenidos360/desarrollo-personal/la-piramide-de-maslow-en-

el-ambito-laboral/#:~:text=La%20Pir%C3%A1mide%20de%20Maslow%E2%80%8B,teor%C3%ADa%20sobre%20la%20motivaci%C3%B3n%20humana%E2%80%9D

Roco-Videla, Á., Orellana, M. H., & González, O. S. (2021). What is the appropriate sample size to validate a questionnaire? *Nutricion Hospitalaria*. https://doi.org/10.20960/nh.03633

Romero, O., & Romero, O. (2023, 29 de noviembre). *Hacia la ciberresiliencia: cómo la PYMEs puede preservar la seguridad empresarial en la era de las amenazas constantes*. RevistaPYMES.es. https://revistapymes.es/hacia-la-ciberresiliencia-como-la-PYMEs-puede-preservar-la-seguridad-empresarial-en-la-era-de-las-amenazas-constantes/

Saint Leo University. (2023, 14 de noviembre). *¿Cuál es la historia de la Ciberseguridad?* https://worldcampus.saintleo.edu/noticias/historia-de-la-ciberseguridad

Saiz Miranda, J. (2022). *Arquitecturas y seguridad en sistemas de control industrial e IoT para infraestructuras críticas* [Trabajo Fin de Máster, Universitat Politècnica de València, Escuela Técnica Superior de Ingeniería Informática]. RIUNET.

Smith, J. (2023). *Metodologías para la gestión de riesgos de ciberseguridad y su potencial interoperabilidad*. We Live Security. https://www.welivesecurity.com/la-es/2023/04/05/metodologias-gestion-riesgos-ciberseguridad-potencial-interoperabilidad/

Solís, L. D. M. (2020, 22 de septiembre). *El enfoque cualitativo de investigación*. Investigalia. https://investigaliacr.com/investigacion/el-enfoque-cualitativo-de-investigacion/

Tofan, D. (2011). Information Security Standards. *J. Mob. Embed. Distrib. Syst.*, *3*, 128–135.

TS4 Strategy. (2023, 5 de octubre). *El Internet de las cosas (IoT): El Futuro Conectado*. https://ts4.mx/blog/el-internet-de-las-cosas-iot-el-futuro-conectado/#:~:text=Se%20estima%20que%20para%20el,inteligentes%20hasta%20soluci

ones%20industriales%20avanzadas.&text=Una%20de%20las%20%C3%A1reas%20m%C3%A1s,aplicaci%C3%B3n%20pr%C3%A1ctica%20en%20diversos%20sectores.

Valle, M. (2022, 19 de octubre). *El 78% de las PYMEs reconocen no estar preparadas en ciberseguridad*. Bit Life Media. https://bitlifemedia.com/2022/10/el-78-de-las-PYMEs-reconocen-no-estar-preparadas-en-ciberseguridad/

Whitman, M. E., & Mattord, H. J. (2022). Principles of Information Security (7th ed.). Cengage Learning.

Apéndices

Este apartado presenta los materiales complementarios que respaldan el trabajo de campo realizado en la empresa Nutriwell, permitiendo una comprensión más profunda del enfoque metodológico mixto adoptado y fortaleciendo la validez de los hallazgos obtenidos en la investigación.

Apéndice A: Cuestionario aplicado a los empleados de Nutriwell

Instrumento estructurado basado en las cinco funciones del Marco de Ciberseguridad del NIST (Identificar, Proteger, Detectar, Responder y Recuperar). Diseñado con escala Likert y validado mediante prueba piloto.

Ítems alineados con las subcategorías del NIST versión 2021.

Evaluación del grado de implementación, percepción organizacional y formación interna.

Aplicado a 169 empleados de diferentes áreas y niveles jerárquicos.

Función NIST	**Subcategoría**	**Pregunta**	**Escala de respuesta**
Identificar	ID.AM-1	¿Se gestiona el conocimiento de los activos de la organización?	1 (Nunca) – 5 (Siempre)
Identificar	ID.RA-2	¿Se identifican y documentan periódicamente las vulnerabilidades?	1 – 5

Función NIST	Subcategoría	Pregunta	Escala de respuesta
Identificar	ID.BA-1	¿Se analizan los impactos empresariales de los ciberataques?	1 – 5
Proteger	PR.AC-1	¿Se controlan adecuadamente los accesos a sistemas y activos?	1 – 5
Proteger	PR.AT-1	¿El personal recibe capacitación en ciberseguridad según su rol?	1 – 5
Detectar	DE.CM-1	¿Se monitorean continuamente los sistemas para detectar anomalías?	1 – 5
Detectar	DE.AE-1	¿Se utilizan herramientas para detectar actividades no autorizadas?	1 – 5
Responder	RS.RP-1	¿Existe un plan documentado y probado de respuesta a incidentes?	1 – 5
Responder	RS.AN-1	¿Se realizan análisis post-incidente para identificar causas raíz?	1 – 5
Recuperar	RC.RP-1	¿La organización cuenta con un plan de recuperación ante desastres?	1 – 5
Recuperar	RC.CO-1	¿Se coordina la comunicación de recuperación con stakeholders?	

	A	B	C	D
	Función NIST	**Subcategoría**	**Pregunta**	**Escala de respuesta**
	Identificar	ID.AM-1	¿Se gestiona el conocimiento de los activos de	1 (Nunca) – 5 (Siempre)
	Identificar	ID.RA-2	¿Se identifican y documentan periódicamente	1 (Nunca) – 5 (Siempre)
	Identificar	ID.BA-1	¿Se analizan los impactos empresariales de los	1 (Nunca) – 5 (Siempre)
	Proteger	PR.AC-1	¿Se controlan adecuadamente los accesos a sis	1 (Nunca) – 5 (Siempre)
	Proteger	PR.AT-1	¿El personal recibe capacitación en ciberseguri	1 (Nunca) – 5 (Siempre)
	Detectar	DE.CM-1	¿Se monitorean continuamente los sistemas p	1 (Nunca) – 5 (Siempre)
	Detectar	DE.AE-1	¿Se utilizan herramientas para detectar activid	1 (Nunca) – 5 (Siempre)
	Responder	RS.RP-1	¿Existe un plan documentado y probado de res	1 (Nunca) – 5 (Siempre)
0	Responder	RS.AN-1	¿Se realizan análisis post-incidente para identi	1 (Nunca) – 5 (Siempre)
1	Recuperar	RC.RP-1	¿La organización cuenta con un plan de recuper	1 (Nunca) – 5 (Siempre)
2	Recuperar	RC.CO-1	¿Se coordina la comunicación de recuperación	1 (Nunca) – 5 (Siempre)
3				
4				

Apéndice B: Carta de consentimiento informada

Documento utilizado para garantizar la participación voluntaria, ética y consciente de los colaboradores. Adaptado con lenguaje claro y presentado mediante sesiones explicativas.

Objetivos, derechos y protección de datos.

Firma individual y acompañamiento del área de Recursos Humanos.

Referido como Apéndice B en la sección metodológica.

Toluca, Estado de México — Septiembre de 2023

CARTA DE CONSENTIMIENTO INFORMADO

Por medio de la presente, yo, _____, colaborador(a) de la empresa Nutriwell, ubicada en Luis Gutiérrez Dosal 140, Parque Industrial Exportec II, San Miguel Totoltepec, Estado de México, manifiesto que he sido informado(a) sobre los objetivos, alcances y metodología del estudio titulado *"La ciberresiliencia en las PYMEs: Metodología para un entorno digital seguro"*, desarrollado por el investigador Yoxan Smilyn González Higueros como parte de su tesis doctoral en la Universidad UNADE de México.

Declaro que:

- He recibido una explicación clara y comprensible sobre el propósito de la investigación, los instrumentos que se aplicarán (encuestas, entrevistas, simulaciones), y el uso que se dará a la información recolectada.
- Entiendo que mi participación es **voluntaria**, que puedo retirarme en cualquier momento sin repercusiones, y que los datos serán tratados de forma **confidencial y anonimizada**, conforme a la legislación vigente en materia de protección de datos personales.

- Autorizo el uso de mis respuestas exclusivamente para fines académicos y científicos, sin que se vincule mi identidad personal o laboral en ningún momento.
- Reconozco que no existen riesgos físicos ni psicológicos derivados de mi participación, y que el estudio busca fortalecer la ciberseguridad organizacional de manera ética y profesional.

Firma del participante: _____ Nombre completo:

_____ Área o departamento: _____

Fecha: _____

Firma del investigador: _____ Nombre: Yoxan Smilyn González Higueros **Doctorado en Proyectos – Universidad UNADE**

Toluca, Estado de México — septiembre de 2023

CARTA DE CONSENTIMIENTO INFORMADO

Por medio de la presente, yo, _____, colaborador(a) de la empresa Nutriwell, ubicada en Luis Gutiérrez Dosal 140, Parque Industrial Exportec II, San Miguel Totoltepec, Estado de México, manifiesto que he sido informado(a) sobre los objetivos, alcances y metodología del estudio titulado *"La ciberresiliencia en las PYMEs: Metodología para un entorno digital seguro"*, desarrollado por el investigador Yoxan Smilyn González Higueros como parte de su tesis doctoral en la Universidad UNADE de México.

Declaro que:

He recibido una explicación clara y comprensible sobre el propósito de la investigación, los instrumentos que se aplicarán (encuestas, entrevistas, simulaciones), y el uso que se dará a la información recolectada.

Entiendo que mi participación es **voluntaria**, que puedo retirarme en cualquier momento sin repercusiones, y que los datos serán tratados de forma **confidencial y anonimizada**, conforme a la legislación vigente en materia de protección de datos personales.

Autorizo el uso de mis respuestas exclusivamente para fines académicos y científicos, sin que se vincule mi identidad personal o laboral en ningún momento.

Reconozco que no existen riesgos físicos ni psicológicos derivados de mi participación, y que el estudio busca fortalecer la ciberseguridad organizacional de manera ética y profesional.

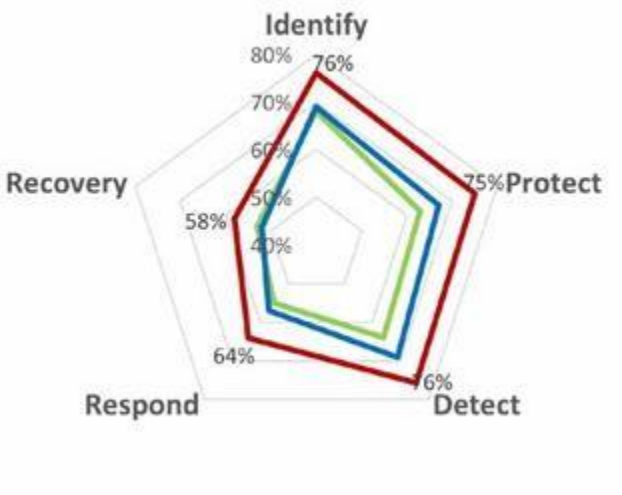
Firma del participante: _____ **Nombre completo:** _____ **Área o departamento:** _____
Fecha: _____

Firma del investigador: _____ **Nombre:** Yoxan Smilyn González Higueros **Doctorado en Proyectos – Universidad UNADE**

Apéndice C: Tablas y figuras complementarias del trabajo de campo

Conjunto de gráficos, instrumentos y matrices desarrolladas por el autor:

Gráfico de radar del Índice de Madurez Cibersegura (CMI).

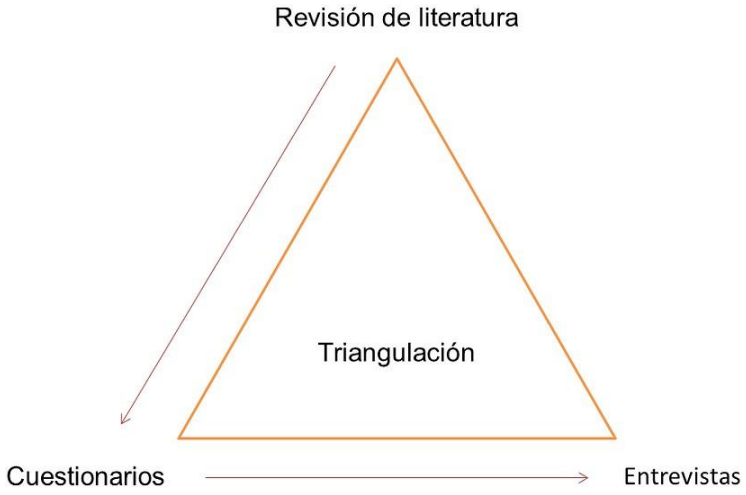


Tablas de análisis por función NIST (Identificar, Proteger, Detectar, etc.).

FUNCIÓN IDENTIFICADOR ÚNICO	FUNCIONES	CATEGORÍA IDENTIFICADOR ÚNICO	CATEGORIAS
ID	IDENTIFICAR	ID.AM	Gestión de activos
		ID.BE	Ambiente de negocios
		ID.GV	Gobernanza
		ID.RA	Evaluación de riesgos
		ID.RM	Estrategia de gestión de riesgos
		ID.SC	Gestión del riesgo de la cadena de suministro
PR	PROTEGER	PR.AC	Gestión de identidad, autenticación y control de acceso
		PR.AT	Conciencia y capacitación
		PR.DS	Seguridad de datos
		PR.IP	Procesos y procedimientos de protección de la información
		PR.MA	Mantenimiento
		PR.PT	Tecnología de protección
DE	DETECTAR	DE.AE	Anomalías y Eventos
		DE.CM	Monitoreo continuo de seguridad
		DE.DP	Procesos de Detección
RS	RESPONDER	RS.RP	Planificación de respuesta
		RS.CO	Comunicaciones
		RS.AN	Análisis
		RS.MI	Mitigación
		RS.IM	Mejoras
		RS.RP	Planificación de respuesta
RC	RECUPERAR	RC.RP	Planificación de la recuperación
		RC.IM	Mejoras
		RC.CO	Comunicaciones

Figuras 18–26 que muestran la percepción sobre políticas, vulnerabilidades, capacitación y cumplimiento normativo.

Matrices de correspondencia entre variables cualitativas y cuantitativas para triangulación.



Apéndice D: Bitácoras de análisis y formatos internos

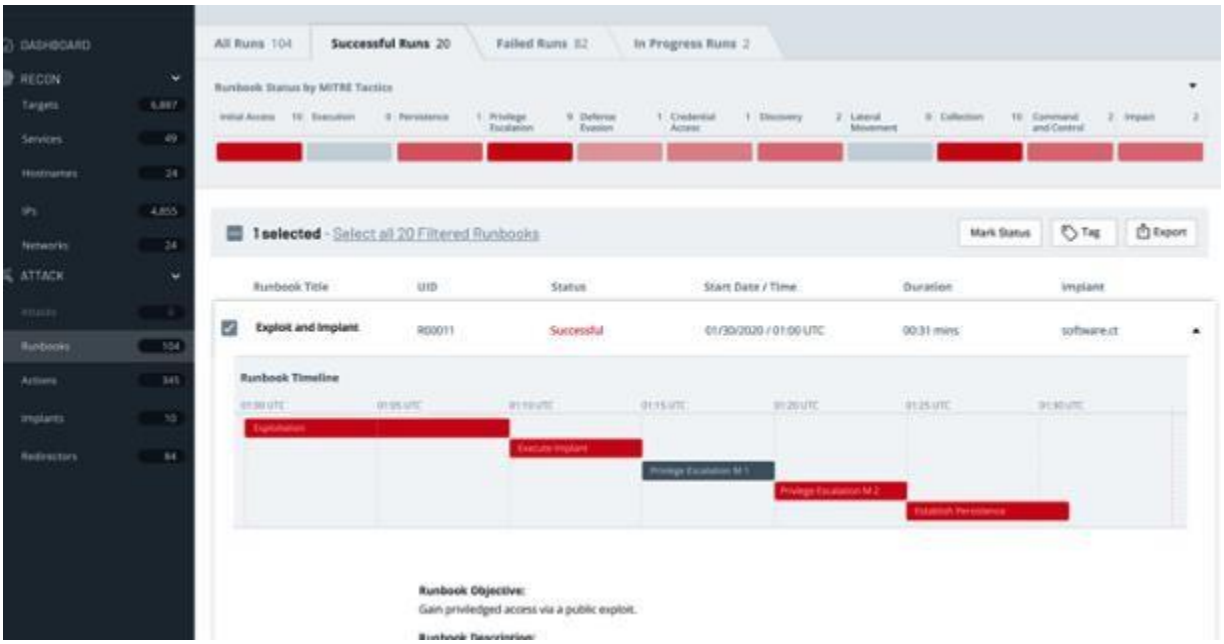
Material auxiliar utilizado en entrevistas, simulaciones y auditoría de ciberseguridad:

Registro de entrevistas (fechas, roles, temas).

Registro de entrevistas

Fecha	Rol	Temas
10/04/2023	Gerente de TI	Estrategias de backup y recuperación
13/04/2023	Analista de seguridad	Mecanismos de detección de amenazas
17/04/2023	Coordinador de operaciones	Capacitación en ciberseguridad
20/04/2023	CEO	Politicas de ciberseguridad

Formatos de simulación BAS con herramientas de código abierto.



Matriz de grupos de interés y mapeo de ciberinfluencia aplicada a Nutriwell.

Escala de evaluacion

	ESCALAS	DEFINICIÓN	1	DEFINICIÓN	4	DEFINICIÓN
IMPACTOS	Riesgos	Un Grupo de Interés tiene herramienta para generar contingencia o daño a la empresa	Seguridad Total	La empresa cuenta con los mecanismos que la dejan exenta de todo daño o contingencia debido al riesgo que implican las acciones de los Grupos de Interés.	Desprotección	La empresa tiene un alto riesgo de paralizar sus funciones operativas y administrativas debido al riesgo que implican las acciones de los Grupos de Interés.
	Oportunidades	El Grupos de Interés genera oportunidades para la empresa	Lejano	El Grupo de Interés no presenta oportunidades significativas para la empresa	Cercano	El Grupo de Interés presenta oportunidades significativas para la empresa.
INFLUENCIA	Poder	Un Grupo de interés tiene el poder para ejercer su voluntad sobre la empresa	Nulo poder de decisión	La empresa no genera espacio para la toma de decisiones, y el Grupo de interés no cuenta con poder para establecer canales de diálogo.	Total poder de decisión	La empresa genera espacios para la toma de decisión, y el grupo de interés cuenta con el poder en los canales de diálogo
	Legitimidad	Un Grupo de Interés percibe a la empresa con un comportamiento inserto en un sistema social de leyes, normas, valores y creencias.	Participante pasivo	El Grupo de Interés actúa de observador frente al actuar de la empresa	Líder de opinión	El grupo de interés se legitimiza y empodera en su accionar, situando a la empresa en una posición favorable o desfavorable.
	Urgencia	Un Grupo de Interés presenta la cualidad de urgente frente a la inmediata reacción de la empresa para que cumpla con los preceptos legales, normativos, acuerdos, contratos y compromisos voluntarios adquiridos.	Necesidades marginales	La cualidad de urgente por parte del Grupo de Interés obedece a necesidades marginales	Necesidades Urgentes	La cualidad de urgente por parte del Grupo de Interés obedece a Necesidades Urgentes